Multipath Routing with Load Balancing in Wireless Ad Hoc Networks

ROMAIN GROLEAU

KTH Microelectronics
and Information Technology

Master of Science Thesis
Stockholm, Sweden 2005

IMIT/LCN 2005-03

Multipath Routing with Load Balancing in Wireless Ad Hoc Networks

Master's Thesis Project
March 2005

Romain Groleau
rgroleau@mit.edu

Massachusetts Institute of Technology, MIT
Computer Science and Artificial Intelligence Laboratory
Advisor: Dina Katabi

CSAIL

Royal Institute of Technology, KTH
School of Information and Communication Technology
Advisor: Gerald Q. Maguire Jr.

Abstract

In recent years, routing research concerning wired networks has focused on minimizing the maximum utilization of the links which is equivalent to reducing the number of bottlenecks while supporting the same traffic demands. This can be achieved using multipath routing with load balancing instead of single path routing using of routing optimizers. However, in the domain of ad hoc networks multipath routing has not been investigated in depth. We would like to develop an analogy between wired and wireless networks, but before that we need to identify the major differences between these two in the case of multipath routing. First, in order to increase the network throughput, the multiple paths have to be independent so they don't share the same bottlenecks. Then, due to radio propagation properties the link capacity is not constant. So using the maximum utilization metric for wireless networks is not suitable. Based on the research done in wired networks, which has shown that using multiple paths with load balancing policies between source-destination pairs can minimize the maximum utilization of the links, we investigate if this is applicable to ad hoc networks.

This paper proposes a multipath routing algorithm with a load balancing policy. The results obtained from an indoor 802.11g network highlight two major points. The maximum throughput is not achieved with multipath routing, but with single path routing. However, the results on the delivery ratio are encouraging, indeed we observe a real improvement thanks to our multipath routing algorithm.

Sammanfattning

På senare år har routning forskningen angående trådnätverken focusen på att minska den maximala användingen av länkar vilket motsvarar än reducering av flaskhalsar medan man stöder samma trafikkrav. Det här kan åstadkommas genom att av multiväg routning med lasta balansering I stället för använder enkelvägrouting med routing optimizers. Emellertid har inom ad hoc nätverken multiväg routning har inte blivit undersökts på djupet. Vi skulle vilja utveckla en analogy emellan trådnätverk och trådlösnätverken.men främföre det behöver identifiera de store differenserna mellan dessa två vid multiväg routning. För det första måste de flerfaldiga vägarna vara oberoende för att öka nätverkens throughput så de inte delar samma flaskhalsar. Sedan är länkkapaciteten inte constant på grund av radiospridningsegenskaperna. Så den maximal användningsmetric för trådlös nätverken passar inte.

Den här arbetetet föreslår en multiväg routning algoritm med lasta balanseringen. Resultaten få från en indoor 802.11g nätverk framhåller ger två store meningen. Den maximala throughput är inte åstadkoms med multiväg routing, men med enkelväg routning. Emellertid är resultaten på den leveransförhållande uppmuntrande; vi observera en verklig förbättring tack vare vår multiväg routning algoritmen.

Acknowledgements

This master's thesis is my final work for the Master of Science in Computer Science at the Royal Institute of Technology (KTH) in Stockholm. It was performed at the Massachusetts Institute of Technology (MIT) in Cambridge, USA under the supervision of Dina Katabi. I would like to thank her for her help and assistance during the entire work. I also would like to express my appreciation to John Bicket, Sanjit Biswas, and Srikanth Kandula for valuable information and fruitful discussions. Finally, I would like to acknowledge Professor Gerald Q. Maguire for his support and for being my examinator at KTH.

I would like to express also my gratitude to the following people for their support, assistance, and cooperation during my master's thesis project.

- My labmates at MIT Sachin Katti and Shan Sinha for their help and the good environment in the office. Michel Gorazko for his availability and technical support.

- My mother Danielle, my father Frederic, and my brother William who have been very supportive throughout my education.

- My two opponents for their valuable remarks and advices: Vincent Hag and Mina Sagha Zadeh.

- All my friends in Sweden, in the USA, and in France for their good mood and their support: Abdennour, Yoann, Paola, Graham, Jason, Tony, Renaud, Thomas, Fabien, Yannick, Frederic, David, Jonathan, David, Timo, Xavier, Boris, Hilary.

- And anybody I missed who deserves to be mentioned.

Table of Contents

Table of Figures

1 Introduction

1.1 Problem

Originally a wireless rooftop network offers not just a new technology, but a new economic model that relieves the current dependence on phone or cable companies to propagate local access infrastructure. The Rooftop Network uses innovative wireless technology to allow deployment of fast, robust, community networks, which are constructed entirely by the end-users, and which are *free* of monthly operating charges [50]. The goal of our wireless rooftop network has a different philosophy. MIT Roofnet [4] is an experimental rooftop wireless network in development at MIT LCS 's Parallel and Distributed Operating Systems group (PDOS). The goal of the project is to build a production-quality self-organizing network capable of providing Internet service while researching scalable routing protocols.

Given this wireless rooftop network, we would like to maximize the aggregate throughput while supporting certain traffic demands. The approach we are considering to achieve this goal is to multipath routing in the wireless rooftop network. The objective is to provide low cost, high performance Internet access to the nodes. Therefore the majority of the traffic will be sent to gateway nodes connected to the Internet.

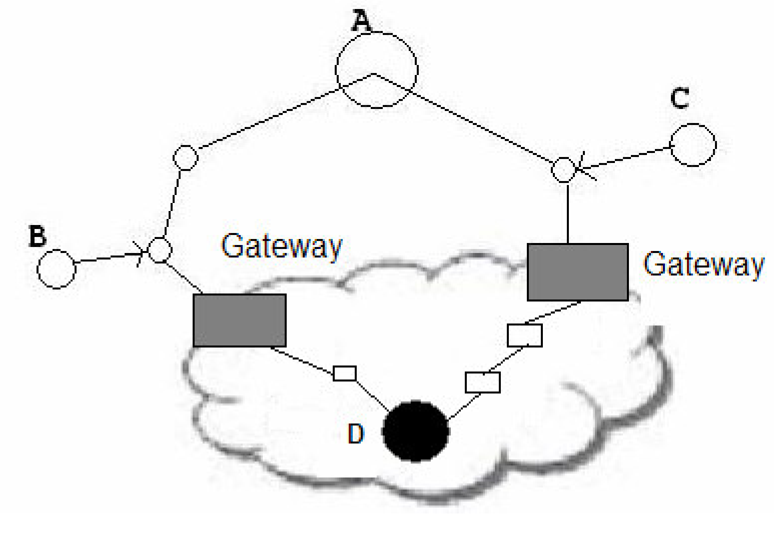


Figure 1: Wireless Rooftop Network node sending traffic

In figure 1, we consider node A which wants to send traffic to a machine D in the Internet. The radio medium around the two gateways is also used by node B and node C. Node A has two paths to the Internet. These two paths are assumed to be interference free. In this configuration, splitting the traffic simultaneously onto these two paths, node A can achieve a higher throughput than using a single path.

The factors which affect throughput are link congestion (related to the number of active users), and propagation factors such as range and multipath fading. Dividing the traffic between the best paths using a metric which takes into account all these factors will enable us to maximize throughput while minimizing packet losses.

The project is different from previous work on multipath routing [2, 3, 24, 26, 31, 32] because it focuses on the ideal environment for multipath routing: wireless rooftop networks. This environment is ideal because the number of nodes is small which implies that the number of hops is also small, the nodes are static, and the traffic is mainly going to the nodes from the Internet and vice versa. In such networks, any gateway can be used as an entry point to the Internet; therefore there are often many paths between a source and the several gateways. The paths can be interference independent if the gateways are chosen far enough from each other. This implies the only congestion will be around the gateways and not around a node in the center of the networks as in [2] and [3]. In a rooftop network the nodes are static so the topology won't change quickly. Thus the nodes won't experience packet losses due to route rediscovery. We assume that the communication between two gateways on the wired network will enjoy low latency and high throughput because the capacity of the wired links (100Mbps for two third of the gateways) is much larger than the one of the wireless links. This is an important assumption to ensure that TCP works properly. Indeed packet reordering has a bad effect on TCP congestion protocol.

As part of this project, we will develop a multipath routing protocol for a rooftop wireless network and test on the indoor testbed of the Roofnet project [4]. The routing protocol will balance the traffic onto a subset of the best available paths towards the gateways, so as to maximize the throughput and minimize packet loss. We will evaluate our routing protocol to see if it is TCP friendly.

The issue of multipath routing in wireless networks is a very recent topic. Publications by Pham and Perreau and Ganjali and Keshavarzian are good examples. Multipath routing has been well studied in wired networks, but it is not clear that it can be adapted to wireless network [3]. Furthermore the topic of multipath routing in wireless networks is multidimensional, as it includes wireless communication theory, wired-cum-wireless environments, normal routing, and transport level issues. Indeed in multipath routing, a metric is needed to find the best routes. Choosing the appropriate metric requires examining the radio propagation properties of the link: loss rate, throughput, and capacity. The background of the project is Roofnet [4] a MIT wireless ad hoc network which is made of wireless nodes, static antennas, and gateways to the Internet. When a node in the network wants to access the outside of the network, it has to go through any of the gateways. This raises the issue of how to handle TCP fragments. Indeed all the Roofnet nodes are using NAT. In the case of multipath routing, one node will send its packet through multiple gateways. This is why it is needed to have a special means to reassemble packets before sending them to the Internet. Finally the design of a routing mechanism is a key result of the project.

1.2 Experimental environment

The experimental environment for this project is an outdoor testbed and its indoor testbed [46] under development at MIT LCS's Parallel and Distributed Operating Group [37]. MIT Roofnet [4] is an experimental rooftop wireless network testbed.

1.2.1 MIT Roofnet

The goal of MIT Roofnet project is to build a production-quality self-organizing network capable of providing Internet service while researching scalable routing protocols. It consists of about 50 nodes deployed in East Cambridge, Massachusetts, near MIT's LCS as shown in figure 2. Three of the nodes at the lower right have Yagi antennas on top of ten-story MIT buildings and act as gateways to MIT's wired campus net. The other nodes are in apartment buildings. The typical radio communication range is 100 meters, but it varies a lot. The nodes are installed by volunteers affiliated with MIT.

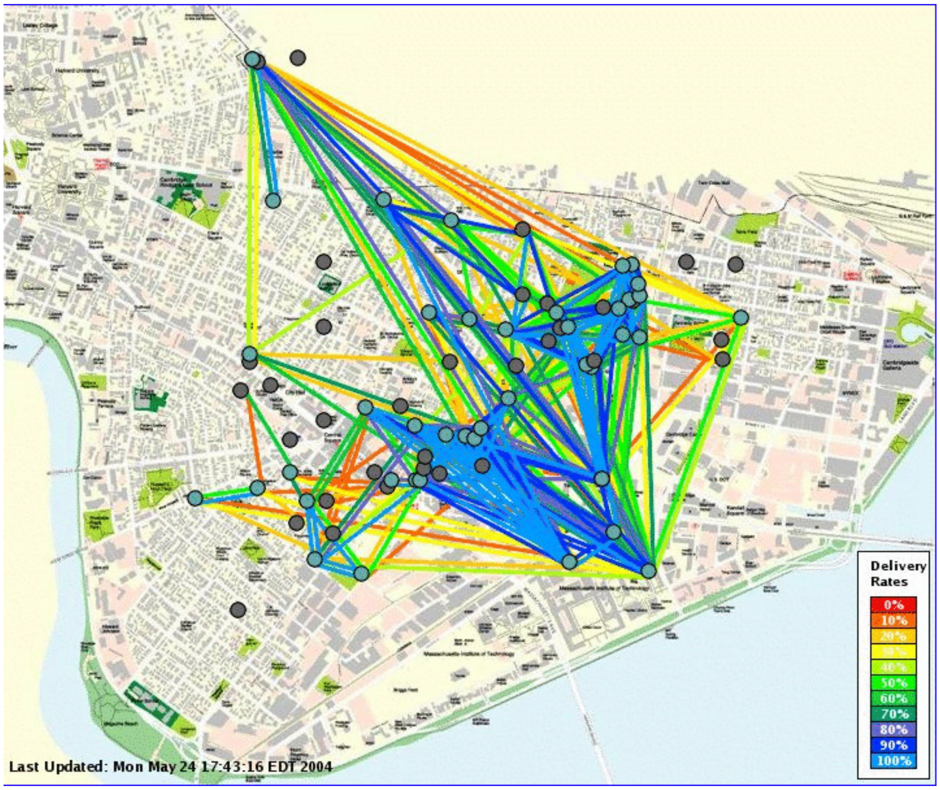


Figure 2: Roofnet Connectivity Map

MIT Roofnet and SFLAN (San Francisco Local Area Network) aim to provide wireless access over large areas. SFLAN was intended to provide Internet access to San Francisco population whereas MIT Roofnet is directed more toward the research community. It only provides Internet access to MIT affiliates. The technical characteristics are also quite different. The biggest one is that SFLAN has an engineered architecture with designated and coordinated nodes whereas MIT Roofnet has an unplanned architecture. A complete survey has been done in [42].

Forty Roofnet nodes cost around $26k while residential ADSL prices start from $29.95/month in Boston [51]. In fact it takes two years to amortize the costs of the Roofnet nodes. Nevertheless, the principle goal is to allow the growth of community networks with open access policies and allow unmanaged deployment and operation while researching protocol designs.

1.2.2 Hardware

The necessary hardware is loaned to each user. It includes a computer with pre-installed software, an 802.11b card, an antenna with a chimney mount, 50 to 150 feet of low-loss LMR400 cable, and printed instructions. The total cost is about $650. The computer is a $250 iDOT Slim PC, with a 500 MHz x86 CPU, a Mini-ITX motherboard, a 40 GB hard disk, a CD-ROM (for software upgrades), built-in Ethernet, and one PCI slot [6].

All nodes are equipped with a Hyperlink Technologies 8dBi omni-directional antenna [6]. Omni-directional antennas facilitate the growth of the network because a new user only has to install the antenna and need not know the direction to his neighbors. They also increase reliability as they provide a richly connected mesh. We can notice that smart antennas could have been chosen but for costs issues Omni-directional antennas were preferred. The network has to remain dense to provide connectivity. Moreover a lot of different error rates occur with such omni-directional antennas which require use of more sophisticated routing algorithm as we will see. The 802.11b card used is the Prism2 802.11b PCMCIA card, in a PCI adapter. They are used in 802.11 ad hoc mode.

1.2.3 Software

For software, the nodes run Red Hat 9 Linux and the Click software router toolkit [8] for route discovery and packet forwarding. They also run a Web Server along with a NAT and DHCP server on their wired Ethernet port. The DHCP and NAT allow a users' home computer to use the node as a router. The Web Server is used as an interface to configure the node and also to monitor the routes and their metrics.

1.2.4 Routing

The name of the protocol used in Roofnet has been changed to protect the anonymity of a pending conference submission. We are going to call it RNR in the following for Roofnet is RoofNet Routing [5], also called srcRR in some papers. It aims at finding high-throughput routes. The main issues to address are intermediate quality of links, asymmetric link loss rates, frequent changes in link loss rates and frequent losses of routing protocol packets. RNR [5] was inspired by DSR [17] which uses source routing. We will discuss these routing protocols later. Roofnet first used DSDV[13], but the broadcast updates were more likely to be lost when competing with data traffic. Most of the traffic is destined to and from the Internet and each user can configure their Roofnet node to act as a gateway. Each non-gateway node chooses a gateway through which to route its Internet traffic. The Roofnet uses internal IP addresses of the form 10.x.x.x for management and RNR routing. When a node receives an IP packet on its Ethernet port for traffic, it NATs the packet to its own 10.x.x.x address, encapsulates the IP packet inside a RNR packet addressed to the current gateway. There the gateway un-encapsulates it, NATs it again as if it is from the gateway's global IP address and sends it out the Ethernet port. With this scheme the 10.x.x.x addresses are hidden from the Internet. A node switches gateways only if the current one is unreachable, this may cause a node to use a gateway with low quality route even if better gateways are available.

1.2.5 Performance

1.2.5.1 Throughput

The experiment [53] to measure the throughput was 15 seconds one-way TCP transfer; throughput is measured in terms of data bytes delivered to the receiving application. Each transfer is preceded by a 30 second quiet interval during which the sender sends pings once per second to establish the routes. The results are shown in figure 3.

Hops	Pairs	Average Throughput (in kB/s)
1	179	316.4
2	354	97.7
3	354	46.0
4	256	33.9
5	127	27.3
6	54	30.5
7	38	22.5
8	17	20.5
9	6	19.2

Figure 3: Average TCP throughput between each pair in the network.

The routes with low hop-counts have much higher throughput than those with many hops. Figure 4 shows the average TCP throughput for each node to its gateway. It can be seen that the averages for each hop-count are higher than in the all-pairs data because the gateways are slightly better placed than the average Roofnet node. At four hop counts the average of 47kB/s is comparable to many DSL links on the uplink.

Hops	Nodes	Average Throughput (in kB/s)
1	18	357.2
2	10	112.0
3	9	52.8
4	7	47.3

Figure 4: Average TCP throughput to each node from its gateway.

1.2.5.2 Range and Density issues

The density is a key point in the architecture of Roofnet, if Roofnet works so well it is due in part because the node density is high enough so they are well connected. To determine how Roofnet would perform in a less-dense environment, the authors in [53] have run throughput measurements for various size subsets of Roofnet. Four nodes are chosen to be part of each subset so the measurements can be compared properly. Results in [53] shows that the four nodes almost always become fully connected with ten other nodes. It corresponds to a density of ten nodes per square kilometer. When more nodes are added beyond that point of 10 nodes, the throughput increases. When the node density is high, the routing protocol of Roofnet has more choices and in particular more short distance links with lower loss or higher usable transmit bit-rate.

1.2.5.3 Architectural alternatives

[53] compares the Roofnet architecture to a traditional architecture with access points. Each node is connected over a single hop to the access point which is connected to the wired Internet. The authors analyzed off-line the TCP measurements exposed in 1.2.5.1 between all the N^2 pairs in the network. They also ran direct single hop measurements between all pairs in order to simulate the infrastructure architecture. Figure 5 shows the comparison between the two architectures.

APs or Gateways	Multi-Hop		AccessPoint	
	Cntd	Throughput (in kB/s)	Cntd	Throughput (in kB/s)
1	41	119.00	25	20.47
2	41	202.08	34	86.52
3	41	235.08	38	108.07
4	41	261.87	40	143.05
5	41	255.50	41	144.86
6	41	273.47	41	201.75
7	41	287.06	41	232.84

Figure 5: Comparison of mesh and access-point architectures.

The ‘Cntd’ field indicates the number of connected nodes (nodes with non-zero throughput) to a gateway or an access point. The data show that five access points are needed to cover the entire Roofnet network. More would be required to match the average throughput provided by Roofnet’s gateways. Moreover Roofnet mesh architecture provides higher average throughput.
The results above are for an optimal placement of the gateways and the access points. In [53] they proposed other results for a random placement of the gateways and the access points. So, 25 access points would be required to cover all Roofnet nodes. 90% of the nodes could be covered with 10-13 access points.

1.2.5.4 Collisions and Contentions

RTS/CTS is a mechanism which is supposed to solve the ‘hidden terminal’ problem and thus avoid collisions. Figure 6 shows the results of throughput measurements with and without RTS/CTS, taken between a random subset of node pairs. RTS/CTS does not seem to improve the performance. For these experiments the same channel is used for all nodes.

Hops	No RTS/CTS		With RTS/CTS	
	count	Throughput (in kB/s)	count	Throughput (in kB/s)
1	6	228.18	4	166.37
2	9	81.85	11	75.67
3	16	40.91	14	42.28
4	4	40.01	4	36.07
5	3	20.68	4	25.08

Figure 6: TCP throughputs with and without RTS/CTS

In [53] they conducted a test in each they insert delay between each packet sent so that each packet is forwarded to its final destination before the next packet starts. This technique applied to two selected two-hop routes increased throughputs from 70 to 107kB/s and 70 to 125kB/s. This shows that contentions are likely to be a cause of the lower values for the larger hop count routes.

1.2.5.5 Loss pattern

The mean delivery ratio is 80% but 10% of the links have delivery ratios less than 50%.

1.2.5.5.1 Spatial distribution

[54] shows that there is a correlation with distance, but it is not consistent. There are several cases where receivers close together from the sender had very different delivery ratios and on the contrary nodes far away from the sender received many more packets than one might expect. The irregular propagation is caused by obstacles, variations in the receiver heights, and multi-path fading.

1.2.5.5.2 Time variation of loss rate

[54] shows that in Roofnet non busty links are predominant. This means that the links are not really alternating between “up” and “down”. The major consequence is that we can predict the future loss rates of most links over intervals as short as a few seconds.

1.3 Scope

We will develop a multipath routing protocol for environments similar to Roofnet. These environments are characterized by the following:

- No mobile nodes: the topology is static.
- The nodes do not communicate between each other, they only try to reach hosts on the Internet through the gateways.
- All TCP connections originate from nodes in the Roofnet, as we assume NAT is enabled.
- The network size doesn't exceed a few hundred nodes.
- Three gateways are always in use. Two are connected to 100Mbps links and one is connected to a cable modem (4Mbps downlink, 384kbps uplink). Two additional nodes turn on their gateway mode sometimes.

2 Background

2.1 Wireless ad hoc Networks

A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other over a wireless channel. They maintain connectivity in a distributed manner. Packets are sent to their destination via other nodes which act as routers. It is also called a multihop wireless network. There are different types of wireless ad hoc networks including packet radio networks, sensor networks, personal communication systems, WLAN, and rooftop networks.

2.1.1 Wireless layers model

A radio device can be divided in two parts [10]: the radio modem which corresponds to the first layer of the ISO OSI seven layer model [9] and the Media Access Control (MAC) controller device which corresponds to the second layer. The first one is the part transmitting the data via the radio and receiving other transmissions. The second one is responsible for the MAC protocol.

2.1.1.1 Physical Layer

The first layer called the physical layer, is implemented as a radio modem in wireless systems we will consider here. The main characteristics are: frequency band, spread spectrum technique, range, modulation technique, interference, and sensitivity.

Roofnet uses the unlicensed specific frequency bands Industrial, Scientific and Medical (ISM) at 2,4Ghz. Nevertheless some rules are defined for such frequency bands such as the maximum power transmitted and the use of spread spectrum techniques, such as either Direct Sequence or Frequency hopping in order to meet the requirements of the FCC [11].

Spread spectrum is a technique which uses increased bandwidth to improve reliability. Direct sequence spread spectrum is also known as direct sequence code division multiple access (DS-CDMA). The signal is spread over a larger band by modulating a higher bit rate pseudo random code sequence. It helps to minimize localized interference and reduces the effect of narrow-band background noise. Frequency hopping is also known as frequency hopping code division multiple access and uses a set of narrow channels. It divides the frequency band into narrow channels and periodically the system jumps to a new channel following a predetermined pattern. Thus jumping from one channel to another avoids narrow band interference. DS-CDMA yields better performance and is more reliable while FH-CDMA consumes less power.

Radio propagation depends on many factors such as reflection. So it is hard to define a precise range. Some parameters must be taken into account: Transmitted power, Sensitivity, Attenuation, and Signal to Noise Ratio (SNR). The transmitted power is measured in Watts. Setting a high transmitted power will emit strong signals that won't be influenced by the interferers in the band. Sensitivity measures the weakest signal that may be successfully decoded from a channel by the receiver. It characterizes the performance of the receiver. The attenuation is defined as the loss of power, it is expressed in dB. SNR is a measure of signal strength relative to background noise. The ratio is usually measured in decibels (dB) and depends on the quality of the receiver and the transmitter.

Some phenomenon such as fading, transmission errors, multipath, and delay spread affect wireless transmissions. Fading includes all types of temporal variations of the signal attenuation due to its propagation. A Rayleigh fading model or a Ricean Model is often used to describe the pattern of attenuation. The first model is used when there is no line of sight path and the second when there is a line of sight along with other paths. As the distances increase, the attenuation due to fading increases until the transmitter and the receiver lose communication. Antenna diversity is a way to overcome the effect of fading. Antenna diversity utilizes more than one antenna, in such a way that the receiver can choose the best antenna based on SNR which is supported by the Roofnet wireless cards but not used. A way to fight transmission errors is to use Forward Error Correction (FEC); it adds some redundant bits in every transmission. However, in wireless 802.11b LANs FEC is ineffective and retransmission at the MAC level is preferred because when the signal is weak the packet has a lot of errors or when a collision happens most of the packet is corrupted [10]. This would imply using a strong FEC code which would generate too much overhead. Then come the multipath and delay spread. Radio waves reflect or diffract on obstacles. Multipath is defined as what a receiver sees when a signal transmitted takes a lot of different paths. The receiver only sees a combination of these reflections which because of a delay spread these signals don't arrive at the same time hence the signal is combined with various attenuated copies of itself. An equalizer is used to overcome this problem by estimating the different components of the signal using a training sequence.

2.1.1.2 Data-Link layer

The second layer called Data Link layer is divided in two sublayers the Media Access Control Layer (MAC) and the Logical Link Control (LLC) level in wireless systems.

2.1.1.2.1 Media Access Control layer (MAC)

The main issues at this sub level are: different types of MAC, different techniques for Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA). The aim of the MAC protocol is to coordinate the usage of the medium and to define bits and frames. This is done through a channel access mechanism which is a way to allocate resources between nodes and a radio channel. It indicates when the nodes can transmit and receive data.

CSMA/CA is very similar to Carrier Sense Multiple Access /Collision Detection. CSMA/CD is the basis of Ethernet used in wired networks. CSMA/CA is a channel access mechanism widely used in WLANs. The basic operations are: listen before talk and a mechanism to resolve contention. When a node wants to transmit, it first listens to the network (carrier sense) and if it is idle, it sends the first packet in the output buffer. If it is busy, the node waits until the end of the current transmission and starts the contention resolution process which involves waiting a random amount of time. When this timer expires, if the channel is idle, the node can start sending its packet. Each node is given an equal chance to access the channel.

Some additional techniques can be used with CSMA/CA to improve the performance. In wired LANs packet losses are low. If a packet is lost, TCP assumes that there is congestion so it slows down. So we can say that TCP doesn't accommodate well packet losses by the radio medium. That is why now most MAC protocols implement positive acknowledgment and MAC level retransmissions. Each time a node receives a packet, it sends back an ACK to the transmitter. If after sending a packet, no ACK is received, then after some time the node will retransmit the packet. The MAC protocol generally uses a stop and go mechanism which enables a node to send a new packet only if the ACK for the previous packet was received. Depending on the MAC, if the packet to transmit is long and contains only one error, the node will have to retransmit it entirely. Because of that fragmentation is used, this splits the big packets into small ones. Two advantages of fragmentation are that the retransmission of small packets is faster and small packets are more likely to get through noisy channels without errors.

All nodes may not hear each other because the attenuation is too strong between them. So when CSMA/CA is used they may transmit at the same time. RTS/CTS (Request To Send/Clear To Send) is a form of handshaking to avoid this. Before sending a packet, the transmitter sends a RTS and waits for a CTS from the receiver. The reception of a CTS indicates that the receiver was able to receive the RTS. At the same time, each node in the range of the receiver hears the CTS. All nodes which heard a CTS won't send even if this carrier sense tells them that the medium is free.

2.1.1.2.2 Logical Link Control layer (LLC)

The LLC layer controls frame synchronization, flow control, and error checking. Wireless LLC is the same as in IEEE 802.2.

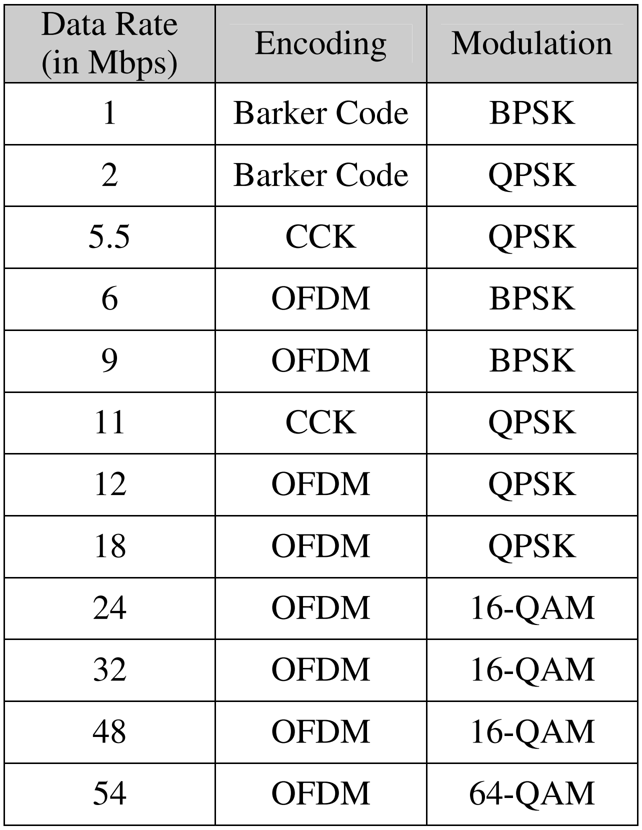
2.2 IEEE 802.11b and IEEE 802.11g

Wireless networking has been working its way into the mainstream corporate environment for several years. The three technologies which are in wide use are 802.11a, 802.11b, and 802.11g. First of all, 802.11b and 802.11g works in the same ISM band, i.e. 2.4 GHz. They both use Direct Sequence Spread Spectrum as a transmission scheme. However, 802.11b uses Complementary Code Keying (CCK) for its highest data rates and 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM). The details are shown on figures 7 and 8. [47] compares these two schemes in more detail.

Roofnet uses 802.11b technology whereas the indoor network uses 802.11g. We are going to describe the similarities, the differences, and the compatibility between these two wireless technologies.

Data Rate (in Mbps)	Encoding	Modulation
1	Barker Code	BPSK
2	Barker Code	QPSK
5.5	CCK	QPSK
11	CCK	QPSK

Figure 7: 802.11b data rate specifications



Data Rate (in Mbps)	Encoding	Modulation
1	Barker Code	BPSK
2	Barker Code	QPSK
5.5	CCK	QPSK
6	OFDM	BPSK
9	OFDM	BPSK
11	CCK	QPSK
12	OFDM	QPSK
18	OFDM	QPSK
24	OFDM	16-QAM
32	OFDM	16-QAM
48	OFDM	16-QAM
54	OFDM	64-QAM

Figure 8: 802.11g specifications [47]

2.2.1 Standards

802.11g utilizes OFDM technology while preserving backward compatibility with the large installed base of existing 802.11b equipment (about 40 million units world wide, and growing). OFDM was previously adopted for WLAN applications as part of the IEEE 802.11a Standard. Since 802.11g operates at 2.4 GHz, it provides much longer range than 802.11a based equipment because the lower operating frequency has better propagation properties especially for indoor WLAN environments.
When the 802.11b Standard was adopted, FCC regulations prohibited the use of OFDM in the 2.4GHz band. That restriction was lifted in May of 2001.

2.2.1.1 CCK

The main challenge for a WLAN equipment designer is signal impairment due to Multipath. [48] describes how multipath interacts with CCK.
At 11Mbps, IEEE 802.11b devices employ a waveform known as CCK. The underlying modulation is single-carrier Quadrature Phase Shift Keying (QPSK). At 11Mbps, groups of 8 QPSK symbols are used to form code words. Each code word represents 8 bits of information are sent at a rate of 1,375 million symbols per second (MSps). Thus a symbol period is about 91ns. However, some secondary paths delays are 400 to 500ns. In this case, Inter-Symbol Interference (ISI) can cause the distortion of as many as five or six subsequent symbols as shown in figure 9.

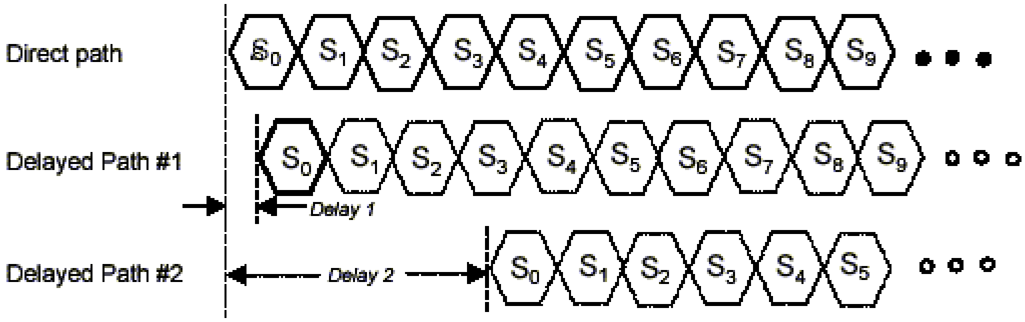


Figure 9: effect of multipath on CCK [48]

The effects of multipath can be compensated by employing time domain based equalization techniques. As data rates increased, equalizer complexity must increase to maintain an acceptable level of performance.

2.2.1.2 OFDM

OFDM systems eliminate the problem for multipath-induced ISI as described in [48]. They distribute the data payload among many ‘subcarriers’.
OFDM uses a guard interval of 800ns for 802.11 applications as shown in figures 10 and 11. This interval is selected to be longer than the delayed paths encountered. When the receiver process the signal, the guard interval is rejected, the remaining rectangular period is completely free of multipath-induced ISI. However, distortion due to multipath is still possible from within the same symbol. This can be compensated for on a

subcarrier-by-subcarrier basis by means of an amplitude shift and phase correction. These two parameters are constant over the entire remaining rectangular period.

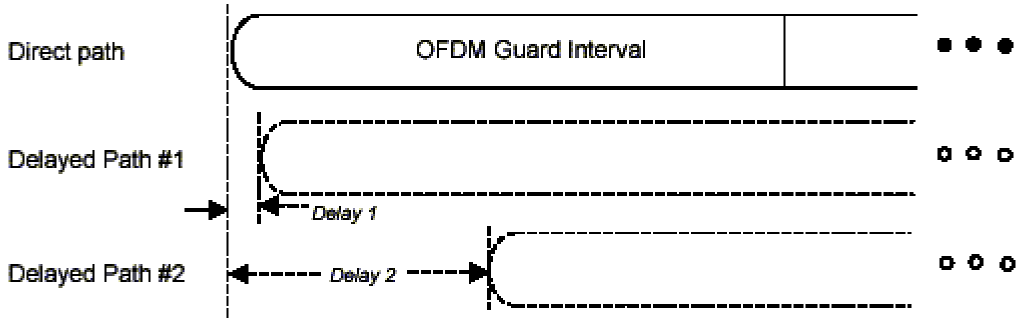


Figure 10: Effect of multipath on OFDM [48]

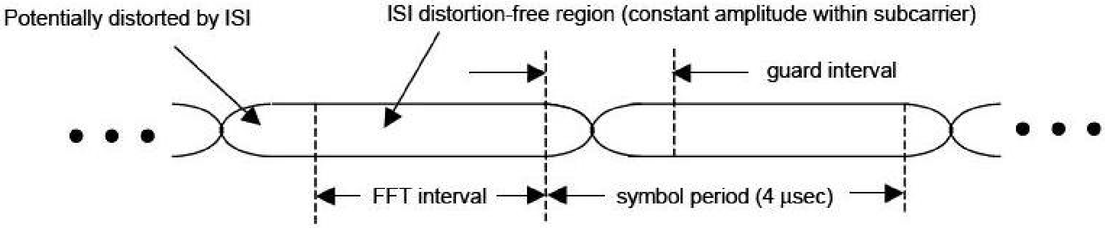

Potentially distorted by ISI
ISI distortion-free region (constant amplitude within subcarrier)
guard interval
FFT interval
symbol period (4 µsec)

Figure 11: OFDM Symbol Contains a Guard Interval [48]

In the frequency domain, the rectangular period remaining after having removed the guard interval can be represented by a sync function with zero-crossings at intervals corresponding to the inverse of the pulse period: 312.5Khz (1/3200ns). This is the frequency spacing for the subcarriers. As shown in figure 12, at zero crossings, there is no energy from adjacent subcarriers, this is why they are said to be orthogonal. They don’t interfere with each other.

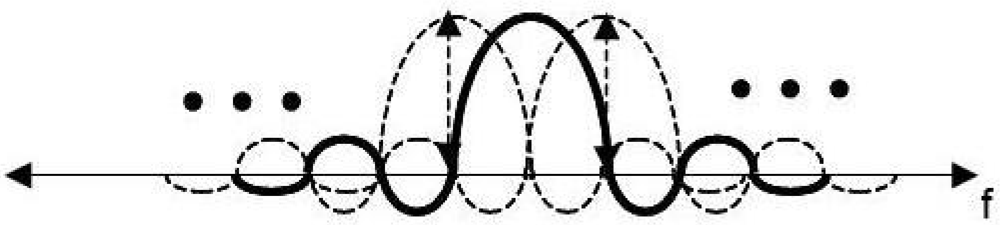


Figure 12: Frequency representation of the subcarriers [48]

A Fast Fourier Transform (FFT) algorithm can be used to perform compensation. The main difference from CCK is that the circuitry complexity does not increase because frequency-domain methods are used instead of time-domain methods.

2.2.2 Compatibility between 802.11b and 802.11g

The main channel sharing mechanism for 802.11 WLAN systems is carrier sense multiple access/collision avoidance (CSMA/CA). Legacy 802.11b radios are effectively unable to hear newer 802.11g radios using OFDM. The 802.11g Task Group solved this problem by use of a request-to-send/clear-to-send (RTS-CTS) feature that is already supported by every 802.11 radio. This is shown in figures 13a, b and c.

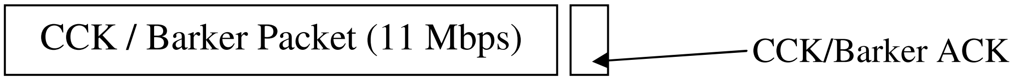


Figure 13a: Conventional 802.11b Packet Exchange

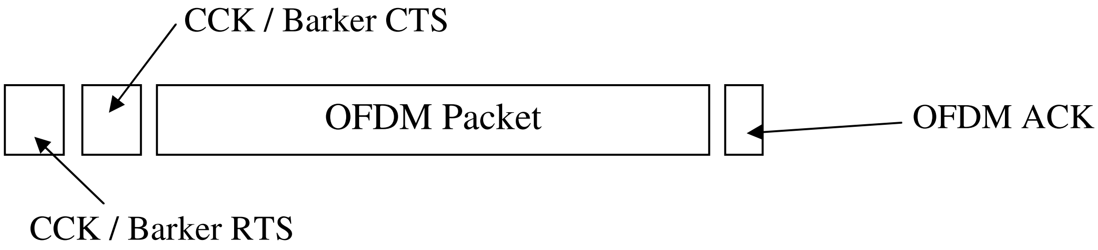


Figure 13b: 802.11g Packet Exchange with RTS-CTS

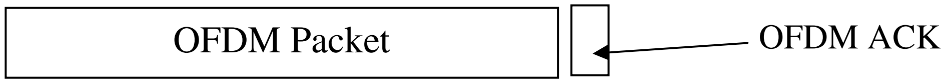


Figure 13c: 802.11g OFDM Packet Exchange without RTS-CTS

2.2.3 Throughput and Coverage area issues

Intersil in [48] conducted extensive indoor tests. In these texts the ceilings are 9 feet high and internal wall construction is drywall over studs. They compared throughput and range for 802.11g and 802.11b technologies. They used 802.11g equipment using OFDM and 802.11b equipment using Packet Binary Convolutional Coding (PBCC). RTS-CTS was not used for these experiments. From [48] experiments for 802.11g we can note that connectivity is preserved in all but the extreme edge of the floor plan with peak throughput around 22Mbps. From [48] experiments for 802.11b the peak throughput is approximately 7 Mbps. This is less than half of the one achieved by 802.11g equipment.

2.3 Wireless Routing

2.3.1 The Path Metric

In our project we consider splitting the traffic onto multiple paths. As has been said above, the choice of a good metric for these paths is really important. In the actual implementation of Roofnet, the single path routing protocol RNR uses the ETX metric [5]. Using the Roofnet experimental results, they have noted that using hop count is inadequate in wireless ad hoc networks in the case of a single path. [5] shows experimental evidence of the lack of efficiency of existing hop count routing protocols in ad hoc networks. They generally choose paths with minimum hop counts, but with less total capacity. Other protocols use the product of the per-link delivery ratios, but fail to account for inter-hop interference. For example, a route with two hops may be chosen instead of a one hop route with a 10% loss ratio even if this later route has much better throughput. An end-to-end Delay metric can cause routes to oscillate from the good path. The solution Decouto et al. [5] propose is based on the expected total number of transmissions of a packet along a path. The forward delivery ratio of a link is d_f and its reverse delivery ratio is d_r. Here d_f is the probability that a data packet is received while d_r is the probability that the ACK packet is received. ETX is defined as $\frac{1}{(df \times dr)}$. The goal of this metric is to choose a high end-to-end throughput path. The main characteristics of ETX are:

- it is based on delivery ratios,
- it detects and handles asymmetrical links, and
- it takes advantage of low hop-count routes since they are less affected by interferences.

This paper highlights the process of choosing a good path metric. ETX with Dynamic Source Routing (DSR) experiments results show that ETX significantly improves initial route selection, but only slightly improves the overall performances of DSR as the link-layer feedback enables DSR to avoid high loss ratio links.

2.3.2 Wireless Unipath Routing Protocols

The routing protocols meant for wired networks can not be used for ad hoc networks because of the asymmetry of the links and the high link failure probability. For nodes which are within communication range, multihop routes have to be established without the help of a central authority. So each node is responsible for acting as a router i.e., finding routes, maintain them, and relaying packets along those routes. There are two main classes of ad hoc routing protocols: table-driven and On-demand protocol [12, 40].

The first class of protocols evaluates the routes periodically and maintains routes for each node in the network. Thus every node keeps a full topological view of the network. One big disadvantage of this type of protocol is that it reduces the capacity of the system because a high percentage of transmitted packets are sent to carry information about the topology of the network. Some examples of table-driven protocols are DSDV [13], Destination Sequence Distance Vector Routing [14], CGSR[15], Cluster-head Gateway Switch Routing and, WRP Wireless Routing Protocol [16].

The second class of protocols initiate route discovery only when a source needs a route towards a destination. This implies using much less memory and resources like bandwidth than table-driven protocols. However, it increases the initial delay of the system since it takes a while for a node to find a path to its destination. Some examples of On-demand routing protocols are: ad hoc On-Demand Distance-Vector Routing (AODV) [16], Dynamic Source Routing (DSR) [17], Lightweight Mobile Routing (LMR) [20], Temporally Ordered Routing Algorithm (TORA) [20], Associatively-Based Routing (ABR) [13], Signal Stability Routing (SSR) [22], and RNR (e.g. the protocol currently used in Roofnet).

A hybrid table-driven/demand-driven routing protocol is also possible; an example of such protocol is the Zone Routing Protocol (ZRP) [23]. To gain insight into table driven and on-demand routing algorithms, we describe the most famous algorithms, including the one used in the Roofnet project, e.g., DSDV [13], AODV [16], DSR [17], and RNR.

2.3.2.1 DSDV

Destination-Sequenced Distance-Vector (DSDV) [13] is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. Every node has at any time a routing table with all the destinations and the number of hops to reach each destination and the sequence number assigned by the destination node. This sequence number is used to avoid the formation of loops. Each node periodically exchanges its routing table with their immediate neighbours. It also transmits its routing table when a significant change occurs. A full dump or an incremental update can be sent, depending on how many changes occur in the network. The route with the most recent sequence number is used, if there is a tie between two routes then the best metric is used as the criteria to choose the route.

2.3.2.2 AODV

AODV [16] is an improvement on the DSDV [13] algorithm. It minimizes the number of broadcasts by creating routes on-demand as opposed to all possible routes as in DSDV. It is a loop-free, unipath, distance vector protocol based on hop-by-hop routing approach. Path discovery and path maintenance are the main procedures in AODV. When a source needs to send traffic to a destination it floods the network with a route request RREQ which is uniquely identified with a sequence number. When an intermediate node receives an RREQ it first checks that an RREQ with this sequence number has not previously been received, then it records the previous hop and checks whether there was already an entry for this destination in its own table. If it finds an entry, it sends back a RREP Route Reply to the source; otherwise the node rebroadcasts the RREQ. As the RREP travels back to the source, each intermediate node along the path sets up a forward pointer, updating the time-out and records the destination sequence number. A node updates its own routing table if the destination sequence number is higher or if a shorter route is found. Disconnections are detected by periodic hello message exchanges. If disconnect occurs a RERR route error is sent back to all sources to erase route entries using that link.

2.3.2.3 DSR

Dynamic Source Routing (DSR) [17] as it name says, uses source routing. That means that the source has a complete sequence of nodes through which to forward the packet to the destination. It includes two main phases as in AODV [16]: route discovery and route maintenance. When a source wants to transmit a packet to a destination, it first checks whether it has a route to the destination stored locally in its routing table. If so, it then uses that route to send packets towards the destination. Otherwise, the node initiates a route discovery process by broadcasting a route request packet. This packet contains the address of the source and the destination and a unique identification number. Each intermediate node checks whether it knows a route to the destination, if not it appends its address to the route record and forwards the packet to its neighbours. An intermediate node can forward a particular request packet only once. A route reply is generated when either the destination or an intermediate nodes has in its table the destination information requested by the source. When a route failure is encountered a route error packet is sent back to the source. The route error packet contains the addresses of the hosts at both ends of the hop in the event of an error. As the route error traverses back, all routes in the route caches of all intermediate nodes containing the failed link will be removed from the caches.

2.3.2.4 RNR

RNR is similar to DSR [17]. The process to find and compute a route is the same as DSR. RNR differs from DSR in the use of the ETX[5] metric. ETX continuously measures the loss rate in both directions between each node and its neighbours using periodic broadcasts. On each link the number of transmissions of a packet is estimated, i.e. the number of times a packet will have to be transmitted before it receives an 802.11 MAC ACK. The best link metric is one. The ETX route is the sum of all the link metrics. Thus ETX penalizes both long routes and routes that include links with high forward or reverse loss rates.

A node forwards a query if it has not seen the query before, or if the query's total route metric is better (lower) than the best instance of the query the node has seen so far. This increases the amount of query traffic, but decreases the algorithm's bias in favor of shortest hop count. Nodes also delay for a random period less than one second before forwarding a query to avoid contention. When a node forwards a query, it includes the link ETX metric to whatever node it heard the query from; nodes store these metrics in their link-state databases, and use them to compute the route metric to minimize via Dijkstra's algorithm. Route maintenance uses the following techniques. Each time a node forwards a packet it updates the source route of the packet to the latest ETX metric from the preceding nodes. After 10 packets in a row have failed to elicit an ACK, the node will send the link metric to the source. Thus the source is aware of asymmetric links (i.e. the link sends data in only one direction), broken links (no data is seen in either direction) and good quality links (the metric is the same in both directions). Each time a node learns a new metric for a route it was using, it recomputes routes via Dijkstra's Algorithm in order to always have the best routes. If a source realizes that a route has a current metric only half as good as the best it has seen since the last query, it will broadcast a new query. RNR operates at the data-link layer. It uses 32-bit addresses. In the usual case it is carries IP addresses in its headers. RNR nodes have a table mapping RNR addresses to 48-bit 802.11 MAC addresses obtained from the broadcast queries which is equivalent to an ARP cache.

2.3.3 Wireless Multipath Routing Protocols

All the routing protocols described above are unipath routing algorithms and this is what earlier work has mostly focused on. However, when a route is broken, the nodes drop packets and launch a new route discovery. As many phenomenons such as fading, interference, and collision can occur and create link failures, unipath protocols are suboptimal for wireless ad hoc networks. Multipath using alternate routes can help to solve this problem, for each route discovery initiated, multiple routes can be discovered. In this way when the primary route disconnects, the source can still used alternate routes. Some results show that multipath reduces the route discovery latency and the overheads. Although this is one approach to multipath routing, considering one primary route and alternate routes in case of a disconnection; another approach called downward demultiplexing uses multiple paths at the same time by splitting the traffic onto these multiple routes. In both approaches the protocol aims to find disjoint paths. For the first case, it is obvious that if the alternate paths are disjoint from the primary path when a link goes down on the primary route, it won't affect the alternate routes. For the second case, if multiple non-disjoint routes are used, bottlenecks can appear as traffic will go through the same links. Much research has focused on finding independent paths; many criteria have been used such as minimizing energy, avoiding interferences, and link or node disjointness. We will look at some of these methods in the related work part below.

While efficiency is one area that may benefit from multipath routing, some other characteristics can be improved such as fault tolerance and security. For example, the impact of link failures is reduced when using multipath, eavesdropping also becomes more difficult as the attacker has to sniff multiple links. It does not apply to Roofnet as all the traffic goes out the gateways. In wireless networks, some multipath routing protocols using one path at a time have been designed and they are in general extensions of unipath routing protocols.

2.4 Wireless Multipath Routing

2.4.1 Disjoint Paths

2.4.1.1 Interference free paths

In [33] the authors want to find what is the maximal throughput that can be supported by a specific placement of wireless nodes in a physical space and under a specific workload. The key issue is to minimize interference. The final aim is to build an interference-aware protocol. Thus they define a conflict graph to incorporate wireless interference into the formulation of the problem.
They define two interference models: a protocol model and a physical model. In the protocol model a transmission between A and B is successful if B is within the transmission range of A and if no one in this transmission range area is transmitting. In the physical model a transmission is successful if the SNR of B for a transmission received from A is greater than a certain threshold.

To find the optimal throughput they based their method on a Linear Programming (LP) formulation for wired networks shown in equation 1. Under the Protocol Interference Model, they show that it is NP-hard to find the optimal throughput and to approximate it. So they suggest heuristics for obtaining the lower bound and the upper bound on the throughput. They add some constraints to the LP formulation to find the lower bounds. The upper bound uses the conflict graph; it is based on the cliques constraints and is tight enough in perfect graphs. Under the Physical Interference Model, a weighted conflict graph is needed. They add some constraints to the Linear Programming (LP) formulation to compute the lower bound. This bound could be tightened using maximal schedulable sets in the conflict graph. For Single Path Routing, the LP formulation is solvable in practice. In our case, as the number of gateways is small and each has a kind of spanning tree, it is practical to compute all the paths for small graphs.

$$\max \sum_{l_{si} \in L_C} f_{si}$$

subject to

$$\sum_{l_{ij} \in L_C} f_{ij} = \sum_{ji} f_{ij} \forall n_i \in N_c \setminus \{n_s, n_d\} < 1 >$$

$$\sum_{l_{is} \in L_C} f_{is} = 0 \qquad < 2 >$$

$$\sum_{l_{di} \in L_C} f_{di} = 0 \qquad < 3 >$$

$$f_{ij} \leq Cap_{ij} \qquad \forall l_{ij} \in L_C \qquad < 4 >$$

$$f_{ij} \geq 0 \qquad \forall l_{ij} \in L_C \qquad < 5 >$$

Figure 14: LP formulation to optimize the throughput
(where f_{ij} is the flow between node i and node j. Here s stands for source and d for destination and Lc is a set of all links) for wired networks.

One interesting point of their paper is that using two non-overlapping channels gives better results than employing multipath routing. But this requires more material as more antennas are needed.

As it was said above the paper was written with the assumption of optimal scheduling which is not the case under 802.11 most of the time. Therefore they want to show that optimal routing is beneficial even in the absence of optimal scheduling. To derive the performance of optimal routing under 802.11 they specify as static routes the routes obtained under single path routing with optimal scheduling. They then compare the results of this method with the standard AODV protocol. The results are good for the first method when the two flows interfere with each other; in this case the optimal path takes a detour. However, optimal path routing does **not** outperform single path routing under 802.11 when the number of flows is high because it becomes difficult to find interference free paths in the absence of optimal scheduling.

The next step is to build a practical interference-aware routing protocol using a conflict graph, and to compute the optimal routes in a distributed manner.
Although in our project all the traffic is sent to gateways, thus a lot of traffic will be concentrated around them. Paths from a source to the gateways are likely to be interference independent as long as the gateways are far enough from each other. It can be verified looking at the ARP cache like table created from the received broadcast probes. In a given gateway, no other gateway entries exist.

2.4.1.2 Other approaches

There have been a lot of papers published on how to find disjoint paths. [35] cite some of them. It is worth noting is that in both cases (edge and vertex disjointness), deciding whether the pairs can be disjointedly connected is NP-complete. Finding independent paths is in the end an optimization problem. One relevant issue for multipath routing protocol designers is to decide whether they need the routes to be node disjoint or link disjoint.

2.4.2 Routing Protocols

2.4.2.1 First approaches

In [31] the authors propose a multipath routing protocol. This scheme works by adding some overhead to each packet as a linear function of the original packet. The packet is fragmented into n smaller pieces. Then m overheads defined as a function of the original packet are added to each fragment and finally distributed among the n+m multiple paths. The goal of the protocol is to increase the reliability of the network. Nevertheless this method affects in a negative way the total effective throughput. In [32], Multipath Source Routing (MSR) is defined; it is an extension to DSR. It distributes load between multiple paths using RTT as a metric.

However, the processing overload of the packets sent to discover the RTT is a drawback of MSR. Moreover RTT as a metric is not sufficient to represent the congestion of the links.

2.4.2.2 Multipath routing with alternate paths

2.4.2.2.1 MDSR

Multipath Dynamic Source Routing (MDSR)[24] is the multipath extension to DSR [17]. It uses the same flooding method as DSR, the first route discovered is the primary route and then the destination computes routes whose links are disjoint from the primary route. Two schemes are available for MDSR: alternate routes only for this source or one alternate route for all the intermediate nodes. In the second scheme, the destination needs to tell each intermediate node on the primary route a disjoint list of alternate routes. This scheme decreases the delivery latency and is more reliable than unipath protocols. On the other hand more route replies will be sent in the network which will cause more overhead for intermediate nodes' caches and more computation or the destination.

2.4.2.2.2 AOMDV

Ad Hoc On-demand Multipath Distance Vector (AOMDV) [25] is a multipath extension to AODV [16]. It uses link-disjoint, loop free paths. Loop freedom is ensured by accepting only lower hop-count alternate routes than the primary route. Intermediate nodes look at each copy of the RREQ to see if it provides a new node-disjoint path to the source. If it does, AOMDV updates its routes only if a reverse path can be set up. The destination then replies with k copies of RREQ where k is the number of disjoint routes. When all routes fail a new route discovery is broadcasted. The advantages are a fast and efficient recovery from failures. The main disadvantage is that path information used is often quite out of date because a new discovery process is initiated only when all the routes fail.
The other type of multipath routing algorithms is load balancing multipath protocol.

2.4.2.3 Multipath routing with Load Balancing

Load-balancing is the concept that allows a router to take advantage of multiple best paths to a given destination. Load-balancing can work per destination, per packet, or per flow. Per-destination load balancing means the router distributes the packets based on the destination address. Given two paths to the same network, all packets for destination1 on that network go over the first path and all packets for destination2 on that network go over the second path. Per-packet load-balancing means that the router sends one packet for destination1 over the first path, the second packet for destination1 over the second path only if both paths have the same bandwidth, otherwise the traffic is sent as a function of the link bandwidth. Research in wired networks has focused on minimizing the maximum utilization while supporting the same traffic demands. This can be achieved using multipath routing with load balancing.

Furthermore there exists routing optimizers in wired networks which help to decide how to balance the load onto the paths. Their aim is to minimize the maximum utilization while supporting the same traffic demands. Two types of optimizers are currently used: on-line and off-line. Off-line optimizers try to estimate the traffic matrix based on long-term average traffic demands. So they do not accommodate sudden changes which may occur in real-time traffic. OSPF weight optimizer [27] and multi-commodity flow optimizer for MPLS networks [28] are two examples of off-line optimizers. On the other hand, on-line optimizers react in real-time and adaptively split the traffic across multiple paths. TeXCP [1] is one of them. It is built on the eXplicit Control Protocol XCP [29]. It reacts quickly to changes in traffic demands, link failures, and traffic spikes. It also avoids congestion within the network. Thus the use of efficient load balancing implies the choice of a good metric when probing for the best paths.

2.4.2.3.1 SMR

Split Multipath Routing (SMR) [26] is a protocol similar to DSR [17] which tends to build two disjoint paths. SMR distributes the traffic across these two paths. When a source needs to send traffic to a destination, it broadcasts a RREQ. Then the destination computes two paths, such as the first path chosen is the shortest delay path and the second path is maximally disjoint from the first path. Then it sends a RREP on these two paths. In this algorithm, intermediate nodes are not allowed to answer the RREQ so that the destination can compute disjoint paths at each route discovery. For route maintenance, there are two policies: with SMR-1, a route recovery is initiated when one of the two routes are broken, while with SMR-2 a route recovery is launched only if both routes are broken. During the forwarding phase, SMR balances the load evenly on the two paths.

2.4.2.3.2 MRP-LB

Pham and Perreau propose a new multipath routing algorithm with load balancing policy which takes into account congestion in the network [2]. They also suggest a theoretical framework to analyze the performances of multipath routing in terms of overheads, connection throughput, and packet loss. The routing algorithm they propose is called Multipath Routing Protocol with Load Balancing (MRP-LB). It consists of four phases: Route Discovery, Data Transmission, Route Maintenance, and Load Balance Maintenance.

During the Route Discovery phase, a source A initiates a REQ (Request packet) made of: source and destination address, a route record, and a sequence number. The route record stores all the nodes the REQ has been through. Note that one node can only forward one REQ per source-destination address with the same sequence number. Progressively the nodes build a Request Seen Table: for each source-destination pair (N_i, N_j) the node associate a sequence number S_{ij}. If it sees a REQ with a higher sequence number, then it updates its request seen table, forwards the REQ. N_u is the maximum number of paths we want to use. So the destination B answers the first N_u REQs it receives. In the REP (Reply packet) there is a special field called “Congested Packet”. B sends REPs to the source with the field “Congested Packet” set to 0. Along the route, the nodes build a Reply Seen Table similar to the previous request seen table. Furthermore they add their number of congested packets to the field “Congested packet”. Finally A, which initiated the REQ, receives N_u REPs corresponding to N_u disjoint and loop free routes and the number of their congested packet.

When A wants to send packets to B, it stores the complete path to B in the packets header. A routes data packets on N_u paths so the total number of congested packets on each route is the same. To do this the source stores the number of packets sent on each route in a Packet Sent Table. Source A chooses the route along which to send a packet according to the following rule: *min* $(C_{A,B,n} * S_{A,B,n} + R_{A,B,n})$ where n is the index of the route, C is the number of packets sent on n, S is the number of hops on route n, and R is the initial number of congested packets on route n.

The nodes exchange Hello packets periodically, a time-out occurs after not receiving a certain number of Hello packets from its neighbors or a certain number of ACK, then an ERR packet is generated. The destinations periodically send Load Packets (LP) to the sources to maintain up-to-date information about the total number of congested packets on routes.

Pham and Perreau compared MRP-LB and DSR [17]. In terms of data packet delivery ratio MRP-LB is 15-20% better. MRP-LB also shows better results in terms of end-to-end delays. As expected, MRP-LB generates more overhead than DSR.

Then they propose analytical models. They define a network model modeling the network as a disk and considering nodes with uniform high density. They compute the total overheads for single path routing and multipath routing. Eventually their conclusion is that there is no significant increase of overheads for N_u up to 3.

In their analytical method they compute the total traffic going through a node at a distance r from the center of the disk which enables them to evaluate the packet loss rate in the networks due to congestion using a M/M/1 model for queuing. They use the following parameters: radius of the disk, the node density, the node processing rate, the node-to-node transmission rate, the average length of route, the storage capacity of a node. They show for multipath routing that the packet loss rate is limited by the average length of the routes.

Then they tackle the issue of improving the connection throughput. They assume that on a route the node (A) closer to the disk center experiences the highest traffic. Thereafter they compute the bandwidth of the routes going through A. They use the following parameters: the bandwidth of the network, the average length of route, the number of nodes, and an angle which depends on the distribution of nodes. For the multipath routing the capacity of the network is inversely proportional to the average length of the route. Finally they derive an upper bound on the average length so that multipath routing is more efficient that single path routing in terms of connection throughput. They show that this upper bound depends only on the network density and the network distribution. For example in the same situation as above the upper bound is 16 hops for an average simulated length of 7 or 8 hops that means that multipath routing is always better in terms of connection throughput. The main result of the authors is that the increase of overhead generated by the multipath routing protocol is completely balanced by the improvements made in terms of connection throughput. The load is balanced evenly among the paths using the number of packets sent on the routes as a metric that means that the protocol doesn't take into account the real utilization of the links.

2.4.2.3.3 Single Path vs. Multiple Paths

Ganjali and Keshavarzian introduce a new model for comparing single-path routing and multipath routing [3]. They show using their model that the performance of multipath routing in wireless networks is nearly the same as single path routing. Their model is based on that of Pham and Perreau studied above, nevertheless they consider that the model is not realistic enough for the load balancing part because it doesn’t take into account the distance from the center of the disk and the number of paths. They claim to generalize it.

Under multipath routing with a high density of nodes, the shortest path is the line segment between a source and a destination and it can be considered that the K shortest paths will form K parallel lines which can be seen as a rectangle. The width denoted 2W depends on the number of paths, and the nature of these paths: link or node disjointness and the node density. Their model is based on finding the locus of the points B such that given two points A and F, F is inside the rectangle created by A and B. The locus of B is the set of points that send traffic to A through F under a multipath routing policy. Finally the area formed by the set of points B depends on the position of A and F and the parameter W. W is half the width of the rectangle. The total traffic passing through F can be obtained by summing up the area multiplied by the density for each position of A. The parameters used are the following: the position of point F, the radius of the disk R, the amount of traffic generated by each flow, the number of paths K, the node density and, W which depends on the path discovery and the communication range T.

Then they show that the parameter W is inversely proportional to density of nodes and the range of communication and they assume that Wk~KW. The curves in [3] are obtained from the analytical model. The nodes close to the center experienced the highest traffic. We start seeing the effect of multipath only when the number of paths is more than 20, while significant changes occur when the number of paths is more than 100. One way to counteract this problem can be to put the load away from the centre of the disc.

In their paper the authors consider that the nodes are sending traffic towards the centre of the network which is not the case in our project. As it is said before the gateways are considered to be on the edge of the disc. That means that the traffic is actually centrifugal (i.e. outward edge and hence away from congestion)

2.4.3 Transport Layer Issues

Another relevant parameter when using load balancing is the granularity of demultiplexing. Indeed multipath routing has a lot of advantages but it leads to persistent packet reordering. The hosts suffer a lot from reductions in throughput due to reordering packets. This latter has to be taken into account seriously as the consequences on the performance effect of the network highly depend on it. As [30] mentions, there are some methods to improve TCP's performance in packet-reordering prone environments. Instead of focusing on what version of TCP to choose, a good choice on the granularity of load balancing can avoid a lot of problems. In the case of small networks, a per-source allocation in the routers and a per-source load balancing policy can be used and solves the problem of reordering packets at the destination since packets from a given source to a given destination will follow a single path. Another approach is to choose a designated gateway for reordering. For instance, in the case of multiple paths to three gateways, the other two gateways will send their packets to the Designated Gateway (DG) through the wired network.

3 Method

This section evaluates whether multipath routing in the rooftop static wireless network works well in terms of throughput. This is equivalent to asking the question whether we can get a higher throughput using multipath routing rather than using a single path routing protocol. First, basic link-level measurements of throughput under 802.11b MAC over a small portion of the network are presented. These measurements show that performances are bounded by the sending rate. Indeed for a sending rate higher than 2Mb/s, the receiver tends to lose most of the frames.

Then we will present throughput measurements over the indoor network in the CSAIL lab for different subsets of nodes. Before Roofnet was installed outside all the protocols were tested on the grid network which was the old indoor network. Even if the characteristics of the outdoor and indoor network are not exactly the same, the indoor network gives a good idea of what to expect from the performances of the protocol before using them in the outdoor network. We will evaluate how the multipath routing protocol implemented with the help of the Click modular router can maximize the throughput and minimize the packet losses. For that we have developed a multipath routing protocol based on the single path version used on Roofnet.

4 Analysis

4.1 The link level measurements

4.1.1 Testbed

The wireless cards are a generic brand based on Prism 2.5 chipset. 802.11b is uses for this experiment. We use a non standard “pseudo-IBSS” mode. This is similar to the standard 802.11b IBSS mode. In that mode, nodes communicate directly without intervening access points. Pseudo-IBSS omits the BSSID mechanism and does not use synchronization beacons. In the standard IBSS mode, partitions were created with different BSSIDs despite having the same network ID. These partitions made it impossible to run Roofnet reliably. Indeed it first suffered from ``BSSID partitioning." If different regions of the network started without being able to talk to each other, they would choose different random 802.11 BSSID identifiers. New nodes that came up within radio range of multiple partitions seemed to choose randomly from them, but the partitions would not always ``coalesce". The problem could eventually worsen until the network consisted of multiple, overlapping BSSID partitions; since a node's 802.11 firmware filters out broadcasts with the wrong BSSID, nodes in the different partitions would be blind to each other despite having radio-level connectivity. The standard package for Roofnet with Click is used for this experiment as well. We use the spatial configuration of nodes shown on figure 15**.** B and C are two senders, A and D are two receivers.

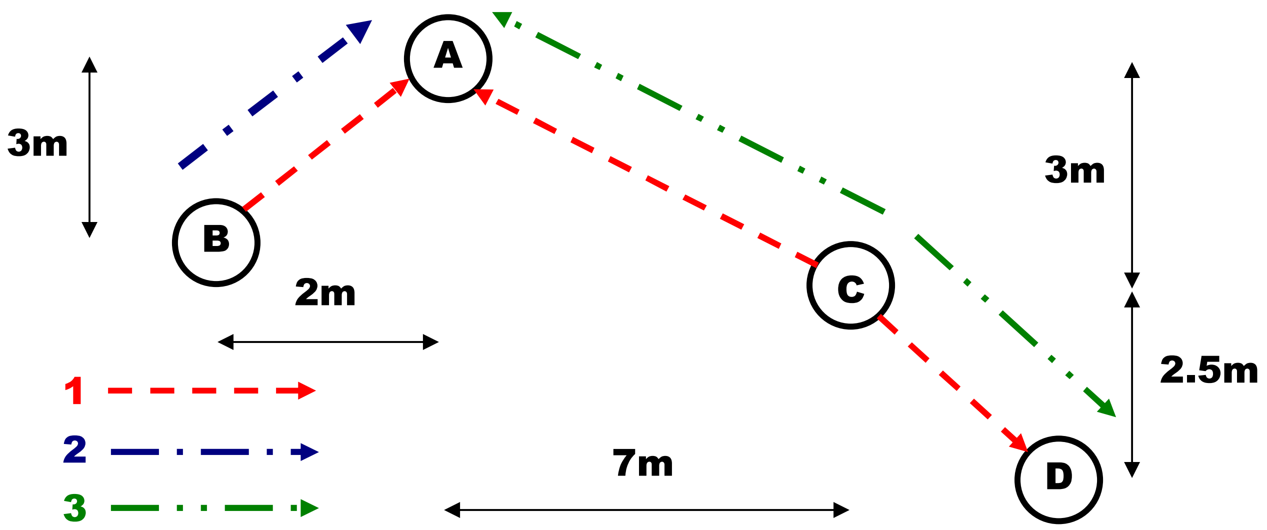


Figure 15: Spatial configuration of the nodes

Throughput results were obtained using link layer broadcasts. In the first phase (1) called dual-sender experiment, B and C send packets that overlap in time. In the second (2) and third phase (3), B first sends 802.11 broadcast packets while the two other nodes passively listen. We record the number of broadcast packets sent at the sender and the number received at A. We used 802.11 broadcast instead of UDP or TCP traffic because for 802.11 broadcasts there are no retransmissions. It enables us to evaluate the effect of collision patterns without letting retransmissions load the network.

In each experiment we can chose the sending rate at A. Normally the maximum broadcast rate is 2Mb/s and Clear Channel Assessment (CCA) is turned off. To enable us to choose the sending rate for both senders we have written our own 802.11 broadcast generator. Disabling CCA allows for both senders to transmit packets concurrently at the maximum rate chosen. Carrier Sense is enabled and RTS/CTS is disabled for this experiment. Indeed RTS/CTS doesn't improve performance in mesh ad hoc networks [52, 53]. In Roofnet for example, the average throughput for a one hop route – which is the case of our experiment here - without RTS/CTS is 228.18kB/s whereas it is 166.37kB/s with RTS/CTS [53].

In the “dual-sender” experiment, B and C are not neighbors this means B does not receive the 802.11 broadcast from C and vice versa. D and A are the only neighbors of C.
A simulates a gateway node in Roofnet. B and C simulate two last hop routers on a route towards A. The goal of this experiment is to see how much traffic with 802.11b MAC one gateway can handle. It will help create an appropriate metric for the multipath protocol.
For this we will compare the throughput at A and the one at D. A receives 802.11 broadcasts from B and C whereas D only receives broadcasts from C.

4.1.2 Results

The two main factors to consider are the loss rate and the maximum achievable throughput.

4.1.2.1 Loss rate

During the single sender experiment we can notice that the loss rate is low especially when compared with the “dual sender” experiment. The average over all the ‘single sender’ experiments of the loss rate is 7.4% for B sending to A and 22.6% for C sending to A. The average over all the “dual sender” experiments of the loss rate for B sending to A is 50.4%, for C sending to A is 74.9%, for C sending to D is 11.7%. In the “dual sender” experiment there is an increase of 681% in the loss rate for the 802.11 broadcast sent from B to A and an increase of 331% for the loss rate from C to A. The average loss rate at a node like A which receives broadcasts from two sources is 62.65% and the one at a node like D which receives broadcasts from only one source is 11.7%, it is 5.35 times less.

	Loss Rate B=>A	Loss Rate C=>A	Loss Rate C=>D
Single Sender	7.4%	22.6%	/
Dual Sender	50.4%	74.9%	11.7%
Increased loss for ‘dual sender’	+681%	+331%	/

Figure 16: Results from the 802.11 broadcast

	B at A	C at A	C at D
Average RSSI	-28dBm	-32dBm	-26dBm

Figure 17: Average RSSI readings from the card.

From figure 18, we can see that node A has problems handling packets from two senders; it tends to lose a lot of packets from one source, here from source C. If we just look at the single sender experiment we notice that the loss rate for the 802.11 broadcast is nearly three times higher for the transmission from C to A than the one from B to C. From the Received Signal Strength Indications (RSSI) readings in figure 17 we notice that the signal strength of node B is much higher than the one of node C. One explanation for the results obtained above is the capture effect.

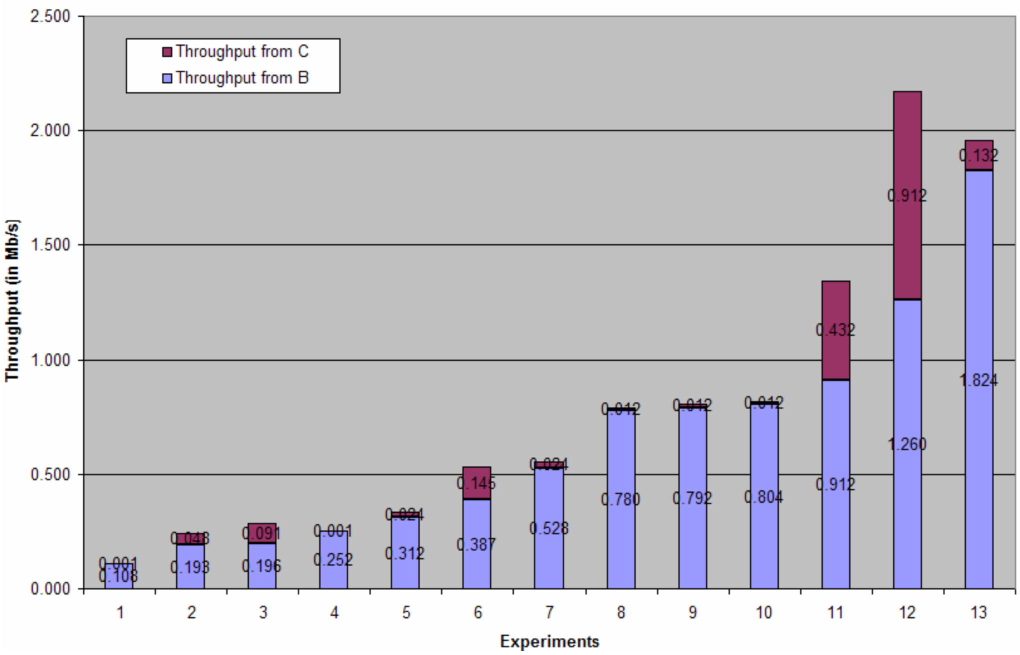


Figure 18: Throughput at A in the dual sender experiment.

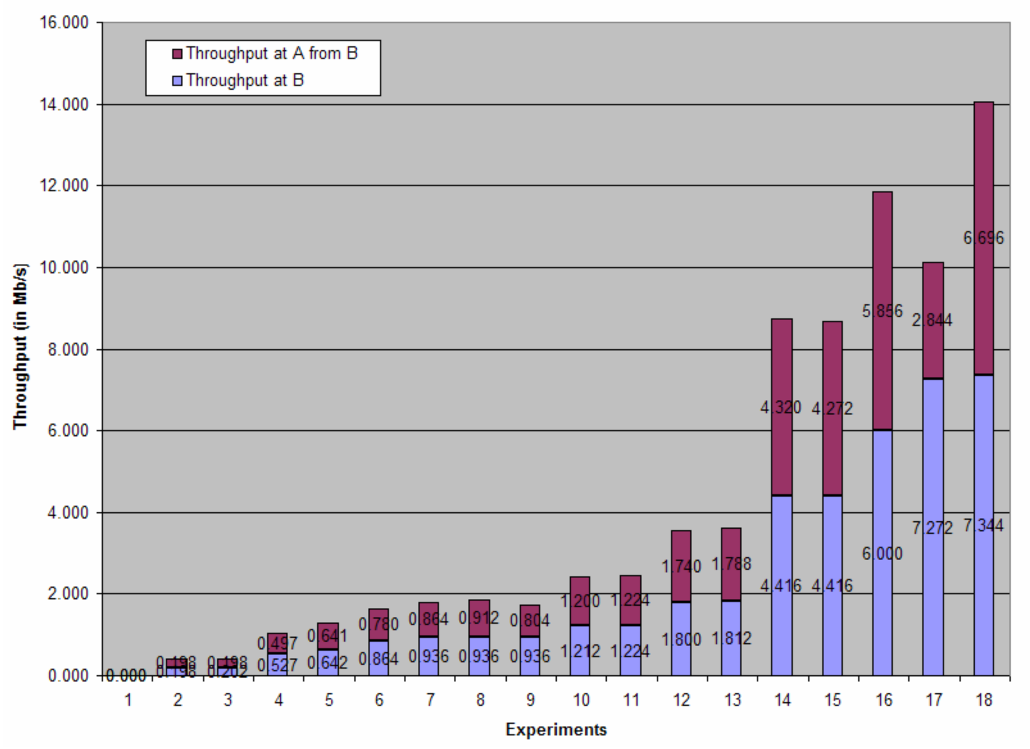


Figure 19: Throughput at A when B is sending.

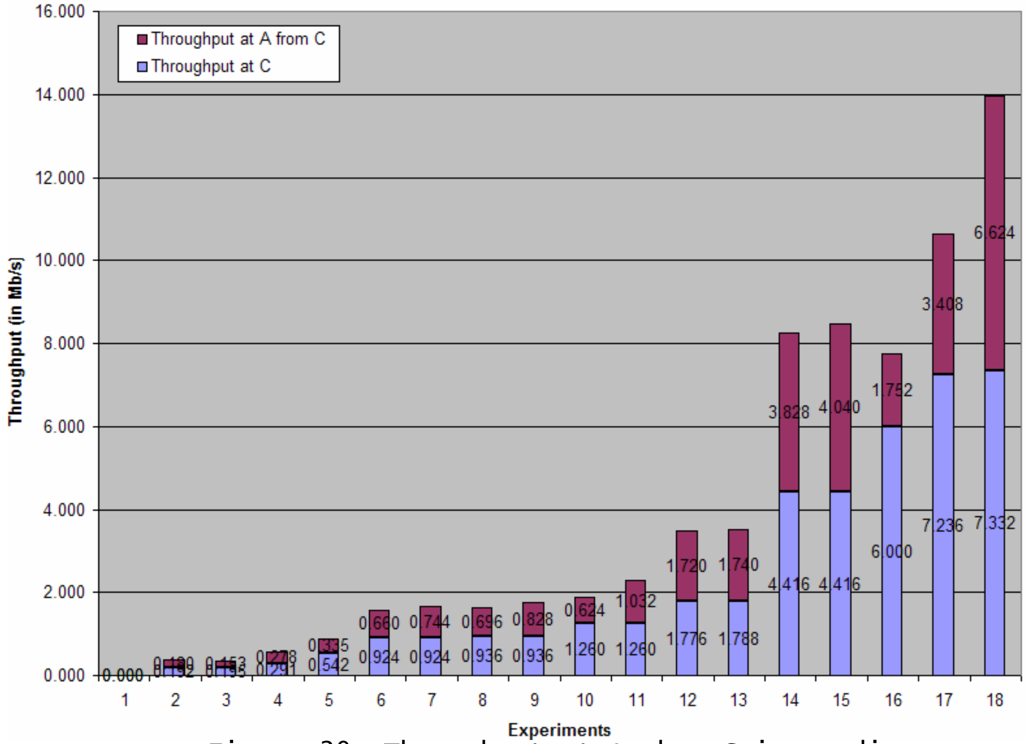


Figure 20: Throughput at A when C is sending.

4.1.2.2 Capture Effect

The capture effect in [36] is defined as a phenomenon, associated with FM reception, in which only the stronger of two signals at or near the same frequency will be demodulated. The complete suppression of the weaker signal occurs at the receiver limiter, where it is treated as noise and rejected. In 802.11 wireless networks in the case of multiple senders a receiver will receive the packet with the larger received power. It plays an important role in wireless transmissions as it reduces interference. However, it has a bad effect in our case as the receiver always tends to "capture" the packets with the larger received power in the case of concurrent transmissions.

4.1.2.3 Throughput considerations

In the "dual sender" the maximum throughput achieved is 1.8Mb/s for B and 2.9Mb/s for the aggregate throughput at A. However this maximum aggregate throughput is achieved with a 72% packet loss which is not acceptable. The best solution in terms of low loss rate and good throughput is obtained for a maximum aggregate throughput of 2.2Mb/s with a 13% packet loss. in [56] in a deeper and more detailed experiment the authors obtained throughput of 6.6Mbps which is 3 times higher than ours.

4.1.2.4 Conclusion

The conclusion of this experiment is that when considering 802.11b networks, packet loss is a relevant factor and the load at the gateway should be taken into account in the path metric. We have noticed that the gateway cannot handle traffic with rates higher than 2Mb/s with 802.11b; this is caused by the phenomenon called 'capture effect'.

4.2 Evaluation of M-RNR

4.2.1 The protocol M-RNR

Multipath RoofNet Routing (M-RNR) is based on RoofNet Routing (RNR). The objective of M-RNR is to spread the traffic according to a specific metric into multiple paths that are available for each source-destination pair. Motivated by the results in [44] we spread the traffic at the packet level granularity. The algorithm distributes the load into multiple paths according to the specific metric means that the routes with the best metric will see more packets than the others. M-RNR is a pro-active source-rated protocol inspired by RNR and similar in overall structure to MCL [45]. It performs its own measurement-based transmit bit-rate selection and chooses bit-rate aware and loss-rate aware routes selection using a routing metric derived from ETX [5]. It consists of two phases, *Route Discovery* and *Route Maintenance*.

4.2.1.1 Route Discovery

During the *Route Discovery* phase, a source node attempts to discover routes to a destination by flooding query packets. The queries propagate until they reach the target host. During the query propagation, each forwarding node only forwards one query for each source-destination pair. When the queries reach the target host, the destination generates a route response if the route in the query is better than anything valid seen before. If it sees successively better routes, it will forward multiple query responses.

4.2.1.1.1 Path Metric

Prior versions of RNR used estimated transmission count (ETX) [4] which favors routes with low loss rates which is more likely to be routes with high throughput. The current metric used in Roofnet with RNR is the Expected Transmission Time (ETT). ETT calculates the transmission time for a 1500 byte unicast packet at each of the following rates: 1, 2, 5.5, and 11Mb/s then takes the minimum value. It corresponds to the minimum achievable time to send a packet over a link. ETT takes into account 802.11b transmit bit-rates as well as loss rates.

4.2.1.1.2 Gateway Route Discovery

The proactive part of the description of M-RNR refers to the ‘dummy’ route discovery of gateways. Indeed every 15s for RNR and every 100ms for M-RNR the gateways broadcast advertisements. Every node receives information from all the gateways in the network, and then it creates a table with the following data: RNR IP address of the gateway, Ethernet IP address of the gateway, ETT metric, Gateway load, and last update time where the ‘RNR IP address’ of the gateway is not globally routable, ‘ETT metric’ is the path metric of the route from the gateway to the node, ‘Gateway load’ is the number of bytes sent and received at the gateway and last update is the time at which the last advertisement was received by the node.

The ‘Gateway load’ is a field which has been added to the original gateway advertisement mechanism of RNR in order to take into account the fact that a lot of packets are lost at the gateways when the sending rate is too high at it shown in the first experiment (cf. section 4.1)

4.2.1.1.3 RNR Packet format

The RNR packet header is as shown in figure 21.

version	version of M-RNR in use. It is actually version 10, because M-RNR is just the continuation of RNR.

type	purpose of the packet:
	`PT_QUERY = 0x01,`
	`PT_REPLY = 0x02,`
	`PT_DATA  = 0x04,`
	`PT_GATEWAY = 0x08`

nlinks	number of links included in the packet.
next	index of the next node who should process this packet.
flags	used to indicate errors or update for instance.
dlen	length of the data in the packet.
eth0ip	used in the gateway advertisement mechanism. The gateway puts in this field its own Ethernet IP address.
seq	sequence number.

seq2	used in the gateway advertisement mechanism. The gateway writes in this field the number of bytes received and sent since the last gateway advertisement sent.

Then for each link,

_from	RNR IP address on one side of the link.
fwd_metric	forward metric from _from to _to.
rev_metric	reverse metric from _from to _to.
seq	sequence number assigned to the link.
age	age since the last metric update for this link. With the sequence number and the age, old linkstates are prevented from floating around in the network.
_to	RNR IP address on one side of the link.

<table>
<tr><th>0-7</th><th>8-15</th><th>16-23</th><th>24-31</th></tr>
<tr><td>version</td><td>type</td><td>nlinks</td><td>next</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">checksum</td></tr>
<tr><td colspan="2">flags</td><td colspan="2">dlen</td></tr>
<tr><td colspan="4">eth0ip</td></tr>
<tr><td colspan="4">qdst</td></tr>
<tr><td colspan="4">seq</td></tr>
<tr><td colspan="4">seq2</td></tr>
<tr><td colspan="4">_from</td></tr>
<tr><td colspan="4">fwd_metric</td></tr>
<tr><td colspan="4">rev_metric</td></tr>
<tr><td colspan="4">seq</td></tr>
<tr><td colspan="4">age</td></tr>
<tr><td colspan="4">_to</td></tr>
</table>

Figure 21: M-RNR header

4.2.1.2 Data Transmission

4.2.1.2.1 General Description

There are two different mechanisms to send data over the network: one is to send data within the wireless network and one to send data outside the wireless network. For the first method, M-RNR and RNR are similar. Once the routes are established, the source node places the complete path to the destination in each packet's header and starts sending them to the destination. Intermediate nodes forward data packets according to the route specified by the packets themselves.

The mechanism to send data outside the network is the key difference between M-RNR and RNR. For this mechanism we define two sets of traffic: UDP or TCP traffic and the others. For all data which destination is outside the network and which are not UDP datagrams or TCP fragments the mechanism is similar to the one for the data sent within the network. That means that the best gateway is chosen in the table using the metric Estimated Transmission Time with Gateway load correction (GETT) which is going to be described below.
For UDP or TCP traffic, the data are spread over multiple paths towards the gateways. The concept of M-RNR is that multiple paths are only used on the forward path and a single path is used on the reverse path. To achieve this, the use of a designated gateway is necessary. Indeed each gateway must use a NAT because the RNR IP addresses are not routable. Reassembling is thus done at a specific gateway which is responsible for sending the reordered packets outside of the wireless network.

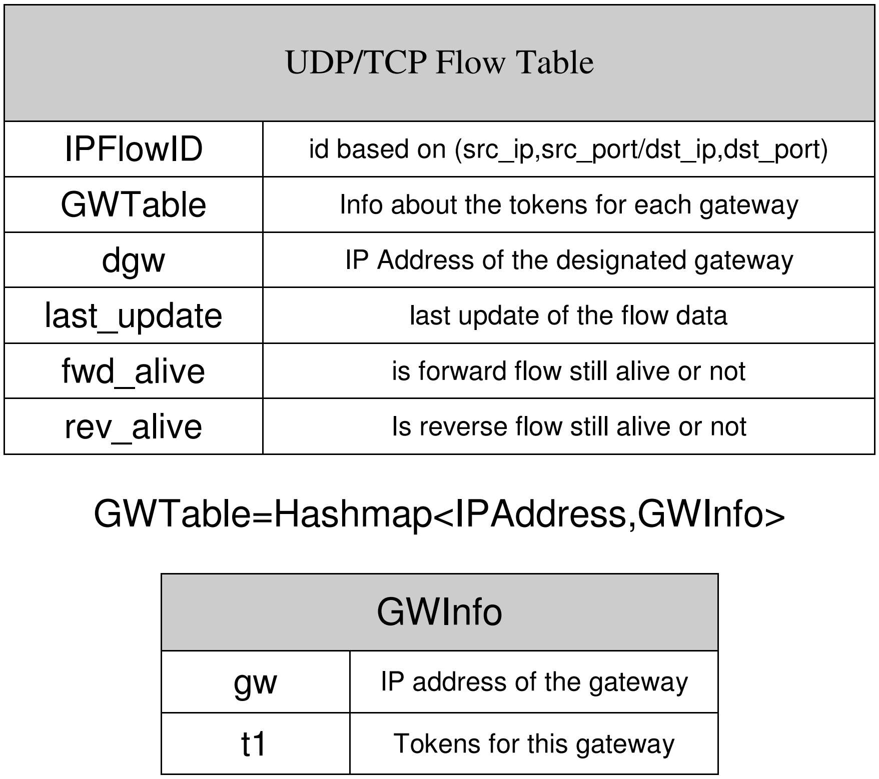
4.2.1.2.2 GETT

In the following, n is the number of paths used, L is the aggregate load at the gateway, and T the period of the gateway advertisement. The metric to choose the best n gateways is the following:
ETT is the time in μs it takes to transmit a 1500 bytes packet so $\frac{1.5\times10^6}{ETT}$ is the available bandwidth of the link in kB/s. $\frac{L}{T}$ is the load at the gateway in kB/s.
m = $\mathrm{Max}(0,\frac{1.5\times10^6}{ETT}-\frac{L}{T})$ with ETT in s, L in kB and T in seconds. Here

T is 0.1s.
When the throughput at the gateway is greater than 2Mb/s the metric should be 0 so we test for each gateway if L is larger than 250, if so, then GETT is set to 0.

4.2.1.2.3 The Gateway Table

For each new UDP or TCP flow an entry in the flow table is created, this entry in the flow table is updated every T seconds. The Gateway Table is shown in figure 22.



UDP/TCP Flow Table	
IPFlowID	id based on (src_ip,src_port/dst_ip,dst_port)
GWTable	Info about the tokens for each gateway
dgw	IP Address of the designated gateway
last_update	last update of the flow data
fwd_alive	is forward flow still alive or not
rev_alive	Is reverse flow still alive or not

GWTable=Hashmap<IPAddress,GWInfo>

GWInfo	
gw	IP address of the gateway
t1	Tokens for this gateway

Figure 22: TCP/UDP Flow Table

The IP flow Identification is unique, it is based on the source IP address, the source port, the destination IP address and the destination port. In order to achieve the load balancing policy, tokens are assigned to the gateways. When a packet is about to be sent the algorithm checks which gateway has the largest number of tokens and sends the packet towards this gateway. The GWTable gathers the information about the tokens for each gateway involved in the flow. The 'dgw' field indicates the IP address of the designated gateway. The use of a designated gateway is given below. Each new flow is randomly assigned a designated gateway which remains the same for the whole flow. The designated gateway is picked from among the best gateways. Each entry in the GWTable needs to be updated every T seconds in order to have always the latest information about the gateway load and the ETT metric. The 'last_update' field is used to keep track of these updates. The 'fwd_alive' and 'rev_alive' fields are only used for TCP traffic. The forward flow is alive until the sender sets the flag RST or FIN. The reverse flow is alive until the recipient sets the flag RST or FIN. When both of the fields 'fwd_alive' and 'rev_alive' are set to false, the data concerning the flow are erased.

4.2.1.2.4 The load balancing algorithm

Once the n best gateways are selected, the packets are balanced over the n paths according to a deficit round robin algorithm. Tokens are associated to each gateway, it enables to determine over what path to send the packets. Let's consider:

* G_i with $i \in \{1..n\}$ is the ith best gateway.

* s_k the size of a packet k (where $k \geq 0$).

* m_i the GETT metric with $i \in \{1..n\}$.

* t_i^k the number of tokens for G_i before having sent packet k and t_i^0 is the number of tokens at the first packet of a new flow or when the metric is reinitialized (e.g. every T seconds). Therefore,

$$t_i^0 = \frac{m_i}{\sum_{j=1}^{n} m_j} \times s_0$$

For every packet which has to be sent, the load balancer module makes a decision of over what path to send the packet. For packet k and for the gateway i the number of tokens is updated according to the following equation: $t_i^k = t_i^k - t_i^0 \times s_k$. For packet k, if $t_\alpha^k = \max_i(t_i^k)$ then the packet will be sent towards G_α and the tokens corresponding to G_α will be updated:

$$t_\alpha^k = t_\alpha^k - s_k$$

At this point the load balancer module marks the IP packet with the Ethernet IP address of the designated gateway and with the RNR IP Address of the gateway towards which the packet is being sent. Eventually the packet is encapsulated within a RNR-packet and sent over the network.

4.2.1.2.5 At the gateways

When the packets reach a gateway they are not sent directly to their final destination outside the network. A designated gateway for a flow is the one which forwards all the packets for this flow to its final destination. So basically all the gateways forward to their Ethernet interface through a UDP socket all the packets for the given flow they have received on their wireless interface. All potential designated gateways are listening to the port 5212.

4.2.1.3 Route Maintenance

ETT metrics are updated in different ways. First, ETT probes are sent out periodically by the ETT metric module. During the gateway advertisement phase the ETT metric are also updated.

Link measurements expire after a set amount of time and consequently nodes won't forward queries with stale link data. Nodes generate a query again if their metric to the destination is worse than twice the best observed metric. The factor of two is to prevent spurious requeries, since metrics are expected to change slightly over time.

4.2.2 M-RNR in the indoor network

We are going to evaluate the protocol on the new indoor network [5] at the Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT.

4.2.2.1 The Indoor network

The indoor network is installed on the 7th, 8th, and 9th floor of the Stata Building.

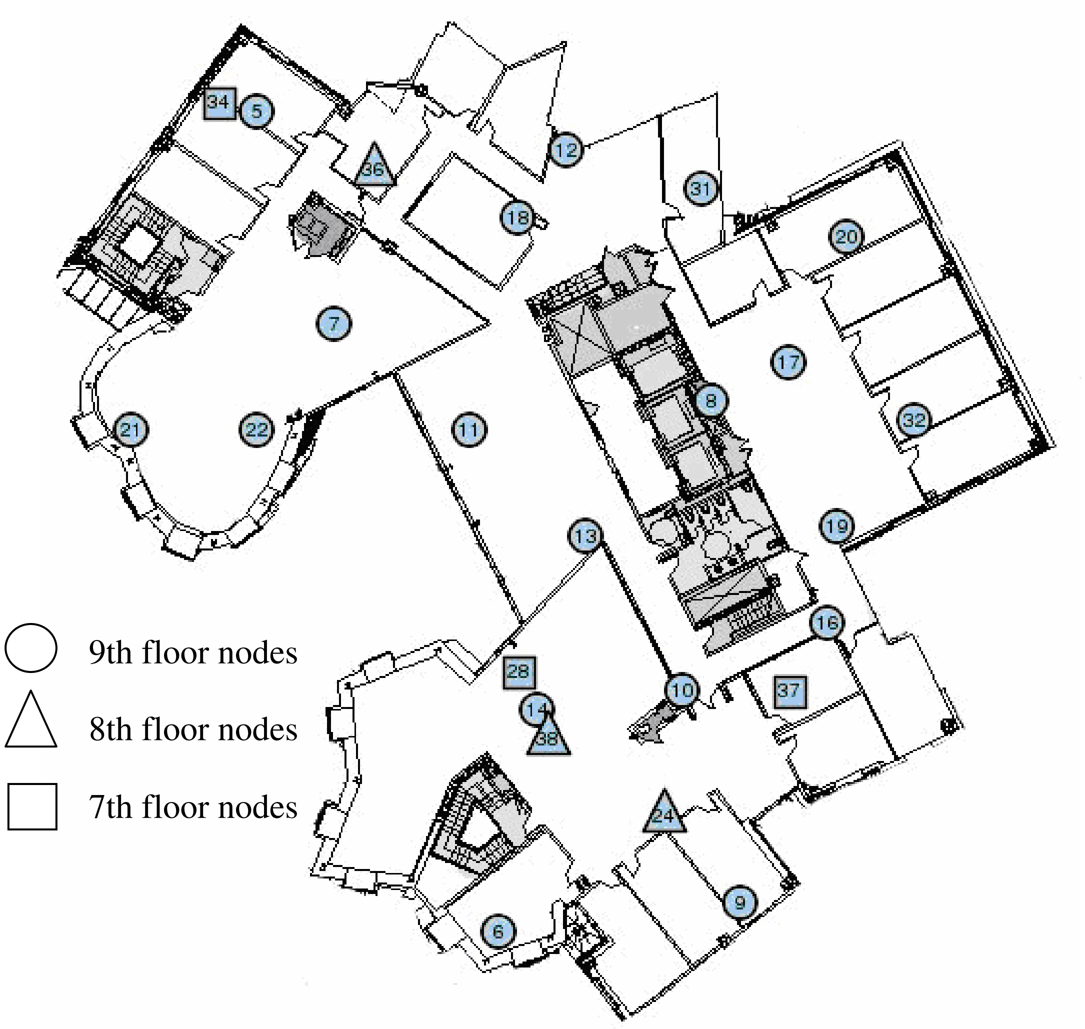


Figure 23: indoor network.

The nodes which can be used for the experiments are the circles in figure 23. The triangles represent the 8th floor nodes while the squares represent the 7th floor nodes. Most routes between any of these nodes are one, two, or three hops.

The indoor nodes are desktop machines shown on figure 24.

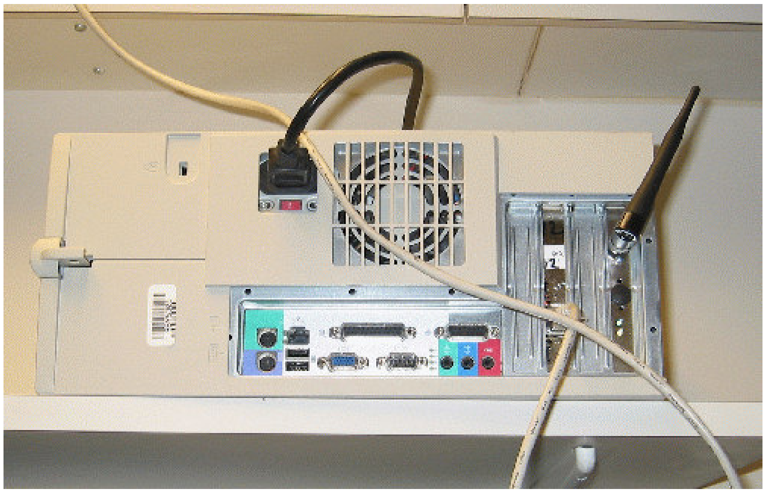


Figure 24: Indoor network node

These nodes are using the Atheros 802.11b/g chipset. In all the experiments presented, the cards transmit at 2.462Ghz at +23dBm (200mW) transmission power. The cards are used in 802.11g mode. All the remarks concerning the Roofnet architecture are valid here:

- No mobile nodes: the topology is static.
- The nodes do not communicate between each other, they only try to reach hosts on the Internet through the gateways.
- All UDP/TCP connections originate from nodes in the Roofnet, as we assume NAT is enabled.
- The pseudo IBSS mode is used, CCA is disabled, Carrier sense is enabled and RTS/CTS is disabled.
- All the gateways are connected to 100Mps links.

4.2.2.2 Experiment description

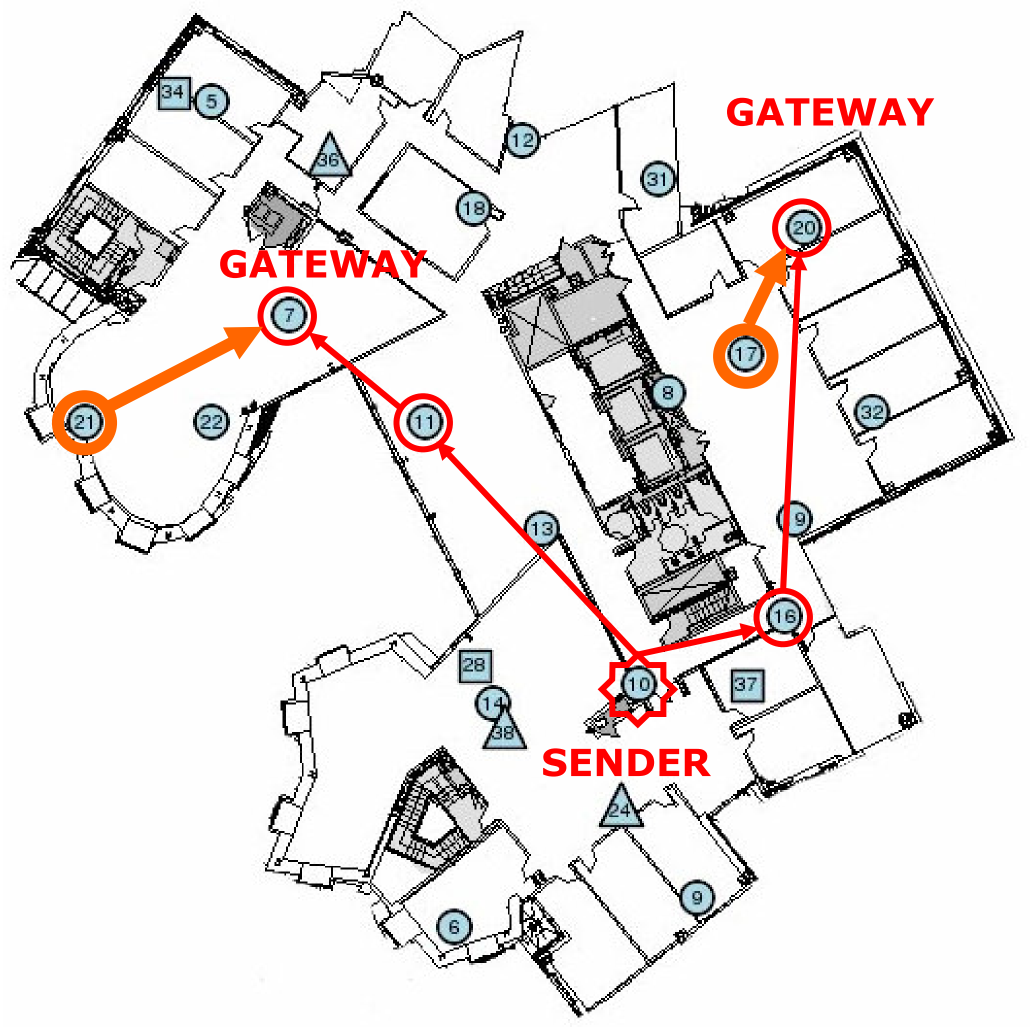


Figure 25a: Map with the nodes used for the experiment.

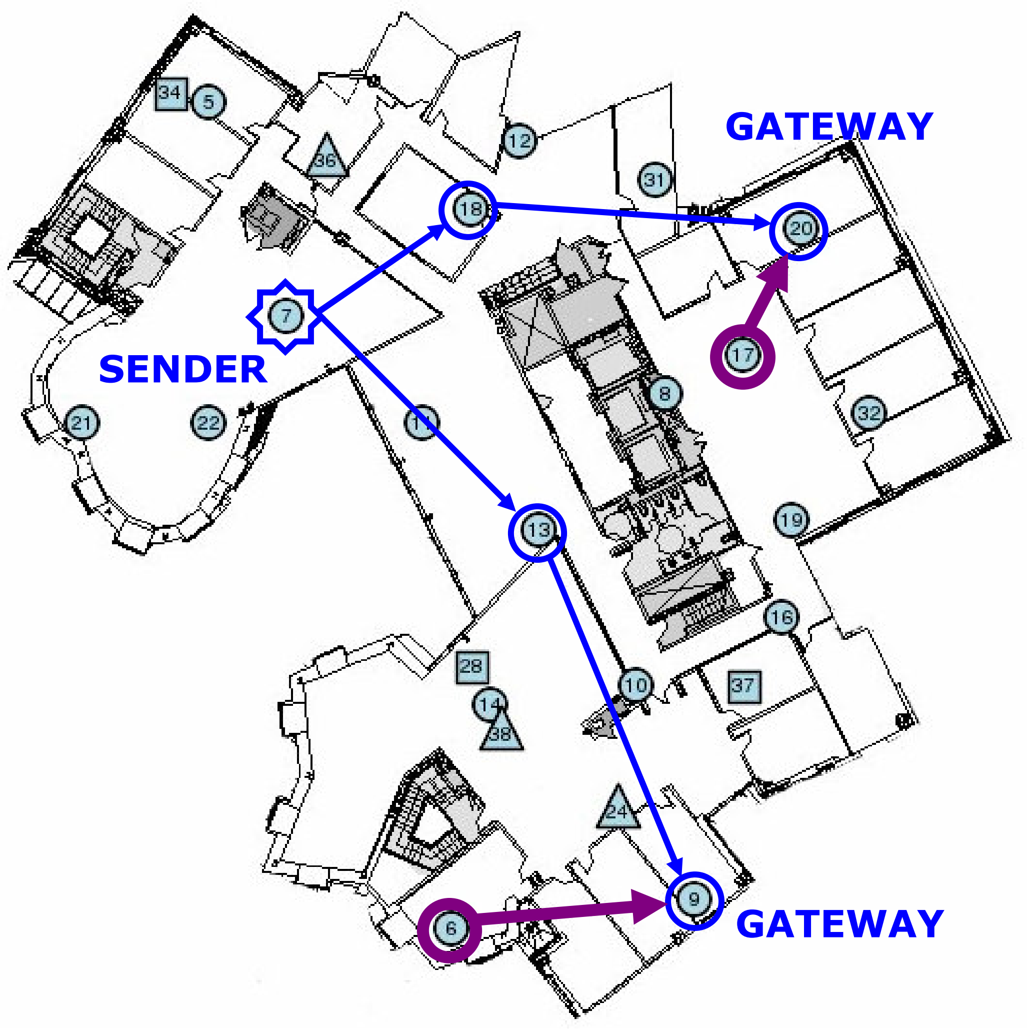


Figure 25b: Map with the nodes used for the experiment.

As it is shown in figure 25a and 25b, the experiment is realized with two subsets of nodes. One node, number 10 on figure 26 is configured to be the sender and two nodes, 7 and 20 are configured to be gateways. 11 and 16 are two intermediate nodes. In the second subset 7 is the sender, 9 and 20 are the gateways and 13 and 18 are two intermediate nodes. 13, 22 and 17 for the first subset, and 31 and 11 for the second subset have also M-RNR running i.e. they are just forwarding gateway advertisements and ETT probes. The four routes 10-11-7, 10-16-20, 7-13-9, and 7-18-20 remain stable for all the experiments. The metallic structure (including the lift and the stairway to the floor) in the middle of the floor prevents 16 and 20 from being direct neighbors with 7 and 11, and for the second subset neither 18 nor 20 are neighbors with 13 and 9.

There were no other experiments run on these nodes by other researchers in the lab. Before each experiment, using a sniffer we checked if no other wireless projects were running some 802.11b experiments at the same time as ours. An agreement was made with the other projects in the lab in order not to run experiments at the same time. On the wireless cards we are using we don’t have the opportunity to choose between 802.11b/g and 802.11g so we will be working under 802.11b/g mode.

We use a UDP traffic generator [49] at nodes 10 and 7 to send datagrams to a machine outside the network. On this destination machine, we use a UDP sink. During all the experiments, the gateways see traffic from both nodes 10 and 17 for 20, from both 10 and 21 for 7, from both 17 and 7 for 20, and from both 7 and 6 for 9.

The experiment is divided in two phases. In the first phase, the multipath protocol M-RNR is used whereas in the second phase the single path protocol RNR is used with 20 as the gateway. In each phase the results were obtained using a 15 seconds one-way UDP transfer; throughput is measured in terms of data bytes delivered to the receiving application. Each transfer is preceded by a 30 second quiet interval during which the sender sends 64-byte pings once per second to establish the routes. The parameters of the experiment for the first subset of nodes are summarized in figure 26.

	1st phase	2nd phase
Datagram size	1300B	1300B
Duration of the experiments	45s	45s
Number of gateways	2 (nodes 7,20)	1 (node 20)
Gateway Ad Period	100ms	15s

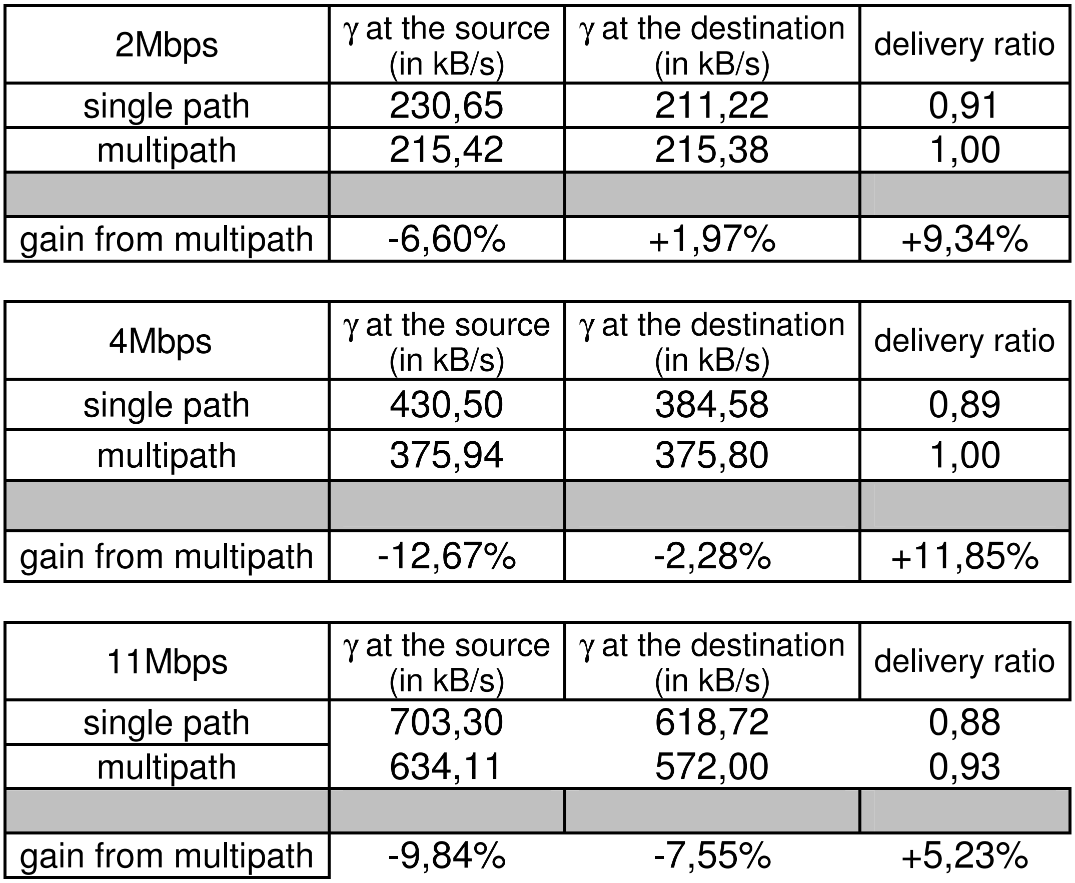
Figure 26: Parameters for the UDP measurements.

4.2.2.3 Results

The first thing to notice is that there is no problem with the saturation we observed before with 802.11b. Even when two sources are sending to one receiver, the loss rate is not even comparable with the one we obtained for 802.11b. Our goal when implementing the protocols was to maximize the throughput and minimize the packet losses. Below we look at the results of these experiments.

We have divided the results into three parts corresponding to the three sending rates we have set at the UDP traffic generator: 2Mbps, 4Mbps, and 11Mbps. Indeed for rates higher than 11Mbps, the throughput was stagnating; i.e., with a two-hop links we could not achieve higher throughput. In our results we have shown the throughput at the source and at the destination, the latter being a machine outside the wireless network.

Figure 27 represent the average throughput (γ) at the source and at the destination and the average delivery ratio over the series of experiments with perturbation. The means are taken of the results of the two subsets of nodes. Perturbation means that 21 and 17 or 6 and 17 are sending UDP datagrams in the case of multipath and only 17 in the case of single path towards the destination at the same time when 10 or 7 is sending.



2Mbps	γ at the source (in kB/s)	γ at the destination (in kB/s)	delivery ratio
single path	230,65	211,22	0,91
multipath	215,42	215,38	1,00
gain from multipath	-6,60%	+1,97%	+9,34%

4Mbps	γ at the source (in kB/s)	γ at the destination (in kB/s)	delivery ratio
single path	430,50	384,58	0,89
multipath	375,94	375,80	1,00
gain from multipath	-12,67%	-2,28%	+11,85%

11Mbps	γ at the source (in kB/s)	γ at the destination (in kB/s)	delivery ratio
single path	703,30	618,72	0,88
multipath	634,11	572,00	0,93
gain from multipath	-9,84%	-7,55%	+5,23%

Figure 27: Results from the UDP throughput experiments

What can be inferred from the tables above is that one of the two goals is achieved and the other one is not achieved or at least not fully. Indeed we can see that multipath routing minimizes the packet losses, the delivery ratio is around 10% higher for rates lower than 3.2Mb/s and is around 5% higher for higher rates.

We can also see that for low rates (around 2Mb/s) with multipath the throughput is slightly better than the one with single path. However for higher rates, the throughput is worse with multipath. The maximum throughput obtained with these experiments was with a single path. With a two-hop route the maximum throughput obtained is 687kB/s which is nearly 5.5Mb/s. The maximum throughput obtained with multipath is 634kB/s which is nearly 5.1Mb/s.

We can also notice that the sending rates are different for multipath routing and single path routing. But if we look at the gain from multipath numbers for different rates it can be inferred that the module in click in charge of sending the packets on the wireless interface has some bugs and need to be corrected.

4.2.2.4 Interpretations

Unfortunately the main reason for implementing this protocol was not achieved; indeed the maximum throughputs were obtained with a single path protocol. One explanation for this is the high amount of overhead generated by the gateway advertisements every 100ms. We decreased the advertisement period in order to always have the latest load at the gateway and thus take into account the saturation of the gateways. However, as we have noted it at the beginning of the results section, with 802.11g the load at the gateways is no longer relevant (unlike the case of 802.11b). Hence gateway load can be removed from the metric. At lower data rates we see that the throughput is slightly better than for single paths. It can be inferred from this result that the gateway advertisement has a low impact at lower rates because the network is not congested. At higher rates when the network starts to become congested, the overhead due to the gateway advertisements tends to *decrease* the performances of the multipath protocol in terms of throughput.

The second reason this protocol was implemented was to minimize packet loss. The load balancing policy with multipath done via the ETT metric takes into account the loss rate of the links. The multipath protocol tends to eliminate the congestion and therefore it improves the delivery ratio.

The results were obtained with a UDP traffic generator at the source and a UDP sink at the destination. No specific TCP traffic measurements because the previous results obtained with UDP were not good enough. Indeed the tests made with TCP and the current version of M-RNR gave throughput no higher than 60kB/s. There were also a lot of problems of reordering due to the absence of reordering at the designated gateway. It could not be done due to other activities in the lab which prevented us from running tests on the indoor network. We leave it as a future work.

The indoor network is like Roofnet, but inside, it uses commodity PCs & 802.11 hardware, omni-directional antennas. Although not identical, the results on the indoor network were expected to be indicative of the

Roofnet. The average throughput in Roofnet with 2 hops is 81kB/s, with 802.11g we managed to obtain throughputs up to 600kB/s. Therefore we might consider for the Roofnet 802.11g instead of 802.11b. Indeed 802.11g can function outdoors even better than 802.11b when using 2.4 GHz as it is more robust to multipath.

5 Conclusions

5.1 Conclusion

In this report we have presented a new routing protocol inspired by RNR, i.e., the Roofnet routing protocol with its specific metric ETT. A key distinction from previous work is that it focuses on rooftop, i.e., static networks and that the load balancing policy uses the ETT metric which takes into account the loss rate of the links. This master's thesis project yields some interesting results about multipath routing protocol with load balancing in wireless 802.11g ad hoc network. Thanks to the load balancing policy, the performance in terms of delivery ratio are improved compared to that for the single path routing protocol. However, the maximum throughput is obtained with the single path routing protocol.

5.2 Future work

There is still a lot to explore in the area of multipath routing in wireless ad hoc network. Due to the properties of the architecture of Roofnet, one omni-directional antenna per node is used. Multiple paths are therefore not independent; a way to counteract this problem could be to give up 802.11b and use a multi-radio MAC. In this scenario, a network node has multiple radios each with its own MAC and physical layers. Communications in these radios could be independent. Thus, a virtual MAC protocol such as the multi-radio unification protocol (MUP) [55] on top of a specific could be used to coordinate communications in all channels. In fact one radio can have multiple channels. This would eliminate the problem of coupling at the source.

Another open problem is the reordering of TCP fragments at the designated gateway. However there are ways to reorder the packets.

In the case of 802.11g as we have seen earlier, there is no saturation at the gateways so the current load at the gateway can be removed from the gateway advertisements.

Implementing 802.11g is another work to be done. It is well known that 802.11g is more robust vis-à-vis multipath thanks to the OFDM technology. Roofnet can therefore draw a lot of benefits from it in terms of throughput and delivery ratio.

References

[1] D. Katabi, S. Kandula, A. Qureshi, and S. Sinha “T*eXCP: Intra-Domain Online Traffic Engineering with an XCP-Like Protocol”*, March 2004. http://nms.lcs.mit.edu/~dina/texcp.html

[2] P. Pham and S. Perreau, "*Increasing The Network Performance Using multipath Routing Mechanism With Load Balance*", Proceedings of the Workshop on the Internet, Telecommunications and Signal Processing, Wollongong, December 2002.

[3] Y. Ganjali and A. Keshavarzian , “*Load Balancing in Ad Hoc Networks: Single path Routing vs. multipath Routing”*, *Proceedings of the IEEE INFOCOM'04*. Hong Kong

[4] MIT Roofnet, http://www.pdos.lcs.mit.edu/roofnet/, 2002.

[5] Douglas S. J. De Couto, Daniel Aguayo, Benjamin A. Chambers, and Robert Morris, "*Performance of multihop wireless networks: Shortest path is not enough*," in Proceedings of the First Workshop on Hot Topics in Networks (HotNets-D, Princeton, New Jersey, October 2002, ACM SIGCOMM.

[6] B. A. Chambers, "The grid roofnet: a rooftop ad hoc wireless network," Master's thesis, Deparment of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology - MIT, June 2002.

[7] Cisco Aironet Antenna Reference Guide. Cisco Systems Inc., April 2002. http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/agder_rg.h tm.

[8] Click documentation index. http://pdos.lcs.mit.edu/click/doc/, August 2004

[9] http://www2.rad.com/networks/1994/osi/layers.htm, June 2004.

[10] Jean Tourrilhes, *Wireless LAN Resources, March 2003* http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/

[11] http://www.wavewireless.com/classroom/whitepapers/FHSSvDSSS.pdf, May 2000.

[12] Jun Miao, U Teng Wong, and Ji Hui Zhang, "*Survey of Multipath Routing Protocols for Wireless Mobile Ad Hoc Networks*", May 2002. http://ihome.ust.hk/~miaojun/project/comp660G.doc

[13] V.D. Park and M.S Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks", INFOCOM '97, *Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Driving the Information Revolution. , Proceedings IEEE*, Volume: 3, March 1997, pp 1405 -1413.

[14] C.C. Chiang, H.K. Wu, W. Liu, and M.Gerla, "*Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel*", *The IEEE Singapore International Conference on Networks*, November 1997, pp197-211.

[15] S. Murthy and J.J. Garcia-Luna-Aceves, "A*n Efficient Routing Protocol for Wireless Networks*", ACM Mobile Networks and Applications Journal, Special issue on Routing in Mobile Communication Networks, Volume: 1, No. 2, September 1996.

[16] C.E. Perkins and E.M. Royer, "A*d hoc On-Demand Distance Vector (AODV) Routing*", IETF Internet Draft, draft-ietf-manet-aodv-08.txt, March 2001

[17] D. Johnson and D. Maltz, "*Dynamic source routing in ad hoc wireless networks*", Mobile computing, chapter 5, Kluwer Academic, August 1996

[20] M. Scott Corson and A. Ephremides, "*A distributed routing algorithm for mobile wireless networks*",, *ACM Baltzer, Journal of Wireless Networks*, 1(1) May 1995, pp61-81.

[22] C.K. Toh, "*Associativity-based routing for ad hoc mobile networks*", *Wireless Personal Communication*, vol. 4, February 1997, pp103-139.

[23] R. Dube, C.D. Rais, K.Y Wang, and S.K. Tripathi, "*Signal stability-based adaptive routing (SSA) for ad hoc mobile networks*", IEEE Personal Communications, Volume: 4 Issue: 1 , Feb. 1997, pp 36 –45.

[24] A. Nasipuri and S.R. Das, "*On-Demand Multipath Routing for Mobile Ad Hoc Networks*," Proceedings of IEEE ICCCN'99, Boston, MA, Oct. 1999, pp. 64-70.

[25] K. M. Mahesh, and S.R. Das "*On-demand Multipath Distance Vector Routing in Ad Hoc Networks*".*Proceedings of* IEEE ICNP, November 2001.

[26] M. Gerla and S.J. Lee, "*Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks* ," in Proceedings of ICC'01, Helsinki, June 2001.

[27] Matthew Roughan, Mikkel Thorup, and Yin Zhang, "*Traffic Engineering with Estimated Traffic Matrices*", Internet Measurement Conference, Miami, June 2003
http://www.research.att.com/~albert/tomo-gravity/Papers/ospf_traffic_matrices.pdf

[28] A. Elwalid, Low C. Jin, and I. Widjaja, "*Mate: Mpls adaptive traffic engineering*", In Proceedings of IEEE INFOCOM 2001, November 2001, pp 1300-1309.
http://www.eecs.umich.edu/~chengjin/infocom01_mate.pdf

[29] Dina Katabi, Mark Handley, and Charles Rohrs, "*Internet Congestion Control for Future High Bandwidth-Delay Product Environments.*" ACM Sigcomm 2002, August 2002.
http://ana.lcs.mit.edu/dina/XCP/

[30] TCP-PR, TCP for Persistent Packet Reordering, October 2003.
http://www-rcf.usc.edu/~junsool/tcp-pr/tcp-pr.html

[31] A. Tsirigos and Z.J. Haas. "*multipath routing in the presence of frequent topological changes.*" IEEE Communications Magazine, November 2001, pp 132-138.

[32] L. Wang, et al., "*Multipath source routing in wireless ad hoc network*" in Canadian Conf. Elec. Comp. Eng., vol. 1, 2000, pp. 479-83.

[33] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu "I*mpact of Interference on Multi-hop Wireless Network performance*" in MobiCom'03, September 14-19, 2003, San Diego, USA, pp 66-80.

[34] A. Srinivas and E. Modiano "*Minimum Energy Disjoint Path Routing in Wireless ad hoc Networks*"in MobiComí03, September 14-19, 2003, San Diego, USA.

[35] D. Sidhu, R. Nair, and S. Abdallah. "*Finding disjoint paths in networks"*. In Proceedings of SIGCOMM 1991, August 1991,pp 43-51.

[36] Federal Standard 1037c, http://glossary.its.bldrdoc.gov/fs-1037/fs-1037c.htm, February 1996.

[37] MIT Laboratory for Computer Science, http://www.lcs.mit.edu/

[38] Alberto Cerpa, Naim Busek, and Deborah Estrin. *“SCALE: A Tool for Simple Connectivity Assessment in Lossy Environments.”* Technical Report 0021, UCLA Center for Embedded Network Sensing, Sep 2003

[39] Chiping Tang and Philip K. McKinley ,”*Modeling multicast packet losses in wireless LANs*”,Proceedings of the 6th international workshop on Modeling analysis and simulation of wireless and mobile systems, November 2003, pp 130-133.

[40] Padmini Misra, Routing protocols for Wireless Networks, February 2004. http://www.cse.ohio-state.edu/~jain/cis788-99/ftp/adhoc_routing.pdf

[41] Ewgenij Gawrilow, Olaf Jahn, Rolf H. Möhring, Martin Oellrich, and Andreas S. Schulz, “*Disjoint Routing in Telecommunication Networks*”, June 2004, http://www.math.tu/berlin.de/coga/research/disjoint_routing/

[42] Krista Gettle, http://www.sims.berkeley.edu/~kristag/portfolio/, University of California at Berkeley, October 30, 2003.

[43] Jack Glas, “*The Principles of Spread Spectrum Communication*”, August 29, 1996 http://www.airlinx.com/index.cfm/id/1-10.htm.

[44] R. Krishan and J. Silvester, “*Choice of allocation granularity in multi-path source routing schemes*” in *IEEE INFOCOMM’93*, vol. 1. IEEE, 1993, pp. 322–29.

[45] R. Draves, J. Padhye, and B. Zill, ”*Comparison of Routing Metrics for Static Multi-Hop Wireless Networks*”, ACM SIGCOMM, Portland, OR, August 2004.

[46] MIT CSAIL PDOS indoor network, http://grand.csail.mit.edu/, june 2004.

[47] James McPherson, “*The tale of the tape: 802.11g vs. 802.11b*”, August 19th, 2004. http://techrepublic.com.com/5100-6350-5309224.html

[48] Jim Zyrenm, Eddie Enders, and Ted Edmonson “*IEEE 802.11g offers higher data rates and longer range*”, 10 December 2002, Intersil White papers.

[49] Sebastian Zander, June 2002, http://www.fokus.gmd.de/research/cc/berlios/employees/sebastian.z

ander/private/udpgen

[50] David A. Beyer , Mark D. Vestrich , and J. J. Garcia-Luna-Aceves, "*The rooftop community network: free, high-speed network access for communities, The first 100 feet: options for Internet and broadband access"*, MIT Press, Cambridge, MA, 1999

[51] http://www.dsl-service-dsl-providers.info/boston.html, 2005.

[52] K. Xu, M. Gerla, and S. Bae. "*Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks*" Ad hoc Network Journal, 1997

[53] J. Bicket, S. Biswas, D. Aguayo, and R. Morris, "*Architecture and Evaluation of the MIT Roofnet Mesh Netwok*", January 2005.

[54] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, and Robert Morris, "*Link-level Measurements from an 802.11b Mesh Network"*, SIGCOMM 2004, Aug 2004.

[55] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "*A multi-radio unification protocol for IEEE 802.11 wireless networks*", in: International Conferences on Broadband", Networks (BroadNets), 2004.

[56] Enrico Pelleta and Héctor Velayos, "*Performance measurements of the saturation throughput in IEEE 802.11 access points",* to appear in Proc. of IEEE WiOpt 2005, Trentino, Italy, April 2005.

Appendix

List of abbreviations

2FSK	Binary Frequency Shift Keying
4FSK	Four level Frequency Shift Keying
ABR	Associativity Based Routing
AM	Amplitude Modulation
AODV	Ad hoc On demand Distance Vector
AOMDV	Ad hoc On demand Multipath Distance Vector
CCA	Clear Channel Assesment
CCK	Complementary Code Keying
CGSR	Cluster Head Gateway Switch Routing
CSAIL	Computer Science and Artificial Intelligence Laboratory
CSMA/CA	Carrier Sense Multiple Access/Congestion Avoidance
CSMA/CD	Carrier Sense Multiple Access/Congestion Detection
DG	Designated Gateway
DHCP	Dynamic Host Configuration Protocol
DS-CDMA	Direct Sequence Code Division Multiple Access
DSDV	Destination Sequence Distance Vector
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
ETT	Estimated Transmission Time
ETX	Estimated Transmission count
FCC	Federal Communications Commission
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
GETT	Estimated Transmission Time with Gateway load correction
IBSS	Independent Basic Service Set
IP	Internet Protocol
ISI	Inter Symbol Interference
ISM	Industrial Scientific Medical
LCS	Laboratory of Computer Science
LLC	Logical Link Control
LMR	Lightweight Mobile Routing
LP	Linear Programming
MAC	Media Access Control
MDSR	Multipath Dynamic Source Routing
MPLS	Multi Protocol Label Switching
M-RNR	Multipath RoofNet Routing
MRP-LB	Multipath Routing Protocol with Load Balancing
MSR	Multipath Source Routing

NAT	Network Address Translation
NMS	Network and Management Systems group
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnect
OSPF	Open Short Path First
PBCC	Packet Binary Convolutional Coding
PDOS	Parallel and Distributed Operating Systems group
PM	Phase Modulation
QPSK	Quadrature Phase Shift Keying
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RSSI	Received Signal Strength Indications
RTS/CTS	Request To Send/Clear To Send
RTT	Round Trip Time
SFLAN	San Francisco Local Area Network
SMR	Split Multipath Routing
SNR	Signal to Noise Ratio
SSR	Signal Stability Routing
TCP	Transport Congestion Protocol
TDMA	Time Division Multiple Access
TORA	Temporarily Ordered Routing Algorithm
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WRP	Wireless Routing Protocol
XCP	eXplicit Congestion Protocol
ZRP	Zone Routing Protocol

IMIT/LCN 2005-03

www.kth.se