University of Twente
Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS)

Medium Access and Routing In Multi Hop Wireless Infrastructures

Ayman Wazwaz

Master Thesis
M.Sc. Telematics

Project Supervisors:

Dr. ir. Geert Heijenk (first supervisor)
Prof. dr. ir. B. R. H. M. Haverkort
Prof. dr. J. L. van den Berg

Design and Analysis of Communication Systems (DACS)
Faculty of EEMCS, University of Twente
Enschede, the Netherlands
2005

Abstract:

Multi hop wireless infrastructures can be used as an extension to fixed infrastructures, where wireless nodes form a large network that provides access to the fixed network infrastructure, such as the internet, via multiple wireless hops. Wireless LANs and routing techniques, used in ad hoc networks, can be used in such a network. In this work, we use the IEEE 802.11 standard, extended with power control to optimize the performance of such a network.

This work focuses on the Medium Access Control (MAC) mechanism, through Carrier Sense Multiple Accesses with Collision Avoidance (CSMA/CA). By limiting the transmission power to the level just sufficient for correct reception at the receiver, the network is able to have multiple transmissions performed simultaneously, and reduces the interference between transmitting nodes. Further, we propose a routing algorithm that uses paths as efficient as possible in terms of power, interference level and number of hops.

Validation of some of the proposed mechanisms has been done with the OPNET modeler simulator, using different models for path loss, traffic distributions, and topologies. The results show higher performance when using power control for data and control packets, and higher throughput when assuming path loss models causing less interference. For the different distributions of nodes in the network, we noticed high throughputs in long chains and network grids where the distances between nodes are symmetric.

Acknowledgments

I’d like to thank all people who supported me:

- My mother and Amal for their support.
- My colleagues in my home university (PPU).
- My colleagues and friends from all nationalities at university of Twente.
- All staff in the University of Twente, and especially in DACS group.
- And finally Nuffic, the Netherlands organization which financed my study for 2 years.

Thank you all

Table of Contents

Chapter 1

Introduction and Problem Definition

1.1 Introduction

Over recent years, wireless communication systems performed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the face of the earth. Hundreds of millions of people exchange information every day using pagers, cellular telephones, laptops, and other wireless communication products. With tremendous success of wireless telephony and messaging services, it is not surprising that wireless communication is beginning to be applied to the area of personal and business computing.

Wireless Local Area Networks (WLANs) is one of the wireless technologies that are very successful, but they are in enhancement and development, especially in cases of ad-hoc networks and multi hop networks. This work shows how we can utilize the resources offered by wireless networks, and how to use the available bandwidth. Furthermore, how to reduce interference as much as possible, and to enhance performance in wireless multi-hop networks; where the nodes are used to serve each other forming series of relaying stations to reach other networks. Thus they do not totally depend on access points to reach all nodes.

This research will present the main features of wireless LANs and multi-hop networking bases on IEEE 802.11 [7] standard and its extensions and Carrier Sense Multiple Access with Collision Avoidance (CSMA\CA) technique. In this work we will propose some modification to enhance the performance of the wireless multi hop networks.

The rest of this chapter will be about the objectives of the research through the problem statement, assumptions and approach of the work, and will discuss related works.

Chapter 2 will provide more theoretical background about 802.11 and other related algorithms and techniques, which we will use in our assumptions and modeling of the multi-hop wireless network.

Chapter 3 will explain the design issues of power control in wireless networks, ad hoc routing, and network configuration in the initial phases.

Chapter 4 is the practical part where experiments and results are explained. This part focuses on the power control in wireless networks, analysis of models, and the changes to be applied to have better performance.

Finally, chapter 5 is the concluding part which focuses on the general remarks and results, and discusses some open issues and the future work.

We will start by an example of application; researchers in Microsoft Research Redmond, Cambridge, and Silicon Valley are working to create wireless technologies that allow neighbors to connect their home networks together [1]. There are many advantages to enabling such connectivity and forming a community mesh network, including capacity and range enhancement, privacy and security, self-stabilizing and multi-path multi-hop routing, auto-configuration, bandwidth fairness, etc. the following figure (1-1) shows one way of using such a network for internet connection sharing, the figure shows a gas station that is connected to the internet service provider, this station has a wireless router and provides the internet service to the neighbors by forwarding data to and from other users' routers, and other routers relay data for each other forming a mesh network.

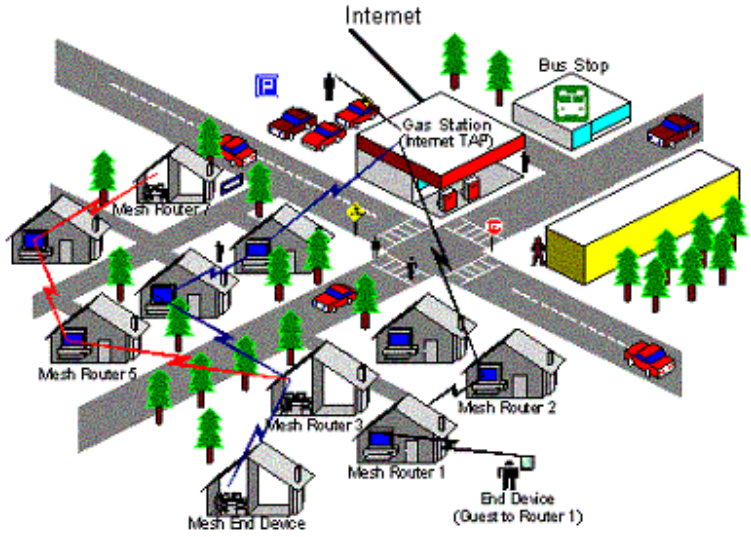


Figure 1-1: Internet connection sharing through wireless mesh networks [1]

1.2 Problem Statement

The usage of the available bandwidth in wireless networks is very low because of the collisions, retransmission, and the delay in the bottleneck nodes and Access points. Using the CSMA/CA in the wireless medium access control MAC manages the multiple connections, but still can not ideally use the available bandwidth.

Besides increasing the capacity, wireless LANs need scalability enhancements, since adding more stations to a network means increasing collisions and decreasing performance. Further, the exchange

of packets between some peer stations can be done locally and directly between nodes, without interfering and causing collisions next the access points and bottleneck nodes.

So we need some enhancements for accessing the medium and routing data packets through the wireless connections, making the wireless LANs more scalable, reliable, and efficient.

We assume having a fixed network or central node (Ethernet for instance) which offers some services (mail, DNS, FTP, web ...). Some stations in the wireless network have direct access to the fixed network. The farther nodes which are distributed over a geographical area form a set of nodes, and access each other directly or indirectly using multi hop access through other nodes. So for the farthest node, it can reach the fixed network by passing more nodes to reach the fixed network.

Stations also exchange packets between themselves (peer to peer or client server), so we need some extra functionality for the nodes to be as sources or destinations, and to relay packets to other nodes. This functionality already exists in ad hoc wireless nodes.

The proposed architecture can be described as shown in figure 1-2; it has a fixed infrastructure network with servers, services and stations, access points to provide wireless connections for the wireless nodes, the nodes are distributed over a space where some of these nodes can reach the fixed network directly and others can not. The nodes form an ad hoc network with a connection to an infrastructure for some nodes, this is called multi hop wireless mesh network.

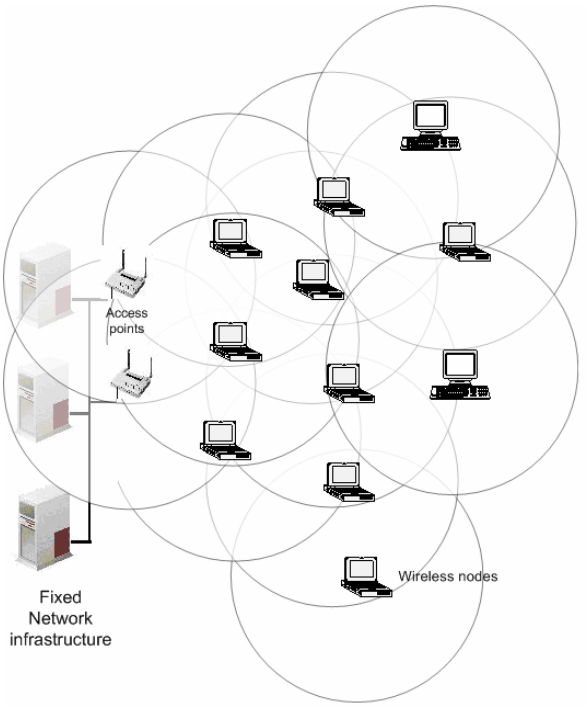


Figure 1-2: The proposed architecture for the wireless multi-hop network, a fixed network and a set of wireless nodes

The main objectives of this work are:

- To design a network topology detection and discovery during the initialization and maintenance periods, this information will be used in routing and power control.
- To use a power control mechanism to save power and reduce interference by sending packets with a power efficient technique. Using different levels of power for transmission to different frame type and for different destinations. This way will decrease power consumption and noise, and increase the total throughput of the network.
- To use routing protocols to decrease the interference between transmissions to enable parallel exchange of data frames. We will study the effect of some routing metrics as the hop count, the power level, the interference level.

To summarize, we will study different scenarios to enhance the wireless network performance for a hybrid network that uses multi hop environment through optimizing power, routing and load balancing relaying packets between the nodes in the network and considering the bottlenecks and QoS requirements.

1.2 Assumptions and Approach

For the network architecture we assume:

- IEEE 802.11b with CSMA/CA extension.
- Stationary nodes: nodes are not moving and the topology does not include rapid changes.
- Nodes have a router and a station role; can relay packets to other stations.
- Interference based routing protocols are used to allow multiple transmissions between different nodes.
- Symmetric links: if node1 can reach node2, then node2 can reach node1 with the same connection quality.

The approach of this work is to study and analyze the existing models of wireless nodes, use a simulation tool to analyze and model the existing architecture, and configure the new assumptions and the proposed changes, and make experiment with different scenarios.

The OPNET [6] simulation tool was used; this tool a discrete-event system simulator, C/C++ programming, and it has the ability to model the requirements and assumptions needed for different types of networks and devices. In the experiment, OPNET modeler version 11.0.A has been used.

1.4 Related Work

As mentioned before, this topic has a lot of work and developments, here we will mention some general comments on related papers, and will discuss two other papers with explanations , one related to the power and MAC layer and the other is related to routing and interference.

The routing metrics in ad hoc networks have been studied and simulated in different works. In [15], the authors used the *expected transmission count* metric (*ETX*) in routing protocols (DSDV and DSR), and they noted higher throughputs in long paths compared to hop count metric. While in [16], they compared new metrics with the ETX; per-hop RTT and per-hop packet pair metrics, results showed that the ETX metric has the best performance when all nodes are stationary, and the per-hop RTT and per-hop packet-pair metrics perform poorly due to self-interference.

Power control is used in [17], three power protocols are discussed: CLUSTERPOW, aims to increase the network capacity by increasing spatial reuse in a cluster, Tunneled CLUSTERPOW, allows a finer optimization by using encapsulation, and MINPOW that provides an optimal routing solution with respect to the total power consumed in communication. In [18], minimum power was used and compared with other power levels; and the conclusion is that the transmission power should be adaptive to the specific conditions in an ad-hoc network in order to maximize throughput performance.

In [19], authors proposed and evaluated a power control loop, similar to those commonly found in cellular CDMA networks, for ad hoc wireless networks. They showed that this power control loop reduced energy consumption per transmitted byte by 10 - 20%, and it increases overall throughput by 15%.

Power control is proposed as a means to improve the energy efficiency of routing algorithms in ad hoc networks as discussed in [20], Each node in the network estimates the power necessary to reach its own neighbors, and this power is used both for tuning the transmit power, it is noted transmit energy savings, while introducing limited degradation in terms of throughput and delay.

There are more papers, but we will finish by discussing two other related works with more details:

- **Balanced Interference Routing Algorithm (BIRA) [4]**

BIRA is a pre-determined routing algorithm for multi-hop wireless network; the algorithm assumes the Code-Division Multiple Access (CDMA) and Time Division Multiple Access TDMA The new infrastructure presented in [4] is based on a combination of CDMA and TDMA; the connections between mobile terminals and base stations use CDMA and the connections between base stations use the combination of CDMA and TDMA.

The algorithm is composed of 2 steps:

- Calculate the new link cost considered of interference level and the fixed link cost of each link
- Compute the routes based on the Dijkstra algorithm.

The routes are determined from the link cost matrix by using Dijkstra algorithm. BIRA considers the interference from the sender side. For each sender, it is determined how much interference other node will experience because of a transmission to a specific destination.

BIRA can overcome the frequent and fast updates; it stables the paths by minimizing the interference from the sender side. Since the distance between all the base stations is known, the sender station could expect which is the optimal path to generate least interference to the other nodes. The other

nodes will also get the benefit from it, because they will receive the least interference from the neighbor station. And the interference in the whole network will also decrease.

- **A Power Control MAC Protocol for Ad Hoc Networks** [5]

In [5] the authors presented a power control MAC protocol that allows nodes to vary transmit power level on a per packet basis. The idea of the power control schemes is to use different power levels for RTS-CTS and DATA-ACK. Specifically, maximum transmit power is used for RTS-CTS, and the minimum required transmit power is used for DATA-ACK transmissions in order to save energy. The authors showed that these schemes can degrade network throughput and can result in higher energy consumption than when using IEEE 802.11 without power control.

They proposed PCM, a Power Control MAC protocol, which periodically increases the transmit power during DATA transmission. Simulations they did showed that PCM achieves energy savings without causing throughput degradation.

One possible concern with PCM is that it requires a frequent increase and decrease in the transmit power which may make the implementation difficult. An alternative approach is to replace this higher power level for data by a busy tone at *pmax* in a separate channel as shown in figure 1-3, with one channel being used for the busy tone and the other channel for RTS-CTS-DATA-ACK.

Figure (1-3) below shows how the transmit power level changes during the sequence of an RTS-CTS-DATA-ACK transmission. After the RTS-CTS handshake using *pmax*, suppose the source and destination nodes decide to use power level p1 for DATA and ACK. Then, the source will transmit DATA using *p1* and periodically use *pmax*. The destination uses *p1* for ACK transmission. As described, the key difference between PCM and the original scheme is that PCM periodically increases the transmit power to *pmax* during the DATA packet transmission. With this change, nodes that can potentially interfere with the reception of ACK at the sender will periodically sense the channel as busy, and defer their own transmission.

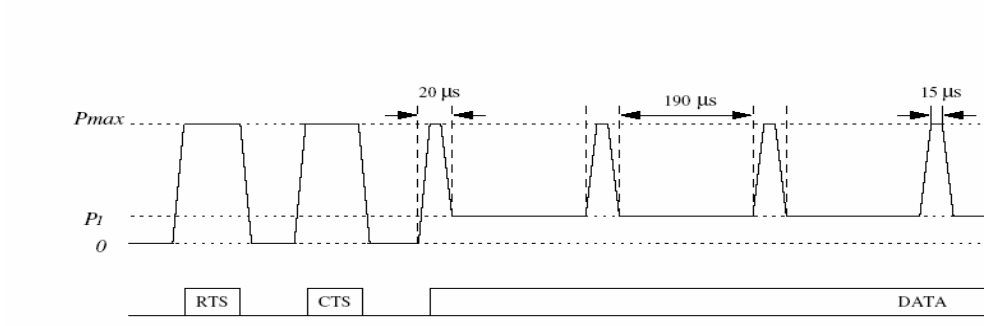


Figure 1-3: Power Control MAC Protocol [5]

As a variation of PCM, a different time interval can also be used between the transmissions at *pmax* during a packet transmission. In this variation, there is a trade-off between performance and energy savings. Although PCM provides energy saving it does not yield improved spatial reuse as compared to IEEE 802.11.

Chapter 2

Wireless LANs Background

2.1 IEEE 802.11 Standards

The aim of the IEEE 802.11 [7] standard was to develop a medium access control layer (MAC) and a physical layer (PHY) for wireless connectivity to fixed, portable and moving stations within a local area [7]. The higher OSI layers in 802.11 are the same as in any other 802 standards, which means that at this level there is no difference perceptible between wired and wireless media. The 802.11 standard describes the functions and services required by a compliant device to operate within ad hoc and infrastructure networks as well as the aspects of station mobility. The standard defines the MAC procedures to support the asynchronous MAC service data unit (MSDU) delivery services, and several PHY signaling techniques and interface functions that are controlled by the IEEE 802.11 MAC.

The MAC and PHY characteristics for wireless local area networks (WLANs) are specified in the 802.11 standards; 802.11b, 802.11a, and 802.11g. The MAC layer in these standards is designed to be able to support additional physical layer units as they may be adopted, dependent on the availability of spectrum and new modulation techniques.

The logical link control (LLC) layer is the highest layer of the IEEE 802.11 Reference Model. The purpose of the LLC is to exchange data between end users across a LAN that uses 802-based MAC protocols. The LLC provides identification of the upper-layer protocol (ULP), data-link control functions, and connection services. It is independent of the topology, transmission medium, and

medium access control techniques used at the MAC and PHY layers. Higher layers, such as the network layer, pass user data down to the LLC, expecting error-free transmissions across the network. Figure 2-1 shows the physical and data link layers, the physical layer has different types of medium and spectrum, and data link layer is divided into two sub-layers: the medium access control (MAC) and the logical link control (LLC) sub-layers.

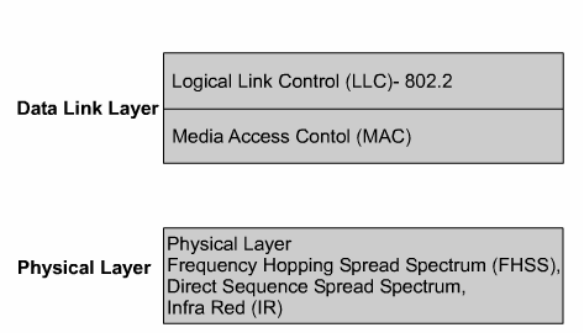


Figure 2-1: 802.11 physical and data link layers [3]

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) created the first WLAN standard. They called it 802.11 after the name of the group formed to oversee its development. Unfortunately, at the beginning 802.11 only supported a maximum bandwidth of 2 Mbps which is too slow for most applications. Later newer standards were introduced which support higher bandwidth services [7].

802.11b

IEEE expanded on the original 802.11 standard in July 1999, creating the 802.11b specification. 802.11b supports bandwidth up to 11 Mbps. 802.11b uses the same radio signaling frequency - 2.4 GHz - as the original 802.11 standard.

802.11a

When 802.11b was developed, IEEE created a second extension to the original 802.11 standard called 802.11a; 802.11a was created at the same time. Due to its higher cost, 802.11a fits predominately in the business market, whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in 5 GHz frequency range. Compared to 802.11b, this higher frequency limits the range of 802.11a. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions. Because 802.11a and 802.11b utilize different frequencies, the two technologies are incompatible with each other [7].

802.11g

In 2002 and 2003, WLAN products supporting a new standard called 802.11g began to appear on the scene. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

802.11h

This standard is supplementary to the MAC layer to comply with European regulations for 5GHz WLANs. European radio regulations for the 5GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimize interference with other systems [7].

2.2 The 802.11 operating modes

There are two operating modes defined in IEEE 802.11: Infrastructure Mode and Ad Hoc Mode. (Figure 2-2) [8]. There is a 3rd mode which combines properties of the first two; this mode is the Hybrid mode, or the wireless multi hop.

Infrastructure mode

In infrastructure mode, the wireless network consists of at least one access point (AP) connected to the wired network infrastructure and a set of wireless end stations. An access point controls encryption on the network and may bridge or route the wireless traffic to a wired Ethernet network or the Internet.

This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) consists of two or more BSSs forming a single sub network. Traffic is forwarded from one BSS to another to facilitate movement of wireless stations between BSSs. Almost always the distribution system which connects this networks is an Ethernet LAN. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links).

Ad-Hoc Mode

Ad-Hoc mode is a set of 802.11 wireless stations that communicate directly with each other without using an access point or any connection to a wired network. This basic topology is useful in order to quickly and easily set up a wireless network anywhere a wireless infrastructure does not exist. Ad-Hoc Mode is also called peer-to-peer mode or an Independent Basic Service Set (IBSS)

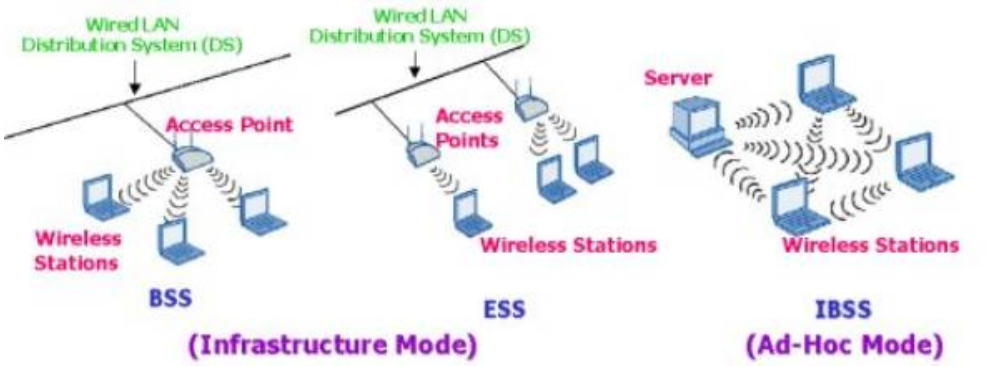


Figure 2-2: Wireless LAN operating modes [8]

When talking about ad-hoc networks, we are interested in the capacity of this configuration. The capacity of wireless ad-hoc networks can be very low, due to the requirement that nodes forward each others' packets. Capacity is the limiting factor; a large mobility causes a high volume of routing queries and updates which brings along high congestion, which leads to packet losses.

Hybrid Mode

This mode combines the properties of the two modes. It uses the ad hoc properties and communicates via the access points with other networks. The multi hop wireless mesh networks discussed in chapter1 can be classified in this category.

2.3 WLAN Physical Layer

The wireless LAN physical layer (PHY) is the interface between the MAC and the wireless media where frames are transmitted and received. The PHY provides three functions. First, the PHY provides an interface to exchange frames with the upper MAC layer for transmission and reception of data. Second, the PHY uses signal carrier and spread spectrum modulation to transmit data frames over the media. Finally, the PHY provides a carrier sense indication back to the MAC to verify activity on the media [3].

WLAN Physical sub-layers

- **Physical Layer Convergence Procedure (PLCP)**

The PHY convergence function adapts the capabilities of the physical medium dependent (PMD) system for the MAC service. PLCP defines a method for mapping the MAC sub-layer protocol data units (MPDUs) into a framing format suitable for sending and receiving between two or more stations (STAs) using the associated PMD system[3]. Figure 2-3 shows these layers.

- **Physical Medium-dependent (PMD) System**

The PMD system defines the characteristics and methods of transmitting and receiving data through a wireless medium between two or more STAs, each using the same PHY system.

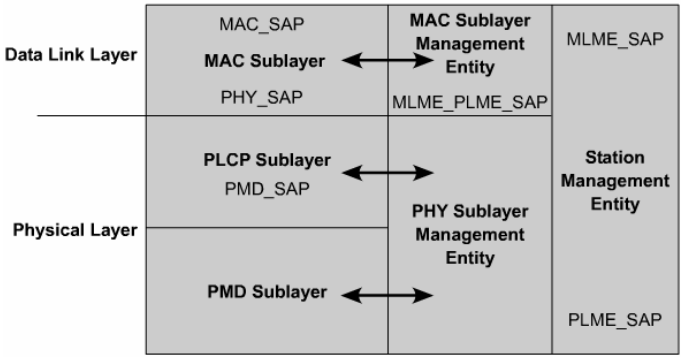


Figure 2-3: 802.11 data link and physical sub-layers [3]

802.11 Physical characteristics

The two types of spread-spectrum radio are Direct Sequence Spread Spectrum (**DSSS**) and Frequency Hopping Spread Spectrum (**FHSS**) [3]. DSSS generates a redundant bit pattern called a chip or chipping code, for each bit to be transmitted, FHSS uses a narrowband carrier that changes frequency in a pattern known to both the transmitter and the receiver.

If everything stays properly synchronized this creates a single logical channel, even though the frequency is constantly changing. Early implementations of 802.11 used FHSS, however 802.11b standardized on DSSS.

Both FHSS and DSSS support 1 and 2 Mbps data rates. An extension to the 802.11 architecture (802.11a) defines different multiplexing techniques that can achieve data rates up to 54 Mbps. Another extension to the standard (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 (HR/DSSS). 802.11b also defines a rate shifting technique where 11 Mbps networks may fall back to 5.5 Mbps, 2 Mbps, or 1 Mps under noisy conditions or to inter-operate with legacy 802.11 PHY layers.

Orthogonal Frequency Division Multiplexing (OFDM) is an FDM modulation technique; it is used for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions.

Currently the 802.11a and 802.11g standards, operating up to 54Mbps, use OFDM instead of DSSS. OFDM limits the crosstalk or interference of transmitting channels. OFDM is used in European digital audio broadcast services. Compared to DSSS, OFDM allows more speed [9].

Reliability and connectivity

Wireless LANs include mechanisms to improve the reliability of the packet transmissions to be at least the same level as wired Ethernet. Using the TCP/IP protocols will help protect the network

against any loss or corruption of data over the air. Further, WLANs have extensions to enhance performance and security.

2.4 WLAN Medium Access Control (MAC)

The 802.11 MAC layer provides functionality to allow reliable data delivery for the upper layers to work over the wireless physical (PHY) media. The data delivery itself is based on asynchronous, best-effort, connectionless delivery of MAC layer data. There is no guarantee that the frames will be delivered successfully, that's why it needs acknowledgment. Another function for MAC is the multiple access control for sharing a single medium between multiple nodes.

A third function of the 802.11 MAC is to protect the data being delivered by providing security and privacy services. Security is provided by the authentication services and by *Wireless Equivalent Privacy* (WEP) [7], which is an encryption service for data delivered on the WLAN.

MAC Architecture
Before transmitting a frame, a station (STA) must gain access to the medium using one of two methods:

1. The fundamental access method of the IEEE 802.11 MAC, carrier sense multiple access with collision avoidance (CSMA/CA), is called the Distributed Coordination Function (**DCF**). The DCF is implemented in all STAs, for use within both ad hoc and infrastructure network configurations.
2. The IEEE 802.11 MAC may also incorporate an optional access method, the Point Coordination Function (**PCF**), which creates contention-free (CF) access period. The PCF can only be used on infrastructure network configurations through access points (APs).

Coexistence of DCF and PCF

The DCF and the PCF can both operate concurrently within the same BSS. When this is the case, the two access methods alternate, with a CF period followed by a contention period. In addition, all frame transmissions under the PCF may use less waiting time between frames, which is smaller than waiting time used for frames transmitted via the DCF; this waiting time is explained later as the Interframe Space (IFS). The use of smaller IFS implies that point-coordinated traffic shall have priority access to the medium over STAs operating in DCF mode.

Frame Types
The three main types of frames used in the MAC layer are:

1. Data frames
2. Control frames
3. Management frames

Data frames are used for data transmission. Control frames, such as Request to Send (RTS), Clear to Send (CTS), and Acknowledgment (ACK), control access to the medium using RTS, CTS, and ACK frames. Management frames, such as beacon frames, are transmitted in the same manner as data frames to exchange management information, but are not forwarded to upper layers.

Interframe space (IFS)

The time interval between frames is called the interframe space (IFS). Each IFS interval is defined as the time from the last bit of the previous frame to the first bit of the preamble of the subsequent frame, as seen at the air interface. Four different IFSs are defined to provide priority levels for access to the wireless media. The IFSs are listed in order, from the shortest to the longest:

1. SIFS is the short interframe space
2. PIFS is the PCF interframe space
3. DIFS is the DCF interframe space
4. EIFS is the extended interframe space

The different IFSs are independent of the STA bit rate. The IFS timings are defined as time gaps on the medium and are fixed for each PHY, the different types of IFS are shown in figure 2-4.

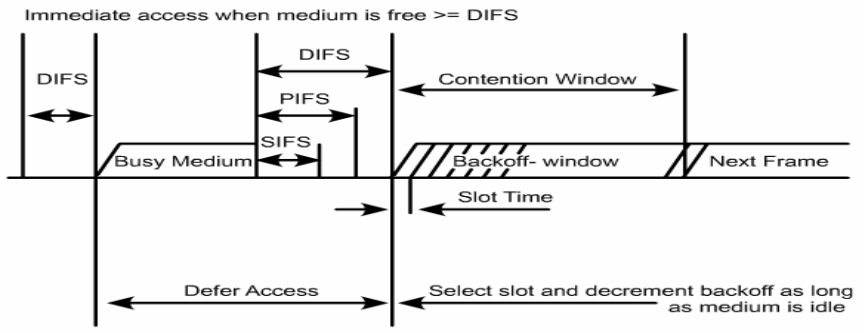


Figure 2-4: Interframe spaces in 802.11 MAC [3]

For the different types of interframe spaces, they have different ways of use, figure 2-5 shows an example of the using SIFS and DIFS in data exchange between nodes where the RTS and CTS frames are used. It shows that DIFS is used to separate completions and starts of frames transmission, and SIFS is used after RTS and CTS frames, and between data and acknowledgments frames.

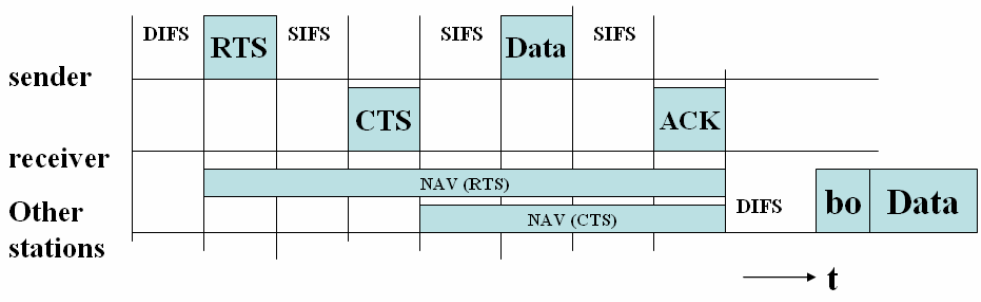


Figure 2- 5: Using SIFS and DIFS example [3]

Carrier-sense mechanism

Physical and virtual carrier-sense functions are used to determine the state of the medium. When either function indicates a busy medium, the medium is considered busy. If the medium is not busy it will be considered idle. A physical carrier-sense mechanism is provided by the PHY. The details of physical-carrier sense are provided in the individual PHY specifications.

The MAC provides a virtual carrier-sense mechanism. This mechanism is referred to as the network allocation vector (NAV). The NAV maintains a prediction of future traffic on the medium, based on information in the duration field of unicast frames. The duration information is also available in the MAC headers of all frames sent during the contention period [7].

Carrier Sense Multiple Access with Collision Avoidance CSMA/CA

The fundamental access method of 802.11 is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) which works by a "listen before talk scheme". This means that a station wishing to transmit must first sense the radio channel to determine if another station is transmitting. If the medium is not busy, transmission may proceed, else it will defer accessing the medium.

The CSMA/CA protocol avoids collisions among stations sharing the medium; it works by utilizing a random back-off time if the station’s physical or logical sensing mechanism indicates a busy medium. The period of time immediately following a busy medium is the highest probability of collisions occurring, especially under high utilization.

The CSMA/CA scheme implements time gapping between frames from a given user as shown in figure 2-4. Once a frame has been sent from a given transmitting station, that station must wait until the time gap is elapsed and try to transmit again. Once the time has passed, the station selects a random amount of time (the back-off interval) to wait before "listening" again to verify a clear channel on which to transmit. If the channel is still busy, deferred stations do not choose a randomized back-off time, but continue to count down, stations that have waited longer have the advantage over stations that have just entered. This type of multiple access ensures careful channel sharing while avoiding collisions [3].

The hidden terminal and the exposed terminal problems

The problem of hidden terminal arises when two sender nodes out of range of each other transmit packets at the same time, to the same receiver, resulting in collisions at the receiver. Since sender nodes are out of range of each other, they do not detect carrier even though the other node is sending data, and if their data packets reach the destination at the same time, these packets are dropped due to collision at the receiver [14]. Figure 2-6 shows 4 nodes, if nodes A and C are transmitting to node B at the same time, there will be a collision at node B.

In the exposed terminal problem, when node B has a data packet to send to node A in figure 2-6, node C on hearing the RTS packet (though data packet is meant for node A), node C refrains from sending data packet to node D. Here node C is *exposed* to node B's transmission. The result is poor resource utilization.

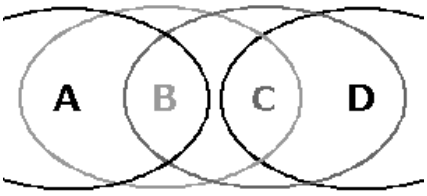


Figure 2-6: hidden and exposed terminal problems

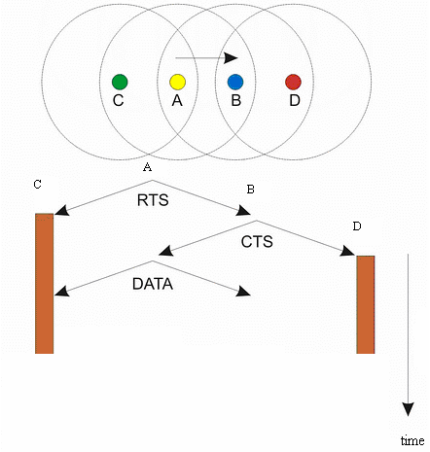


Figure 2-7: MACA protocol Using RTS, CTS signals in 802.11 MAC

MAC-Level acknowledgments

The reception of some frames requires the receiving station to respond with an acknowledgment, generally an ACK frame, this technique is known as positive acknowledgment. Lack of reception of an expected ACK frame indicates to the source station that an error has occurred. It may be possible that the destination station may have received the frame correctly and that the error may have occurred in the delivery of the ACK frame. To the initiator of the frame exchange, these two conditions are indistinguishable.

The rule in CSMA/CA is that the transmitter sends data only if it senses the signal level as being free for a fixed length of time DIFS (Distributed Inter-Frame Space) agreed upon by all the transmitters. If the signal is not free, the transmitter waits for the DIFS plus a random multiple of a fixed time slot. Both of these protocols reduce the probability of collisions and do not solve the hidden terminal problem.

The hidden and exposed terminal problems are solved by the Multiple Access Collision Avoidance (MACA) protocol. In this protocol, transmitters can broadcast RTS and CTS packets. These inform all other transmitters within range that data transmission is about to take place. Figure 2-7 shows how MACA protocol uses the RTS and CTS signals to coordinate data transmissions and to avoid collisions.

In figure 2-6, if both A and C wished to communicate with B, they would both send an RTS signal. B would respond with a CTS signal heard by both A and C, but with an identifier saying only C can send. If the RTS signals had collided at B, both A and C would not have received the CTS signal, and would have retried after a random amount of time.

The CSMA used by the 802.11 as a medium access control (MAC) has some performance drawbacks including:

- Throughput and delay: Throughput is generally measured as the percentage of successfully transmitted radio link level frames per unit time. Transmission delay is defined as the interval between the frame arrival time at the MAC layer of a transmitter and the time at which the transmitter realizes that the transmitted frame has been successfully received by the receiver. In CSMA, collisions of RTS/CTS packets cause retransmissions of these packets, but since these packets are small, the occurrence of collisions is less likely to happen, and the use of RTS and CTS decreases the collisions in the data packets, and increases the throughput.
- Fairness: Generally, fairness measures how fair the channel allocation is among the flows in the different mobile nodes. The node mobility and the unreliability of radio channels are the two main factors that impact fairness. High power transmissions may block other transmissions causing unfair distribution of bandwidth.
- Energy efficiency: Generally, energy efficiency is measured as the fraction of the useful energy consumption (for successful frame transmission) to the total energy spent. MAC without power control sometimes uses much higher power than required; this causes more power consumption and higher rate of interferences and collisions.

2.5 AD HOC Routing protocols

Wireless networks with infrastructures support access points to enable nodes to reach the fixed networks; this is not the case for an ad-hoc network. A destination may be out of range of the source, so it needs intermediate nodes to relay the packets until it reach the destination. In ad hoc networks, each node must be able to forward data for other nodes. [3]

A routing protocol is the mechanism by which user traffic is directed and transported through the network from the source node to the destination node. Objectives include maximizing network performance form the application point of view, while minimizing the cost of network itself in accordance with its capacity. The application requirements are delay, throughput, loss rate, stability, jitter, cost, etc [11]

Five basic routing functionalities for mobile ad hoc networks are:

- Path generation; which generates paths according to the assembled and distributed state information of the network and of the application, so the routing tables are built.
- assembling and distributing network and user traffic state information,
- Path selection; which selects appropriate paths based on network and application state information; here the path is assigned for the current packet.
- Data forwarding; forwards user traffic along the selected route
- Path Maintenance: maintaining of the selected route.

Routing in ad hoc networks check whether nodes should keep track of routes to all possible destinations; or instead keep track of only those destinations that are of immediate interest. A node in an ad hoc network does not need a route to a destination until that destination is to be the recipient of packets sent by the node, either as the actual source of the packet or as an intermediate node along a path from the source to the destination.

Here we will discuss four different classes of routing protocols. These classes are: flooding, proactive, reactive, and hybrid protocols. They are mentioned with examples:

- **Flooding:**

  In flooding protocols, sender broadcasts data packets to all its neighbors. Then, each node receiving the data packets forwards these data packets to its neighbors. Flooding uses broadcasting which creates significantly high overhead cause network congestion.

  One of the advantages of flooding is to deliver packets to the destination on multiple paths, so from this point of view flooding is reliable. Also, flooding may be more efficient that other protocols when rate of information transmission is low. [11]

- **Proactive (table driven routing):**

  Protocols that keep track of routes for all destinations in the ad hoc network, these protocols have the advantage that communications with arbitrary destinations experience minimal initial delay from the point of view of the application. When the application starts, a route can be immediately selected from the routing table.

  In Table-driven routing, protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes, then the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network, and the number of necessary routing-related tables. [10]

  Such protocols are called proactive because they store route information even before it is needed. They are also called table driven because routes are available as parts of a well-maintained table. Certain proactive routing protocols are Destination-Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Clusterhead Gateway Switch Routing (CGSR).

Proactive protocols suffer the disadvantage of additional control traffic that is needed to continually update stale route entries. Since the network topology is dynamic, when a link goes down, all paths that use that link are broken and have to be repaired. [11]

- **Reactive (on demand routing):**

To overcome the wasted work in maintaining not needed routes, on-demand, or reactive protocols have been designed. In these protocols, routing information is acquired only when it is actually needed. Reactive routing protocols save the overhead of maintaining unused routes at each node, but the latency for many applications will drastically increase. Most applications are likely to suffer a long delay when they start because a route to the destination will have to be acquired before the communication can begin.

In contrast to table-driven routing protocols all up-to-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid until the route is no longer needed. [10]

Some reactive protocols are Cluster Based Routing Protocol (CBRP), Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA), Associativity-Based Routing (ABR), Signal Stability Routing (SSR), Location Aided Routing (LAR). [11]

Reactive protocols may not be optimal in terms of bandwidth utilization because of flooding of the route discovery request, but they remain scalable in the frequency of topology change. Reactive strategies are suitable for networks with high mobility and relatively small number of flows.

- **Hybrid Routing:**

Hybrid routing protocols use both techniques proactive and reactive; hybrid protocols aggregate a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information, to route packets between different zones, the reactive approach is used.

Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric such as the number of hops. Each node keeps a record of routing information for its own zone.

In hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. Examples of hybrid routing protocols are the zone routing protocol (ZRP), zone-based hierarchical link state (ZHLS) routing protocol, and distributed dynamic routing algorithm (DDR). The hybrid protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subjected to the size of a zone and the dynamics of a zone. The hybrid approach is an appropriate candidate for routing in a large network. [11]

Other routing metrics

There are many routing metrics used to decide the best route for a destination, examples are: hop count, delay, throughput, interference level, loss rate, stability, power, and reliability, but a mixes of

more than one metric are also used. This is done by forming a formula of cost which is considered as total value of specific weight for each metric.

An example from [3] in computing the total cost, it can be computed as a compound of hop count (H), interference (I), and reliability (R) as:

$$\cos t = \alpha H + \beta R + \sigma E$$

Where α, β, and σ are the weights, and these weight should be chosen carefully since they are different types of values and units. In the design part of this work, we used a mix of three metrics for the proposed routing protocol: hop count, interference level, and the power needed to the destination.

Chapter 3

System Design and Description

3.1 System overview

This chapter presents the network behavior and description of the network system, and the changes to be done to enhance the performance of the network for individual nodes and for the whole network; we assume 3 major factors to be developed to enhance the performance:

- Network discovery and initialization process.
- Power control mechanism.
- Routing processing mechanism.

These issues together are needed to enhance the multi hop network in terms of bandwidth, reliability, and effort saving. At heavy loaded networks, wireless networks face problems in load sharing, power saving, information updates, scalability, and latency in data delivery. The changes to be done are in different layers of the wireless network: the physical, the data link, and the network layers. Only the power control mechanism is implemented and validated in this work.

The changes in the different layers have different effects on the network, the network discovery will add some extra load to the network at the beginning, but this information and the updates that come later are essential to utilize the network facilities, the power control will add extra load in checking destinations and distances and changing power levels, but this process will increase the throughput significantly in addition to the power saving.

Ad hoc and multi hop routing protocols have different strategies to make the nodes reach each other, and these protocols as mentioned in chapter 2 are classified into different types, here the proposed routing process is a table driven protocol which uses different metrics to manage data exchange and routing; these metrics are mix of power, interference, and hops distance.

Other design alternatives

There are other design alternatives, like using different metrics, or use the power control in the MAC layer without considering it in the network layer as a metric, but we see that these metrics are so related together and it is important to find the best configuration for different types and topologies of networks. In this design, we try to implement the requirements of different layers and enhance the network performance through different parameters consideration.

Another alternative is to use these metrics in on demand routing protocols, by replacing the parameter of the routing protocol to the mix of metrics used in our design, this option is also possible and can be used as different way of implementation, but in that case the network discovery design will need changes, because on demand routing has less updates.

For infrastructure networks, in some cases, the use of the available access points is better than distributing access points all over the possible places of the users, so using the multi hop routing is easier in implementation, especially for environments where users move from time to time, where the access points may not able to serve all nodes.

3.2 Network Initialization and Detection

Before exchanging and relaying data packets between nodes in the wireless network, nodes should know other nodes' location and routing information, this knowledge needs a discovery process. So we need a process to enable the nodes in the network to discover the network information. This information from different nodes will make a clear picture for the topology and the best routing and power configuration when exchanging packets.

Without a fixed network, we have only an ad hoc wireless network, we will start with a central controller to manage network updates, like an access point in a fixed network connected with other wireless stations, the node that controls the updates and reservations can be one of the access points or a wireless node in the network. Initially, we will consider the fixed network is working; and this network provides services to the wireless nodes through access points, and one of the access points is elected to be the controller.

Update interval:

Update interval is defined as the time specified for nodes to exchange their routing information and nodes configurations, this interval is divided into time slots, a slot for each node, this interval is repeated periodically and its size is expandable if needed, in terms of number of slots, as shown in figure 3-4. Each time slot can be reserved by one node, and the update interval is managed by the manager node which is the access point (H) in the fixed network in this case.

The Initialization process

- Start with no nodes except the fixed network or the manager node, and ignoring the state where only normal wireless nodes are available.
- The fixed network starts announcing through the access point about the network information and services in the updates interval, and it reserves the first time slot in the updates interval.
- A broadcasting node sends its announcements with the highest power. Receiving nodes recognize the discovery announcements and measure the power and distance according to the received power level, the receiving node records for each reachable node its required power to exchange packets, and the received information as reachable nodes and cost from that node to other nodes.
- If there is more than one access point (AP) in the same network, only one can supervise the reservations, and the other APs should behave normally as other nodes. If this AP fails, another AP may takeover the supervision role, but this needs a recovery process design, which is not discussed in this work.
- The update interval is used to distribute the time between the nodes to announce their parameters including status and reach ability for other nodes. These time slots are very short in time and small in packet sizes. Figure 3-1 shows an update interval between data exchange intervals, the "H" denotes the node identity that will use this time slot to announce its parameters, the first identity in the central node.

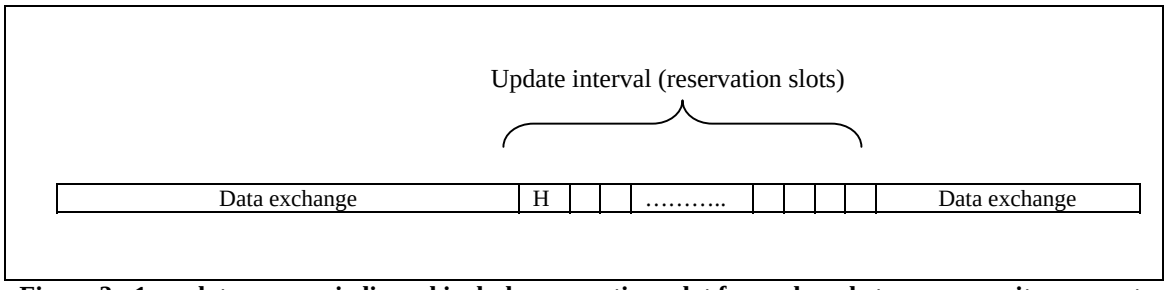


Figure 3 - 1: updates are periodic and include reservations slot for each node to announce its parameters.

- Since the update interval is very short compared with normal data exchange interval, the remaining time will be data and services requests and responses. The updates and synchronizations start from the fixed network and continue to cover all the nodes.
- The number of reserved time slots increase when the number of active nodes increase, and the size is updated by the Access point connected to the fixed network when the reservation table is nearly full.

- If there are active stations, they will receive the announcements, and will try reserve their own time slots later, and synchronize through the update interval by reserving time slots for each of them. The reservation table is known for all nodes in the network.
- New wireless nodes coming later will hear the announcement of the reachable nodes and/or the fixed network, and will try reserve their own time slot in the new updates interval. They can choose the first free time slot, and reserve it by broadcasting at that time slot since no node is transmitting at that moment and it is a free slot.
- If a collision occurs in the reservation process, requesting nodes will wait for the coming rounds of update intervals, in that case the central node or access point will not reserve the colliding requests, the requesting nodes will not see their reservations in the table approved by the central node, and will try again later. To avoid collisions in the coming rounds, stations choose different random waiting time before broadcast and sense the medium before start.
- Broadcasts are sent as UDP packets, these packets have no acknowledgments.
- Reservations in the time slots are distributed all over the network, so all nodes know who reserves what time slot.
- Two types of tables are used: metrics tables which are used to contain the neighbor nodes metrics; here the cost to the neighbor node is calculated. And the routing table which contains the destination nodes, the next hop to reach that destination, and the total cost to reach that destination. So the metrics tables are limited by the neighbors and the routing tables are global for the whole network.
- During one time slot, a specified node broadcasts its parameters including the routing table with the maximum power level, and the receivers can estimate the needed power to reach that node, and from the power received the distance can be computed.
- When the controller access point broadcasts its information, the nodes that are mentioned in the reservation table are considered, and have the right to exchange packets. So if a node could see its identity in the reservation table, then its reservation is successful, otherwise it should try another reservation later and find a free slot.
- To keep the routing tables up to date, there will be a beaconing interval which restarts the whole process of discovery, so if there is incorrect information, it will be deleted. This interval is chosen to be reasonable and suitable to the network size and activity.

The description of the initialization process can be implemented with the IEEE 802.11, but it needs some extra functionality in the central node that controls the updates. In the update interval, the central node uses the point coordination function PCF [3] to assign the free time slots to other requesting nodes from the neighbors, like in the infrastructure mode. For the farther nodes, the requests are relayed until they reach the central node, and then approved. Each node calculates its start time by determining the start of the update time and its turn in the table. If we go to further details of description, we may need to change some tasks here to comply with the standards.

The data exchange periods work normally as an ad hoc network with known costs. So nodes can relay and exchange packets depending on the routing tables they built during the update intervals.

After initialization, the nodes can now know the active nodes and their metrics and the routing information for other nodes. After that, they can relay packets or request/respond services.

3.3 Power Control in WLANs

The purpose of power control is to use efficient power levels for different type of frames, these levels depend on the network topology and spacing between nodes. This mechanism will reduce the inference and collisions and save the power, we propose three levels of power:

- Level 1 (maximum power for updates advertisements): used by each node to announce its location and required power to reach. Receivers can estimate the required power to reach that node.
- Level 2 (medium power for RTS CTS): used for the normal RTS CTS packets, to request the medium for transmission, less power than level 1.
- Level 3 (minimum power used for data exchange): this level in nearly the threshold power required to reach a station. This will save power and decrease the collisions.

In the simulation part in chapter 4, levels 2 and 3 are used for control packets (RTS and CTS), and data exchange packets respectively. Figure 3-2 shows the three levels for one node (wn1) surrounded by an access point and other wireless nodes , the three levels of power are level 1 denoted by L1, level2 denoted by L2, and level3 denoted by L3.

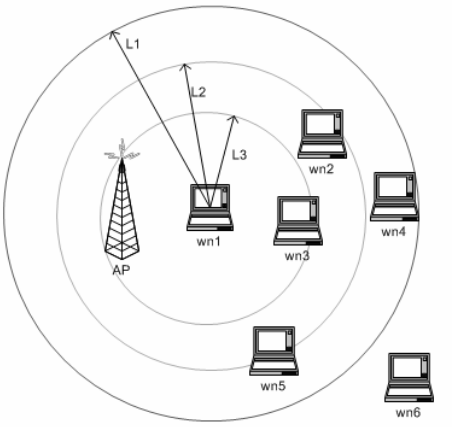


Figure 3 - 2: three levels of power used to announce and communicate with other nodes.

For each frame, its type should be checked and the suitable power level is assigned to it, the power value assigned for data frames (level3) is considered in the routing process later, since the majority of the packets are data packets.

For the different types of frames, it needs extra processing to check each frame type and its destination, and use the power control mechanism to specify the power value to be assigned to that frame. In chapter 4, we will focus on this issue and use different topologies and loads and check the better power values to use for each case.

Since we will not implement the advertising process, we will use two levels of power which are the control power; used in RTS and CTS frames, and the data power, which are shown as level2 (L2) and level3 (L3) in figure 3-2. The power control mechanism is implemented at the MAC layer in the WLANs; it checks the frame type and destination address, the power value is also used at the network layer as one of the routing metrics.

There is a region where the receiver will not be able to detect the signal, but the signal may disturb other signals [3], which is the *interference region* as shown in figure 3-3. Higher power means wider interference region. To make performance better, the path can be determined by the less number of nodes interfere with a specific node, the less interfering nodes the better. The interference level for a node is simply calculated by summing the directly reachable nodes and the nodes that are affected by these node transmissions at one hop distance. Figure 3-3 shows a wireless node (wn0) and its transmission range, the interference range, and the nodes that are in the interference range. For node wn0 the interference level is 3 which is the number of nodes in the interference range. In the power control, the interference region depends on the path loss model, and for higher path loss models, the power should be increased to enable the receiver to distinguish the signal.

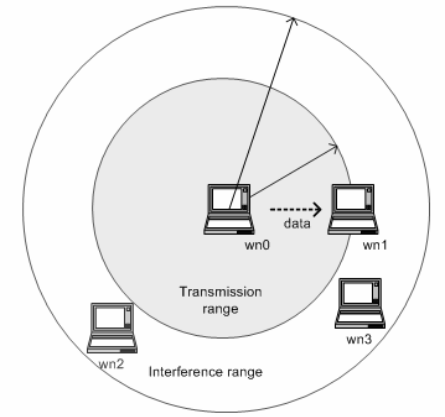


Figure 3 - 3: transmission range and interference range

The power specification depends on different parameters including the distance between the sender and the receiver, the path loss which depends on the surrounding environment, the threshold power for the receiver which specifies the level of power that is distinguished as an accepted data.

To compute the received power in a wireless transmission, we need to compute path loss. Path loss depends on the distance between the sender and the receiver (d), and the wave length (L). The wavelength lambda (L) of the packet transmission is given by the propagation velocity of light (C) divided by the frequency (2.4 GHz).

Light speed (C) = 3.0 E+8.0 meter / second

The wavelength lambda (L) in meters is given in equation Eq3.1:

$$L(meter) = \frac{C(meter/\sec)}{Frequency(Hz)} \quad \text{…..……. (Eq3.1) [2]}$$

$$\text{The Path Loss (PL)} = \frac{16\Pi^2 d^i}{L^2} \quad \text{..... (Eq3.2) [2]}$$

Where *i*=2 for free the space environment, and *i*=3 or *i*=4 for normal environments.

When the transmitted power (tx_power) and the received power (rx_power) are measured, the received power depends on the path loss as in equation Eq3.3, where isotropic antennas are used in the transmitter and the receiver, and the path loss is a function of distance squared (Eq3.2). The farther the distance, the much power needed, so it is not a linear effect, but squared.

$$\text{rx\_power} = \frac{tx\_power}{PL} \quad \text{..... (Eq3.3) [2]}$$

An example taken from table 4-3 in chapter 4, assume a node needs a threshold power equals 0.00025 watt to transmit to another node, if they are 150 meters apart, it will need 0.001 watt if the distance is 300 meters, so it needs four times the power if the distance is doubled, and it needs more power if the environment has higher path loss. So when computing the cost, the effect of the power is important if the weight of the power is high in the cost equation.

3.4 System Routing

Simple routing protocols depend on the hop count in determining the routing information, the hop count is the number of relaying nodes between the source and the destination, note that this is not always a good choice especially for asymmetric links, in that case longer paths may be a better choice. Hop count is also useful to discover some problems like infinite loops, figure 3-4 shows a chain of nodes, to reach from the access point AP to the last node (wn4), it needs to pass through 3 other nodes to reach the destination, in addition to the last hop, so the hop count here is 4, since 4 transmissions are required to deliver packets to the destination.

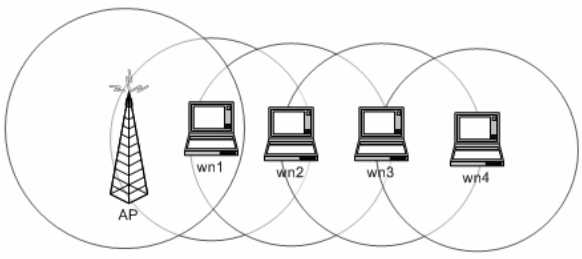


Figure 3 - 4: transmission goes through multi hop path to reach the destination

In our design, we are interested in the hop count as one of the metrics, but not the only one, we need to change the routing process to have better visualization and routing in the network. To implement the changes in the routing process, we are interested in three main factors which are used in this protocol description:

1. Power used: by this factor, we need to optimize the power usage through the whole path from source to destination. Here the maximum power (level1) used in advertisements is predetermined, because it will be used as the reference for computing the distance and the required power for other types of frames.
2. Interference Level: this factor plays an important role in reducing the collisions, and find out alternative routes to make less interference to other reachable nodes.
3. Hop count: the number of relaying nodes in the path.

Distance vector algorithm is used to specify the routes, but with a cost metric that includes power, interference and hop count.

Having 3 factors with their weights

- Power needed * X
- Interference * Y
- Hop count * Z

Where X, Y, and Z are weights to be defined and carefully optimized to determine the path and the next hop for data exchange. Since the units of the metrics are from different types and have different scales of values, the cost computing should consider these differences to reflect the real ratio of each metric.

The interference is computed by hearing the surrounding nodes and estimating the distances. For each node, when it hears other nodes, it will add the node's identity and measure the required power to reach that node. Knowing how many nodes are reachable or affected by a node is the interference level. And knowing the distance from a specific sender node to a receiver node that can be reached directly, then the required power can be calculated. And for the hop count, it is 1 for the neighbor nodes.

The cost is computed by knowing the metrics in the case of direct reachable nodes, and for other nodes, it is calculated by adding the cost for each hop, from the source to the destination.

Equation Eq3-4 is used to compute the cost between two nodes, the metrics and their weights are computed for each hop and the sum of the costs for all hops in the path is considered as the cost between the source and the destination, so equation Eq3-4 represent a cost for a direct link for one hop distance.

Cost = Power * X + Interference * Y + Hop count * Z ……. (Eq 3-4)

For the interference and the hop count, both are integer values (1, 2, 3,...), but the power is a value in watts and it is very small real number, so to have a balanced effect on the cost for the three metrics, the weight X of the power should be much higher, so we multiply it by a number to make the weight and its effect reasonable comparing with the other metrics.

Example: to have equal effect for the three metrics, 1/3 for each, assume we have two peer nodes, one hop distance, interference level of 3, and the needed power is 0.01 milli-watt. Then we have:

Power = 0.01 milli-watt = 0.00001 watt

Hop count = 1

Interference level = 3

For Y and Z they are 1/3 for each, but for the power it should be multiplied by 100000, at least to have the same effect as the hop count.

So we have, Y = Z = 1/3

And X = (1/3) * 100000

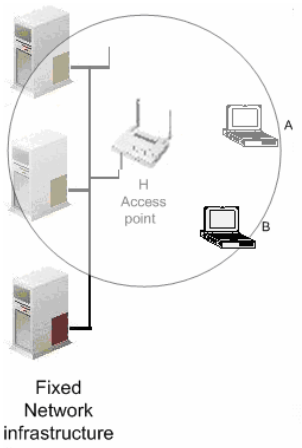
➔ Cost = (1/3 * 100000 * 0.00001) + (1/3 * 3) + (1/3 * 1) = 1.667

The tables in the table-driven protocol are built accumulatively; for each new node or path, it will be added to the existing entries of the routing table. As mentioned before, the cost is computed for the direct neighbors, and then these values are forwarded to all the nodes in the network after adding the cost of the current node.

The redundant paths are treated as known in the distance vector algorithm [14] listed in appendix A, for each path the least cost is kept and the new updates are compared with it, and the less cost replaces the current cost.

3.5 Example

Consider the network in figure 3-6; it has one access point H and two wireless nodes A and B. consider the access point H is the central manager node.



Also consider the values:

One time slot = ts seconds;
Update interval = 100 ts seconds;
Update interval start time = UIST.

Figure 3 - 5 : simple multi hop network example

Assumptions:

- Add (100 ts) to updates interval if more than 70% of the time slots are reserved.
- **Cost = 0.4 * 10000 * power + 0.4 * interference + 0.2 * hop count ….(Eq 3.2)**

Here we multiplied the power cost by 10000 to have the same effect ratio, since the power values are very small compared with interference and hop count values, so we have around 40% of the effect is for the interference, 40% for the power, and 20% for the hop count.

Building the metrics and routing tables

- Step 1:

The metrics and the routing tables are empty, table 3-1 shows the metrics table for node H. Node H reserves the first time slot (figure 3-6), and announce the network information; like the number of active nodes, the reserved nodes, the start time, and the slot time duration.

Node H:

Node	Via node	Power	Hops	Inference	Cost
-	-	-	-	-	-

Table 3 - 1: node H metrics table initialized

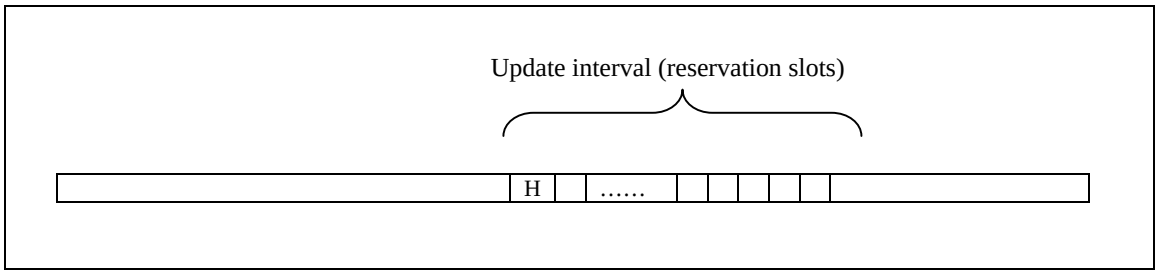


Figure 3 - 6: the updates interval, H reserves the first slot

- Step 2:

Now A and B will receive the broadcast and compute the distance from the power and add node H to their metrics tables.

Node A:

Node	Via node	Power	Hops	Inference	Cost
H	H	0.0001	1	1	-

Node B:

Node	Via node	Power	Hops	Inference	Cost
H	H	0.00009	1	1	-

Table 3 - 2: Nodes A and B metrics tables after hearing node H broadcast

Note that both A and B considered the interference level as 1 at this moment, because both assume that node H is the only interfering node.

- Step 3:

Both A and B can now try to reserve the next free time slot, using the back off algorithm [3] they will send a broadcast. The first which send will reserve the first free slot, the other will wait for the next round to reserve another free slot. If a collision occurs in the reservation process, both will wait for the coming rounds of reservations periods, in that case the node H will not put neither A or B in the successful reservations.

Let us assume that A reserved the next free slot, then:

H start time = UIST and A start time = UIST + ts.

During the broadcast interval for H (the fixed network access point), it will announce the reservations for the time slots. The reservation table will be propagated to all nodes in the network, if a node sees its identity in the reservation entries, then it is accepted to participate in the specified time slot, if not, then there were a problem (maybe collision) and this node will try to reserve different time slot in the coming cycles.

After the successful reservation for node A, then it will send its broadcast in its period (figure 3-7). Then nodes H and B will hear node A's broadcast

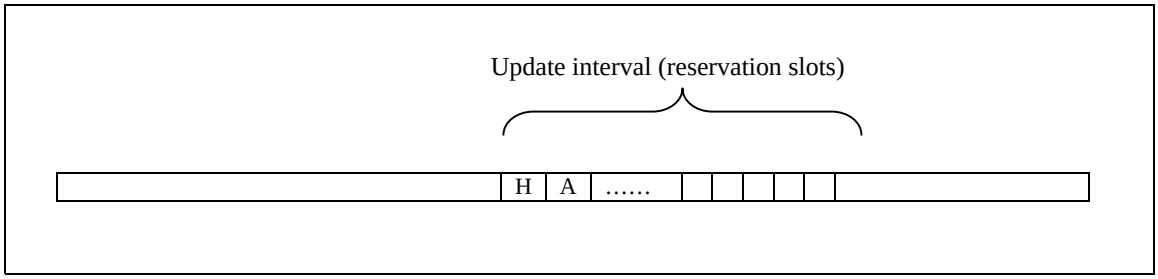


Figure 3 - 7: the updates interval, node (A) reserves the second slot

Table 3-3 shows the updates in the metrics tables in nodes H and B after node A's broadcast.

Node H:

Node	**Via node**	**Power**	**Hops**	**Inference**	**Cost**
A	A	0.0001	1	1	-

Node B:

Node	**Via node**	**Power**	**Hops**	**Inference**	**Cost**
H	H	0.00009	1	2	-
A	A	0.00008	1	2	-

Table 3 - 3: nodes H and B metrics tables after hearing the broadcast of node A.

- Step 4:

In the coming cycles, node B can reserve the next free slot, Figure 3-8 shows the successful reservations for all nodes, so these nodes can announce their information at these specified intervals, and table 3-4 shows the content of the metrics tables for these nodes.

H start time = UIST

A start time = UIST + ts.

B start time = UIST + 2 ts.

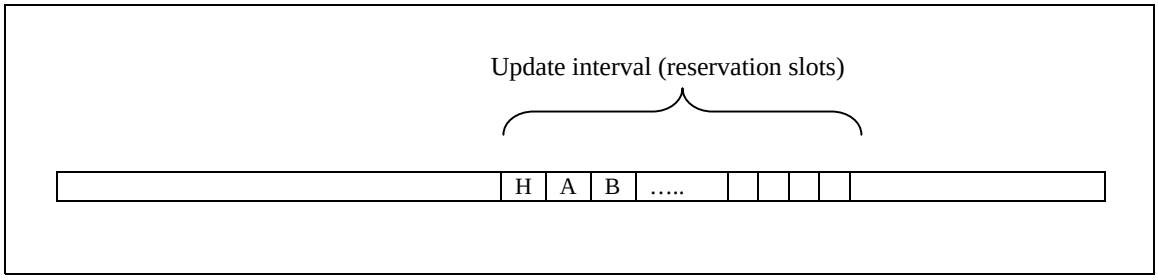


Figure 3 - 8: the updates interval, B reserves the third slot

Node H:

Node	Via node	Power	Hops	Inference	Cost
A	A	0.0001	1	2	1.4
B	B	0.00009	1	2	1.36

Node A:

Node	Via node	Power	Hops	Inference	Cost
H	H	0.0001	1	2	1.4
B	B	0.00008	1	2	1.32

Node B:

Node	Via node	Power	Hops	Inference	Cost
H	H	0.00009	1	2	1.36
A	A	0.00008	1	2	1.32

Table 3 - 4: metrics tables after hearing the broadcast of node B

- Step 5:

Now, computing the routing costs in the routing tables. The routing table includes the destination node, the next hop, and the total cost for each node (figure 3-9), so it will produce redundant entries with different paths and different costs, where the cost for the current hop will be added to original cost to the destinations, as shown in table 3-5.

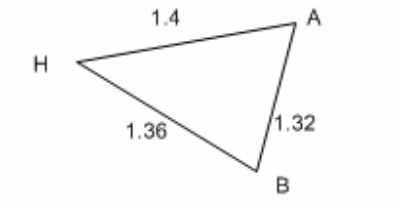


Figure 3 - 9: the three nodes H, A, and B with their costs graph

Node H:

Dest. Node	Via node	Cost
A	A	1.4
B	B	1.36
A	B	1.36+1.32=2.68
B	A	1.4+1.32=2.72

Node A:

Dest. Node	Via node	Cost
H	H	1.4
B	B	1.32
H	B	1.32+1.36=2.68
B	H	1.4+1.36=2.76

Node B

Dest. Node	Via node	Cost
H	H	1.36
A	A	1.32
H	A	1.32+1.4=2.72
A	H	1.36+1.4=2.76

Table 3 - 5: Routing tables for all nodes with redundant paths.

- Step 6:

Then the redundant paths are compared and the less cost path is chosen according to the distance vector algorithm [3]. The resulted routing tables with least cost are shown in table 3-6. These values will be compared with the new costs that come later after new updates arrive. The less costs paths will be kept.

Node H:

Dest. Node	Via node	Cost
A	A	1.4
B	B	1.36

Node A:

Dest. Node	Via node	Cost
H	H	1.4
B	B	1.32

Node B

Dest. Node	Via node	Cost
H	H	1.36
A	A	1.32

Table 3 - 6: Routing tables with least costs

Note:
From the scenario described above it seems that the initialization process takes long time, this happens because there is a need to multiple cycles to detect the whole network. So the performance at the initialization expected to be low, and then it will increase when the network stabilizes.

Figure 3-10 shows another example, where a fixed network with two Access points H and F, and six wireless nodes.
In this network, after some time, each node will have the information about the other nodes, and the neighbor nodes will know each other metrics.
Table 3-7 shows an example of the routing table for A in this network after the network information is known.

Node A

Node	Via node	Cost
F	F	2
B	B	2.5
D	D	2
C	B	5
E	D	6
G	D	7
H	F	5

Table 3 - 7: node A routing table, node A is shown in figure 3-10.

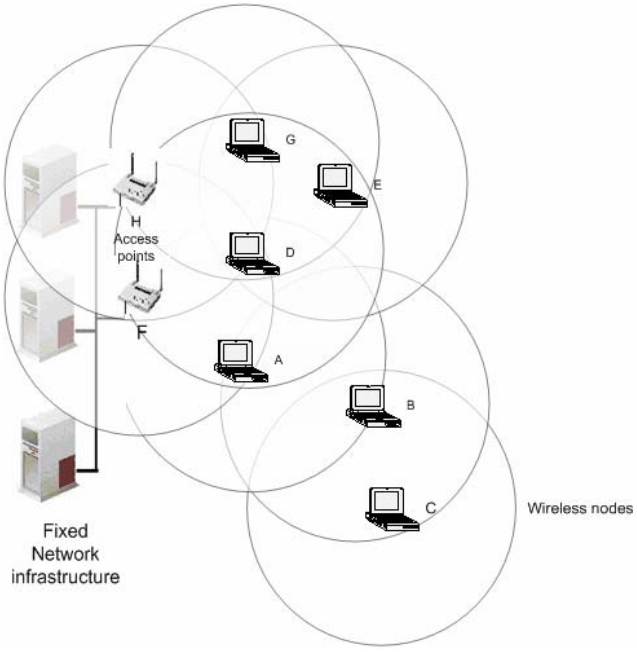


Figure 3 - 10: multi hop network example

Chapter 4

Modeling and Simulations

4.1 Introduction: Modeling Definitions

This chapter presents the modeling process, description of the experiments, and results of these experiments with explanations and conclusions.

In the following sections, the used models conform to the 802.11b standard, the changes which are made are in the configuration of the network, or changing the power of different types of frames. OPNET modeler [6] accepts changes on different levels, either by changing the properties of a specific object or node, or using alternative processes or functions to model a specific task, or even changing the entire C/C++ code which is the basic programming language for OPNET.

In our implementation, the changes were mainly on the configuration of the topology and nodes properties, and on the power control within the MAC layer process module (*wireless_lan_mac*), and changes on interference calculations in power LAN module (*wlan_power*) which are all coded in C/C++.

4.1.1 OPNET models

OPNET has models for different devices of WLAN; one of these devices is the Mobile Ad-hoc Network (MANET) node. MANET node has the ability of generating traffic by defining streams of packets and the ability of forwarding packets using the ad-hoc routing protocols like AODV and DSR.

The following figure (4.1) shows the process model of the MANET station; the lower layers of WLAN are the modeled as RX and TX ports as the physical layer, and *wireless_lan_mac* process as the MAC layer.

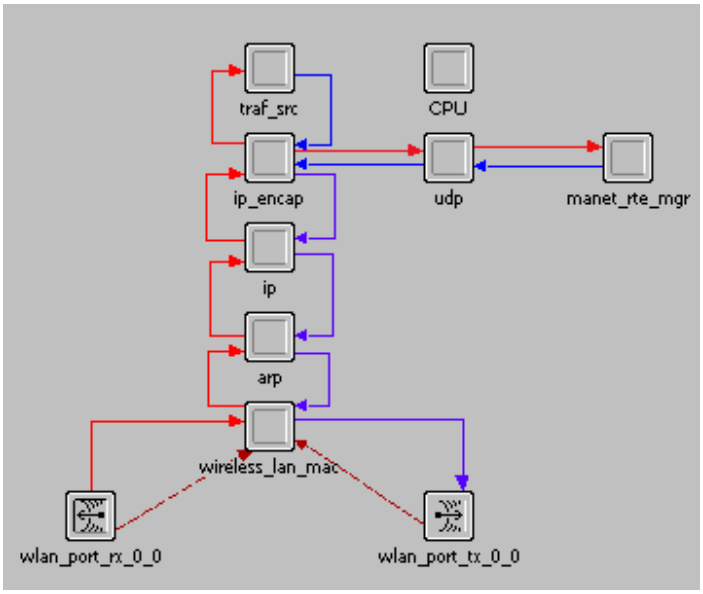


Figure 4 - 1: MANET station Model (OPNET modeler [6])

During simulation we are interested in values of measurements:

- **Load**: Total number of bits received from the higher layer to the MAC layer. Packets arriving from the higher layer are stored in the higher layer queue.
- **Throughput**: Total number of bits sent to the higher layer from the MAC layer. The data packets received at the physical layer are sent to the higher layer if they are destined for this station, and they will arrive to the IP layer if they are rerouted to other station.
- **Dropped data packets** due to the overflow of higher-layer buffer, so they are not part of the load.
- **Traffic:** it is the upper layers packets forwarded downstream to the network, all this traffic is supposed to be converted to load after adding the headers of the network and the data link layers. If the traffic size exceeds the capacity of the lower layers, part of the traffic will be dropped and the load is only the acceptable part of the traffic.

The upper layers' headers and control packets as the routing packets are counted as a part of the load and the throughput. So using very small packets will increase the headers overhead in measuring the load and throughput values.

In the coming experiments, the packets are exponentially distributed in size with mean of 10,000 bits, and the inter-arrival time between packets is exponentially distributed with mean of 1 second. To generate more traffic in a second, the number of packets generated is changed by adding more entries of packets, for example if we need traffic of 1 Mbps size, we may use a 100 entries of packets, 10000 bits each.

If the traffic size is manageable to be sent without drop, extra bytes will be added to the load and the throughput as headers and routing protocols packets, if it the traffic overflows the lower layer buffer and medium, then dropping packets will occur and the load is lower than the traffic.

4.1.2 Data collection procedure

OPNET enables us to configure when to start collecting results, the following configuration was used: Firstly, the simulator was configured to start collecting results after 10 seconds of the run time. Secondly, each experiment is done 10 times with different seed values, so we can figure out different

results for different seeds but within a specific range of values. Thirdly, OPNET generates the results as graphical functions, these functions can be sampled into discrete values, a 100 samples for each run, each sample is the average of values over a short time, for more precise sampling we can choose higher number of samples, but if the change is not at very high rate, the 100 sample is sufficient.

Finally, we will have 100 samples, then by omitting the initial period and part of the end period, because these intervals does not represent the normal behavior, we will have around 80 values, taking the average for each experiment, and repeating the same experiment 10 times with different seeds, we can compute the average, standard deviation, and the confidence interval for the results of the 10 seeds. Normally we are interested in performance in the highly loaded cases, so we start normally with acceptable loads without drop and start increasing the traffic, so for different configurations we need to measure the better throughputs and points of changes.

In the following experiments, the time used for running the experiments has been chosen to be representative for the long runs, for the small networks of few nodes we used run time of 300 seconds, and the first 10 seconds are omitted, for the more populated networks like a grid of nodes, we used 90 seconds of run time. For 90 seconds of runtime in a grid of 42 nodes, at the highest acceptable traffic, it took around 4 hours of system time for 10 different seeds.

4.1.3 Statistical analysis procedure

In the following experiments, 10 runs are done with different seeds and we took the averages and computed the confidence intervals. The detailed statistics for all experiments are shown in appendix A2.

Confidence intervals: $[\, a - \frac{z\sigma}{\sqrt{n}} , a + \frac{z\sigma}{\sqrt{n}} \,]$ ……..Eq4.1 [5]

Where

a : Average value of the experiments (the average of the 10 values)

σ : The standard deviation of the values

n: the number of experiments (here it is 10 times)

z: the normal distribution parameter, z reflects the number of standard deviations above or below the mean.

The value *(z)* depends on the needed interval of confidentiality in the normal distribution; it is the point where a certain percentage of the values exist between -*z* and *z* in the normal distribution.

An example is shown in figure 4-2, for 95% of the values, in the normal distribution, it exists between the z values -1.96 and +1.96 as shown in figure 4-2 and table 4-1.

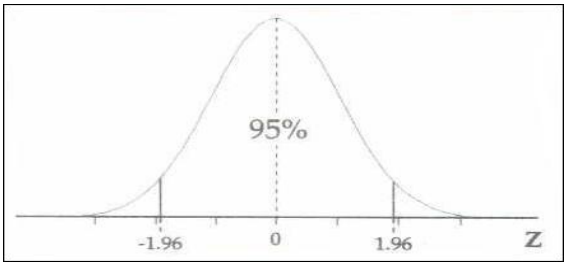


Figure 4 - 2: Normal Distribution

z (90%)	*z (95%)*	*z (99%)*
1,645	1,96	2,575

Table 4 - 1: z values for different confidence intervals

A 95% confidence level tells us that 95% of an entire data set is found within ±1.96 standard deviation of the mean. At 1.96 in the normal distribution table we find value 0.4750 which is half of 0.95. The total is 0.4750 + 0.4750 = 0.95 = 95% of the values.

So, if we use a confidence level of 95%, we can say that we are 95% confident, or certain, that 95% of the values, including the mean, is contained in that range.

4.1.4 General configurations

The global parameters for the MAC layer in the stations are

Data Rates	11 Mbps
Transmit power	0.001 watt
RTS threshold	256 bytes
buffer size	256000 bits
Packet reception power threshold	-90 dBm

Table 4 - 2: WLAN MAC configurations

From table 4-2, we see that the data rate is 11 Mbps, the transmit power is 1 milli watt, the RTS is used only for packets of 256 bytes or more, the buffer size in the MAC layer is 256000 bits, and the power threshold (PT) in dBm is -90 dBm which can be converted to watts using the formula:

Reception power threshold (watts) = $\frac{10^{PTdBm/10}}{1000}$ ……Eq4.2 [2]

-90 dBm = 1.0 E-9.0 mw = 1.0 E-12.0 watt.

Received Power and Path Loss Calculations

To compute the received power in a wireless transmission, we need to compute path loss. Path loss depends on the distance, and the wave length. The wavelength lambda (L) of the packet transmission is given by the propagation velocity of light of light (C) divided by the frequency (2.4 GHz).

Frequency = 2.401 GHz = 2.401E+9.0 Hz, which is the IEEE 802.11b frequency [7].

Light speed (C) = 3.0 E+8.0 meter / second

Lambda (L) in meters is given by:

$$L(meter) = \frac{C(meter/\sec)}{Frequency(Hz)} \quad \text{…..……. (Eq4.3) [2]}$$

For 2.401 GHz, L $= \frac{3.0E+8.0}{2.401E+9.0} = 0.124947938$ meter

The Path Loss (PL) $= \frac{16\Pi^2 d^i}{L^2}$ ……. (Eq4.4) [2]

Where *i*=2 for the free space environment, and *i*=3, or *i*=4 for normal environments.

For example, in a network of 2 wireless nodes, 300 meters away from each other. The path loss is:

$$PL = \frac{16\Pi^2 (300)^2}{(0{,}124947938)^2} = 8.193067966\ E{+}09$$ .....(For the free space environment)

NOTE:

The received power calculation considers the gains apply in both the transmitter and the receiver antennas as shown in Friis equation (Eq4.5).

$$P_R = \frac{P_T G_T G_R}{L_P}$$ ……(Eq4.5), Friis equation [13]

Where P_R : the received power (watts)

P_T : the transmitter power (watts)

G_T: the transmitter antenna gain

G_R: the receiver antenna gain

L_P: the path loss

For the gains in the transmitter and the receiver, we assume isotropic antennas which provide no gain because it sends symmetric signal in all directions. Isotropic antennas have a perfectly symmetric behavior with respect to all possible signal paths. The gain of an antenna in a particular direction is measured in comparison to an isotropic antenna. It is defined as the ratio of signal power produced by the antenna at a given distance and the isotropic power that would be measured at the same distance. Gain is a unit less and its value is 1 in our calculations.

The expected received power (rx_power) is computed from the transmitted power (tx_power) using the formula:

$$rx\_power = \frac{tx\_power}{PL}$$ ……. (Eq4.6) [2]

where tx_power and rx_power are in watts and path loss is unit less.

$$rx\_power = \frac{0.001}{8.193067966\,E+09}$$

= 1.09849E-12 watt

The threshold as mentioned in the configuration is 1.0 E-12.0 watt, which means the received power is just higher than the threshold, so for 300 meters, the needed transmission power is 0.001 watt when a reception power threshold of -90 dBm (1.0 E-12.0 watt) is used.

The packets which are received with a power higher than threshold are considered as valid packets. They are sensed by the MAC and they can be received successfully unless they get bit errors due to interference, background noise and/or colliding with other valid packets.

Unless the default transmission power is considerably lowered, all the WLAN packets should reach at their destinations with sufficient power to have a valid packet, when the propagation distance between the source and destination is less than 300 meters as required by the IEEE802.11 WLAN standard. Knowing the threshold and the threshold received power (1.0E-12 watt) we can compute the needed power as a function of distance.

NOTE:

OPNET computes the Path loss the other way around, but later it multiplies with the path loss which produces the same expected received power.

$$PL = \frac{L^2}{16\Pi^2 d^2} \quad \text{……..…..(Eq4.7) [6]}$$

rx_power = tx_power x path loss ……..…… (Eq4.8) [6]

Transmission Power Calculations

Consider figure 4-3, we have a transmitter (node0), and two receivers (node1 and node2); we need to calculate the sufficient power for node 2 which is 50 meters from the sender. Note that we already found that for 300 meters spacing, the threshold transmission power is about 0.001 watt.

The common attributes are L = 0,124947938 meters, the value $16\Pi^2$ =157,9137

tx_power = rx_power x PL

tx_power = rx_power $\frac{16\Pi^2 d^2}{L^2}$

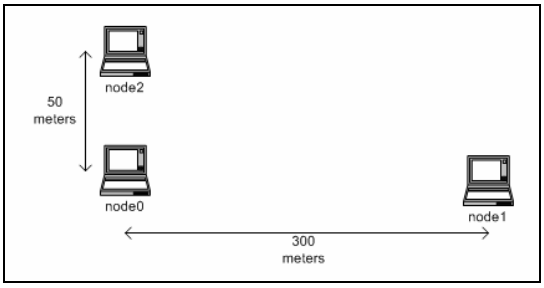


Figure 4 - 3: transmission power for different distances

$$rx\_power(d) = rx\_power(d_{ref})(\frac{d_{ref}}{d})^2 \quad \text{…….. (Eq4.9) [2]}$$

Where d_{ref} is the reference distance where we want to have the threshold received power compared with the known distance d, and *d* is the typical distance, here d is 300 meters

For example when node0 is sending to node1 and node2 with a transmission power (tx_power = 1 milli-watt), the path loss and the received power at node1 as shown before is:

PL (distance 300) = 8.193067966 E+09

rx_power = 1.09849E-12 watt

The received power at node2 which is 50 meters (reference distance) away from node0

$$rx\_power(d_{ref}) = rx\_power(d)(\frac{d}{d_{ref}})^2 \quad \text{…….(Eq4.10 , } \textit{Eq4.9 reordered}\text{)}$$

$$rx\_power(50) = rx\_power(300)\ (\frac{300}{50})^2$$

$$= 1.09849E\text{-}12 \times 36$$

$$= 3{,}95456E\text{-}11 \text{ watt}$$

To have the received power for different distances to be the threshold power (1.09849E-12 mw) we need to modify the transmission power with the same factor in Eq4.8.

$$tx\_power(\text{distance } d_{ref}) = \frac{d_{ref}^{\ 2}}{d^2} \times tx\_power(d) \ldots\ldots\ldots\ldots\ldots\ldots (Eq4.11)$$

As we can see, the ratio depends on squared distance ratio, and the 300 meters distance is the default distance and if we have less distance we can decrease the power by the factor $(d_{ref}/300)^2$.

Examples:

For $d_{ref} = 50$

$$tx\_power(50) = \frac{50^2}{300^2} \times tx\_power(300) = 2{,}77778E\text{-}02 \times 0.001 = 2{,}77778E\text{-}05 \text{ watt}$$

For $d_{ref} = 150$

$$tx\_power(150) = \frac{150^2}{300^2} \times tx\_power(300) = 0.25 \times 0.001 = 0.00025 \text{ watt}$$

Table (4-3) shows the required power for the following references distances

d_{ref} (meters)	Path loss	tx_power (watt)
50	3,95456E-08	2,77778E-05
60	2,74622E-08	0,00004
70	2,01763E-08	5,44444E-05
80	1,54475E-08	7,11111E-05
90	1,22054E-08	0,00009
100	9,88641E-09	0,000111111
150	4,39396E-09	0,00025
200	2,4716E-09	0,000444444
250	1,58183E-09	0,000694444
300	1,09849E-09	0,001

Table 4 - 3: path loss and transmission power for difference distances for a threshold of -90 dBm

Interference

The interference level for a node depends on the transmission power and the power model, in the first experiments [6]. In the beginning, we assumed that the interference range and the transmission range are the same, which means if the power at a node is the threshold power, then the interference will not propagate farther.

It depends on the environment how much the interference will go beyond the transmission range, so at the final experiments, this issue is discussed with experiments.

Path Loss (OPNET code):

As mentioned before, OPNET computes the Path loss the other way around, but later it multiplies with the path loss instead of dividing by it, which produces the same expected received power.

```
688  sdistance = 50.0;
689          /* Compute path loss using simple 1/r^2 formula */
690          frequency_mhz1 = wlan_min_freq_for_chan (channel_num);
691          lambda1 = C / (frequency_mhz1 * 1.0E+6);
692          if (sdistance > 0.0)
693                  {
694          path_loss1 = (lambda1 * lambda1) / (SIXTEEN_PI_SQ * sdistance * sdistance);
695                  }
696          else
697                  path_loss1 = 1.0;
698                  /* Path loss computed in dB */
699          pathloss_threshold_dbm = log10(path_loss1*1000)*10;
700          /* the path loss is less than the threshold identified by the settings parameters*/
701           ex_rc_power = tx_power / rx_power_threshold ; /* Expected received power  */
702
703          tx_power_data = tx_power*(sdistance*sdistance/90000.0);
```

Table 4 - 4 : OPNET code to change the data power according to the distance

The code listed in table 1 shows how OPNET computes the path loss (line 694) and changes the transmission power according to the distance (line 703). This is also changed where we used other models of path loss as explained later; it is multiplied by the distance ratio to the power 3 and 4 for higher path loss models, but here it is to the power 2 in the free space model.

Here we assumed the data power (tx_data_power) is the reference value which we will use later for data packets, and we will use multiples of this value for RTS CTS power

$$\text{For a distance=sdistance, tx\_power\_data(sdistance)} = \frac{sdisance^2}{300^2} \text{ x tx\_power (300)}$$

Here (sdistance) is changed according to the network configuration.

The original code was to use the same power for all distances, if it is less than or equal 300 meters, then the transmission will occur, otherwise it will not. For the short distances the received power exceeds the threshold, and the signal will propagate to farther distances and interfere with other signals.

For using different values of power for different types of frames we check frame type for each frame and use the suitable power value, some experiments later will check the RTS and CTS signales power effect; here we changed the ratio (R) for each experiment.

In the code listed in table (4-5), we are interested in distinguishing between two groups of frames: data and data acknowledgment frames (WlanC_Data and WlanC_Data_Ack), and the RTS and CTS frames (WlanC_Rts , WlanC_Cts) , for the first group we use data power (tx_power_data) value, which is the threshold transmission power. For the second group we use the control power

(tx_power_cntrol) value, which is a ratio (R) multiplied by the data power, where the ratio R is greater or equal to 1.

```
2230        Usedpower=0.0;
2231        tx_power_cntrl = tx_power_data*R;
2232            if (frame_type == WlanC_Rts || frame_type == WlanC_Cts)
2233            { usedpower=tx_power_cntrl;
2234            }
2235        else
2236        if ((frame_type == WlanC_Data) || (frame_type == WlanC_Data_Ack))
2237            {
2238            /* Adjust the transmission data rate based on the operational speed.*/
2239            tx_data_rate = operational_speed;
2240            usedpower=tx_power_data;
2241            }
2242            else
2243            {
2244            usedpower=tx_power_data;
2245            }
2246            op_ima_obj_attr_set (txch_objid, "power", usedpower);
```

Table 4 - 5: OPNET code to change the power according the frame type.

The original code was to use the same power (tx_power) for all types of frames.

The last change in the code is in the wlan_power model, which computes the path loss, different formulas for the path loss used for last experiment, for the free space path loss, the default formula used:

```
path_loss1 = (lambda1 * lambda1) / (SIXTEEN_PI_SQ * sdistance * sdistance);
```

And for other environments, we used the power 3 or 4 of the distance.

```
path_loss1 = (lambda1 * lambda1) / (SIXTEEN_PI_SQ * sdistance * sdistance* sdistance);
```

Or

```
path_loss1 = (lambda1 * lambda1) / (SIXTEEN_PI_SQ * sdistance * sdistance* sdistance* sdistance);
```

***Section 4.5 (experiment 11) explains more about these formulas.**

- **Traffic parameters**

Start time (seconds)	1.0
Packet inter arrival time (seconds)	Exponential(1)
Packet size (bits)	Exponential (10000)

Table 4 - 6: traffic configuration at the source nodes

The traffic at MANET stations can be specified by the parameters listed in table 4-6, the start time of traffic generation in the run time, the distribution of the inter arrival time of packets, here it is means the arrival of packets is exponentially distributed with a mean of 1 second, so if we have more than

one entry of packets, which is the case, not all packets are generated at once, but they are generated at different instances from the entire second.

Finally the packet size is not always the same, but it is distributed exponentially with a mean of 10000 bits in size, this means we may have different size of packets. To generate more traffic we use multiple entries of packets as mentioned earlier.

Regardless the value of the packet size, if the size of a higher layer packet is larger than the maximum MSDU size allowed by the IEEE 802.11 WLAN standard, which is 2304 bytes, then such a packet will not be transmitted by the MAC, and it will be immediately discarded since we consider no fragmentation and large packets to be dropped [6].

4.2 Normal 802.11 Experiments

In the experiments of this section, we will test the normal behavior of the 802.11 for one sender to one receiver network, and for six senders to six receivers within the transmission range of each other.

- ### 4.2.1 One sender and one receiver

  - 4.2.1.1 **One sender and one receiver, exponential traffic (Experiment 1.a)**

Here we have two nodes operating at 11 Mbps bandwidth and 300 meters range as shown in figure 4-4. The RTS CTS packets are used to reserve the channel of transmission with same power of data packets. Here node0 is the sender where we measure the load and node1 is the receiver where we measure the throughput.

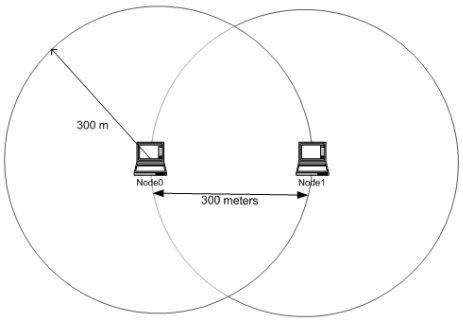


Figure 4 - 4: One sender to one receiver

Traffic is generated at node0 and sent to node1, the packets are exponential distributed in with mean of 10000 bits. For each traffic size listed in table 4-7, the values of load, traffic, and dropped packets were measured.

Traffic (Mbps)	Load (bps)	Throughput (bps)	Drop (bps)
0	0	0	0
1	1013109	1012947	0
2	2025691	2025374	0
3	3070303	3068862	0
4	3716917	3716622	387695,7
5	3476618	3476389	1627939
6	3236251	3236077	2871047
7	3017528	3017102	4130903

Table 4 - 7: One sender to one receiver results, experiment 1.a

Looking at the results in table 4-7, we note that for the low traffic sizes (less than 4 Mbps), we see no drop because all the traffic is forwarded down to the network and the load is the traffic size in addition to the headers of the upper layers. The throughput at the other side is almost the same value of the load.

For the higher traffic sizes (more or equal to 4 Mbps), the dropping of packets happened because the sender capacity can not accept all the traffic generated. So the sender could only handle up to 3.72 Mbps at 4 Mbps traffic size. For the higher values of traffic, load and throughput started to decrease again.

This happens when the traffic is exponentially distributed in size; here we have the MAC layer buffer is limited by 256000 bits, and the buffer is almost full all the time. When there is a space for small packet in the buffer, and a big frame arrives, it will be dropped directly. The more traffic the more probability of having frames bigger than the space in the buffer and the fewer loads and traffic as shown in figure 4-5.

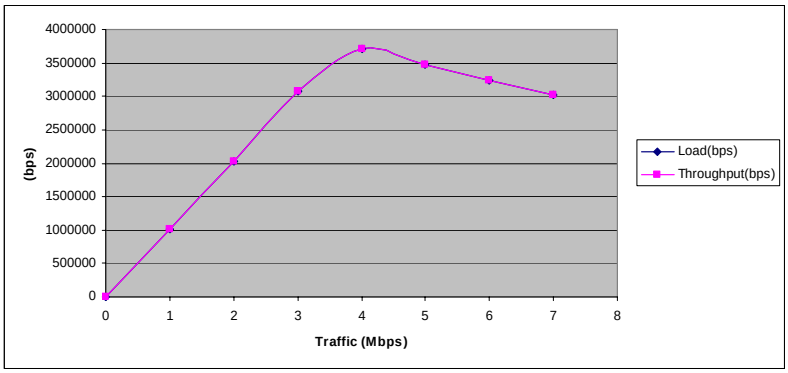


Figure 4 - 5: Load and throughput: one sender to one receiver, experiment 1.a

Table 4-8 shows the statistical results for the case where a traffic of 5 Mbps, it appears that doing the same experiment 10 times will produce a mean throughput of 3.62 Mbps with relatively small confidence intervals.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
3623278,645	32409,56186	0,008944816	3603191	3643366	3595023	3651535

Table 4 - 8: Throughput results for traffic of 5 Mbps in one to one network, experiment 1.a

- 4.2.1.2 **One sender and one receiver, constant traffic (Experiment 1.b)**

Now the same experiment with different attribute of traffic packets, in this case we are using constant packet size entries, 10000 bits each.

Table 4-9 and figure 4-6 show higher loads and throughputs (up to 4.08 Mbps) comparing to exponentially distributed packets in size case (experiment 1.a), it also shows stable values after the network exceeds its capacity, this happened because having when constant size packets, the probability of drop is less since larger packets have higher probability of dropping, also when the network is overloaded more, there will be no change since all packets are equal, and that's why it produces stable behavior after the highest capacity reached.

A note for both experiments, they produced relatively low loads and throughputs, it is expected to have higher than 5 Mbps, but since the RTS CTS signals are used for each packet, this will cause higher waiting time for each packet although there is only one sender and one receiver.

Traffic (Mbps)	Load (bps)	Throughput (bps)
0	0	0
1	1016990,78	1013625,652
2	2027856,738	2027784,681
3	3052809,787	3052341,418
4	3988556,596	3987927,455
5	4081870,071	4081563,83
6	4079095,887	4079095,887
7	4079258,014	4079276,028

Table 4 - 9: One sender to one receiver Results, experiment 1.b

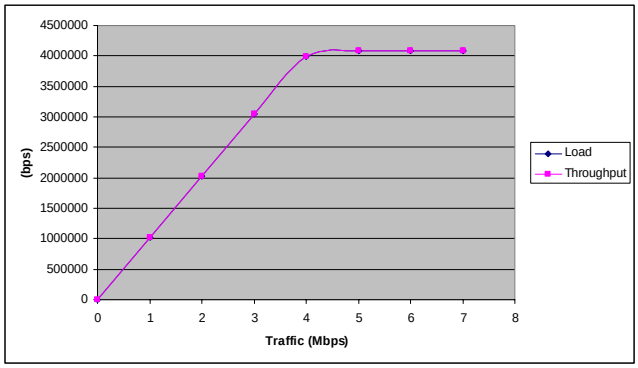


Figure 4 - 6: Load and throughput: one sender to one receiver, experiment 1.b

- **4.1.2 Six senders to six receivers**

- 4.1.2.1 **Six senders to six receivers, exponential traffic (Experiment 2.a)**

In this experiment, within the same distance (300 meters), six senders are sending data to six receivers; six one-to-one transmissions. As shown in figure 4-7, distances between senders are 60 meters, so the total distance from the first sender to the farthest sender is 300 meters, and the same apply for the receivers, so all senders and receivers are within the transmission range and not more than one transmission can take place at a time, and the total bandwidth will be divided between the competing transmissions.

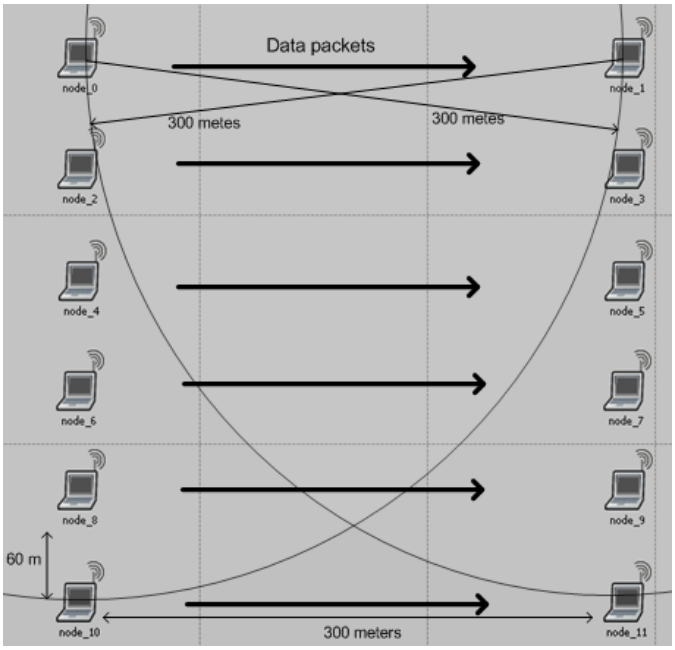


Figure 4 - 7: Six senders to six receivers

Here load is measured for all senders as sum of loads for the six sender nodes, and the throughput as well is measured as the sum of throughputs in the six receivers, the traffic is distributed over the senders equally, one sixth for each sender.

The traffic packets are defined as in experiment 1.a, exponentially distributed in size with mean 10000 bits, and we will check the case of constant size packets in the next experiment.

Table 4-10 and figure 4-8 show the loads and the throughputs for different traffic values, the results show that the maximum load and throughput are around 4.02 Mbps, and then the values started decreasing again after the traffic exceeded 4.5 Mbps. This happens when the traffic is exponential distributed is size; here we have the MAC layer buffer is limited, and the arriving packets may get dropped if the remaining space in the buffer is smaller than the packet size, so the number of large packets increase if the traffic size increase and cause more dropping and less load and throughput.

Traffic(Mbps)	Load(bps)	Throughput(bps)	Drop (bps)
0	0,0	0,0	0,0
1,5	1525621,8	1525610,2	0,0
3	3061188,6	3061156,7	0,0
4,5	4016563,2	4016400,6	574845,2
6	3724968,4	3725008,3	2381876,5
7,5	3473684,7	3472997,3	4171892,1

Table 4 - 10: Six senders to six receiver results, experiment 2a

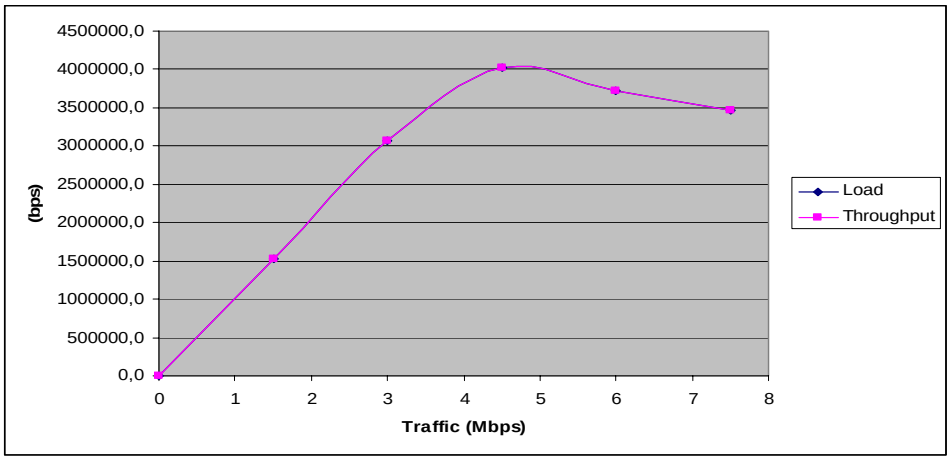


Figure 4 - 8: Load and throughput: six senders to six receivers, experiment 2.a

Table 4-11 shows the statistical results for the case where a traffic of 4.5 Mbps, it appears that doing the same experiment 10 times will produce a mean throughput of 4.016 Mbps with relatively small confidence intervals.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
4016400,6	6628,96752	0,00165	4012292	4020509	4010621	4022180

Table 4 - 11: throughput results for traffic of 4.5 Mbps in six senders to six receivers' network, experiment 2.a

Here we can see the maximum throughput is about 4.02 Mbps at 4.5 Mbps traffic, comparing to one-to-one transmission, it was about 3.6 Mbps with exponential packets size traffic. When one node is transmitting; for each packet, the node will draw a new contention waiting period after DIFS period and the start of the new transmission of the RTS (figure 4-9). The start time will be random between 0 and contention window (CW) size and it will be CW/2 on the average. While for six senders when a node ends its transmission, it will draw a new contention waiting period, but the other nodes will resume count down their timers in the contention period and the minimum of the timers will win and start transmission for the next round [3].

Taking the minimum waiting time instead of waiting w/2 on the average will increase the throughput of six senders over the one sender case, so the less waiting time for the next RTS caused the better throughput for six senders over the one sender cases.

Finally, the RTS and CTS packets will help in the case of six senders from collisions and retransmissions between senders, and the collisions of RTS packets that may occur has low probability since RTS and CTS packets are very small.

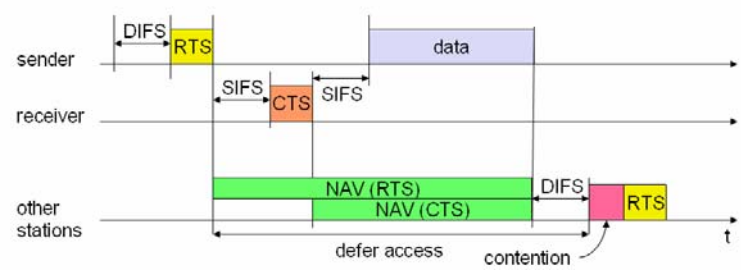


Figure 4 - 9: The contention window after a sender finishes its transmission [3]

- 4.2.2.2 **Six senders to six receivers, exponential traffic (Experiment 2.b)**

Now the same experiment with different attribute of traffic packets, in this case we are using constant packet size entries, 10000 bits each.

Table 4-12 and figure 4-10 show higher loads and throughputs (up to 4.325 Mbps) comparing to exponentially distributed packets case (experiment 2.a) which is about 4.02 Mbps.

The same justification applies here as in experiment 1.b, since when having constant size packets, the probability of drop is less since larger packets have higher probability of dropping, also when the network is more overloaded, there will be no change since all packets are equal, and that's why it produces stable behavior after the highest capacity reached.

Traffic (Mbps)	Load (bps)	Throughput (bps)
0	0,0	0,0
1,5	1520433,191	1520415,177
3	3051170,496	3050900,284
4,5	4324034,752	4322305,39
6	4325349,787	4324971,489
7,5	4322233,333	4321620,851

Table 4 - 12: Six senders to six receivers Results, experiment 2.b

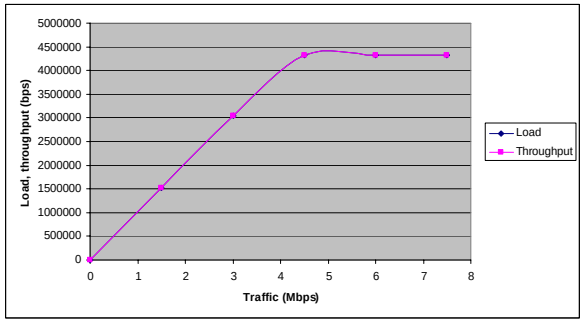


Figure 4 - 10 : Load and throughput: six senders to six receiver, experiment 2.b

4.3 Using power control experiments

- **4.3.1 Chain of 4 nodes (Experiment 3)**

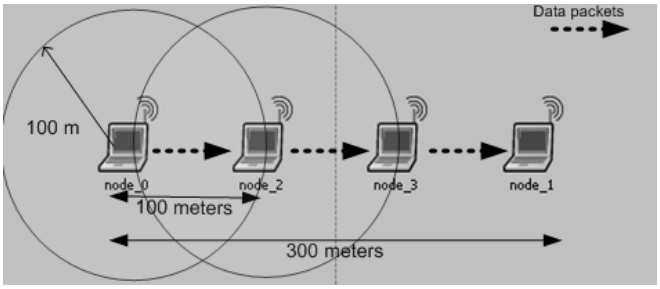


Figure 4 - 11: Four nodes chain with power control

The configuration in this experiment shown in figure (4-11); the source (node_0) and the destination node (node_1) can not reach each other directly, since the power used is only sufficient to reach the direct neighbor nodes, so they will use the intermediate nodes to deliver the data to each other. The traffic is generated at node_0 at left side and destined to node_1 at the right side; the spacing between nodes is 100 meters, and the power used in transmission is only sufficient to transmit up to this distance.

Because the RTS and CTS packets will force the nodes that are not part of the current transmission to wait, there will be only one active transmission at a time. So the total throughput is divided by the number of hops (here 3).

In this experiment we will measure the load at the source node, and the throughput at the destination node, and we will see the maximum total throughput as the sum of throughputs in all nodes.

As shown in the results in table (4-13) and figure (4-12), the maximum throughput for the destination node is about 1.15 Mbps which is less than one third of the maximum throughput is a single hop (3.62 Mbps). This happens because in one to one transmission, only one RTS CTS packet is needed to deliver one data packet to the destination, in addition to the waiting times which will happen in the three transmissions. More time will be used as control packets, and more waiting time, this which will produce fewer throughputs as we have here.

Traffic (Mbps)	Load (bps)	Throughput (bps)
0	0	0
0,5	507940,4	507799,6
1	1007069	1007053
1,5	1145994	1145658
2	1045446	1045332

Table 4 - 13: Load in the source node and throughput in the destination node for 4 nodes chain

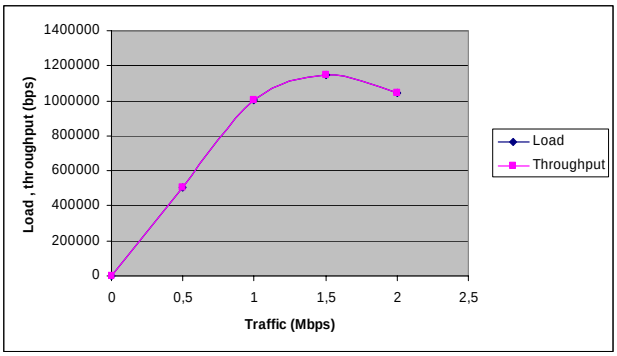


Figure 4 - 12: Load and throughput in 4 nodes chain with power control

Table 4-14 shows the confidence intervals for maximum throughput at the destination node; it shows that the node_1 maximum throughput mean is about 1.147 Mbps when the traffic is 1.5 Mbps, with relatively small confidence intervals, and for doing the experiment 10 times with different seed values.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
1145658,04	4594,783395	0,004010606	1142810	1148506	1141652	1149664

Table 4 - 14: Throughput results in the destination node (node1) for traffic of 1.5 Mbps in 4-nodes chain network

Table (4-15) shows the total throughput, it is measured as the sum of throughputs in all nodes in the best case (1.5 Mbps traffic).

Number of experiments	total throughput (bps)	Standard deviation (stdev)	Stdev/average	Conf. interval (95%)
10	3437111,174	14003,93381	0,004074333	[3428431,3445791]

Table 4 - 15: The maximum total throughput in 4-nodes chain

From tables (4-14 and 4-15) we can see that the throughput is lower than expected, and the reason as mentioned before is that the RTS and CTS packets, in addition to the waiting time which will decrease the throughput when the network is over loaded. And since the number of nodes is few, there will be no spatial reuse for the bandwidth, because there is a chance for only one transmission at a time to take place.

Per node throughput in the 4-nodes chain network

In this part, we will see the throughput in each node in the chain, table (4-16) shows the values of the source node load and the relaying nodes throughputs till the destination. We can see there is decrease in the throughput along the chain as shown in figure (4-13), this decrease is normal since in the high load network, there is always a chance for collisions and drops and maximum throughput for a node is what it receives from the previous node. The difference between the source load and the destination throughput is not high (less than 0.04 %), since it is a short chain, for longer chains the difference will be higher as we will see later in the next experiment (experiment4).

Note:
(nodei_thr = nodei throughput)

Node	(bps)
node0_load	1142947
node2_thr	1142913
node3_thr	1142722
node1_thr	1142532

Table 4 - 16: nodes throughputs and node_0 load in the 4-nodes chain with a traffic 1.5 Mbps

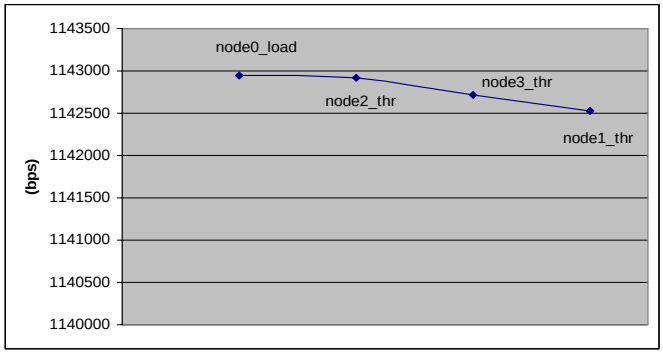


Figure 4 - 13: per node throughput in 4-nodes chain network

- **4.3.2 Chain of 7 nodes (Experiment 4)**

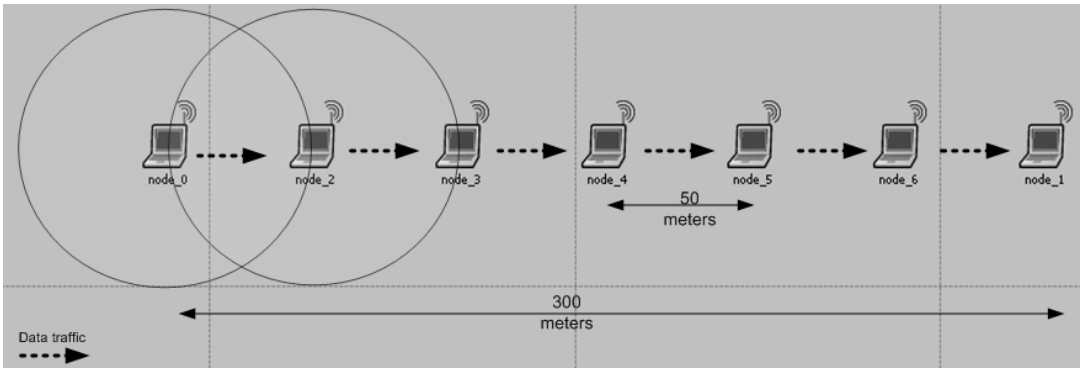


Figure 4 - 14: seven nodes chain with power control

In the this experiment we will use the same total distance between the source node (node_0) and destination (node_1) , which is 300 meters, but the spacing between nodes in the chain will be 50 meters, which means there is 6 hops and 7 nodes, and the power in only sufficient to deliver packets to the direct neighbors within the 50 meters.

In this case a transmission in the first nodes will not interfere with the transmissions after the middle of the chain, because neither the RTS nor the CTS signal will affect the far transmissions, so we may have 1 or 2 transmissions at a time. So a spatial reuse will increase the destination node's throughput as shown in the results of table (4-18) and figure (4-14).

Traffic (Mbps)	Load (bps)	Throughput (bps)
0	0	0
0,4	412793,7	412825,8
0,6	616105,5	615884,7
0,8	811826,1	805156,9
1	1011124	855492,9
1,2	1167622	805656,3

Table 4 - 17: load in the source node and throughput in the destination node for 7-nodes chain

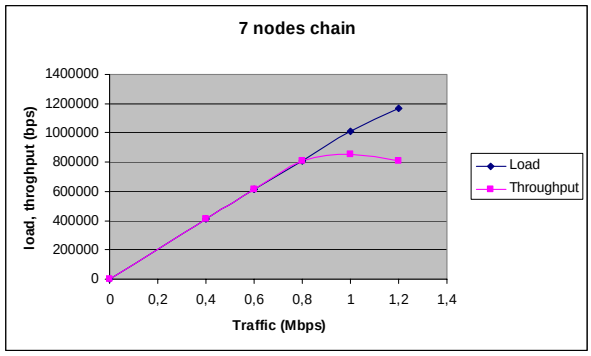


Figure 4 - 15: load, throughput in 7-nodes chain with power control

As we can figure out from the results, the maximum throughput at the destination node (node1) is about 855 kbps, and if there is no spatial reuse it is expected to be 600 kbps at most (3.6 Mbps divided by 6 hops). But since more transmissions can take place, an increase in the throughput is identified.

It depends on the active node whether other nodes can transmit or not, for the nodes in the middle (node_3 and node_4), if they are exchanging packet, no other transmission can take place because the RTS CTS signal will block them. But when a transmission at the is taking place near the source at the left , an other transmission near the destination at the right can take place as well, so we may have 1 r

2 active transmissions, so that's why the throughput is higher than the one to one transmission, but not doubled.

At high traffic, the throughput at the destination is less than the load at the source. As we will see later, there will be a drop in the throughput for farther nodes from the source, this happens clearly when there are more than one active transmission, and the chance of collision and drop exists when there are large data packets being transferred.

Table (4-18) shows the throughput, it is measured throughput at the destination node (node_1) in the best case where the traffic is 1 Mbps.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
855492,9436	5874,0954	0,006866328	851852,1	859133,7	850371,7	860614,2

Table 4 - 18: Throughput results in the destination node (node_1) for traffic of 1 Mbps in 7-nodes chain network

Table (4-19) shows the total throughput, it is measured as the sum of throughputs is all nodes in the best case where the traffic is 1 Mbps; the total throughput is much higher than the one to one case and the 4-nodes chain network, because of the spatial reuse of the bandwidth, it also shows that the confidence interval is very small.

Number of experiments	Total throughput (bps)	Standard deviation (stdev)	Stdev/average	Confidence interval (95%)
10	5291803,108	25907,11407	0,004895706	[5275746,5307860]

Table 4 - 19: The maximum total throughput in 7-nodes chain

Throughput per node in the chain:

In this measurement we compute the throughput for the individual nodes through the chain; from the source passing by the relaying nodes up to the destination node (node1).

Node	Throughput (bps)
node2	999084
node3	872685,5
node4	855894,2
node5	855527,7
node6	854962,8
node1	854856,7

Table 4 - 20: per node throughput for 1 Mbps traffic

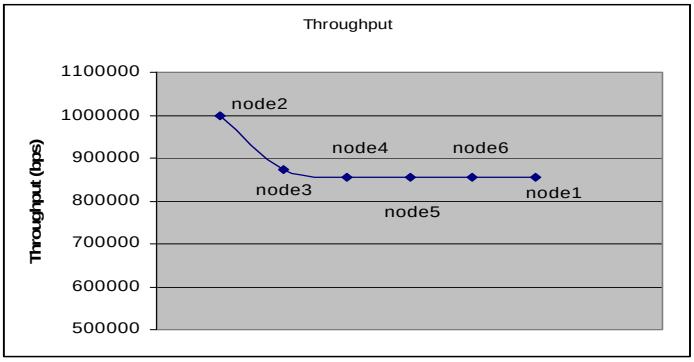


Figure 4 - 16: per node throughput in 7-nodes chain network

as shown in table 4-20, and figure 4-16, when there 1 Mbps traffic at the source node, we can see the throughput is decreasing as the packets go farther from the source, but it is getting stable after passing the first nodes in the chain, at the first receiver (node_2) the throughput is high. In the first transmission, there is less possibility if transmissions to interfere (node2 throughput), but going

farther, the effect of other transmissions possibility is higher. Then the throughputs reach acceptable values with no drop, so there is slightly drop after passing few nodes because the traffic in the network can be handled.

4.3.3 Six senders to six receivers through Chains – network grid (Experiment 5)

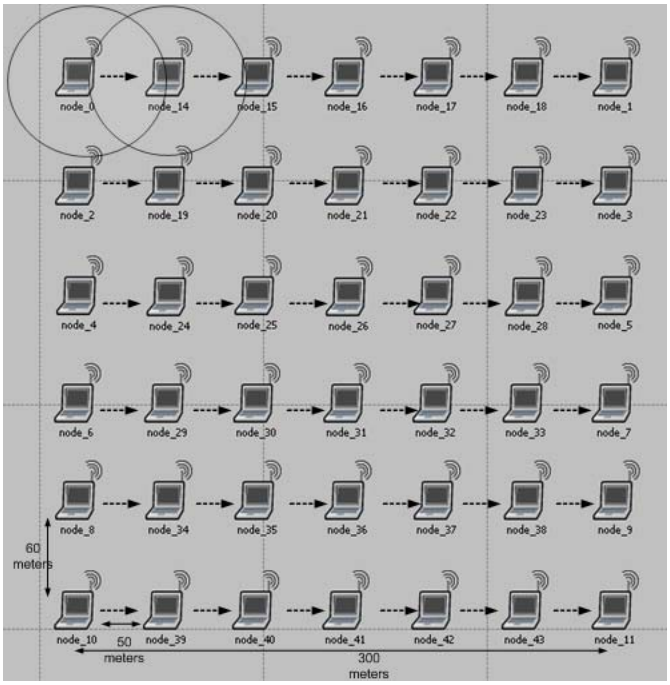


Figure 4 - 17: multiple senders to multiple receivers through chain using power control.

In this scenario, we have a squared region 300 by 300 meters; six horizontal chains with six hop each. The vertical spacing between nodes is 60 meter and the horizontal spacing is 50 meters, the total number of nodes is 42 as shown in figure (4-17). The traffic is generated at the left side and destined to nodes at the right side nodes. So we have six senders at the left are sending packets to other six nodes at the right through chains of nodes and power control, the power level used is only enough to transmit packets one hop for a distance of 50 meters.

All nodes in the network grid are active; by sending, receiving or relaying packets. The measured load is the sum of loads in all senders at left and the throughput is the sum of throughputs in the receivers at the right side. Table 4-21 and figure 4-18 shows that the maximum throughput at destinations is around 5.13 Mbps, which is 6 times the throughput in one chain shown in experiment (4), which resulted from the spatial reuse of the bandwidth through power control between chains.

Traffic (Mbps)	Load (Mbps)	Throughput (Mbps)
0	0	0
2,4	2,423775	2,423989
3,6	3,689857	3,688024
4,8	4,859307	4,819905
6	6,049526	5,128671
7,2	6,997323	4,834464

Table 4 - 21: values of the load in the sources, and the throughput in the destination nodes in a network grid.

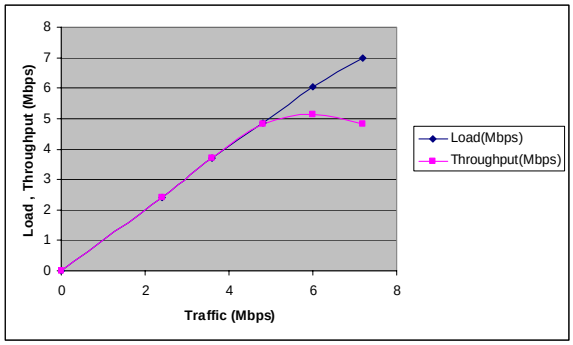


Figure 4 - 18: load in the sources, and throughput in the destinations in a network a grid of 42 nodes.

Table 4-22 shows the results and statistic results for throughput summation in the receiver nodes when the traffic summation in the source nodes is 6 Mbps, when doing the experiment 10 times.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
5128671,352	13515,734	0,002635329	5120294,2	5137048,5	5116888	5140455

Table 4 - 22: Throughput summation results in the destination nodes for traffic of 6 Mbps in a 42-nodes grid network

Measuring the total throughputs in all the 42 nodes, it shows a very high utilization of the network total throughput, the total throughput in all nodes is about 31.7 Mbps as appears in table 4-23, which is almost 8 times the six senders to six receivers (*experiment 2*) in the same spacing of 300 meters without power control.

Number of experiments	Total Throughput (average)	Standard deviation (stdev)	Stdev/average	Confidence interval (95%)
10	31706657,5	56449,21595	0,001780358	[31671670,31741645]

Table 4 - 23: Total throughput in all the 42 nodes for traffic of 6 Mbps.

Here we notice the reuse of the bandwidth in both directions: vertically between chains, and horizontally between nodes when the transmissions in different chains don't interfere with each other.

4.4 RTS CTS Power effect

This section discusses the different power levels of RTS and CTS signals (frames), which are used before exchanging data. The same networks checked before will be used to check the power effect.

4.4.1 RTS CTS power effect in a chain (Experiment 6)

Here, we are using the same network used in experiment 4 (section 4.3.2). A chain of seven nodes, distances between nodes are 50 meters each. The total distance between the source node at the left side to the destination node at the right side is 300 meters. Data power used is only sufficient to deliver packets to the direct neighbor in the chain.

The RTS and CTS power levels are changing; we will use multiples of the threshold data power level. For each level, we will check the total throughput for all the nodes in the chain. Figure 4-19 shows the nodes in the network and the reachable distances for each power level of RTS and CTS signals. The symbol R appears in figure 4-19 refers to the ratio of the power, where R=1 means the used power for RTS and CTS signals is the same as the data power, and R=16 means the ratio is 16 times the data power, and so on. Here data power is the threshold power for the 50 meters distance.

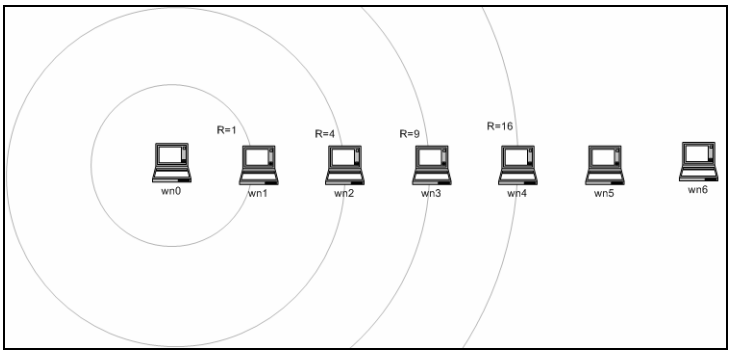


Figure 4 - 19: RTS and CTS power levels in a chain

RTS, CTS Power = R x data power.

Where: R is the multiplier of the data power.

Figure (4-19) shows the reachable distance for the RTS and CTS signals for the power levels of 1, 4, 9 and 16 times the data power. So at R=16, when the second node (wn1) send data to the third node (wn2), then the RTS signal will reach up to wn5 and the RTS will reach up to wn6, this will block all other transmissions since the network allocation vector (NAV) allocated to both RTS and CTS will make other transmissions to be postponed until the transmission's end.

Comparing to experiment 4, where the used power is the same for all packets, and the threshold power is used; this caused the total throughput to increase, since the spatial reuse of the bandwidth can take place and more than one transmission to happen at once. In this experiment, spatial reuse depends on the power level that affects the reachable distances. For high values of power, transmissions will block each other, and only one transmission, for the lower levels, there will be spatial reuse and the total throughput varies for each level.

The results shown in table 4-24 and figure 4-20 shows the total throughput in all nodes in the chain, the used traffic at the source node is 0.6 Mbps for all the different power levels, results show a decrease in the total throughput for the higher levels. This happens because the spacing between nodes is the same, and the data direction is the same for all nodes, so using lower power levels has better performance and throughput.

R	Total Throughput (bps)
1	5295944
4	4011093
9	3765417
16	3624160

Table 4 - 24: total throughput in the 7-nodes chain network for different RTS, and CTS power levels.

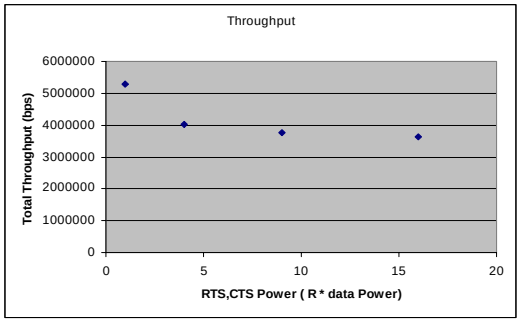


Figure 4 - 20:Effect of RTS CTS power in a chain

Table 4-25 shows the results and statistic results for total throughput in all the nodes when the traffic in the source nodes is 0.6 Mbps and the power of RTS and CTS is 9 times the threshold power.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
3765417,181	18159,2653	0,004822644	3754162	3776672	3749585	3781249

Table 4 - 25: total throughput in all the nodes when the traffic in the source nodes is 0.6 Mbps and R= 9.

4.4.2: RTS CTS power effect is a grid (Experiment 7)

In the network grid of 42 nodes shown in figure (4-21), the spacing of nodes causes more interference when using higher power for RTS CTS packets; the higher power level will make the interference reaches other chains in addition to the nodes in the same chain.

So the total throughput which is the throughput in all the nodes in the network will decrease significantly, since the network allocation vectors (NAV) of the RTS and the CTS will forbid the nodes that can hear these signals from transmitting packets during the NAV periods.

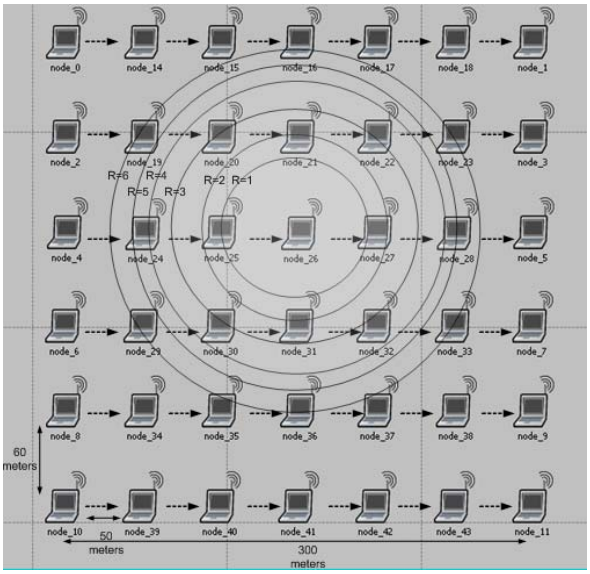


Figure 4 - 21: RTS CTS power effect in a grid of 42 nodes

Table 4-26 and figure 4-22 shows the total throughput in all the nodes for different ratios of RTS and CTS power, where total traffic in the source nodes at the left is 4.8 Mbps (6 senders x 0.8 Mbps

each). There is a high drop from R=1 to R=2, this drop is the difference between the full spatial reuse in the 6 chains, and the interference caused by the increasing the power and make it hearable by other chains at R=2.

For higher values of R, more nodes and more chains can hear each other, and the decrease will continue until only 2 parallel transmissions can take place at a time for the higher values of R listed in table 4-26.

R	Total Throughput (bps)
1	28942283
2	14986923
3	12508536
4	10614640
5	9133313
6	7224518

Table 4 - 26: Effect of RTS and CTS power levels in a 42 nodes network grid

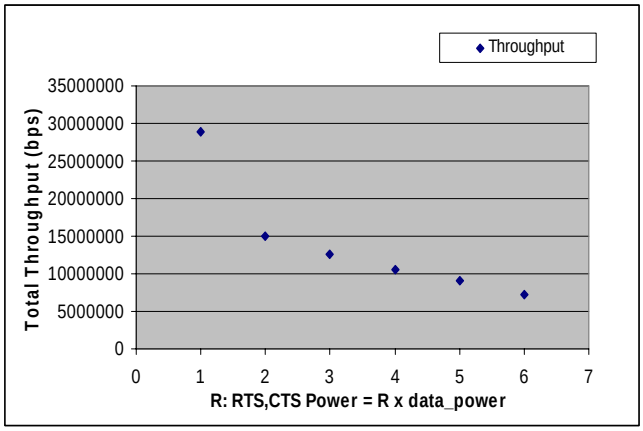


Figure 4 - 22: Effect of RTS CTS power in a grid

Table 4-27 shows the results and statistic results for total throughput in all nodes of the grid, when the total traffic in the source nodes at the left is 4.8 Mbps (6 senders x 0.8 Mbps each) and the RTS and CTS power ratio is R=2. Doing the experiment 10 times produced around 14.987 Mbps with relatively small deviation and confidence intervals.

Average throughput (bps)	Standard deviation	stdev/average	Conf. interval 95%		Conf. interval 99%	
14986923,45	64089,5504	0,004276365	14947200	15026647	14931048	15042799

Table 4 - 27 total throughput in all the 42-nodes nodes when the traffic in the source nodes is 4.8 Mbps and R=2.

We can see that for networks where nodes are distributed over equal distances, and for a traffic distributed equally, the higher power levels caused a decrease in the throughput. This decrease came from blocking of transmissions to each other, when using high power for control signals. In the next experiments, the networks are different in spacing and traffic distribution over nodes.

4.4.3 RTS CTS power effect in different spacing and different power levels networks (Experiment 8)

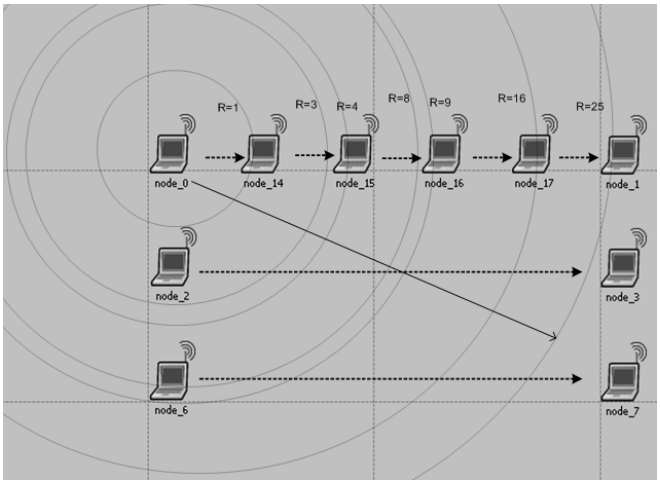


Figure 4 - 23: Chain of nodes near 2 senders and 2 receivers with high power transmissions

The network shown in figure 4-23, has 3 source nodes; the vertical distances between senders is 60 meters each, the horizontal distance between sources and final destinations are 250 meters. Nodes in the chain uses the threshold power for data transfer, it uses a power which is only sufficient for one hop (50 meters). The other senders (node_2 and node_6) use power to reach their final destinations directly, so we have a chain with low power levels and 2 high power senders.

For the traffic, when it is distributed equally over senders with high load for each, the two higher-power senders block totally the chain data transfer, because they almost destroy all packets when high loads are applied. So, the configuration is changed to have the highest percentage of the traffic in the high power senders, and leave the rest of the bandwidth to the chain, and check the effect of using different power levels on the chain.

The traffic for the source nodes are 0.6 Mbps for node_0, 1.2 Mbps for node_2, and 1.2 Mbps for node_6. In this experiment we will change RTS and CTS power in the chain only, and see the effect on the throughput for the whole network and for the individual nodes, especially for node_1. For nodes 2, 3, 6, and 7, the power for the control signals (RTS and CTS) and data is the same, and enough for each pair to communicate directly.

Table 4-28 displays the naming of nodes and measurements which we will use to show the results; beside each number the measurement name and its unit.

Node number	Value of
1	Node_0 traffic (bps)
2	Node_14 throughput (bps)
3	Node_15 throughput (bps)
4	Node_16 throughput (bps)
5	Node_17 throughput (bps)
6	Node_1 throughput (bps)

Table 4 - 28: Nodes' numbers and IDs for experiment 8.

Table 4-29 displays the results for the different nodes' measurements in the chain, for each level of RTS and CTS power, where RTS and CTS power = R x data power.

Node_0 traffic is the same for all cases (0,6 Mbps), here are the mean values of throughputs for each power ratio and node, where the unit of measurements is bit per second.

Node number	Node name	R=1	R=3	R=4	R=8	R=9	R=16	R=25
1	Node_0	600000	600000	600000	600000	600000	600000	600000
2	Node_14	320587,4	505475,1	523319	560725,8	541914,3	404617,3	382107,5
3	Node_15	245002,6	201001,6	183978,1	310512,6	325417,1	255645,8	275015,3
4	Node_16	191106,1	147708	116750,9	84190,42	85056,2	218222,2	216850,9
5	Node_17	188326,7	146748,4	109971,1	70166,46	55195,57	182451,5	200648,3
6	Node_1	185313,3	143741,4	108728,7	68534,65	52373,85	58766,22	169778,8

Table 4 - 29: Chain nodes' throughputs for different power levels of RTS and CTS, values in bps

For R=1, the drop in the throughput from source to the nearest node is very high, because the RTS from the first node is not heard by the senders below which are transmitting at high power and high traffic, which causes interference and collisions at the receiver as shown in figure 4-24.

For R=3, the RTS can be heard from node_2 which is sending below the chain, this will decrease the collision at the first receiver in the chain (node_14) as shown in figure 4-24. But for the next receiver in the chain (node_15), it has very high drop (from 0.5 to 0.2 Mbps), this caused by the limited RTS power in the node_15 from reaching the senders below.

The throughput at the end in node_1, for both R=1 and 3 is very low because both have drop either at the first or at the second receivers. Even for higher traffic at the second node, the drop is higher as we notice for R=3, which is lower at the end than R=1 because the network is heavily loaded and higher traffic over a certain limit will decrease the throughput dramatically. The other thing is that the effort applied at the first receiver is wasted at the second receiver.

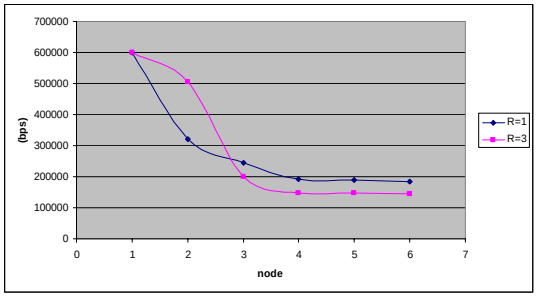


Figure 4 - 24: Throughputs in the chain nodes for cases R=1 and 3

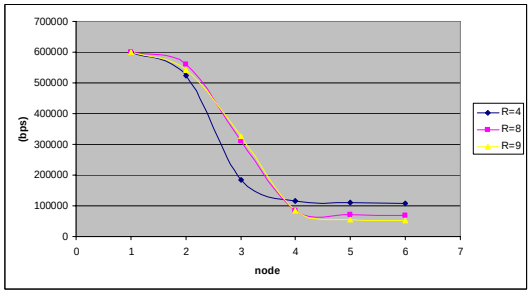


Figure 4 - 25: Throughputs in the chain nodes for cases R=4, 8 and 9

For R= 4,8 and 9 (figure 4-25) there is a decrease in the throughput at the end because less nodes can communicate parallel "less spatial reuse", because the RTS and the CTS signals will force other nodes in the chain to postpone transmission. R = 4 case is similar to R=3 case in the behavior and less in throughput because of the less reuse. The major drop in throughput is at node_15 (number 3) because it is interfering with two senders below.

When R=8, the RTS power from the first two nodes in the chain can reach to the second sender below, which means that both senders (node_2 and node_6) are aware of the transmission taking place in chain, but not for the whole chain. So once the transmission passes the first two nodes, fewer throughputs again happen.

In the case R=9, no spatial reuse any more; so only one transmission can take place in the chain at a time. About the RTS and CTS power effect, it is the same behavior as R=8 except less throughput in most of the nodes caused by no spatial reuse.

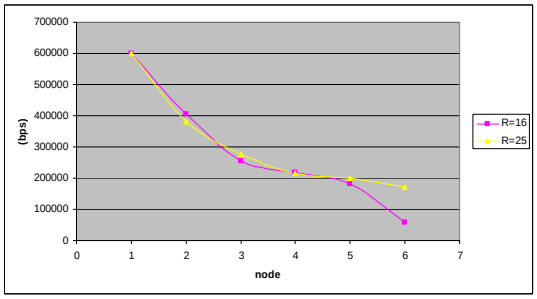


Figure 4 – 26: Throughputs in the chain nodes for cases R=16 and 25

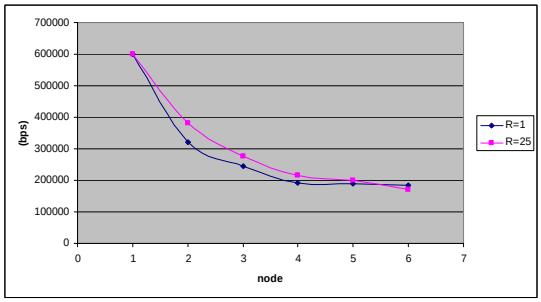


Figure 4 - 27: Throughputs in the chain nodes for cases R=1 and 25

In the R=16 case, shown in figure 4-26, the senders below are aware of transmissions in the first four nodes of the chain, but the last two nodes power is insufficient to reach the two senders below, so the transmissions between the last two nodes will suffer from interference and collisions.

Now for R=25 (figure 4-26),all senders are able to hear the RTS and CTS signals of each other, as we can see the difference between R=16 and R=25 is at the last hop. At R=25 the transmission at the end has higher throughput at the destination node and, so the throughput is only related to the ability of the nodes in the network to handle the high traffic loaded to the network.

Comparing the extreme cases R=1 and R=25 (figure 4-27), we can see they are around each other, this happened because when R=1 there were an advantage of the spatial reuse and in the R=25 case, there were the less collision caused by the other senders, but in general it depends on the network topology to decide which is better and which is worst.

About the total throughput, it is the throughput in all nodes in the network including the chain and the other 4 nodes which are transmitting and receiving at high power. Total throughputs for all cases with different RTS and CTS power are listed in table 4-30.

Power Ratio	R=1	R=3	R=4	R=8	R=9	R=16	R=25
Total throughput (bps)	3571808	3589229	3473577	3545307	3474693	3549001	3675475

Table 4 - 30: Total throughput in all the nodes for the network shown in figure 4-23 with different RTS and CTS power levels.

As figure 4-28 shows, the total throughput is not linear, but changing according to the power level and reachable distances of the RTS and CTS signal in the chain.

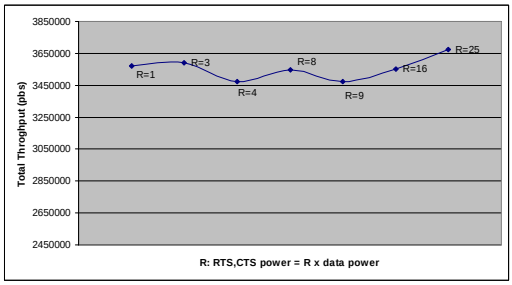


Figure 4 - 28: Total throughput in all the nodes, (experiment 8)

We can see that at R=3, it has higher total throughput than R=1, but this caused by the higher throughput at the first transmissions in the chain, but this increase is wasted later in the next hop, so the effective throughput at the destination nodes is almost the same, and the same case applies for the difference between R=4 and R=8.

Comparing the cases R=1, where the total throughput is 3571808 bps, with R=4, where the total throughput is 3473577 bps, we notice higher total throughput at R=1 because of the spatial reuse of the bandwidth.

For ratios ($R \geq 9$), no spatial reuse any more, but the difference is in the ability of the RTS and CTS packets to reach other sender nodes. For R=9 and R=16, the loss at the last node in the chain is high which is the destination node that makes less effective throughput at destinations.

Finally comparing R=1 and R=25, we see higher throughput in the case of R=25, but this difference is due to the higher throughput in first few nodes in the chain, but for the destination node, the throughput is almost the same.

We note from these results that the power levels has different effect on the performance and behavior, it depends on the spacing, load distribution, as well as power levels. The next experiment will discuss two different network configurations, with different RTS and CTS power levels effect.

4.4.4 RTS CTS power effect with different nodes locations (Experiment 9)

Changing the location of the nodes will produce different measurements, since the RTS reach ability depends on the distance and the power. In this experiment, we have two scenarios; the first is shown in figure 4-29, the places of the senders and the receivers are changed around the chain compared to the previous experiment (experiment 9.a), and the other has different distances between the chain and the high-power senders and receivers (experiment 9.a).

4.4.4.1 Experiment 9.a

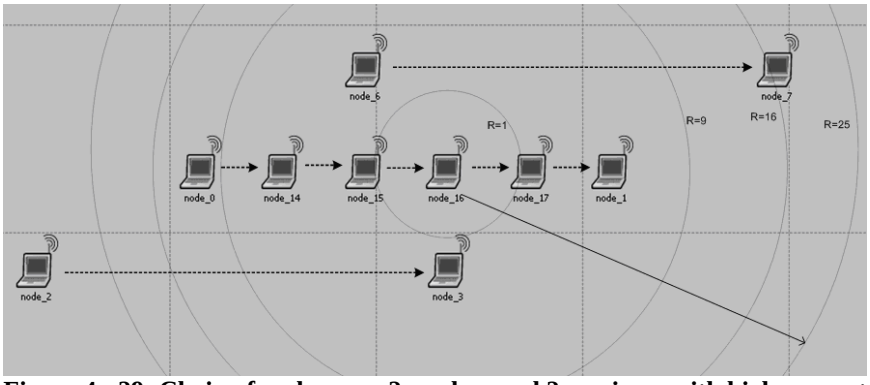


Figure 4 - 29: Chain of nodes near 2 senders and 2 receivers with high power transmissions, experiment 9.a

We still have two high power senders and two high power receivers, and a chain of low power nodes, the location is the only thing changed, the first pair of high power sender and receiver is above the chain and shifted right, and the other pair is below the chain and shifted left, the vertical distance between the pairs and the chain is 60 meters, and the horizontal distances between nodes in the chain are 50 meters, and between the sender and the receiver in the high power pairs are 250 meters as the previous experiment.

The traffic for the source nodes are 0.6 Mbps for node_0 in the chain, 1.2 Mbps for node_2, and 1.2 Mbps for node_6. In this experiment we will change the RTS and CTS power in the chain only, and see the effect on the throughput for the whole network and for the individual nodes, especially for node_1.

The experiment is done for 4 different levels and will be compared with next scenario. For this scenario, table 4-31 shows the throughputs of the nodes in the chain for different power of RTS and CTS signals, the results can not be predicted easily because there is more than one source of interference, and they are located in different places as the traffic moves from one node to another in the chain. The results show better throughput for the higher power cases of the RTS and CTS signals, but still the difference is not big.

Node ID		R=1	R=9	R=16	R=25
1	Node_0 traffic (bps)	600000	600000	600000	600000
2	Node_14 throughput (bps)	212130,4	232643,7	394879,3	312474,5
3	Node_15 throughput (bps)	163624	130298,8	237202,4	246672,7
4	Node_16 throughput (bps)	152496,9	118683,6	156408,9	214525,6
5	Node_17 throughput (bps)	147599,3	97374,29	131394	180170,9
6	Node_1 throughput (bps)	142088,6	58557,97	109437,9	162790,1

Table 4 - 31: Chain nodes' throughputs for different power levels of RTS and CTS, values in bps, experiment 9.a

Figure 4-30 shows that the throughput when R=1 is better that R=9 case, because at R=1 the spatial reuse in the chain is still possible, while for ratios ($R \geq 9$), no more spatial reuse, also when R=9, there is noticeable decrease in the throughput at the end nodes, this is caused by collisions near the end nodes from the high power nodes that can not hear the chain nodes.

At R=16, the throughputs is better than R=9, since less interference s, but still less than R=1 which has the spatial reuse advantage. At R=25, the throughput is the best since all nodes can hear each other's transmissions, even better than R=1, because effect of the reuse is less than the drop effect caused by interference and collisions.

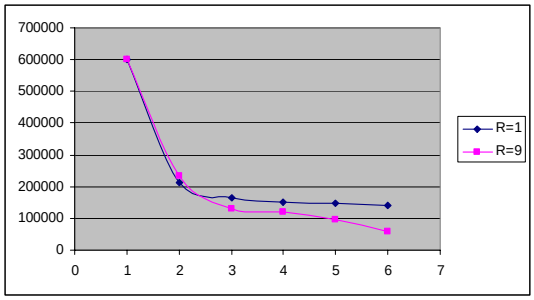


Figure 4 - 30: Throughputs in the chain nodes for cases R=1 and 9. (experiment 9.a)

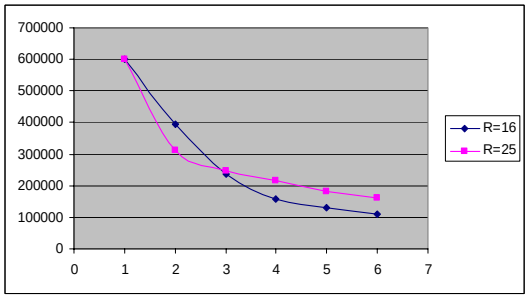


Figure 4 - 31: Throughputs in the chain nodes for cases R=16 and 25. (experiment 9.a)

In this topology, we can see clearly that the spatial reuse has less effect on the throughput, and higher power has better performance on both the throughput in the destination node as shown in table 4-31, and on the total throughput in all the nodes in the network including the high power receivers as shown in table 4-32.

	R=1	R=9	R=16	R=25
Total Throughput	3252928	3071743	3464031	3539505

Table 4 - 32: Total throughput in all the nodes for the network shown in figure 4-29 with different RTS and CTS power levels

Figure 4-32 shows higher total throughput for R=16 over R=1, and less throughput in the destination node in the chain, the effort applied at the first nodes in the chain is wasted in other nodes later.

The highest throughput in the destination node and in all nodes is at R=25, where there is full awareness of all nodes about transmissions, and the least is at R=9 where neither spatial reuse nor full awareness of all transmissions.

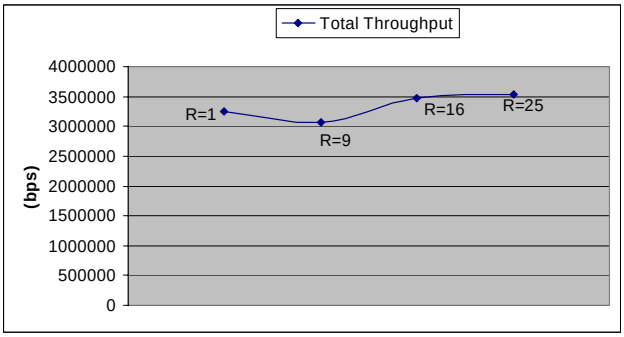


Figure 4 - 32: Total throughput in all the nodes, (experiment 9.a)

4.4.4.2 Experiment 9.b

Now, changing the location of the nodes shown in figure 4-33, where the high power senders and receivers are farther but still can interfere with chain nodes, and the distances are even not equal, 100 metes and 150 meters from the chain and in different locations.

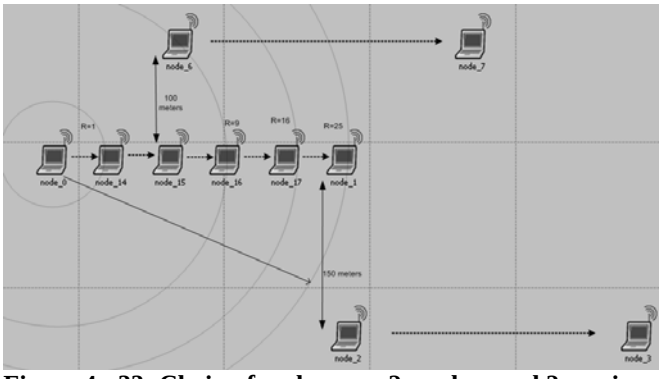


Figure 4 - 33: Chain of nodes near 2 senders and 2 receivers with high power transmissions, (experiment 9.b)

All other configurations regarding traffic and chain nodes settings are the same as experiment 9.a, so only geographical locations are changed.

Table 4-33 shows the throughputs of the nodes in the chain for different power of RTS and CTS signals, the results here also can not be predicted easily because there is more than one source of interference, and they are located in different places as the traffic moves from one node to another in the chain. The results show better throughput for the higher power cases of the RTS and CTS signals.

The results shows higher throughput for the higher RTS and CTS signals in most of the cases, for both the destination node throughput and for the individual nodes in the chain. This happened because the nodes are farther than before in previous experiment (9.a), and the awareness of transmitting nodes to be known needs more power.

Node ID		R=1	R=9	R=16	R=25
1	Node_0 traffic (bps)	600000	600000	600000	600000
2	Node_14 throughput (bps)	195421,4	264171,6	325126,6	358206,7
3	Node_15 throughput (bps)	160555,2	220687,2	252876,6	326278,2
4	Node_16 throughput (bps)	145405,7	207292,9	233036,1	289924,9
5	Node_17 throughput (bps)	140125,9	190704	225126,4	272965,4
6	Node_1 throughput (bps)	137173,4	123971,3	214337,4	266710,8

Table 4 - 33: Chain nodes' throughputs for different power levels of RTS and CTS, values in bps, experiment 9.b

Figure 4-34 shows better throughput for R=9 for all the nodes except the destination node, this happens, as explained before, as the higher power can reach most of other senders and receivers but still not all. And R=1 has the advantage of spatial reuse. Then the higher power the better for cases R=16 and R=25; even both are better than R=1 case in all nodes, figure 4-35 shows a noticeable increase in the throughput in all nodes for higher RTS and CTS power values.

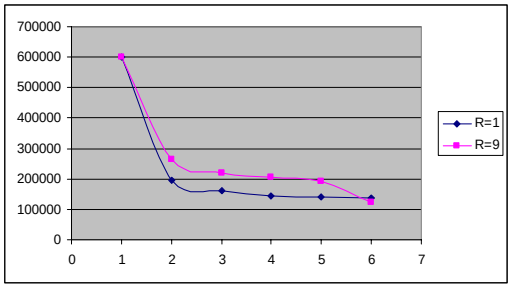


Figure 4 - 34: Throughputs in the chain nodes for cases R=1 and 9. (experiment 9.b)

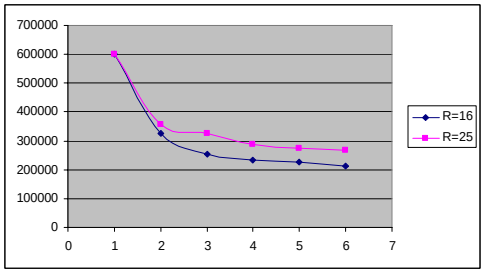


Figure 4 - 35: Throughputs in the chain nodes for cases R=16 and 25. (experiment 9.b)

In this topology, we can see clearly that higher power has better performance on both the throughput in the destination node as shown in table 4-33, and on the total throughput in all the nodes in the network including the high power receivers as shown in table 4-34.

	R=1	R=9	R=16	R=25
Total Throughput (bps)	3212239	3316982	3542799	3734649

Table 4 - 34: total throughput in all the nodes for the network shown in figure 4-33 with different RTS and CTS power levels.

Figure 4-36 shows a continuous increase in the throughputs, the highest throughput in the destination node and in all nodes is at R=25, where there is full awareness of all nodes about transmissions. For R=9 there is an increase in the total throughput, but it has low throughput at the destination node, because in that case neither spatial reuse nor full awareness of all transmissions happen.

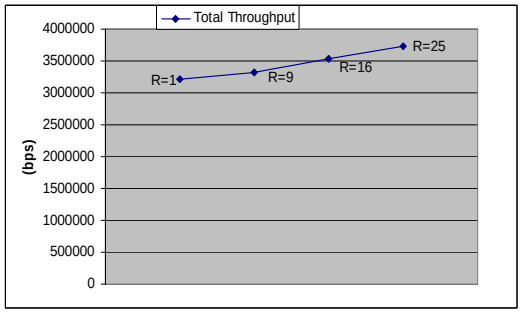


Figure 4 - 36: Total throughput in all the nodes, (experiment 9.b)

Moving high power nodes nearer or farther from the chain will affect the needed power to make these nodes aware of the active transmissions, for example if we moved node_2 in figure 4-33 closer to the chain, then it will need less power to inform it about the transmissions in the chain.

4.5 Path Loss and Interference Effect

4.5.1 Interference range measurement (Experiment 10)

In the experiments done before, the assumption was that the interference range was limited by the transmission range. However, for the normal cases there is a region where the receiver will not be able to detect the signal, but the signal may disturb other signals, which is the interference region.

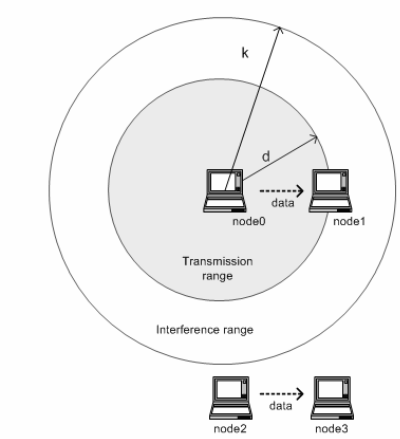


Figure 4 - 37: Transmission and interference regions in wireless LANs. [3]

In the free space, the path loss formula with the squared distance is used, the interference region is wide. In other environments where there are walls, obstacles, and other types of networks, the distance to the power 3 or 4 is used in calculating the path loss.

In this experiment we will measure the interference distance (k) for the three cases as shown in figure 4-37.

Case 1: Path loss (PL) $= \frac{16\Pi^2 d^2}{L^2}$ ……. (Path loss with distance to the power 2)

Case 2: Path loss (PL) $= \frac{16\Pi^2 d^3}{L^2}$ ……. (Path loss with distance to the power 3)

Case 3: Path loss (PL) $= \frac{16\Pi^2 d^4}{L^2}$ ……. (Path loss with distance to the power 4)

Where

L: the wave length (Lambda) in meters.

d: the distance between the transmitter and the receiver nodes.

Now for transmission power (tx_power) setting; in case 1 the power will be multiplied with ratio of distances squared as shown in equation 4.11 which is explained earlier in this section (4.1.4). But for case 2, the ration should be to the power 3, and the transmission power for a distance (d) should be

multiplied by (d) because the path loss here increased. The same applies for case 3, where we need to make the distances ratio to the power 4, and the transmission power to be multiplied by d^2.

$$\text{tx\_power (distance d}_{ref}) = \frac{d_{ref}^{\ 2}}{d^2} \text{ x tx\_power } (d) \ldots\ldots\ldots\ldots\ldots\ldots (\text{Eq4.11})$$

Note that for cases 3 and 4, the power of transmission should be increased to be able for the receiver to detect the signal. Because the path loss increased by factor d and d^2 , then the power of transmission will be multiplied by these values.

Here, we will measure the effect of the interference model which represents the environment on the throughput of parallel transmissions. Using the different models, we will see the impact on total throughput for a network.

Experiment (10) Configuration:

We have 4 nodes, 2 senders and 2 receivers as shown in figure 4-37, the distance between each sender and its peer receiver is d, where d is 50 meters. The traffic for each sender is 2.5 Mbps, so when there is no interference, the total throughput should be around 5 Mbps. For each case we will try different distances, distances between the senders, and find the approximate distance (k) where the interference starts to disappear.

Consider

tx_power1: the threshold transmission power in case1, tx_power1 (300) = 0.001watt

tx_power2: the threshold transmission power in case2

tx_power3: the threshold transmission power in case3

Then

tx_power2 (300) = 0.001watt x 300

tx_power3 (300) = 0.001watt x 300 x 300

Case1:

Power threshold: -90 dBm (1.09849E-12 watt)

Power of transmission:

$$\text{tx\_power1 (50)} = \frac{50^2}{300^2} \text{ x tx\_power1 (300)} = \text{2,77778E-02 x 0.001 = 2,77778E-05 watt}$$

Distance: k (meters)	Total throughput (Mbps)
100	2.94
120	3.05
140	3.39
150	4.50
160	5.11

Table 4 - 35: Throughput at different distances, case1.

Table 4-35 shows that the interference region disappeared at around 160 meters. It shows that the interference distance is more than 3 times the transmission distance, so the interference propagates far in the free space environment.

Case2:

Power threshold: -90 dBm (1.09849E-12 watt)

Power of transmission:

$$\text{tx\_power2 (50)} = \frac{50^3}{300^3} \text{ x tx\_power2 (300)}$$

$$= \frac{50^3}{300^3} \text{ x tx\_power1 (300) x 300}$$

$$= \text{1,388889E-03 watt}$$

Distance: k (meters)	Total throughput (Mbps)
80	3.07
90	3.38
100	4.68
105	5.03
110	5.10

Table 4 - 36: Throughput at different distances, case2.

Table 4-35 shows that the interference region disappeared at around 110 meters.

Case3:

Power threshold: -90 dBm (1.09849E-12 watt)

Power of transmission:

$$\text{tx\_power3 (50)} = \frac{50^4}{300^4} \text{ x tx\_power3 (300)}$$

$$= \frac{50^4}{300^4} \text{ x tx\_power1 (300) x 300 x 300}$$

$$= \text{6,944444E-02 watt}$$

Distance: k (meters)	Total throughput (Mbps)
70	3.40
75	4.10
80	4.60
85	5.11
90	5.12

Table 4 - 37: Throughput at different distances, case 3.

Table 4-35 shows that the interference region disappeared at around 85 meters.

By comparing the total throughputs in the three tables above, we notice that the total throughput start increasing at a specific distance, and finally it reaches the maximum value when there is no interference any more.

The increase in the total throughput is caused by the reduced noise region, for the models of interference where the path loss is higher; the interference region is limited by closer distances. And

for less path loss, the noise and collisions region is wider which produces reduced throughputs, and that explains the different values of the total throughput according to the distance.

Now comparing the maximum total throughput in each case, we see that the interference stopped in shorter distance when the path loss is higher, so the signal will not propagate for farther distance and cause interference to other transmissions.

In the free space the first case applies, but since there are always obstacles and walls near wireless networks. In the previous experiments the assumption was that the interference range is the same as the transmission range, but in real systems the interference range is farther and it depends on the surrounding environment.

4.5.2 Interference and path loss effect in a chain (Experiment 11)

This experiment is to measure the total throughput in the 7-nodes chain for 4 cases; the three cases explained in experiment 10 and the last case when the interference range stops at the transmissions range. We will measure the total throughput in all the nodes for the all cases when having different traffic values at the source node, and compare the maximum throughputs.

Figure 4-38 shows the chain network, where the spacing is 50 meters between nodes in the chain, and the threshold power is used which is only sufficient to transmit frames for one hop. The traffic generated in the source at the left side will pass through all nodes to reach the destination at the right side.

Figure 4 - 38: Different interference and path loss effect on a chain of nodes

Configuration:

Power threshold: -90 dBm (1.09849E-12 watt)

About the needed power, it is the same distance (50 meters) which used in experiment 10, so the needed power for the different cases are the same.

Distance = 50 meters.

We will measure the total throughput in the chain for the different cases of path loss and interference models, and change the transmission power as needed in each case. Also, we will check the case where the interference stops at the transmission distance.

The four cases with their path loss and needed power are:

1. PL_P2: the path loss is computed with the squared distance

$$\text{Path loss (PL)} = \frac{16\Pi^2 d^2}{L^2} \ldots\ldots\ldots \text{(Path loss with distance to the power 2)}$$

tx_power1 (50) = 2,77778E-05 watt

2. PL_P3:

$$\text{Path loss (PL)} = \frac{16\Pi^2 d^3}{L^2} \ldots\ldots\ldots \text{(Path loss with distance to the power 3)}$$

tx_power2 (50) = 1,388889E-03 watt

3. PL_P4:

$$\text{Path loss (PL)} = \frac{16\Pi^2 d^4}{L^2} \ldots\ldots\ldots \text{(Path loss with distance to the power 4)}$$

tx_power3 (50) = 6,944444E-02 watt

4. PL_Cut: similar to PL_P2, but the interference model is disabled and the transmission distance is considered as the interference distance.

tx_power4 (50) = 2,77778E-05 watt

We will measure the total throughput in all nodes in the chain for different traffic values at the source node (node_0), table 4-38 and figure 4-39 shows the results for PL_P2 and PL_P3, it shows higher total throughput for the PL_P3 since the less interference range the possibility of spatial reuse in this case is higher, but for the PL_P2, the interference range propagates farther as explained in experiment 10 results, so we see noticeable higher throughput.

node 0 Load (Mbps)	PL_P2 total throughput (bps)	PL_P3 total throughput (bps)
0	0	0
0,5	2923076	3062545
0,6	3282902	3635466
0,7	3370888	4141079
0,8	3368406	4264598
0,9	3358382	4224002

Table 4 - 38: Total throughput values for PL_P2 and PL_P3 cases

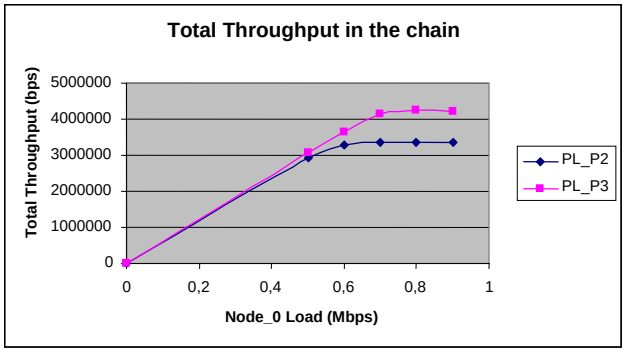


Figure 4 - 39: Total throughputs for PL_P2 and PL_P3 cases

Table 4-39 and figure 4-40 shows more increase in the total throughput for PL_P4 case and PL_cut where the interference stops at the transmission distance; this happens since less propagation in case of PL_P4 of interference and no propagation in the PL_cut case after the transmission range, so the spatial reuse rate is higher and there is less noise and fewer collisions.

node 0 Load (Mbps)	PL_P4 total throughput (bps)	PL_cut total throughput (bps)
0	0	0
0,5	3038380	3110027
0,8	4870371	4850630
0,9	5154990	5269746
1	5181139	5283726

Table 4 - 39: Total throughput values for PL_P2 and PL_P3 cases

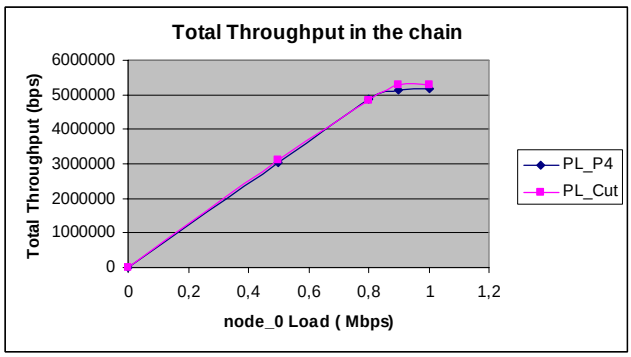


Figure 4 - 40: Total throughputs for PL_P4 and PL_cut cases

We notice that the results of PL_P4 and PL_cut are close to each other in the case of the chain with 50 meters distances, this happened since the interference range for PL_P4 is around 85 meters and 50 meters for PL_cut, and since the next node comes after that is 100 meters away, then the noise possibility is very low and the total throughput is almost the same , but for different networks where the nodes are more closer to each other, the result will be much higher for the PL_cut case over the PL_P4 case, the small difference between these two cases caused by the noise in PL_P4 case, but this noise is very low at 100 meters distance, but it does not exist for the other case where there is no noise after the transmission distance.

Table 4-40 and figure 4-41 show the results for the four cases together, and we can see clearly the better performance for higher path loss or no interference over the less path loss cases.

node 0 Load (Mbps)	PL_P2 (bps)	PL_P3 (bps)	PL_P4 (bps)	PL_cut (bps)
0	0	0	0	0
0,5	2923076	3062545	3038380	3110027
0,6	3282902	3635466		
0,7	3370888	4141079		
0,8	3368406	4264598	4870371	4850630
0,9	3358382	4224002	5154990	5269746
1			5181139	5283726

Table 4 - 40 : total throughput values for PL_P2, PL_P3, PL_P4 and PL_cut cases

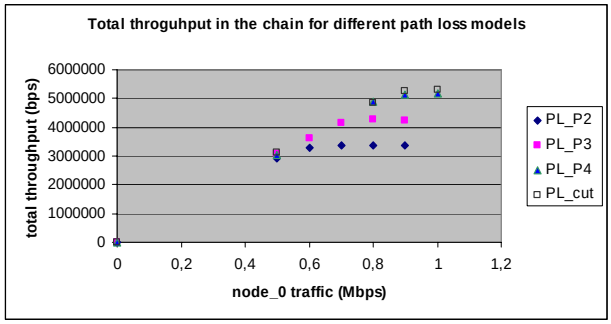


Figure 4 - 41: total throughputs for PL_P2, PL_P3, PL_P4 and PL_cut cases

4.6 Conclusions on the Experiments' Results

During the analysis of the experiments, we discussed the results. To summarize, we will introduce some general conclusions about the results, these are the main conclusions:

- For different types of traffic; constant traffic has higher throughput than exponential traffic in the high traffic cases, exponential traffic causes the network throughput to decrease after a maximum acceptable traffic size, this happens because the buffer size limit can not manage with large packets. But for a constant traffic, the throughput stays at the maximum values if the traffic size increases, because the packets have the same size, and packets have equal probability of dropping. In one sender to one receiver network, in constant size packets the results shows higher loads and throughputs is up to 4.08 Mbps, comparing to exponential size packets case which is 3.72 Mbps.
- When using RTS and CTS signal, the multiple senders to multiple receivers' case has higher throughput than having one sender to one receiver case within the same area. One sender should wait more between packets, while the waiting time is less when having multiple senders, because the least waiting time is used. The maximum throughput in a six senders to six receivers is about 4.02 Mbps, comparing to one-to-one transmission, it was about 3.6 Mbps with exponential packets size traffic for both cases and within the same region.
- In chain networks, when using RTS and CTS signals and power control, the short chain has less spatial reuse than longer chains. Whenever transmissions are farther from each other, the possibility of parallel transmissions and higher total throughput in the network can happen. In 7-nodes chain, the gain was almost 140% over the 4- nodes chain case, since it is possible for two transmissions to take place, but that is not possible for 4-nodes chain when using RTS and CTS signals.
- When using power control in network grids, if symmetric spacing is used between nodes and chains, then we will have spatial reuse in different directions, through the chains themselves, and between different chains. In a 42-nodes network grid, 6 chains with 7 nodes each, the gain in throughput was almost 850% compared with the one sender to one receiver case and within the same area. However, the real throughput is measured at the final destinations only, and it is 6 times the throughput in one chain.
- In the networks where the distances between nodes are symmetric, using higher power for RTS and CTS decreases the total throughput, because the higher power RTS and CTS signal will force more nodes to postpone their transmissions. While in the asymmetric distances between nodes and different power levels, using higher RTS and CTS has better performance some times, but that depends mainly on the network topology. In such a network also, when using low power RTS and CTS signals, higher power senders and receivers could block the low power ones, especially when the load is high, this happens because high power pairs can not hear the low lower pairs' transmissions and may destroy their packets without affecting the high power packets.
- Free space environments have less path loss, but their interference regions are wider and propagate to farther distances, and cause noise and collisions to the neighbor transmissions. Normal environments have higher loss, and need more power, but the interference region is limited, which causes less noise to other transmissions, so it produces higher total throughput in networks, but higher power consumption.

Chapter 5

Conclusions and Future Work

5.1 Concluding Remarks

In this work, the proposed design and implementation were used to enhance the performance of the multi hop wireless networks; we proposed some solutions in the different layers of the WLAN model and implemented the power control part for some cases in the OPNET simulator.

Our design mainly focused on three main changes: initialization process to discover the network topology and configuration, a routing algorithm to find fast and effective paths to exchange packets between nodes in the network using a mix of metrics, and a power control mechanism to reduce the collisions and noise, and to reuse the bandwidth.

The initialization processes suppose to take time, this time is needed for the nodes until the information about each node in the network is know by all other nodes. The number of nodes and the network architecture affect the time required in the network to have the network information available in all nodes in the network. This process will add extra processing in building metrics and routing tables, but it will help in increasing the efficiency of the network.

The routing algorithm is a distance vector protocol with a mix of metrics and different weights, these weights should be carefully selected, because we have different types of values and different scales of the routing metrics (power, interference level, hop count). We are not able to decide the best weights for the routing metrics at the moment, but it should consider the network topology and traffic parameters.

The needed power parameter is used in two layers, the MAC and the network layers. This will add extra control over power from different layers, and that’s why the power selection is a sensitive issue, and it will affect the performance of routing and data exchange in the network.

From experiments’ results, the power control mechanism increased the throughput to high values, especially where the nodes are distributed with equal distances like in chains or grids of nodes (e.g.

850% is the throughput gain in the 42-nodes network grid), and the traffic are distributed in away that the traffic in different senders will not block each other.

Using different levels of power for different types of frames can help in some cases, for example when it is used in non homogeneous networks with different distances between senders and receivers, in that case we can use high power RTS and CTS signals to alert far nodes about the active transmissions.

5.2 Open issues and Future Work

Parts of this work are not all implemented, so these is still a lot of things not specified in the design and implementation phases, the open issues are mainly in the details of the initialization and the routing processes.

The open issues in these two parts are:

- In the initialization process, the needed power from one node to another is have to be calculated, in our simulations, we assumed that the required power is known since we know the distance, and the distances are the same. Also we need to specify the central node or access point and what should happen if this node or AP fails later. And what is the better duration for the time slot and when to start a new discovery from the beginning (beaconing).
- In the routing process, we need to select the best weights for the different network architectures and distribution of nodes. And since it is a table driven protocol, the routes update need expiry duration and refresh rate to keep the routing tables correct.
- The power control algorithm should take into account different parameters for different types of networks and configurations, so there is still a need for more work to develop such an algorithm to cover more situations and suggest the best power control mechanism.

Taking the open issues in the consideration, there is still a lot of work to do, and complete this research. Suggested future works are:

- Implementation of the initialization process with its specifications in more detailed description.
- Implementation of the routing process with its specifications in more detailed description especially the careful selection of the weights for different situations.
- The implementation of power control in chains and grid networks was checked for equal distances between nodes, so more experiments on different distances in chains and grids could be implemented for additional performance measurements.
- In the implementation part of this work we have only stationary nodes, but since some nodes are mobile, mobility modeling should be considered and implemented, because this feature is required in the daily life.
- Add hoc and multi hop routing need extra security consideration, since wireless connection are open links. So for a confidential data exchange, the security is an important issue to be done in future works.

Appendix A1: distance vector algorithm [14]

```
1 Initialization:
2   for all adjacent nodes v:
3      D^x  (*,v) = infinity        /* the * operator means "for all rows" */
4      D^x  (v,v) = c(X,v)
5   for all destinations, y
6      send min_w  D  (y,w) to each neighbor  /* w over all X's neighbors */
7
8  loop
9    wait (until I see a link cost change to neighbor V
10         or until I receive update from neighbor V)
11
12   if (c(X,V) changes by d)
13     /* change cost to all dest's via neighbor v by d */
14     /* note: d could be positive or negative */
15     for all destinations y:  D^x (y,V) =  D^x (y,V) + d
16
17   else if (update received from V wrt destination Y)
18     /* shortest path from V to some Y has changed */
19     /* V has sent a new value for its  min_w D^V(Y,w) */
20     /* call this received new value is "newval"      */
21     for the single destination y: D^x (Y,V) = c(X,V) + newval
22
23   if we have a new min_w  D^x (Y,w)for any destination Y
24      send new value of min_w  D^x (Y,w) to all neighbors
25
26  forever
```

Appendix A2
Experiments Tables

Experiment 1.a: One sender to one receiver, exponential packet size

Traffic (bps)	**Load(bps)**									
	1	2	3	4	5	6	7	8	9	10
1000000	1020443	1037357	1039254	1016543	982657,3	1000392	1004256	996933,8	1019556	1013698
2000000	2053477	2068705	2014623	2033169	2026633	2059128	2009129	2020711	1987385	1983949
3000000	3100182	3058572	3092220	3134729	3083236	3074350	3036521	3068732	3051366	3003124
4000000	3724037	3744178	3730271	3722178	3705086	3711177	3702949	3704202	3701328	3723759
5000000	3482937	3469099	3475443	3466896	3445034	3491351	3490113	3468465	3481698	3495146
6000000	3244071	3240259	3244062	3248664	3240316	3225753	3234672	3226298	3216625	3241793
7000000	3026329	3005641	3015569	3029015	3004383	3038892	3007757	3024524	3016150	3007024

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	Average load	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1000000	1013108,931	17663,75713	0,0174352	1003920	1022298	995099,3	1031119	966734,1	1059484
2000000	2025690,838	28729,4666	0,014182552	2010746	2040636	2007884	2043498	2000643	2050738
3000000	3070303,156	36301,7903	0,01182352	3051419	3089187	3047803	3092803	3038654	3101952
4000000	3716916,52	14218,17213	0,00382526	3709520	3724313	3708104	3725729	3704521	3729312
5000000	3476618,067	14998,75483	0,00431418	3468816	3484420	3467322	3485914	3463542	3489695
6000000	3236251,249	10200,79527	0,003152041	3230945	3241558	3229929	3242574	3227358	3245145
7000000	3017528,257	11739,84476	0,00389055	3011421	3023635	3010252	3024805	3007293	3027764

Traffic (bps)	**Throughput(bps)**									
	1	2	3	4	5	6	7	8	9	10
1000000	1019863	1037357	1038732	1016118	982776,1	1000392	1004047	996933,8	1019556	1013698
2000000	2053477	2068486	2014082	2033169	2025758	2059010	2008999	2020846	1986169	1983745
3000000	3098351	3063126	3090618	3129528	3082458	3076449	3033145	3068631	3047378	2998931
4000000	3726398	3743709	3734545	3721828	3705928	3708477	3703136	3698119	3703002	3721078
5000000	3483080	3469629	3475220	3465859	3444845	3490323	3467977	3481833	3495214	3489909
6000000	3244133	3240118	3244077	3247497	3239979	3225497	3235293	3226376	3216134	3241661
7000000	3022763	3005027	3016230	3028066	3001945	3038898	3006763	3026562	3018068	3006696

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	Average throughput	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1000000	1012947,3	17532,15124	0,017308059	2016254	2034494	2014508	2036241	2010089	2040659
2000000	2025374,048	28919,30497	0,014278501	2010330	2040418	2007450	2043298	2000161	2050587
3000000	3068861,586	36402,49939	0,01186189	3049925	3087798	3046299	3091424	3037124	3100599
4000000	3716621,945	15231,26356	0,004098147	3708699	3724545	3707182	3726062	3703343	3729901
5000000	3476388,674	15016,45408	0,004319556	3468577	3484200	3467081	3485696	3463297	3489481
6000000	3236076,648	10145,8347	0,003135227	3471111	3481666	3470100	3482677	3467543	3485234
7000000	3017101,843	12060,91327	0,003997516	3010828	3023376	3009626	3024577	3006587	3027617

Experiment 1.b
One sender to one receiver, constant packet size

Traffic (bps)	Load(bps)									
	1	2	3	4	5	6	7	8	9	10
1000000	1040319	1016000	1022485	1008434	1008254	1010596	1019062	1005732	1022305	1016721
2000000	2013986	2057580	2019750	1989306	2027677	2021732	2023894	2051095	2041728	2031820
3000000	3030526	3044757	3077003	3061691	3047820	3054125	3060610	3001523	3082948	3067095
4000000	4010858	3990862	3985999	3997528	3998789	3952492	3990682	3990502	4013740	3954113
5000000	4080933	4085257	4084176	4082555	4078231	4082735	4081474	4081113	4081113	4081113
6000000	4078411	4079132	4076790	4083095	4077330	4078952	4079672	4080393	4078411	4078772
7000000	4080753	4078772	4075529	4078051	4080213	4077330	4081834	4082194	4078411	4079492

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1000000	1016990,78	10139,01501	0,010885085	1007886	1019365	1006787	1020464	1004006	1023245
2000000	2027856,738	19519,52311	0,009625691	2017703	2038011	2015758	2039955	2010839	2044875
3000000	3052809,787	23701,1191	0,007763706	3040481	3065139	3038120	3067500	3032146	3073473
4000000	3988556,596	20612,54458	0,005167921	3977834	3999279	3975781	4001332	3970586	4006527
5000000	4081870,071	1943,52931	0,000476137	4080859	4082881	4080665	4083075	4080176	4083565
6000000	4079095,887	1748,190772	0,000428573	4078186	4080005	4078012	4080179	4077572	4080620
7000000	4079258,014	2068,016513	0,000506959	4078182	4080334	4077976	4080540	4077455	4081061

Traffic (bps)	Throughput(bps)									
	1	2	3	4	5	6	7	8	9	10
1000000	1038455	1018945	1022258	1003300	1006245	1006981	1011767	1000723	1013055	1014528
2000000	2013626	2057400	2019930	1989306	2027316	2021732	2023894	2051095	2041728	2031820
3000000	3029265	3044577	3077363	3061871	3046379	3054125	3058989	3002064	3081867	3066915
4000000	4007373	3987891	3988073	3995174	3999544	3949837	3991715	3990986	4012836	3955845
5000000	4081113	4084896	4083275	4082735	4077150	4082014	4080933	4081294	4081113	4081113
6000000	4078952	4079132	4076790	4083275	4077330	4078591	4079492	4080393	4078231	4078772
7000000	4080573	4078772	4075529	4078231	4080213	4077330	4082014	4082194	4078411	4079492

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1000000	1013625,652	11033,4016	0,010885085	2022045	2033524	2020946	2034623	2018165	2037404
2000000	2027784,681	19510,32181	0,009621496	2017636	2037934	2015692	2039877	2010775	2044795
3000000	3052341,418	23580,99628	0,007725543	3040075	3064608	3037726	3066957	3031783	3072900
4000000	3987927,455	20248,31824	0,005077404	3977394	3998461	3975377	4000477	3970274	4005581
5000000	4081563,83	2004,626123	0,000491142	4080521	4082607	4080321	4082806	4079816	4083312
6000000	4079095,887	1790,980001	0,000439063	4080632	4082495	4080454	4082674	4080002	4083125
7000000	4079276,028	2069,323757	0,000507277	4078200	4080352	4077993	4080559	4077472	4081080

Experiment 2.a
Six senders to six receivers, exponential packet size

Traffic (bps)	Load(bps)									
	1,0	2,0	3,0	4,0	5,0	6,0	7,0	8,0	9,0	10,0
0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
1,5	1514312,7	1538592,6	1532687,7	1510455,8	1528527,8	1507079,2	1531572,9	1516041,4	1525831,3	1551116,4
3,0	3068018,2	3071335,1	3056978,9	3062718,8	3066870,7	3049649,2	3047241,2	3056492,0	3077383,7	3055197,9
4,5	4015164,1	4019028,8	4025338,6	4021530,6	4006610,0	4024610,6	4014598,7	4012509,8	4019928,6	4006312,4
6,0	3719443,3	3727545,7	3726851,8	3719080,9	3725552,6	3722757,9	3735139,6	3725991,0	3721708,5	3725612,5
7,5	3475636,9	3473622,0	3471385,9	3476196,2	3479582,9	3465701,9	3470493,9	3473944,1	3481472,8	3468809,9

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
1,5	1525621,8	13766,1	0.009023272	1518460,7	1532782,9	1517089,4	1534154,1	1513619,9	1537623,6
3,0	3061188,6	9717,5	0,003174406	3056133,6	3066243,6	3055165,7	3067211,5	3052716,5	3069660,6
4,5	4016563,2	6751,5	0,001680905	4013051,1	4020075,3	4012378,6	4020747,8	4010677,0	4022449,4
6,0	3724968,4	4668,4	0,001253278	3722539,9	3727396,9	3722074,9	3727861,9	3720898,3	3729038,5
7,5	3473684,7	4814,2	0,001385904	3471180,3	3476189,0	3470700,8	3476668,5	3469487,5	3477881,9

Traffic (Mbps)	Throughput(bps)									
	1,0	2,0	3,0	4,0	5,0	6,0	7,0	8,0	9,0	10,0
0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
1,5	1514312,7	1538564,6	1532687,7	1510383,6	1528527,8	1507079,2	1531572,9	1516041,4	1525815,3	1551116,4
3	3068117	3071357	3056743	3062667	3066900	3049642	3047240	3056554	3076950	3055399
4,5	4012329	4017827	4023812	4022829	4006710	4024393	4014010	4014256	4020998	4006841
6	3719477,7	3727386,5	3726894,1	3719400,2	3725623,2	3722876,3	3734762,3	3725733,3	3722077,9	3725851,5
7,5	3472385,7	3474606,8	3469448,3	3475847,2	3478794,9	3466562,2	3470812,9	3473490,3	3480018,7	3468006,1

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
1,5	1525610,2	13772,04	0,009027238	3053993	3068321	3052621	3069693	3049150	3073164
3	3061156,7	9645,28	0,003150862	3056139	3066174	3055179	3067135	3052748	3069566
4,5	4016400,6	6628,96	0,001650475	4012952	4019849	4012292	4020509	4010621	4022180
6	3725008,3	4486,24	0,001204359	3722675	3727342	3722228	3727789	3721097	3728920
7,5	3472997,3	4446,36	0,001280267	3470684	3475310	3470241	3475753	3469121	3476874

Experiment 2.b
Six senders to six receivers, constant packet size

Traffic (Mbps)	Load(bps)									
	1	2	3	4	5	6	7	8	9	10
1,5	1499501	1540213	1509949	1497519	1525982	1543275	1505626	1505806	1539132	1537330
3	3075742	3057908	3071599	3037912	3044037	3059889	3042956	3037372	3070157	3014133
4,5	4316739	4323945	4319801	4329889	4330430	4325926	4322323	4330610	4323044	4317640
6	4320162	4324125	4335294	4319261	4324485	4329349	4327728	4313677	4325746	4333672
7,5	4324485	4321423	4323945	4329889	4321243	4315838	4321423	4322143	4321243	4320702

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1,5	1520433,191	18515,17	0,012177567	1510802	1530065	1501555	1539311	1471823	1569043
3	3051170,496	19319,77	0,006331923	3041120	3061221	3039196	3063145	3034327	3068014
4,5	4324034,752	5141,84	0,001189132	4321360	4326710	4320848	4327222	4319552	4328518
6	4325349,787	6603,45	0,001526687	4321915	4328785	4321257	4329443	4319593	4331107
7,5	4322233,333	3545,58	0,000820314	4320389	4324078	4320036	4324431	4319142	4325325

Traffic (Mbps)	Throughput(bps)									
	1	2	3	4	5	6	7	8	9	10
1,5	1499501	1540213	1509949	1497339	1525982	1543455	1505626	1505626	1539132	1537330
3	3075922	3056827	3071418	3036831	3043496	3059889	3042416	3037732	3070878	3013593
4,5	4318721	4322864	4326827	4327007	4328628	4319081	4315658	4329349	4320162	4314757
6	4322684	4322504	4334213	4319621	4325026	4328088	4327908	4312235	4322864	4334573
7,5	4324125	4320522	4324485	4328989	4319621	4314757	4320522	4321963	4321783	4319441

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1,5	1520415,177	18580,62	0,012220755	1510750	1530081	1508899	1531932	1504216	1536614
3	3050900,284	19584,88	0,00641938	3040712	3061088	3038761	3063039	3033825	3067975
4,5	4322305,39	5389,85	0,001246987	4319502	4325109	4318965	4325646	4317606	4327004
6	4324971,489	6687,68	0,001546296	4321493	4328450	4320826	4329117	4319141	4330802
7,5	4321620,851	3759,02	0,000869819	4319665	4323576	4319291	4323951	4318344	4324898

Experiment 3
Chain of 4 nodes with power control
(Load in the source node and throughput in the destination node)

Traffic (Mbps)	**Load(bps)**									
	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
0,5	507620,5	494926	513553,9	511362,2	509373,5	507099,3	529464,8	490082,5	514278,2	501643,1
1	1005294	976220,7	1020995	1004608	1024389	1010352	1004520	1004583	1015634	1004089
1,5	1147660	1138209	1151370	1152385	1149223	1143350	1148724	1139236	1146846	1142935
2	1054118	1046164	1033214	1049031	1042111	1047761	1046056	1045028	1043972	1047005

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
0,5	507940,4044	10941,70999	0,021541326	502248,6	513632,2	501158,7	514722,1	498401	517479,8
1	1007068,519	13167,47972	0,013075058	1000219	1013918	998907,2	1015230	995588,6	1018548
1,5	1145993,688	4873,355867	0,004252515	1143459	1148529	1142973	1149014	1141745	1150242
2	1045445,855	5373,066451	0,005139498	1042651	1048241	1042116	1048776	1040761	1050130

Traffic (Mbps)	**Throughput(bps)**									
	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
0,5	507092,5	494883,8	513572,6	511362,2	509162,9	507069,7	529464,8	489501,5	514278,2	501607,6
1	1004346	976248,5	1020885	1004608	1023875	1011046	1004293	1004072	1016207	1004952
1,5	1146442	1138154	1151514	1150161	1149573	1143188	1148236	1139380	1147212	1142722
2	1054133	1046126	1033402	1048930	1042174	1047548	1046045	1044987	1042984	1046988

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
0,5	507799,578	11056,6465	0,021773643	502048	513551,2	500946,6	514652,6	498160	517439,2
1	1007053,363	13153,78636	0,013061658	1000211	1013896	998900,6	1015206	995585,4	1018521
1,5	1145658,04	4594,783395	0,004010606	1143268	1148048	1142810	1148506	1141652	1149664
2	1045331,789	5344,966734	0,005113177	1042551	1048112	1042019	1048645	1040672	1049992

Experiment 4

Chain of 7 nodes with power control, (Load in the source node and throughput in the destination node)

Traffic (bps)	Load(bps)									
	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
400000	423518,6	412392,4	412191,4	425191,4	416226,9	424465,6	403272,4	411954,7	410390,6	388333,3
600000	604504,7	609602,1	616709,6	626827,5	614621,7	644238,2	624803,4	605621,2	602787,2	611339,5
800000	848260,6	792302,4	802540,6	816339,3	814297,7	817816,6	808833,8	811589,7	798017,2	808263,2
1000000	993089,8	1020487	1006575	1034058	1033555	998829,4	989732,5	1028636	1013921	992357,7
1200000	1152934	1186899	1167524	1172353	1170033	1178668	1149382	1157537	1157254	1183635

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0						
400000	412793,7231	11119,12028	0,026936263	407009,6	418577,8	405902	419685,4	403739,6	421847,9
600000	616105,5077	12786,76559	0,020754182	609453,9	622757,1	608180,2	624030,8	605693,4	626517,6
800000	811826,1231	15164,37136	0,018679334	803937,7	819714,5	802427,2	821225,1	799478	824174,3
1000000	1011124,092	17442,34198	0,017250446	1002051	1020197	1000313	1021935	996921	1025327
1200000	1167621,867	13063,50662	0,011188131	1160826	1174417	1159525	1175719	1156984	1178259

Traffic (bps)	Throughput(bps)									
	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
400000	423751,9	412392,4	412191,4	425089,9	416809,2	424026,5	403095,9	412035,6	410777,3	388088,3
600000	605020,5	608773,5	616209,6	626759,5	614264,3	643835,3	624238,4	605383,7	602636,4	611725,8
800000	828843,1	790702,2	795936,7	811158,6	807857,8	812011,6	805186,5	804062,6	790585,1	805224,5
1000000	862227,5	853257,1	850394,1	849139	860184,8	862343,4	853385	851659,6	848929,8	863409,1
1200000	809464,3	803482,4	800383,9	803802,3	803828,1	804231,3	800221,9	806604,6	814890,8	809653,7

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
400000	412825,8462	11171,07861	0,027060027	407014,7	418637	405901,9	419749,7	403729,4	421922,3
600000	615884,7077	12665,32668	0,020564444	609296,3	622473,1	608034,7	623734,8	605571,5	626197,9
800000	805156,8615	11347,18675	0,014093138	799254,1	811059,6	798123,8	812189,9	795917	814396,7
1000000	855492,9436	5874,095424	0,006866328	852437,3	858548,6	851852,1	859133,7	850709,8	860276,1
1200000	805656,3282	4564,623433	0,00566572	803281,8	808030,8	802827,1	808485,5	801939,4	809373,2

Traffic (bps)	Total throughput									
	1	2	3	4	5	6	7	8	9	10
1000000	5311204	5296403	5263159	5281526	5330723	5319696	5254100	5294544	5262701	5303976

Traffic (bps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1000000	5291803,108	25907,11407	0,004895706	5278326	5305280	5275746	5307860	5270707	5312899

Experiment 5: Six senders to six receivers through Chains – network grid
(Load in the source nodes and throughput in the destination nodes)

Traffic (Mbps)	Load (bps)									
	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
2,4	2403162	2389515	2444494	2423216	2476712	2375110	2386007	2493221	2437716	2408597
3,6	3689673	3660719	3648940	3659760	3686117	3705592	3652332	3739372	3724964	3731099
4,8	4816413	4824803	4895717	4846064	4826414	4923315	4890115	4896192	4867042	4806992
6	5999874	6041120	6054303	5952642	6006989	6068004	6109160	6109991	6139839	6013340
7,2	7023935	7008219	6947954	6996589	6876871	6949255	7095546	7024040	7032650	7018171

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
2,4	2423774,952	39260,76	0,016198189	2403352	2444198	2399440,9	2448109	2389546	2458004
3,6	3689856,781	34130,46	0,009249808	3672102	3707611	3668702,5	3711011	3660100	3719613
4,8	4859306,705	40574,66	0,008349888	4838200	4880413	4834158,3	4884455,1	4823932	4894681
6	6049526,057	58475,41	0,009666115	6019107	6079945	6013282,6	6085769,5	5998545	6100507
7,2	6997322,99	59747,64	0,008538644	6966243	7028403	6960291	7034354,9	6945233	7049413

Traffic(Mbps)	Throughput (bps)									
	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
2,4	2403920	2389755	2444774	2424116	2476048	2375168	2387338	2491360	2438252	2409155
3,6	3689676	3658135	3650601	3654574	3683591	3706005	3651214	3736757	3724879	3724807
4,8	4791388	4780338	4870594	4800898	4785838	4870833	4858644	4849922	4822457	4768135
6	5129962	5134402	5139608	5153976	5137796	5118242	5113426	5114060	5114300	5130942
7,2	4876465	4832878	4837354	4824786	4850730	4851499	4800862	4824396	4838931	4806735

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
0	0	0	0	0	0	0	0	0	0
2,4	2423988,59	38594,67	0,015921972	2403912	2444065	2400067,4	2447909,8	2390340	2457637
3,6	3688023,981	33664,47	0,009128052	3670512	3705536	3667158,5	3708889,4	3658674	3717374
4,8	4819904,857	39654,03	0,00822714	4799277	4840533	4795327,1	4844482,7	4785333	4854477
6	5128671,352	13515,73	0,002635329	5121641	5135702	5120294,2	5137048,5	5116888	5140455
7,2	4834463,535	22217,87	0,004595727	4822906	4846021	4820692,8	4848234,3	4815093	4853834

Traffic (Mbps)	Total Throughput (bps)									
	1	2	3	4	5	6	7	8	9	10
6	31615389	31749458	31779224	31782760	31643589	31666722	31671949	31708609	31719639	31729237

Traffic (Mbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
6	31706657,5	56449,21595	0,001780358	31677293	31736022	31671670	31741645	31657443	31755872

Experiment 6: RTS CTS power effect in a chain

Total throughput in all nodes with different power ratios

R	Total Throughput (bps)									
	1	2	3	4	5	6	7	8	9	10
1	5259250	5331682	5317080	5295051	5284468	5300081	5287920	5337467	5261799	5284637
4	3997476	3994443	4027619	4022835	4019952	3944117	4022899	4061489	4007216	4012888
9	3763144	3777987	3757074	3763582	3798944	3745807	3757362	3785478	3737962	3766833
16	3660111	3642288	3579412	3672746	3600467	3633867	3632951	3552047	3645878	3621828

R				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	Average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1	5295943,505	26462,27786	0,004996707	5282178	5309709	5279542	5312345	5272873	5319014
4	4011093,352	30065,24136	0,007495523	3995454	4026733	3992459	4029728	3984881	4037305
9	3765417,181	18159,26535	0,004822644	3755971	3774864	3754162	3776672	3749585	3781249
16	3624159,657	37109,94745	0,010239601	3604855	3643464	3601159	3647161	3591806	3656514

Experiment 7

RTS CTS power effect grid of 42 nodes

Total throughput in all nodes with different power ratios

Traffic (Kbps)	Total Throughput (bps)									
	1	2	3	4	5	6	7	8	9	10
1	28757601	28708717	29236395	28833419	28738205	29262257	29174890	29121826	28964051	28625469
2	15044589	14941666	14979438	14967765	14968083	15053385	14977008	14994007	14858105	15085188
3	12411950	12575329	12488726	12670328	12499403	12423541	12493700	12656989	12392999	12472393
4	10565477	10448409	10536788	10661750	11366950	10380553	10512220	10673056	10563067	10438128
5	9041105	9106720	9779519	9195650	9129239	9056887	9039555	9057357	8981746	8945351
6	7096573	7253317	7969357	7180709	7103390	7123868	7086628	7109141	7120887	7201310

Traffic (Kbps)				Conf interval 90%		Conf interval 95%		Conf interval 99%	
	Average	Stdev	stdev/average	X1	X2	X1	X2	X1	X2
1	28942282,95	239960,8796	0,008291014	28817457	29067109	28697623	29186942	28312285	29572281
2	14986923,45	64089,5504	0,004276365	14953584	15020262	14947200	15026647	14931048	15042799
3	12508535,73	96942,3015	0,007750092	12458107	12558965	12448450	12568621	12424018	12593054
4	10614639,85	280241,1655	0,026401382	10468860	10760420	10440945	10788335	10370315	10858965
5	9133312,819	237906,8438	0,026048253	9009555	9257071	8985857	9280769	8925896	9340729
6	7224517,981	267147,52	0,036977902	7085549	7363487	7058938	7390098	6991608	7457428

Experiment 8: RTS CTS power effect in different spacing and different power levels networks,

Throughput (bps) in nodes with different power ratios

	1	2	3	4	5	6	7	8	
R=1									**Averages**
node14	301704,9	307315,4	312874,8	308794,1	305384,4	362060,6	305894,6	360670,8	320587,4
node15	227863,6	249261	242643,4	249261	262282,1	218027,6	251760,2	258921,6	245002,6
node16	178309,7	196024,6	196822,4	178604,8	181816,1	193980,6	203613,5	199677,3	191106,1
node17	174619,3	192006,9	193630,3	177691,1	176099	191660,1	203154,7	197752,6	188326,7
node1	172248,7	186768,7	192500,8	174501,5	172862,3	190500,5	198695,4	194428,4	185313,3
R=3									
node14	510656	521635,2	501927,1	492294,4	479496,6	490674	541799,1	505318,4	505475,1
node15	204977,5	182661,2	172865,7	206167,1	217777	202762,8	206979	213822,3	201001,6
node16	145224,4	159133,8	142501,9	168387,7	141520,7	146195,9	132495,8	146203,6	147708
node17	142898,5	160334,8	141792	166087,9	142016	143927,4	134558,5	142372,2	146748,4
node1	142641,2	155715,7	135843,7	166251,1	139702,6	140290,7	129987,7	139498,6	143741,4
R=4									
node14	483943,1	513385,6	553971	524317,3	536481,5	530013,5	514743,6	529696,5	523319
node15	203946,3	175937	184097,5	194333,8	182270,8	191885,8	185847,6	153505,7	183978,1
node16	119233,2	119384,9	118993	98472,59	124497,3	110687,3	142205,1	100533,5	116750,9
node17	107608,9	117395	116750	102072,6	114236,1	108260,2	114562,7	98883,69	109971,1
node1	105567	115718,4	116669	101255,1	112619,8	107525,2	112034,7	98440,62	108728,7
R=8									
node14	591731,4	552520,1	571254,4	518969,4	597868,8	539635,7	542814,8	571011,9	560725,8
node15	321745,5	296367	262534,6	328356,4	349901,8	301925,9	298943	324326,6	310512,6
node16	71512,46	81774,32	104181,4	79515,73	76299,91	78998,05	79185,93	102055,6	84190,42
node17	68681,6	71492,92	80263,14	50143,51	67322,34	68095,26	77368,86	77964,06	70166,46
node1	68144,74	70069,66	79131,08	48019,69	63347,45	67579,57	76021,42	75963,57	68534,65
R9									
node14	549427,7	541198,5	544670,8	527766,6	507720,6	582962	532702,3	548866	541914,3
node15	362830,8	327021,8	322016	332982,9	303302,4	323879,9	324292,7	307010,2	325417,1
node16	91664,68	61295,32	69905,18	87578,52	97065,49	81966,97	90561	100412,4	85056,2
node17	44867,2	56245,42	58266,09	48672,74	63108,18	62872,12	55664,74	51868,06	55195,57
node1	54329,11	44842,09	53648,25	50286,03	61794,71	59866,83	50507,32	43716,43	52373,85
R16									
node14	384603,3	395351,4	417161,6	410741,9	398974,3	394589,5	415622,6	419893,4	404617,3
node15	245394,5	256105,8	277206,2	284105,1	262920,6	235119	248803	235512,6	255645,8
node16	210379,6	233592,6	193490	239097,1	220511,3	219311,3	215211,3	214184,4	218222,2
node17	177722,6	186787,4	166325,9	195931,3	191614,8	174039,4	184097	183093,7	182451,5
node1	69027,45	50962,46	58442,09	62867,45	44772,43	59240,37	63479,14	61338,34	58766,22
R25									
node14	412501,2	397197,8	344829,3	366888,1	341164,3	340385	405021	448873,6	382107,5
node15	267163,6	287061,2	274370,2	245005,5	265740,1	286870,4	279778,5	294132,7	275015,3
node16	220429,5	245742,5	194932,7	205704,9	230131,2	222389,9	210911,8	204564,7	216850,9
node17	209670,4	213921,5	191583,3	200762,1	219836,6	201379,7	183937,5	184095,5	200648,3
node1	174807,1	166765	170186,1	174493,3	185995,8	172030,3	160325,4	153627,1	169778,8

Experiment 9: RTS CTS power effect with different nodes locations

Topology 1

		Throughput (bps)			
Node ID		R=1	R=9	R=16	R=25
1	node0	600000	600000	600000	600000
2	node14	212130,4	232643,7	394879,3	312474,5
3	node15	163624	130298,8	237202,4	246672,7
4	node16	152496,9	118683,6	156408,9	214525,6
5	node17	147599,3	97374,29	131394	180170,9
6	node1	142088,6	58557,97	109437,9	162790,1

	R=1	R=9	R=16	R=25
Total Throughput(bps)	3252928	3071743	3464031	3539505

Topology 2

		Throughput (bps)			
Node ID		R=1	R=9	R=16	R=25
1	node0	600000	600000	600000	600000
2	node14	195421,4	264171,6	325126,6	358206,7
3	node15	160555,2	220687,2	252876,6	326278,2
4	node16	145405,7	207292,9	233036,1	289924,9
5	node17	140125,9	190704	225126,4	272965,4
6	node1	137173,4	123971,3	214337,4	266710,8

	R=1	R=9	R=16	R=25
Total Throughput(bps)	3212239	3316982	3542799	3734649

Experiment 10: Interference range measurement

Case 1: Path loss (PL) $= \frac{16\Pi^2 d^2}{L^2}$ ……. (Path loss with distance to the power 2)

Distance: k (meters)	Total throughput (Mbps)
100	2.94
120	3.05
140	3.39
150	4.50
160	5.11

Case 2: Path loss (PL) $= \frac{16\Pi^2 d^3}{L^2}$ ……. (Path loss with distance to the power 3)

Distance: k (meters)	Total throughput (Mbps)
80	3.07
90	3.38
100	4.68
105	5.03
110	5.10

Case 3: Path loss (PL) $= \frac{16\Pi^2 d^4}{L^2}$ ……. (Path loss with distance to the power 4)

Distance: k (meters)	Total throughput (Mbps)
70	3.40
75	4.10
80	4.60
85	5.11
90	5.12

Experiment 11: Interference and path loss effect in a chain

	R	total Throughput(bps)										
		1	2	3	4	5	6	7	8	9	10	**average**
PL_P2												
	50	2995315	2905277	2867530	2937121	2949432	3064977	2857078	2783993	2933795	2936241	2923076
	60	3261012	3257906	3343311	3284064	3308632	3267631	3261541	3294784	3235130	3315009	3282902
	70	3377650	3378210	3379922	3379056	3334292	3388017	3348704	3352652	3351940	3418441	3370888
	80	3394294	3387904	3364225	3366756	3372583	3339478	3381487	3389806	3351479	3336049	3368406
	90	3340381	3325188	3358952	3340743	3321700	3354164	3342818	3417535	3430074	3352265	3358382
PL_P3	**50**	2988094	3146279	3086073	3162708	3127004	2970511	2961181	2957963	3157769	3067863	3062545
	60	3508318	3874374	3846765	3465416	3667837	3548096	3549765	3699911	3641210	3552969	3635466
	70	4075505	4100858	4212968	4113336	4240856	4252557	4198093	4031999	4158845	4025771	4141079
	80	4273128	4258833	4329595	4220734	4275008	4192337	4246987	4289892	4345011	4214454	4264598
	90	4217548	4214084	4259392	4237791	4197489	4222832	4212685	4194611	4230168	4253425	4224003
PL_P4	**50**	3032640	3002467	3116516	3053394	3078031	2909138	2919107	3039430	3142249	3090829	3038380
	80	4828047	4877004	4818708	4795384	4915314	4885219	4923979	4797095	5140459	4722500	4870371
	90	5184646	5203978	5162967	5142850	5143509	5176219	5209617	5088398	5188615	5049100	5154990
	100	5173335	5199927	5199116	5157457	5191539	5186077	5182047	5148140	5158593	5215156	5181139
PL_cut	**50**	3163826	2942473	3038919	3106159	3145462	3197610	3043920	3256693	3045936	3159274	3110027
	80	4922964	4870774	4721571	4764475	5009887	4784445	4786487	5025819	4931820	4688061	4850630
	90	5305519	5267204	5274039	5107992	5287828	5315830	5260466	5315575	5271046	5291962	5269746
	100	5251471	5361605	5285292	5280651	5257780	5248415	5311734	5319457	5256940	5263919	5283726

Appendix A3: References

[1] Microsoft Research homepage: “Self-Organizing Neighborhood Wireless Mesh Networks” http://research.microsoft.com/mesh/#publications , Microsoft corp. 2005

[2] P. Mohana Shankar “Introduction to Wireless Systems”
John Wiley & Sons, Inc., 2002.

[3] Jochen H. Schiller, “Mobile Communications”, *Addison Wesley Inc.*, 2003.

[4] F. Liu, “Routing in Multi Hop Wireless Infrastructures”, Master Thesis, University of Twente, 2004.

[5] E. Jung, N. Vaidya, “A Power Control MAC Protocol for Ad Hoc Networks.” 2002.

[6] OPNET Technologies, Inc. http://www.opnet.com

[7] Institute of Electrical and Electronics Engineers, Inc. (IEEE). 802.11 standards page http://grouper.ieee.org/groups/802/11/

[8] WLAN projekt v. Syddansk Universitet, Denmark http://wlan.nat.sdu.dk/802_11standard.htm

[9] http://www.intelligraphics.com/articles/80211_article.html , Intelligraphics, Inc., 2005

[10] P. Misra “Routing Protocols for Ad Hoc Mobile Wireless Networks” http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/index.html , Computer Science and Engineering, Washington University in St. Louis, 1999

[11] Mobile Ad Hoc Networking & Computing, http://www.eurecom.fr/%7Enikaeinn/adhocNetworks/routing.html , Eurecom Inc., France, 2005

[12] Shailesh N. Humbad, Suitability of Distributed Mobile Wireless Networking for Urban Traffic Congestion Mitigation, http://www.somacon.com/thesis/web/chapter3.html , master thesis , Humbad's Computer Consulting , 2001

[13] S. Haykin, M. Moher,” Modern Wireless Communications”, Prentice Hall, Pearson Education, 2005.

[14] James F. Kurose, and Keith W. Ross, “Computer Networking: A Top-Down Approach Featuring the Internet”, *Addison Wesley Longman, Inc.*, 2001

[15] D. De Couto, D. Aguayo, J. Bicket, R. Morris, “A HighThroughput Path Metric for MultiHop Wireless Routing”,2003

[16] R. Draves, J. Padhye, B. Zill, “ omparison of Routing Metrics for Static Multi-HopWireless Networks”, Microsoft Research, 2004

[17] V. Kawadia , P. Kumar “Power Control and Clustering in Ad Hoc Networks”, ACM digital library,2003

[18] S. Park; R. Sivakuma, “Quantitative analysis of transmission power control in wireless ad-hoc networks”, ACM digital library, 2002

[19] Sh. Srikanth V. Krishnamurthy “Distributed Power Control in Ad-hoc Wireless Networks” , ACM digital library,2001

[20] P. Bergamo, A. Giovanardi , A. Travasoni, D. Maniezzo, G. Mazzini, M. Zorzi, “Distributed power control for energy efficient routing in ad hoc networks”, ACM digital library,2004