Quality of service and routing in wireless mesh networks

Usman Ashraf

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par l' *Institut National des Sciences Appliquées*

Discipline : Systèmes Informatiques

Présentée et soutenue par

Usman Ashraf

Le 8 avril 2010

Qualité de Service et Routage dans les Réseaux Maillés Sans Fil

---

JURY

Président :	Michel Diaz	LAAS-CNRS
Rapporteurs :	Andrzej DUDA	INP-Ensimag
	David SIMPLOT-RYL	Université de Lille 1
Examinateurs :	Edmundo MONTEIRO	University of Coimbra
	Slim ABDELLATIF	Université de Toulouse (INSA)
	Guy JUANOLE	Université de Toulouse (Paul Sabatier)

École Doctorale : École Doctorale Systèmes
Unité de Recherche : Laboratoire d'Analyse et d'Architecture des Systèmes LAAS-CNRS
Directeurs de Thèse : Slim Abdellatif, Guy Juanole

Dedicated to my parents, Muhammad Ashraf (late) and Razia Ashraf.....

Acknowledgements

I would like to express my deepest thanks and gratefulness to Allah Almighty who provided me the opportunity to pursue research in the exciting domain of wireless mesh networks in this strange and beautiful country. It is only with His help and His guidance that I have accomplished this milestone.

I would like to thank Andrzej Duda and Simplot-Ryl for kindly accepting to review my thesis and for being part of the jury and I would also like to express my gratitude to Michel Diaz and Edmundo Monteiro for being part of my jury. I value the insightful and comprehensive feedback of the reviewers as well as the jury members on my dissertation.

I am grateful to my advisors Slim Abdellatif and Guy Juanole who helped me during the long and difficult phases of the doctorate. Their guidance and feedback, and their emphasis on high standards of research significantly improved the quality of this dissertation.

I would also like to express gratitude to my colleagues Mohamed El Masri, Ihsan Tou and Ahmed Akl for their support. Mohamed El Masri has been a constant source of help during my thesis and I appreciate his help in almost every aspect of my stay here in LAAS-CNRS.

For the wireless mesh testbed, a lot of work was required. I would like to acknowledge the long hours of help put in by Ghassen Abassi during the experimental phase of my thesis, in particular during the deployment of the testbed.

Last but not the least, I would like to express my gratitude to my family. They have been a constant and tireless source of support for me and their support and prayers played a key role in enabling me to achieve this significant milestone in my life.

Toulouse, 13 avril 2010.

O Lord, thy sea is so large and my boat is so small....

Abstract

Wireless mesh networks are a promising technology for providing *last-mile* broadband wireless Internet to a large number of users spread across large geographical regions. Due to their peculiar limitations and the increasing demand of users for high performance (high throughput, low delays etc), mesh networks have attracted the attention of researchers world-wide. Towards this goal, this dissertation contributes in several areas of Routing and Quality-of-Service provisioning in IEEE 802.11-based wireless mesh networks. Chapter 1 introduces wireless mesh networks and their architectural and functional components. The difference between mesh networks and traditional wireless multi-hop networks is emphasized. A comprehensive background study of routing and QoS solutions for multi-hop wireless networks is presented with an emphasis on mesh-specific solutions.

Chapter 2 presents our first contribution : *route selection* in wireless mesh networks. A primary research problem in mesh networks is to find the *"best"* available route between a pair of mesh routers. Recent research shows that selecting the *shortest path* is a poor decision as it does not take into account other factors pertaining to link quality. We propose an efficient routing metric - *Expected Link Performance* metric (ELP) which considers a number of factors including link loss ratio, link interference, and link capacity to find the *"best"* route between a pair of mesh routers. Performance evaluation of ELP is carried out against contemporary routing metrics. A part of metric is also evaluated on a mesh testbed. An extension of the metric is proposed for the special case of mesh traffic directed at gateways. A gateway discovery protocol is also proposed which integrates the extended metric and performance evaluation is carried out against traditional gateway and gateway-route selection schemes.

Chapter 3 presents our second contribution : *route maintenance* in mesh networks. After route selection, the next research problem that we consider is the maintenance of that route. The route maintenance mechanism of on-demand routing protocols in 802.11-based mesh networks is inaccurate and results in frequent route breakages which cause route instability and performance degradation. The chapter discusses the problem of route stability for on-demand protocols in detail. The *Efficient Route Maintenance* (ERM) scheme is proposed which improves route maintenance for on-demand routing protocols in wireless mesh networks by using cross-layering to get information from lower layers. The ERM scheme is then extended for multi-radio multi-channel mesh scenarios. ERM is evaluated against classical route maintenance mechanism of the on-demand routing protocols.

Chapter 4 presents the final contribution of the thesis : *QoS framework for bandwidth guarantees* in multi-radio multi-channel mesh networks. Providing QoS guarantees is particularly important for users who use the mesh network to access the Internet. The framework provides flow-specific reservation-based bandwidth guarantees in mesh networks. Link diversity (the availability of multiple redundant links between neighbors) is exploited for proposing a novel QoS provisioning solution which can provide better load-balancing in the network and provide a higher flow admittance ratio.

Table of contents

List of figures

Introduction...

Wireless networks are at the forefront of communication technology, offering innovative and efficient solutions. With their flexible structure, cheap cost and ever increasing data rates, they have revolutionized the way we communicate. Due to the success of the wireless phenomenon, today we have a wealth of wireless technologies at our disposal. A wireless technology that particularly enjoys widespread use is the *Wireless Local Area Network* (WLAN). The standard communication technology for WLAN is IEEE 802.11 [IEE 99] commonly known as "Wi-Fi". Infrastructure-based WLANs are fast replacing their wired counterparts due to their cheap cost, flexibility, and the convenience that they offer over conventional local area wired networks. They have been widely deployed at places like offices, cafés, universities and airports.

Despite their widespread deployment, infrastructure-based WLANs have certain limitations, most notably the need of a wired connection to the access network (typically Ethernet) for every *Access Point* (AP). Extending the wireless coverage of a WLAN by installing multiple APs becomes costly and impractical due to extensive cabling requirements. A promising wireless technology that can successfully address these limitations is the *Wireless Mesh Network* (WMN). Mesh networks have gained enormous attention because of their capability of providing broadband wireless coverage to large areas without infrastructure requirements. Free of any infrastructure requirements, nodes can be added as the situation demands, thus offering excellent flexibility. The network can span miles, providing wireless "*last-mile*" IP connectivity to hundreds of users. The mesh network acts as a common backhaul network providing interconnection between a range of heterogenous networks as well as providing eventual access to the Internet.

Wireless mesh networks are a special case of wireless multi-hop networks. Wireless multi-hop networks come in a range of flavors including *Mobile Ad hoc Networks* (MANETs), *Wireless Sensor Networks* (WSNs) and *Wireless Mesh Networks* (WMNs). Mesh networks comprise of a static wireless backbone without mobility or energy requirements. The nodes interconnect wirelessly, creating a "*mesh*" of connections. The mesh routers act as wireless *Access Points* to which other users and user networks connect. A few routers in the network provide wired connection to the Internet, these routers are called gateways. A number of communication technologies have been proposed for mesh networking, principally, IEEE 802.11 (Wi-Fi) and 802.16 (WiMax). However, due to relatively cheap equipment cost and *off-the-shelf* availability, IEEE 802.11-based mesh networks remain the most popular. The focus of this disserta-

tion is on 802.11-based backbone wireless mesh networks typically used for *last-mile* broadband access and we refer to them simply as wireless mesh networks.

Mesh networks typically service a large number of users who demand efficient performance (high end-to-end throughput, small end-to-end delay, high reliability etc). Moreover, mesh networks are mostly used in the context of providing *last-mile* access to the Internet and therefore, a significant portion of traffic in mesh networks is between users connected to mesh routers and the gateway nodes. This underlying traffic pattern may result in congestion in some areas of the network leading to poor performance. Most importantly, a major performance bottleneck in 802.11-based mesh networks is that a large number of mesh routers are located within the same geographical area and share the same wireless medium which can cause strong "*interference*" between mesh routers. This results in significant performance degradation in terms of the achievable throughput and the end-to-end delays. High interference, unique traffic patterns and high performance requirements from mesh networks mandate research for efficient routing and QoS strategies focused on mesh networks. The focus of this dissertation is on several issues in routing and QoS for mesh networks : *efficient routing*, *optimal gateway selection*, *enhanced route stability* and *per-flow bandwidth guarantees*.

Here, we present a general overview of the contributions and the outline of the thesis. The first two contributions (Chap 2 & 3) fall under the category of performance improvement while the last contribution (Chap 4) provides resource-reservation based QoS guarantees. The following is an outline of thesis :

- **Chapter 1** introduces wireless mesh networks and their architectural and functional components. We elaborate how mesh networks differ from traditional wireless multi-hop networks. Next, we present a literature review of the problem of Quality of Service and Routing in wireless multi-hop networks in general and then focus on solutions proposed specifically for wireless mesh networks.

- **Chapter 2** describes the problem of finding "*good*" routes between mesh nodes within a wireless mesh network. We first analyze popular routing metrics and point out their limitations. We propose the *Expected Link Performance (ELP)* metric which finds "*good*" routes between mesh nodes considering various aspects such as link loss ratio, link capacity and link interference. The proposed metric is evaluated against popular existing routing metrics. Next, we propose *an extension of the metric to tackle the specific case of gateway-oriented traffic*. Along with the extension, we also propose a gateway discovery protocol which incorporates the extended metric.

- **Chapter 3** addresses the problem of route instability due to frequent route breakages for on-demand routing protocols in mesh networks. We provide a comprehensive evaluation of the problem and its impact on performance. We propose the *Efficient Route Maintenance* (*ERM*) scheme which has been designed to

improve route stability in mesh networks. Performance evaluation of ERM in both single-radio single-channel and dual-radio dual-channel mesh networks is presented.

- **Chapter 4** introduces our resource reservation based QoS framework for providing QoS guarantees in a multi-radio multi-channel wireless mesh network by exploiting multi-link availability between neighboring nodes in a multi-radio multi-channel mesh network.

- **Conclusion** Concludes the thesis and discusses future directions of work.

The results of this thesis have resulted in some publications :
[Ashraf 07], [Ashraf 08b], [Ashraf 08a], [Ashraf 08c], [Ashraf 09]

On Wireless Mesh Networks

1

Contents

1.1 Introduction

Wireless multi-hop networks come in a variety of flavors of which wireless mesh networks are a particular case. QoS and routing solutions for mesh networks have therefore been strongly influenced by the previous research carried out for wireless multi-hop networks including MANETs and WSNs. It is therefore pertinent to discuss the literature in the general domain of wireless multi-hop networks. In this chapter we give an overview of QoS provisioning and routing in wireless multi-hop networks and then focus specifically on wireless mesh networks.

The rest of the chapter is organized as follows. First, we present the architectural and functional components of a mesh network. Next, we describe the problem of QoS provisioning in multi-hop wireless networks in general, from a layered perspective. After presenting QoS in wireless multi-hop networks, we present mesh-specific QoS solutions. Next, we describe the broad classes of routing solutions in wireless multi-hop networks and then present mesh-specific routing solutions.

1.2 Basics of Wireless Mesh Networks

1.2.1 Components of a Wireless Mesh Network

Wireless mesh networks come in a range of architectures and functional components. In this section, we describe what comprises a wireless mesh networks, classification of mesh networks, communication technologies for mesh networks and the key differences between mesh networks and traditional wireless multi-hop networks. Mesh networks comprise of three types of nodes : *Mesh Routers* (or Access Points - APs), *Mesh Clients* and *Gateway Routers* as shown in figure 1.1. The gateway routers at the top border provide wired connectivity to the Internet. The mesh routers at the other border act as Access Points for mesh clients and user networks. The following are the components of wireless mesh networks.

Mesh Routers - maintain connectivity, perform routing and provide the wireless backbone. They form an infrastructure of wirelessly interconnected routers that provide service to the users. They usually have minimal or no mobility and are not power constrained. These routers sometimes carry multiple radio interfaces. They are similar to the conventional routers in that they have the gateway/bridging functionality but they also have the added functionality to handle the mesh infrastructure. Instead of acting like terminal or user stations, the mesh routers act as relays to provide access to users and user networks connected to these mesh routers.

Mesh Client - these consist of end user devices such as laptops, PDAs Pocket PCs. The mesh clients can route data among themselves. They are however, much simpler

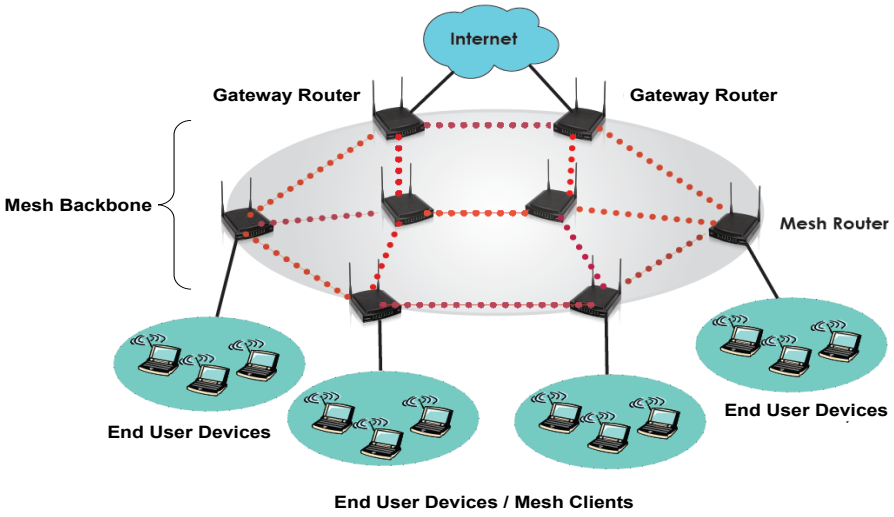


FIGURE 1.1 – *A Wireless Mesh Network*

than the mesh routers and usually carry only a single radio interface. The mesh clients connect to the network either directly through the network gateways, or through the mesh routers.

Gateway Routers - connect the wireless mesh network either directly to the Internet or to the wired access network (typically Ethernet) which is eventually connected to the Internet. Gateway routers act as the bridge between the wireless mesh domain and the wired Internet domain.

Some approaches consider only mesh routers and mesh clients as part of the mesh network [Q. Xue 02]. Others [S. Waharte 06] have adopted a more flexible view that comprises of three types of nodes : *Mesh Routers*, *Mesh Clients* and *Gateway Routers*, similar to the one we have adopted.

1.2.2 Classification of Wireless Mesh Networks

Wireless mesh networks are sometimes classified as ***Backbone*** (or ***Infrastructure***) and ***Client*** mesh networks. Wireless mesh networks are also sometimes classified based on the number of radios and the number of available channels. We elaborate upon each of these classifications in more detail below :

Backbone (or Infrastructure Wireless Mesh Networks) - The backbone mesh network consists of static wireless mesh routers that maintain connectivity, perform routing and provide the wireless backbone. These routers form an infrastructure of wirelessly interconnected routers that provide service to the users and networks. These WMN routers typically carry multiple radio interfaces for the wireless backhaul and one radio interface for connection with the end devices and networks. Usually one

or more of these routers is connected to the wired backbone through gateway routers.

Client Mesh Networks - Client mesh networks consist of a network of end user devices such as laptops. These are self organizing nodes that may perform routing among themselves. They provide network wide services to users and may optionally be connected to a network of backbone wireless mesh routers which may or may not have a connection to the wired Internet. These devices are usually power-constrained with energy-limitations and are typically mobile.

Single-Radio Single-Channel Wireless Mesh Networks - The most basic type of wireless mesh network is a single-radio, single-channel network. Each node in the network is equipped with a single radio and radio interfaces at all nodes are tuned to the same frequency channel. It is the most basic type of mesh network but suffers from performance problems [Gupta 00], the main reason being the single channel and strong interference between mesh routers. In a mesh network, a large number of routers are located in close proximity and traditionally use the IEEE 802.11 communication technology which works on the principle of CSMA (*Carrier Sense Multiple Access*) where nodes contend for access to the channel and a large number of mesh routers contending for access to the same channel can create high interference.

Multi-Radio Multi-Channel Wireless Mesh Networks - Wireless mesh routers are not expensive and due to the limited performance of single-radio mesh networks, it was proposed to equip each node with multiple radios so that a large number of concurrent connections can be maintained. Each node is equipped with one or more radios and the radio interfaces are typically tuned to non-overlapping channels to minimize interference. We can have *Static Channel Assignment*, *Dynamic Channel Assignment* or a combination of the two. In *Static Channel Assignment*, the interfaces at all nodes are permanently tuned to a fixed channel using approaches such as graph-coloring to minimize interference between the routers. In contrast, *Dynamic Channel Assignment* provides a mechanism for dynamically switching the interface to a different channel as the load conditions on the network vary. Dynamic channel assignment is more complex as it requires some underlying channel switching algorithm, a mechanism for synchronizing channel switch and a way to handle the channel switch latency [R. Draves 04b] [A. P. Subramanian 06]. This latency occurs due to limitations of the currently available 802.11 hardware [R. Chandra 04]. A hybrid channel assignment can also be used which is a combination of static and dynamic channel assignment. In these solutions, some of the interfaces are permanently assigned a fixed channel (often referred to as a control channel) while other interfaces can dynamically switch channels. A number of schemes exist for optimized channel-assignment in multi-radio multi-channel wireless mesh networks [Alicherry 05] [K. N. Ramachandran 06].

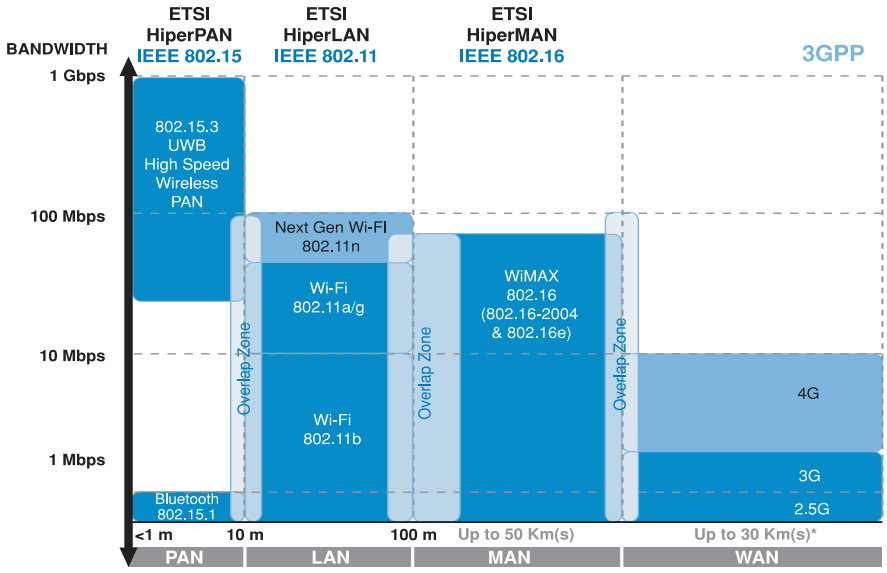


FIGURE 1.2 – *Wireless technologies and ranges*

1.2.3 Communication Technologies for Wireless Mesh Networks

Since the last few years, there has been considerable debate over the future communication technology for providing broadband wireless access to large areas. There are a number of solutions available. Figure 1.2 [Int 04] shows some key communication technologies along with their wireless coverage range and the data rates that they offer. Two technologies that are the key candidates for providing backhaul wireless internet are *Wi-Fi* (IEEE 802.11x) and *WiMax* (IEEE 802.16x). The two technologies have entirely different characteristics and offer different communication solutions. Below we outline some key differences between the two principal technologies :

IEEE 802.11 - The most widely used communication technology for wireless mesh networks is IEEE 802.11. This is mainly due to the fact that it operates in the license-free zone. A *Wi-Fi* mesh network consist of multiple 802.11 *Access Points* (AP) interconnected wirelessly. These nodes act as backhaul wireless mesh network to provide wireless coverage to large areas. Each AP acts as a router, accepting user connections in its locality and routing their data wirelessly over multiple hops to a wired connection and vice versa.The primary benefit of using 802.11 is that *off-the-shelf* 802.11 standard products are easily available and the technology operates in an unlicensed band. The cost of the IEEE 802.11 equipment is cheap and the Initial investment is therefore cost effective for small deployments. Some disadvantages to using IEEE 802.11 as the communication technology are the following. First, the bandwidth is shared among a large group of users. Secondly, due to limited date rate, the achievable throughput is limited and there can be significant delay and jitter. Due to the probabilistic access mechanism of IEEE 802.11, providing QoS is challenging.

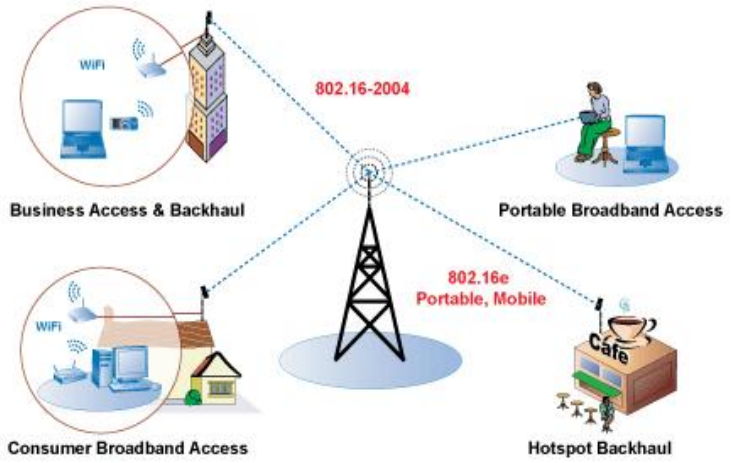


FIGURE 1.3 – *A WiMax Network*

IEEE 802.16 - IEEE 802.11 (figure 1.3) networks were basically aimed at offering data services in a localized area e.g. a university building. The IEEE 802.16 standard in contrast, is aimed at providing wireless broadband to metropolitan areas. During the recent years, 802.16 has begun to be used as the communication technology for backbone mesh networks. WiMAX (Worldwide Interoperability for Microwave Access) is the commercialization of the IEEE 802.16 standard. Initially, the 802.16 standard was aimed at serving fixed subscriber stations (SSs) through the central *Base Station* (BS) by using the P*oint-to-Multipoin*t (PMP) topology. However, in IEEE 802.16-2004 [802 04], which is the current standard, an additional mode called the *mesh-mode* has been introduced. In IEEE 802.16 *mesh-mode*, a mesh *Base Station* (BS) acts as the mesh backbone and controls *Subscriber Stations* (SS). With the centralized scheduling scheme of mesh mode, the Mesh Base Station is responsible for managing the allocation of resources as well as collecting bandwidth requests from subscriber stations. The 802.16 mesh provides some improvements compared to the IEEE 802.11 technology, but has some limitations. For example, the *mesh-mode* only defines *per-link*, *per-hop* QoS mechanisms which is not very appropriate for broadband QoS support in an end-to-end scenario within the mesh network.

1.2.4 The Power of Wireless Mesh Networks

Being a special type of wireless multi-hop networks, mesh networks enjoy certain advantages although some of these advantages are equally applicable to MANETs or WSNs as well :

Self-Organizing and Self-Configuring - Wireless mesh networks are self-configuring and in general, nodes can be added and removed from the network when needed without any special administrative intervention. This makes mesh networks attractive

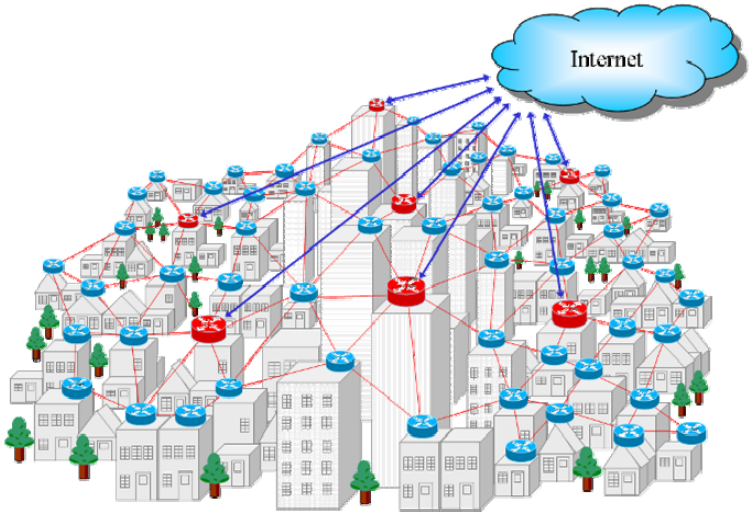


FIGURE 1.4 – *A mesh network spanning a complete city*

for administrators and also for novice users who are interested in quickly joining an existing mesh network by setting up their own mesh node. The nodes in a WMN learn about their neighbors and dynamically route data among themselves. Nodes enter and leave the network, some connections fail, new connections are created. All this is handled by the mesh routing protocol.

Self-Healing - Wireless mesh networks are self-healing in that the failing of some nodes or routes does not necessarily require administrative intervention or disruption of service. In fact, the term "*mesh*" means that the nodes are "*meshed*" together and there exist a number of alternate routes should some routes fail. The extent of self-healing capability also depends on the degree of "*meshing*" which implies the number of alternate available routes. Adding more routers can increase reliability as more alternate routes become available, however care must be taken as the wireless medium is the common channel used for communication and increasing number of nodes may result in increased contention as well.

Rapid Deployment - Compared to traditional infrastructure-based wireless networks, mesh networks are relatively easy to deploy. The principle difference stems from the fact that WLANs require wired connections of APs to the wired access network. However, mesh nodes can be quickly deployed as they do not have strict architectural constraints.

Coverage Extension and Scalability - The range of a wireless mesh network can be significantly extended to cover large areas (figure 1.4) using the multi-hop routing capability. Nodes can be easily added when required to expand the coverage. In contrast, conventional wireless networks such as WLANs have scalability problems due to the requirement of wired connection for every Access Point. Therefore,

WLANs are typically limited to small building or area. Real-world mesh networks as large as up to 800 nodes and spanning several miles [Fre 09] have been successfully deployed in real world environments. In general mesh networks can easily be scaled to cover large geographical areas.

1.2.5 Differences from Traditional Wireless Multi-Hop Networks

Lack of Mobility and Energy Limitations - The most popular wireless multi-hop networks such as Wireless Sensor Networks and Mobile Ad hoc networks comprise of nodes which are mobile and energy-constrained. Nodes in conventional ad hoc networks are typically battery operated and hence energy constrained. Energy conservation is a major area of research for WSNs, and routing protocols are developed with a focus on economizing energy by reducing transmissions and using collaborative sleeping mechanisms. Similarly, routing and QoS problems due to mobility of nodes is an important issue for MANETs. Therefore, mobility and energy conservation are the cornerstone of the ad hoc routing protocols developed for these networks. Backbone mesh networks on the other hand comprise of powerful, dedicated routers which do not have energy-limitations or mobility requirements. Therefore, existing QoS and routing solutions which were focused on mobility and energy conservation must be re-evaluated to optimize their performance for mesh networks.

Network Structure and Traffic Patterns - Conventionally, there is no structure or order among the nodes in an ad hoc network but this is not entirely true for the mesh backbone. The mesh routers may themselves be randomly distributed, but the location of gateway nodes and client networks follows a certain pattern. Client networks will typically be located at one end of the mesh backbone and the gateway nodes at the other. More importantly, most flows are between the client and gateway nodes in contrast to the traffic between random nodes in conventional ad hoc networks. These traffic patterns can pose unique problems. For example, nodes in the proximity of the gateway are much more likely to become congested and become traffic "hot-spots". A single gateway is typical for ad hoc networks which have limited bandwidth requirements. In mesh networks on the other hand, a large number of flows traverse the network and deploying multiple gateways is common. Therefore, issues like efficient load balancing between gateways and avoiding congested regions near the gateway nodes become valid areas of research for mesh networks.

Capacity - Nodes in both sensor and mobile ad hoc networks are usually equipped with a single-radio. However, nodes in the mesh backbone are sometimes equipped with multiple radios in order to meet the bandwidth and performance requirements of a large number of users. Mesh networks therefore have typically larger capacity than conventional ad hoc networks.

Role of Nodes - Nodes in both WSNs and mobile ad hoc networks are almost always user terminals. However, mesh backbone routers are usually relays which act as Access Points to users and user networks. As such, they have more powerful functionalities than conventional user terminals including more memory and specialized functionality which affects the design considerations for routing and QoS solutions. These significant differences of mesh networks from the traditional wireless multi-hop networks make a good case for researching efficient QoS and routing solutions developed specifically for wireless mesh networks.

1.3 QoS in Wireless Multi-Hop Networks

1.3.1 Introduction

Wireless Local Area Networks (WLANs) have been widely popular throughput the world and enjoy widespread deployment for a number of years. QoS provisioning in WLANs has been extensively researched. Wireless networks have since evolved and today we have a rich diversity of wireless technologies at our disposal. Among the new generation of wireless networks, wireless multi-hop networks have become particularly popular in the recent years. Since wireless multi-hop networks differ significantly from WLANs, research was focused on coming up with solutions aimed at wireless multi-hop networks. QoS in wireless multi-hop networks is particularly problematic because of the hidden/exposed station problems, unpredictability of the wireless medium, node mobility and energy limitations. We first describe why QoS provisioning is difficult in wireless multi-hop networks and then we present QoS in wireless multi-hop networks from a layered perspective. Next, we will present QoS solutions specific to wireless mesh networks.

1.3.2 Why QoS is difficult in Wireless Multi-Hop Networks

Wireless multi-hop networks have characteristics entirely different from the conventional wire-line networks. QoS provisioning, can become a challenging task for the wireless networks. Even though a number of QoS solutions exist for WLANs, but wireless multi-hop networks present a new paradigm as they have unique requirements and limitations. Since the focus of this dissertation is on CSMA based wireless networks, below we present some of the key reasons why QoS provisioning is a challenging task in CSMA wireless multi-hop networks :

a). Unpredictable wireless medium - The wireless medium is unpredictable and link qualities vary over time. There are a number of factors which affect link quality including multi-path propagation, signal fading, interference and noise. These factors cause random variations in the link quality which cause packet losses and packet

corruption and can make it difficult to accurately predict link bandwidth and delay.

b). Shared medium - IEEE 802.11 works on the principle of *Carrier Sense Multiple Access* (CSMA) whereby nodes contend for access to the channel. The CSMA based MAC protocol suffers from the classic hidden station [Tobagi 75] and exposed station [Tanenbaum 03] problems. These problems are particularly compounded for wireless multi-hop networks in which a large number of nodes can be distributed in a region. Due to the Hidden/Exposed station problems, there can be unpredictable collisions and delays. Moreover, accurate estimation of QoS metrics for wireless links can very difficult in the face of these problems.

c). Capacity Constraints - Wireless bandwidth is scarce and limited. Moreover, currently most wireless multi-hop networks use a single-radio per node which significantly limits the available capacity. This makes QoS provisioning difficult as most QoS solutions need mechanisms like signalling and control packets to function, but due to the capacity limitations, it can be sometimes difficult to meet these demands.

d). Node Mobility - In a multi-hop wireless network, nodes may be mobile (e.g. MANETs) and due to mobility, existing topology changes over time, routes break and must be re-established. If the route breaks, the reserved QoS guarantee is violated. Moreover, the physical characteristics of the link between nodes changes as the node distance varies. The changing network topology and the varying link characteristics can render the provisionment of QoS difficult.

e). Inaccurate Bandwidth Estimation - A vast majority of QoS solutions for wireless multi-hop networks require the estimation of the bandwidth on the end-to-end path. A fundamental problem with wireless multi-hop networks is that its very difficult to accurately estimate the wireless bandwidth of a link. This can result for a number of reasons including varying load conditions, hidden/exposed station problems, unpredictable collisions and packet corruptions.

f). Energy Limitations - In Mobile Ad hoc Networks and particularly Wireless Sensor Networks, energy efficiency is the cornerstone of routing. The nodes have limited energy and QoS provisioning must take into account the residual battery power as well as the rate of power consumption. The QoS solution needs to corresponding to resource utilization. Thus, QoS solutions must be power efficient.

g). Route Maintenance - Route maintenance is relatively a trivial task in wired network as the topology remains static. However in wireless multi-hop networks, routes can break due to a number of reasons including node mobility, power-outage at some nodes and channel conditions. Route maintenance in terms of ensuring that the route being used is supporting the required QoS is a non-trivial task for

multi-hop wireless networks. QoS solutions must have efficient route maintenance mechanisms.

h). Lack of Centralized Control - Wireless multi-hop networks require completely distributed QoS solutions as there is no centralized mechanism for managing QoS and QoS solutions must be distributed. This proves to be difficult as coordinating QoS between a number of distributed nodes can be a challenging task especially if the network size is large.

1.3.3 QoS From a Layered Perspective

QoS provisioning in wireless networks has been addressed from a number of aspects and QoS solutions can be classified in a number of ways. One possible classification of QoS solutions can from the perspective of the the OSI layer at which they operate. In this section, we describe existing QoS solutions from a layered perspective. In line with the focus of this dissertation, we focus on MAC and Network layer solutions and also discuss QoS frameworks that work across multiple layers.

1.3.3.1 MAC layer QoS Solutions

MAC layer QoS solutions have been extensively researched for WLANs. Wireless multi-hop networks however differ significantly from WLANs and pose new problems. The two main types of MACs for wireless networks are : *Carrier Sense Multiple Access* (CSMA) based and *Time Division Multiple Access* (TDMA). TDMA based MAC protocols can provide real-time QoS guarantees since slots can be reserved deterministically. However, TDMA based solutions are more suited for single-hop WLANs and providing synchronization between distributed nodes in a multi-hop network can be problematic. Therefore, CSMA based MAC have been widely used in wireless multi-hop network, but due to their probabilistic access to medium, they suffer from a range of problems.

The popular IEEE 802.11 technology works on the principle of CSMA. Apart from the problems inherent in the wireless medium such as channel errors, signal fading and interference new problems such as collisions and hidden/exposed station problem are also introduced due to the CSMA mechanism. The IEEE 802.11 standard, although being widely used, lacks mechanisms for providing QoS to flows. Some solutions proposed tuning the different parameters of IEEE 802.11 MAC for QoS provisioning. For example, one of the solutions [L. Bononi] proposes a differentiated distributed coordination function (DDCF) to implement node differentiation. Nodes are assigned different priorities according to their position in a virtual cluster in the network. The clustering mechanism is handled in the upper layers. In the Black-Burst (BB) scheme [J. P. Sheu 04], a priority classification period is used to separate the higher priority stations from the lower priority station. The 802.11e standard [802 02] was

introduced to address the shortcomings of 802.11 for providing Quality of Service. IEEE 802.11e introduces 4 Access Categories (ACs) supporting 8 *User Priorities* (UPs) also known as *Traffic Categories* (TCs) at the MAC layer to provide different priorities to flows. While 802.11e has been widely used for service differentiation in WLANs, their operability and usability for QoS provisioning in wireless multi-hop networks is questionable because the network is completely distributed and there are hidden station problems.

Relatively few QoS solutions have been proposed specifically for providing MAC-level QoS in multi-hop wireless networks. In one solution [Lin 08], authors propose an admission control algorithm for multi-hop WLANs based on contention graphs and the saturation throughput analysis for each maximal clique's capacity estimation. Other solutions [Chu 08] propose admission control algorithms for 802.11e based mesh networks and provide QoS for both *Constant Bit Rate (CBR)* and *Variable Bit Rate (VBR)* traffic. The *Multi-hop Access Collision Avoidance with Piggyback Reservation (MACA/PR)* [Lin 97] is a MAC-layer protocol which uses a reservation-based mechanism to establish a QoS-based connection over a single link. It has both a signaling component and a QoS routing algorithm to provide end-to-end QoS guarantees.

1.3.3.2 QoS Provisioning at Network Layer

Routing forms an integral and a significantly large part of research in wireless multi-hop networks. Most QoS solutions for wireless multi-hop networks work at the network layer and sometimes cross-layer with lower layers. Reservation-based solutions like the IntServ [S. Shenker 94] for wired networks have a signalling phase (RSVP) for reserving resources. Due to the overhead of the signalling phase which is required for each flow, reservation-based approaches were initially thought to be inapplicable to wireless multi-hop networks. On-demand (proactive) routing protocols such as AODV and DSR (for a more detailed discussion of routing protocol see next section), have been designed for wireless multi-hop networks. In the route discovery phase, these protocols broadcast a route request packet which is then re-broadcast by intermediate nodes until it reaches the destination which then sends back a route reply. Recently, by coupling the signaling phase with route discovery in on-demand routing protocols such as AODV [X. Cheng 08], [Xue Q 02], [M.A. Ergin 08a] the signaling phase problem has been solved. On the other hand, some QoS solutions perform stateless admission control i.e. resources are not reserved at intermediate nodes, the protocol just verifies at the time of flow admission if there exists any path from source to destination which meets the QoS requirements of the incoming flow. The following are some broad classes/areas for QoS provisioning in wireless multi-hop networks at network layer :

Resource Reservation Based Solutions at Network Layer

A significant number of QoS solutions for wireless multi-hop networks provide QoS guarantees by integrating routing with resource reservation. In the *Contention-aware Admission Control Protocol (CACP)* [Yang 03], authors propose an admission control algorithm for single-channel multi-hop networks based on the knowledge of local resources available at a node and the effect of admitting the new flow on the neighborhood nodes. They use the carrier sensing mechanism at the MAC layer to estimate the local available bandwidth at a node. CACP works with an on-demand routing protocol such as DSR but is generic enough to work with almost any existing on-demand routing protocol for ad hoc networks. Similar solutions have been proposed [Chen 05] [Xue Q 03] [Xue Q 02] in which the available bandwidth at a node is calculated as the minimum bandwidth within a two-hop neighborhood of the node. The route discovery process is once again coupled with admission control.

Stateless QoS Solutions at Network Layer

Another class of QoS solutions provides admission control without resource reservation. A popular QoS solution in this category is the *Core-Extraction Distributed Ad Hoc Routing - CEDAR* [P. Sinha 99]. CEDAR mainly focuses on the management of a core central network. Within this core, the state information of links with large bandwidth is propagated periodically. Each node belonging to the core must maintain not only the local topology, but also calculate routes for nodes in its vicinity. CEDAR selects routes with the QoS when it is requested. The core path is first created by propagating the control message within the core network. Subsequently, a calculation for QoS of the route is done ir order to reduce the length of the core path by exploiting partial topology information available at the core. The performance of CEDAR depends on the quality of management of local resources by the core nodes. SWAN [G.-S. Ahn 02] uses admission control for real time traffic and adjusts the TCP transmission rate for traffic based on the feedback from MAC layer in order to maintain delay and bandwidth bounds for real time traffic.

Multi-Path QoS Routing

In some cases, a single path between the source and the destination is unable to support the required Quality of Service. To solve this problem, some QoS solutions use a multi-path approach [W.H. Liao 01] in which the algorithm searches for multiple paths for the QoS route, where the multiple paths are jointly considered to meet the QoS requirements. The multiple paths together satisfy the required QoS. This solution also uses the idea of ticket-probing to limit the control overhead. MP-DSR [Leung 01] is a multi-path QoS-aware extension for DSR. MP-DSR attempts to provide end-to-end reliability (calculated from the link availabilities in the path) as the QoS metric.

1.3.4 QoS Frameworks

A QoS framework generally refers to a solution comprising of multiple components to handle QoS and often spans multiple layers of the protocol stack. A number of QoS frameworks have been proposed for QoS provisioning in wireless multi-hop networks :

INSIGNIA
INSIGNIA [S.B. Lee 99] is a QoS protocol proposed for supporting adaptive services in mobile ad hoc networks. INSIGNIA uses *in-band signaling* (refers to the mechanism where control information is carried along with data packets) which provides the restoration and adaptation of the reserved resources to support QoS (minimum bandwidth) to the dynamically changing network conditions. In-band signaling is usually considered to be well suited to the rapidly changing network dynamics of mobile ad hoc networks. The control messages which are used by INSIGNIA are carried within IP data packets, which install soft states for each individual flow in the traversed routers.

iMAQ Framework
The *integrated Mobile Ad-hoc QoS framework (iMAQ)* [K. Chen 02] is basically a framework, designed to support multimedia transmissions over mobile ad hoc networks. There is a routing layer along with a layer for middleware service. iMAQ is works across layers (cross-layered) as these two layers collaborate with each other including the sharing of information in order to be able to provide QoS guarantees to multimedia traffic. The routing protocol used is location-based QoS routing protocol while the middleware layer interacts with both applications and the network protocol to improve the quality of service. An interesting technique used by the middleware layer is partitioning prediction by exploiting location information from the network layer. To improve the accessability of date, the middleware layer replicated data between the different network groups before the network is partitioned.

1.3.5 QoS Solutions for Wireless Mesh Networks

In the context of mesh networks, QoS guarantees are typically provided for bandwidth and/or end-to-end delay. The problem of QoS is important for mesh networks since they are typically used for providing broadband wireless Internet access to a large number of distributed users and networks. In this section we describe some QoS solutions for mesh networks.

WMR protocol [Xue Q 02] is a QoS solution for mesh networks based on *Ad hoc QoS On-demand Routing* (*AQOR*) protocol [Xue Q 03] originally developed for *Mobile Ad hoc Networks* (MANETs). Admission control with QoS requirements is performed jointly with route discovery. In other words, the route discovery mechanism is also

used for the signaling phase similar to IntServ. At each intermediate node in the discovery process, if the available bandwidth is greater than the required bandwidth, route reservation is performed. *QUORUM* [V. Kone 08] is another QoS-aware routing protocol for wireless mesh networks which provides delay guarantees. *QUORUM* sends a stream of dummy packets along the route which have the same size and priority as the data packets, thus effectively emulating real data to get accurate estimate of delay. The delay estimation using QUORUM is fairly accurate but the drawbacks include the latency in setting up a route i.e. route discovery followed by the dummy packet phase and the extra interference that the dummy packets may introduce in the network. Moreover, the proposed solution only provides end-to-end delay guarantees.

In another solution [M.A. Ergin 08b], authors propose two new mechanisms for available bandwidth estimation at a node. The first mechanism uses the increasing of carrier-sensing range so that far off flows near the boundary of the carrier sensing range can also be taken into account. However increasing the carrier sensing range is not supported by current hardware as vendors do not allow low level access to the wireless firmware. The second method that they propose is to use the classical concept of back-to-back packet probes and then using mathematical models to estimate the available bandwidth using probe dispersion observed. Authors integrate bandwidth estimation and admission control with the on-demand *LUNAR* routing protocol i.e. admission control is done during Route Discovery phase. *MARIA* : *Interference-Aware Admission Control and QoS Routing in Wireless Mesh Networks* [X. Cheng 08] is yet another solution. In MARIA, a local conflict graph is computed at each node and admission control performed. Authors also propose an on-demand routing protocol which incorporates the admission control during the Route Discovery phase. In *Quality-of-service Aware Fair Rate Allocation* (*QUOTA*) [B. Wang 08a], authors propose a framework that combines QoS and fair-rate allocation for wireless mesh networks. Real-time flows are guaranteed the required bandwidth while the remaining bandwidth is fairly distributed between the non real-time flows or flows which do not have specific QoS requirements. *QUOTA* suffers from routing packet overhead for the creation of network-wide link contention graph.

A number of TDMA solutions exist for mesh networks. In *Distributed Call Admission Control* (*DCAC*) [Yi Hu 07], authors propose a protocol for TDMA based mesh networks. Some solutions have been proposed for admission control for QoS in backhaul WiMax Wireless Mesh Networks [S. Lee 06a]. However, TDMA in distributed multi-hop wireless networks has been subject of much debate since it is difficult to achieve synchronization for TDMA if the network is large.

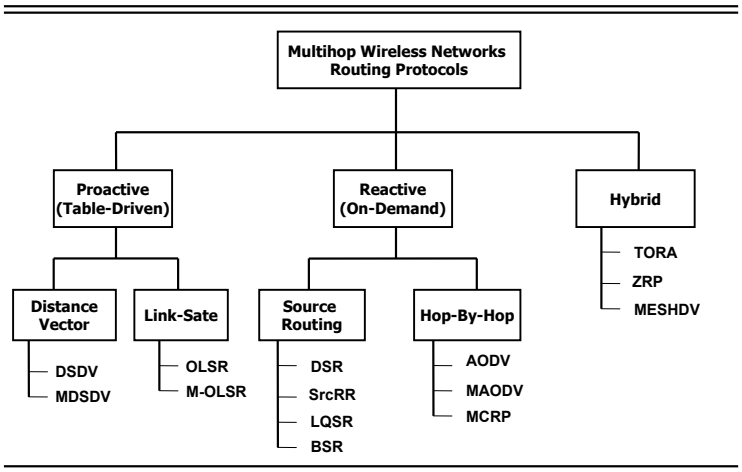


FIGURE 1.5 – *Taxonomy of routing families for wireless multi-hop networks*

1.4 Routing in Wireless Multi-Hop Networks

Ad hoc routing protocols have been widely implemented and rigorously tested, and there are numerous optimizations available. Despite the fact that mesh networks have significantly different architecture and traffic patterns, routing in mesh networks has been heavily influenced by ad hoc routing protocols and many testbed and real world deployments of mesh networks use these protocols or a modified form of these protocols [Karol Kowalik 07] [AA Pirzada 07a] [K. Ramachandran 05a] [A. P. Subramanian 06]. It is therefore pertinent to first discuss the routing approaches in multi-hop networks. After presenting routing solutions in wireless multi-hop networks, we will present mesh-specific routing solutions.

1.4.1 Overview of Routing Approaches in Wireless Multi-Hop Networks

An important classification in routing protocols is whether they are proactive or reactive. The two families employ entirely different mechanisms for route discovery, route maintenance and error recovery. Reactive routing protocols act on the principle of on-demand routing, building routes only when needed. They considerably reduce the routing overhead but introduce delays in communication as routes are not immediately available and must be set up. Proactive protocols follow a table-driven approach in which routing information is periodically broadcast throughout the network so that the routing tables at each node are up-to-date. Hence, routes are available when needed, but there is an overhead of periodic message exchanges. Apart from these two major classes, other types of routing protocols also exist including Hybrid routing protocols which are a mix of the two routing approaches. Figure 1.5 shows the broad classification of routing protocols for wireless multi-hop networks. [1]

1. DSDV [Perkins CE 94], MDSDV [P.J.B. King 07], OLSR [OLS 03], M-OLSR [Paul 08], DSR [D. B. Johnson 03], SrcRR [D. Aguayo 05], LQSR [R. Draves 04a], BSR [Song Guo 05], AODV [C. Perkins 03], MAODV [Royer 99], MCRP [So 04], TORA [Park 97], ZRP [Haas 98], MESHDV [Iannone 05a]

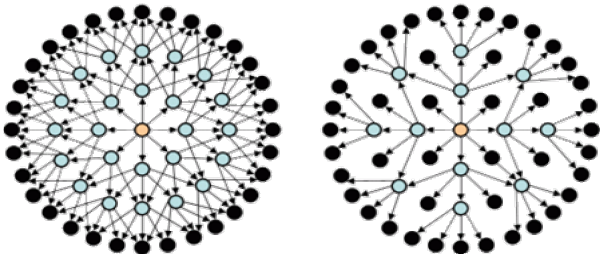


FIGURE 1.6 – *Figure on the right shows the reduction of broadcast by using MRPs*

1.4.1.1 Proactive (Table-Driven) Routing Protocols

Proactive protocols follow a table-driven approach in which every node stores fresh lists of routing information about the complete network. The routing information is periodically broadcast throughout the network so that routing tables are up-to-date. The obvious strength of such a routing scheme is that routes are immediately available when needed, but the disadvantage is the overhead associated with the periodic exchange of messages which creates burden on the network. A proactive protocol can be link-state or distance vector. In link-state routing, every node has a complete map of the network connectivity and it calculates the next best hop without consulting other nodes. This is in contrast to the distance vector routing protocols in which each node shares its routing table with its neighbors and does not know the complete topology of the network. DSDV and OLSR are two of the most popular proactive routing protocols, and we discuss them below.

DSDV - The Destination-Sequenced Distance Vector [Perkins CE 94] is a proactive, distance vector routing protocol based on the classical Bellman-Ford algorithm. Each node maintains a routing table that contains a list of all available destinations, the "cost" to each destination and the next hop for reaching that destination. Each routing table entry is tagged with a sequence number that has been generated by the destination. This number is incremented by the destination each time it sends its reachability information. This ensures the "freshness" of the routing information. Updates are broadcast throughout the network either periodically or when there is any change detected in the routing table. Thus the routing updates are both time-driven and event-driven. If a link is detected as broken, the detecting host broadcasts a routing update, setting the cost to this link as infinity. Thus, each node knows the next hop for reaching any destination in the network along with the associated cost metric. Note that the routing exchange may be "full dump" in which the complete routing table is sent by the node, or incremental in which case, only the routing entries that have changed are sent. DSDV suffers from the possibility of transient routing loops.

OLSR - The Optimized Link-State Routing protocol [OLS 03] is a proactive, link-state

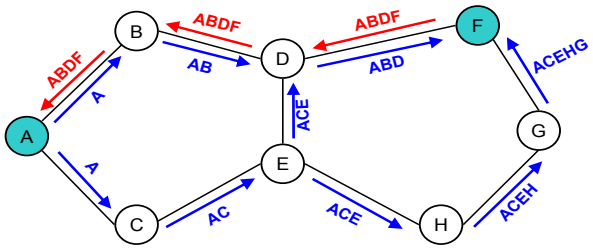


FIGURE 1.7 – *The Route Discovery phase of Dynamic Source Routing Protocol*

routing protocol which is basically a modification of the classical link-state algorithm. Each node periodically broadcasts a HELLO packet containing list of all its neighbors, the nodes' MPRs and "quality" of the links. These hello messages help in neighbor sensing. Apart from the hello message, each node periodically broadcasts Topology Control (TC) messages that contain list of neighboring nodes that have selected this node as their MPR. The TC is flooded throughout the network, but only using the MPRs, thus reducing the overhead. This information enables each node to have a complete map of the network. However, contrary to conventional broadcast that create a lot of overhead traffic, OLSR uses the concept of *Multipoint Relays* (MPRs). Each node selects a subset of its one-hop neighbors as its MRPs (shown by light blue color in figure 1.6 on the right side). The condition is that minimum number of MPRs should be selected such that the ensemble should provide connectivity to the node's two hop neighbors through at least one MPR. Neighbor Sensing is the neighbor discovery phase.

1.4.1.2 Reactive (On-Demand) Routing Protocols

Reactive routing protocols act on the principle of routing on-demand i.e. a node establishes a route only when it needs to send data, there is no periodic exchange of routing information. Reactive protocols reduce the routing overhead significantly but, introduce delays in communication as the routes are not immediately available. Reactive protocols have become the preferred protocols for routing in mobile ad hoc and to some extent, wireless sensor networks. Within the reactive protocols, there are many variations available based on differences in route establishment and route maintenance mechanisms. DSR and AODV are the two most popular reactive routing protocols. Below we discuss their salient features :

DSR - The Dynamic Source Routing [D. B. Johnson 03] protocol is a source routed, reactive protocol particularly preferred for mobile environments. The protocol works entirely on demand without any need for periodic table-update routing messages. This enables DSR to react only to changes and thus easily scale to large network sizes. If a node wants to send data to a destination to which it does not know the path, it starts the *Route Discovery* phase (shown with blue arrows figure 1.7) in which it floods a route request throughout the network. Each intermediate node receiving

the request appends its address in the header of the request packet and forwards it. The destination gets multiple route requests through different paths. It appends its address to the header and sends a reply packet on the reversed route (shown with red arrows). Thus, the source knows the complete route to the destination. Any subsequent data packets sent by the source contain the complete route in the header of packet. Route Maintenance deals with maintaining valid routes and taking corrective measures in case of path breakage. During the flow, if any intermediate node fails to deliver the packet to the next hop it notifies the source by generating a "Route Error" message. Upon the receipt of a route error request, the source concludes that the path is no longer valid and may launch a route request again.

AODV - The Ad hoc On-Demand Distance Vector routing [C. Perkins 03] is a reactive, loop-free protocol based on distance vector routing. It is an on-demand routing protocol that builds and maintains routes only as long as they are needed. Similar to DSR, AODV floods a route request packet throughout the network and the destination responds. All nodes receiving this broadcast store backward pointers to the source node. Finally, the destination receives the route request packet and replies with a route response packet. This time intermediate nodes set up forward pointers to the destination node. Thus routing information is stored locally at each node in contrast to the source routing of DSR. AODV uses sequence numbers to remember the "freshness" of routing messages. AODV maintains routes only as long they are active i.e. data packets are sent along the path. Unused routes eventually time out and are deleted from the intermediate nodes' routing tables. Breakage of a link is reported as route error to the destination. Nodes in the active route periodically exchange small HELLO packets to ensure connectivity. No reception of hello messages from a neighbor during a specific interval is meant that the neighbor is down.

1.4.1.3 Hybrid Routing Protocols

Some routing protocols have both a proactive element as well as a reactive element. The idea is to exploit the strengths of both the approaches to optimize routing. Proactive routing protocols have the problem of network overloading as the routing information needs to be disseminated to all the nodes periodically. On-demand have the drawback of the latency in setting up routes when needed. One such solution [Iannone 05b] proposes a hybrid approach for wireless mesh networks in which proactive routing is used for the backbone while reactive routing is used for setting up paths to the clients. The IEEE 802.11s [802 08] also proposed a hybrid routing protocol which combines on-demand routing with a proactive component.

1.4.1.4 Cross-Layer Routing Protocols

In order to improve performance, recently there has been an increasing interest in protocols which use interaction between different layers of the protocol stack. Tradi-

tionally, a layered approach to routing was adopted in order to keep things compartmentalized, but recent research has shown that at the cost of breaking the traditional layered structure, significant performance gains can be achieved. Cross-layered routing solutions particularly aim at the interaction of lower layers with the network layer. The argument is that the channel information available at the lower layers, particularly the PHY layer is more accurate and using this information at the higher layers in order to make routing decisions can provide significant performance improvements. Recently cross-layer solutions have been proposed for wireless mesh networks [Iannone 05c]. The counter argument against such approaches is that while performance gains do provide a certain motivation, breaking the layered architecture means that it will be difficult to have vendors adopt the solution.

1.4.2 Design Considerations for Routing Protocols in Mesh Networks

Routing in wireless mesh networks differs significantly from the wired networks or the conventional ad hoc networks. In WMNs there are no mobility requirements or energy constraints. Routing protocols that have been proposed for ad hoc networks such as MANETs and WSNs thus need to be improved and new protocols must be proposed that cater for the unique architecture and characteristics of the WMNs. While designing routing protocols many design options are available at various levels. In the context of Wireless Mesh Networks, we consider the following criteria for classifying and evaluating routing protocols.

Type of Protocol An important classification in routing protocols is whether they are proactive or reactive. The obvious strength of a proactive routing scheme is that routes are available when needed, but the disadvantage is the overhead associated with the periodic refreshing of messages. The advantage of a reactive routing scheme is the small routing overhead, but they introduce delays in communication because the routes are not immediately available. A third type of routing protocols also exists that is a mix of the above two types and is called hybrid routing. In some scenarios, hybrid protocols are the most promising approach as they can combine the strengths of the two types. Choosing a correct protocol depends heavily on the network scenario in which routing will take place.

Base Protocol Quite some research has been done on routing protocols in ad hoc networks and several efficient and rigorously tested protocols have been proposed. Since WMNs are a type of ad hoc networks therefore protocols for ad hoc networks have received much attention of the researchers. Many of the protocols suggested for WMNs have their roots in these protocols such as SrcRR [D. Aguayo 05], AODV-MR [A. A. Pirzada 06], AODV-ST [K. Ramachandran 05a]. Thus routing protocols for these networks can be developed by basing them on some existing protocol.

Network Structure Routing in infrastructure mesh networks differs significantly from routing in the backbone mesh. This is primarily because the client nodes are usually

mobile and will be generally battery constrained while the backbone mesh network has no mobility or energy constraints. Thus while developing the protocol for WMNs it must be kept in mind that which type of infrastructure are we targeting.

Radio Interfaces and Channels Currently the most common type of mesh networks are the single-radio because of the simplicity of architecture and cheap cost. Using multiple radio interfaces over non-overlapping channels can significantly improve the capacity of the network and improve performance by reducing interference. It is a design parameter to consider that whether the protocol being developed will be used for single-radio, single-channel mesh networks or multi-radio multi-channel mesh networks. The design principles of the protocol will differ significantly for the different architectures.

Protocol Structure Conventionally the protocol stack is a structured entity with clear separation between the different layers of the stack. Interaction among the layers takes place across well defined interfaces. This ensures that changes and improvements can be made in one layer without having to worry about the other layers. Due to the peculiar characteristics of the wireless mesh networks sometimes the conventional layering does not yield the optimal approach. We may have to melt down multiple layers into one layer in order to fully exploit the channel characteristics of the WMNs. Some works suggest that improvements in capacity throughput can be achieved by adopting a cross-layering approach. Thus choosing to stay with the conventional structured routing structure or adopting a cross layered approach is another important design decision.

Underlying MAC protocol Some routing protocols are MAC independent while others rely heavily on the type of MAC layer. Two broad classes of MAC protocols are : TDMA based MAC and CSMA based MAC. The routing solutions for these two classes of protocols will differ significantly.

1.4.3 Mesh-Specific Routing Protocols

A lot of routing protocols have been proposed for Wireless mesh networks. We seek to give the reader a flavor of the different approaches adopted by researchers.

SrcRR The SrcRR protocol [D. Aguayo 05] is used by the Roofnet mesh testbed [D. Aguayo 04] at MIT. The initial routing protocol used in the test-bed was DSR with *Expected Transmission Count - ETX* [De Couto 03] as the routing metric. For bulk TCP transfers, the protocol performed quite poorly and so the authors proposed an optimized version of the DSR called SrcRR. The SrcRR protocol is a reactive protocol with source-routed traffic. Every node running SrcRR maintains a link cache in which it had ETX metric values for links about which it has heard recently. SrcRR improves on DSR with ETX in many ways. It improves route stability by making less frequent changes and prefers using the same route as long as the new route offers only

slight improvement. It also avoids discarding immediately packets due to link-level transmission failures. It retries persistently to avoid TCP time-outs and the resulting under-utilization. With all these improvements the authors have shown a significant increase in the TCP throughput.

LQSR *Link Quality State Routing protocol* [R. Draves 04a] is based on the DSR protocol. It is a link-state protocol with source-routed data. LQSR uses the *Expected Transmission Time* - ETT [R. Draves 04b] routing metric which is the expected time to transmit a fixed-size packet on a particular link. The MR- LQSR [R. Draves 04c] is an extension of the LQSR protocol. It is a reactive, source-routed, link-state routing protocol derived from DSR and uses WCETT as link quality metric. It is an extension of the LQSR to handle multiple radio interfaces per node, which as they show yields better results. The ETT metric used by the LQSR only considers the loss-rates of the paths and does not cater for their bandwidths and it does not give any preference to channel diverse paths. Thus the LQSR protocol is modified to handle multiple radio interfaces per node and uses more sophisticated metrics in the decision for path selection.

AODV-ST The *AODV-Spanning Tree routing protocol* [K. Ramachandran 05b] has been proposed in the context of a framework for routing in mesh networks. It is a routing protocol for infrastructure wireless mesh networks. The authors define the architecture as comprised of relay and gateway nodes. The relay nodes act as Access Points and provide access to the client nodes. The relay nodes interconnect wirelessly to form a self-configuring, managed and secure wireless backbone that transfers packets. The relay nodes consist of two types of interfaces : access and relay and the gateway nodes consist of relay and backhaul interfaces. The access interfaces are used to provide service to clients whereas the relay interfaces are used for relaying packets between the relay nodes. The backhaul interfaces at the gateway nodes are used to connect to the internet. The AODV-ST is a reactive protocol which uses the Expected Transmission Time (ETT) metric. AODV-ST improves AODV in many ways. AODV-ST allows the use of high throughput metrics like ETT instead of the sub-optimal hop-count metric used by AODV. It allows the pro-active maintenance of Spanning Trees whose roots are the gateway nodes, thus reduces route discover latency and improves performance. It also reduces the size of routing tables maintained at nodes.

MRS The *Mesh Routing Strategy* [Iannone 05d] is a routing solution for WMNs that sets it apart from the other routing solutions proposed in that it uses a cross-layering approach. The authors argue that the main limiting factor in routing performance is that interference that each packet transmission generates for the surrounding nodes. The main approach here is to control the power used in transmissions at the physical layer as to minimize interference. The protocol uses physical layer level metrics such as rate and interference and Packet Error Rate (PER). The rate is the raw rate that the wireless card can send over the channel. The interference caused is estimated locally. The PER is the packet losses on the physical channel.

HWMP (IEEE 802.11s Standard) The upcoming IEEE 802.11s draft standard proposes the *Hybrid Wireless Mesh Protocol* (HWMP) as the default routing protocol for mesh networks. HWMP uses a proactive routing approach for gateway discovery in mesh networks. Gateways periodically broadcasts special Route Request packets which are flooded throughout the network and mesh routers select the best gateway based upon a routing metric. Within the mesh network itself, the standard proposes an on-demand routing protocol (based on AODV) to find the routes between mesh peers. While 802.11s proposes using the Airtime metric for routing within the mesh network, the choice of a routing metric for gateway selection is left open.

1.5 Conclusion

In this chapter, we introduced wireless mesh networks along with their components, classification and technologies. The differences of mesh networks from traditional wireless multi-hop networks were emphasized. The chapter explains why QoS and routing is difficult in wireless multi-hop networks in general and in mesh networks in particular. The chapter gave a general overview of QoS provisioning and routing in wireless multi-hop networks in general and then presented mesh-specific routing and QoS solutions.

Route Selection in Wireless Mesh Networks 2

Contents

2.1 Introduction

For a long time, traditional ad hoc routing protocols used the strategy of finding the shortest path between the source and destination in a network. This motivated the hop-count metric for route selection in ad hoc routing protocols. There are other underlying reasons as well which supported such a choice. Two wireless multi-hop networks that have enjoyed particularly high degree of research interest and applications are MANETs and WSNs. In the context of these networks, it was understandable as to why the shortest route may have seemed like a good choice. Mobility has always been a major research area in MANETs and selecting the shortest path between a node pair reduced the probability of route breakage due to the mobility of an intermediate node. Other factors being equal, the smaller the number of hops between the source and destination in a MANET, smaller is the probability of a broken route due to an intermediate node moving out of range of its communicating neighbor. Similarly, energy has been a major research area in WSNs and the longer the route, the more hops data must traverse and consequently, the greater the usage of energy. However, as discussed in chapter 1, energy and mobility are not valid concerns for mesh networks which have other strict requirements (throughput, delay and reliability). Need was felt to improve route selection in mesh networks by considering new metrics. The argument against the hop-count metric (shortest path) is simple. Selecting the shortest path between two nodes is a good choice only if every wireless link in the mesh network has exactly the same characteristics. In reality, there can be huge differences between wireless links (for example link delay, link loss ratio, link capacity) and hence the hop count metric is not a good approach [Couto 02] particularly for Internet-based applications which require good performance. A realistic metric needs to take into account multiple factors pertaining to link quality.

In a mesh network, we distinguish between two types of traffic : *peer-to-peer* traffic and *gateway-oriented* traffic. The *peer-to-peer* traffic refers to traffic between users connected to mesh routers within the mesh network. This traffic is limited to the mesh network and also called *intra-mesh* traffic. The *gateway-oriented* traffic refers to traffic originating from users within the mesh network, destined for the Internet and passes through the gateways. Figure 2.1 shows the two types of traffic.

This chapter includes four parts. The first part presents design considerations for routing metrics in mesh networks. The second part presents a review of existing routing metrics for mesh networks along with their limitations. The third part presents our proposed routing metric - *Expected Link Performance (ELP)* metric aimed at finding the "*best*" available route between mesh routers for *peer-to-peer* traffic. Performance evaluation results against popular existing metrics are also presented. The fourth part presents the extension of the ELP metric - *ELP-Gateway Selection* (*ELP-GS*) which is used to handle gateway and route selection for *gateway-oriented* traffic. We also pro-

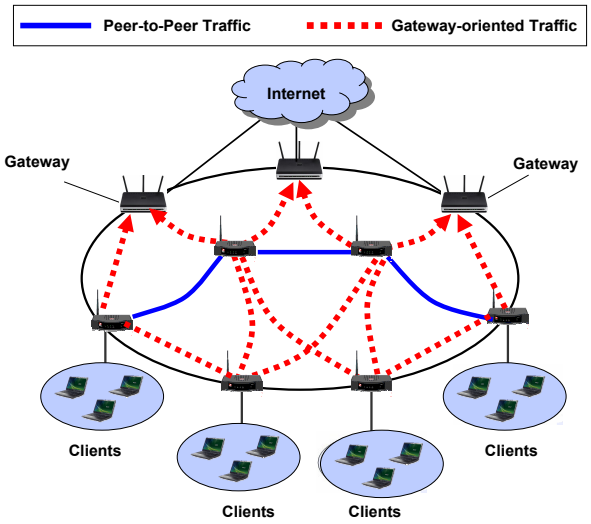


FIGURE 2.1 – *Mesh-oriented and gateway-oriented traffic*

pose a gateway discovery protocol along with ELP-GS to help evaluate the extended metric. Performance evaluation results against existing solutions for gateway and route selection for *gateway-oriented* traffic are also presented.

2.2 Design Considerations for Routing Metrics in Mesh Networks

A pioneering work on designing routing metrics was done by Yang et al. [Y. Yang 05a] in which the authors have proposed four principle requirements for a routing metric to be efficient. Since the design principals are well expressed, we follow more or less the same approach with some additions. First, the routing metric must be stable i.e. the routes should neither change frequently, nor need excessive routing packets for disseminating the changes in the routes. Second, the metric must be able to reflect the fundamental characteristics of mesh networks (e.g. interference) at both link and path level. Third, the calculation of the cost of a route should not be NP-hard. The fourth requirement is that the routing metric should be designed so that it does not cause loops. We elaborate upon each of these requirements in detail :

2.2.1 Route Stability

Metric-based route selection between a node pair selects the route with the minimum cost path. The "*cost*" of the path is the routing metric which can be number of hops, link-quality, energy at nodes etc. If the path costs changes very frequently, we will have frequent route switches which will result in poor performance of the network. Moreover, frequent metric changes can also cause excessive routing overhead as some routing protocols such as DSDV (distance-vector based) need to disseminate the path cost changes throughout the network. We can have two approaches to improve route stability, one at the metric level and the other at the protocol level :

- The routing metric can be efficiently designed to reduce excessive sensitivity to small changes. This is particularly true for routing metrics which depend on frequently changing factors e.g. network traffic.
- The protocol can be made to ignore insignificant changes in end-to-end path cost [D. Aguayo 05] [K. Ramachandran 07a]. Defining the threshold for a "significant" change is obviously a design decision. In general, this approach can improve route stability by reducing frequent switching of routes and limits on routing overhead for certain protocols such as DSDV.

It is important while designing routing metrics to take route stability into consideration so that routing can be made more stable.

2.2.2 Elements for Specifying Routing Metrics

Routing metrics must be able to capture the characteristics of mesh networks that impact the performance of paths. There are two important aspects to consider :

- ***Link and Path Level Aspects*** - We can analyze characteristics from the point of view of a link or from the point of view of a complete end-to-end path. At link level, we have characteristics such as link loss ratio, link interference (explained below), link capacity etc. At the path level (a path is a particular sequence of nodes and links), we have more "global" characteristics such as path length.

- ***Physical Aspects vs Protocol Aspects*** - Another classification of elements for specifying routing metrics can be whether they capture physical level effects or protocol-level effects :
  - *Physical Aspects :* - The physical aspects refer to phenomenon such as the frequency band, the link capacity or bit-rate (which depends on the modulation technique and the physical distance between the nodes of a link), and other disturbances which can affect a flow which is transmitting in the frequency band of the link (e.g. noise, interference of other flows which share the same frequency band).
  - *Protocol Aspects (MAC layer function) :* - Protocol aspects concern the sharing of the frequency band of the link by different flows using it. Two techniques are most frequently used : TDMA (in this case, there is deterministic interference as each flow must wait its turn of time slot for using the frequency band) and CSMA-CA (in this case, there is probabilistic competition between flows for accessing the medium) which gives rise to the interference phenomenon.
  - *Protocol Aspects (Network layer function) :* - The routing overhead generated by the routing protocol (which incorporates the computation of the metric)

is an important aspect to consider and has an impact on the performance of the routing metric.

We describe the five essential elements for specifying routing metrics for wireless mesh networks :

A - Link Capacity - An important characteristic that the routing metric must take into consideration is the capacity (transmission rate) of the wireless link at each hop. Link capacity in this context can be understood as the data rate of the transmitting radio on the link. Nodes are usually equipped with multi-rate radios which adjust their transmission rate based on the quality of the link to the neighbor. The link quality depends on a lot of factors including the physical distance between the nodes. A transmission at a high data rate takes a small amount of channel time whereas transmission at a lower transmission rate takes longer time which means that the node will occupy the medium for a longer period of time and disturb other nodes in vicinity. The goal of the routing metric should be to favor wireless links with higher transmission rates in order to achieve better performance.

B - Link Interference - Interference is a term that has been used to refer to a number of different things. We adopt the definitions and understanding of interference presented by Misra [Misra 00]. Similar to the authors, within the context of 802.11-based wireless networks, we distinguish between two types of interference : *Radio Interference* and *Channel Contention Interference*. *Radio Interference* represents a physical interference that can influence electromagnetic waves. It represents a superposition of signal/waves which changes the original signal (amplitude in particular) and causes bit alterations which in turn cause data and/or *Frame Check Sequence* alteration. The result of this alteration is that the link layer may drop packets resulting in a failed transmission. *Channel Contention Interference* stems from the medium access protocol (in our case, *Carrier Sense Multiple Access with Collision Avoidance* - CSMA/CA based MAC protocol of 802.11) which obliges the station to wait until the channel is free to start its transmission. *Channel Contention Interference* primarily refers to the deferred access to medium caused by the protocol (CSMA-CA based MAC) because the shared channel may be occupied by transmission from other nodes within the *Carrier Sensing* range of the node and this represents *"interference"*. *Channel Contention Interference* has been referred to as *Interference at the MAC layer* [Genetzakis 08] and *Traffic Interference* [Devu Manikantan Shila 08]. *Channel Contention Interference* therefore refers to *"logical"* interference as it is the interference which occurs *before* transmission. On the other hand, *Radio Interference* comes into play during the actual transmission of the packet when interfering signals may cause failed transmissions. From this point on, we will refer to Radio Interference as *Physical Interference* and to Channel Contention Interference as *Logical Interference*.

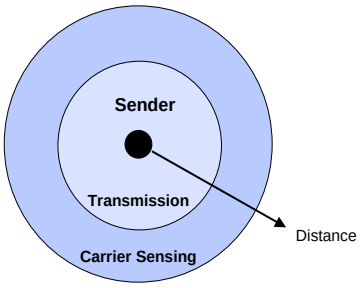


FIGURE 2.2 – *Transmission and Carrier Sensing Range*

• ***Transmission Range*** *- The transmission range is defined as a certain radius around the sender within which transmission is possible, i.e., a receiver receives the signals with an error rate low enough to be able to communicate and can also act as sender.*

• ***Carrier Sensing Range*** *- The Carrier Sensing Range is the range within which detection of the transmission is possible, i.e., the transmitted power is large enough to differ from background noise. However, the error rate is too high to establish communication.*

Figure 2.2 shows the general relationship between the transmission range and the carrier sensing range and their definitions. The *Logical Interference* encompasses communication taking place on the same channel within the carrier sensing range of the node. There will be contention between mesh routers located within this region for access to the channel and two nodes cannot simultaneously transmit successfully in this area. The delay that nodes have to face for accessing the channel is due to the *Logical Interference*. *Logical Interference* therefore determines *when* the node can actually transmit on the channel i.e. it comes into play *before* transmission. *Physical Interference* refers to interference at the signal-level *during* transmission of the data.

From another perspective, interference can be classified in two broad categories : *Intra-flow Interference* and *Inter-flow Interference*. *Intra-flow Interference* refers to interference within a flow traversing multiple wireless hops. Successive links in the path of a flow can interfere with each other and impact performance. The routing metric must take the possible *intra-flow interference* into consideration. *Inter-flow Interference* refers to interference between flows sharing the same channel and competing for medium access. A simple solution to reduce the problem of interference is to increase the channel diversity i.e. by selecting different non-overlapping channels for adjacent hops of a path for a given flow. However, these solutions work for multi-channel mesh networks and reducing interference in a single-channel single-radio mesh network can be more challenging where we don't have the luxury of using non-overlapping channels. The routing metric should attempt to select routes with smaller interference (both intra-flow and inter-flow).

C - Link Loss Ratio - A very basic yet effective metric for gauging the link quality is the link loss ratio. A node may need to retransmit a packet several times (at link layer) due to repeated losses which may occur due to interference, noise, or some

other factor. This is an indication of poor link quality and represents an inefficient use of resources. The routing metric should aim to select links with lower packet loss ratio (or higher delivery ratios).

D - Path Length - Other factors being equal, the greater the number of hops between a source and destination, the greater is the resource usage (medium time) and the greater is the delay and packet loss probability. While the shortest path alone is not always the best solution, but reducing the path length should be one goal of a routing metric as excessively long paths can be counter-productive. The routing metric should increase the cost associated to the path as the path length increases.

E - Routing Overhead - The routing overhead depends on two things. First, whether the metric requires *Active Measurement* which involves for example, the periodic broadcast of small probes to estimate link delivery ratios [De Couto 03]. Some solutions propose *Passive Measurement* in which the information is gathered locally without introducing any extra routing packets. However, there is a trade-off of accuracy vs. routing overhead as active measurements are in general considered more accurate but introduce routing overhead. Second, routing overhead can also result from stability of the metric (frequency of cost changes) as in some protocols (e.g. DSDV) routing updates are triggered due to cost changes. The objective of a routing metric must be to reduce the number of routing packets and the size of these routing packets as they strain network capacity.

2.2.3 Efficient Algorithm to Calculate Minimum cost Path

In wireless multi-hop networks, the routing protocols need to select the end-to-end route between any pair of routers. Among multiple available routes, the routing protocol selects the end-to-end route with the least "cost". Most common routing protocols use Dijkstra's or Bellman-Ford algorithms. In order for these algorithms to find the least cost path, the routing metric must have a property called "isotonicity". A detailed discussion of isotonicity can be found in the works of Yang et al. [Y. Yang 05a] and Sobrinho [Sobrinho 01].

Briefly, isotonicity refers to the fact that the order relation in the cost of two paths remains the same if a common third path prefixes or appends them. For example, consider figure. Let $C(abc)$ and $C(ad)$ represent the "costs" of paths $a \rightarrow b \rightarrow c$ and $a \rightarrow d$ respectively. We assume that $ab \odot ea$ denotes the concatenation of paths ab and ea. Now, in figure, we can see that the costs of paths $a \rightarrow b \rightarrow c$ and $a \rightarrow d$ are $C(abc) = 2$ and $C(ad) = 1$ and therefore, $C(ad) < C(abc)$. According to the property of isotonicity, adding a third common path ea with a cost of w in this case to either the start or the end of the two paths should not change the relationship between them i.e. $C(ea \odot ad) < C(ea \odot abc)$ and $C(ad \odot de) < C(abc \odot ce)$. That is, we can say that

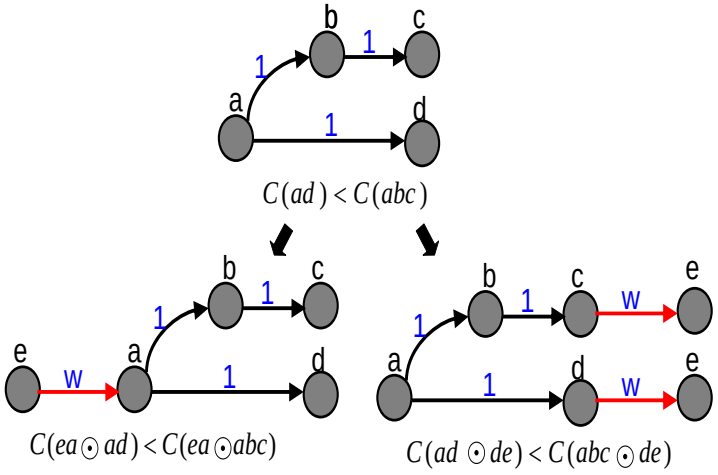


FIGURE 2.3 – *The isotonicity property*

$w + 1 < w + 2$ and $1 + w < 2 + w$. The basic idea here is that appending or prefixing existing paths with a common path should not change the relationship between the costs of those paths. If a metric is isotonic, then simple and efficient algorithms can be used to find the least cost path. However, if the metric is non-isotonic then we need algorithms with exponential complexity to find the solution. Therefore, while designing a routing metric, it should be ensured that the metric is indeed isotonic.

2.2.4 Loop-Free Routing

For reactive routing protocols, e.g. protocols based on source routing, routing loops are not a problem. For proactive routing protocols we have two sub-types : distance-vector based and link-state based. Proactive, distance-vector based protocols have in-built mechanisms to solve the problem of routing loops. For link-state routing protocols, routing loops can occur if the metric is non-isotonic.

2.3 Review of Routing Metrics for Wireless Mesh Networks

Before delving into the details of routing metrics, it is important to clarify a few terms with respect to routing metrics.

Link and Path Metrics

The *link metric* refers to the cost calculated for traversing a single link. The *path metric* refers to the cost of the end-to-end path. The path cost is derived in general, as a function of the individual link costs. The function can be any one or a combination of the following (similar to functions for QoS metrics presented in chapter 1) :

- **Summation** - The simplest and the most widely used function for the path metric is the summation of the link metrics. Examples of these additive metrics can be end-to-end delay or number of transmissions required.

- **Multiplication** - The values of link metrics are multiplied to get the end-to-end path metric. The probability of the successful delivery of a packet from source to destination is an example of the multiplicative function.
- **Statistical Measures (average, maximum, minimum)** - The path metric is calculated as a statistical function of the link metrics. This can include the minimum function, maximum or average function. Example is the bandwidth which is the minimum function.

Next, we present a comprehensive discussion of the various routing metrics used or proposed for mesh networks and discuss which limitations of the previous metrics each new metric addressed.

2.3.1 ETX - Expected Transmission Count

One of the pioneering work in the domain of routing metrics was *the Expected Transmission Count* (*ETX*) metric [De Couto 03]. ETX is one of the most popular routing metric and most contemporary routing metrics are based on the ETX metric. The ETX metric is defined as the expected number of transmissions (retransmissions included) at link-layer to successfully transmit a packet over a link. In ETX, neighboring nodes periodically exchange small probe packets (one probe broadcast every second). Every node thus knows the ratio of probes received both in the forward and reverse direction on the link. Nodes calculate the Expected Transmission Count (ETX) as the product of forward delivery ratio d_f i.e. the ratio of probes that the neighbor successfully received during the last w seconds (which translates to delivery probability of data packets) and d_r the ratio of broadcast probes that the node successfully received from the corresponding neighbor in the reverse direction (which translates to the delivery probability of the ACK packets). The authors propose using a moving window of 10 seconds to consider long-term link performance. The link metric becomes :

$$ETX = \frac{1}{d_f \times d_r} \tag{2.1}$$

The ETX of a path is the summation of the ETX of all the links in that path. Therefore, the ETX path metric for path p becomes :

$$ETX(p) = \sum_{link\ \ell \epsilon p} ETX_l \tag{2.2}$$

ETX selects routes with knowledge of the delivery ratios which is a more pertinent information as compared to the hop count metric, thus increasing the throughput and improving network utilization. The authors have implemented this routing metric in modified versions of DSDV and DSR for WMNs and have shown its superior performance. The ETX metric takes into account both link loss ratios and path length since each additional hop results in the addition of the ETX for that hop into the total cost. It is an isotonic metric which ensures easy calculation of loop-free, minimum cost

paths for all routing protocols. The probe delivery ratios provide an approximation of the link quality in terms of quality of the propagation channel of the link, the noise on the link and the physical interference (both intra-flow and inter-flow) on the link as these contribute to reasons for lost probes.

2.3.2 ETT - Expected Transmission Time

ETX assumes all radios have the same transmission rate which is not necessarily true. The ETT metric was subsequently proposed [R. Draves 04b] which seeks to improve the ETX metric by integrating the transmission rate of the radios. ETT is defined as the ''*bandwidth-adjusted*'' version of the ETX. The ETT of a link is defined as the expected MAC layer duration for the successful transmission of a packet over the link. The cost of a path is simply the summation of the ETT's for all the links in that path. The following equations show the ETT for a link and the ETT path metric :

$$ETT = ETX * \frac{S}{B} \qquad [S = Size\,of\,Probe\ ,\ \ B = Transmission\,Rate\,of\,Link] \tag{2.3}$$

$$ETT(p) = \sum_{link\ \ell \epsilon p} ETT_l \tag{2.4}$$

By introducing the link bandwidth into the calculation of the path cost, the ETT metric captures the impact of link capacity on the performance of the path. ETT performs better than ETX which does not take into consideration links bandwidths. Since ETT is based on the ETX metric, therefore it also captures the physical interference (both intra-flow and inter-flow) of the link but does not explicitly capture *Logical Interference*. ETT is an isotonic metric.

2.3.3 WCETT - Weighted Cumulative Expected Transmission Time

The WCETT metric [R. Draves 04b] is an extension to the ETT metric by the same authors. The main motivation for WCETT was to specifically reduce intra-flow interference by minimizing the number of nodes on the same channel in the end-to-end path so that the channel diversity minimizes the intra-flow interference. The WCETT of a path p is calculated as follows :

$$WCETT(p) = (1-\beta) \sum_{link\ \ell \epsilon p} ETT_\ell + \beta \max_{1 \le j \le k} X_j \tag{2.5}$$

β is a variable parameter with the constraint $0 \le \beta \le 1$ and X_j represents that how many times the channel j is used on links in the end-to-end path. The $\max_{1 \le j \le k} X_j$ part in the equation can be interpreted that it explicitly captures the intra-flow interference since the paths which have more channel diversity will have lower weights. WCETT does improve performance compared to ETT because it attempts to captures intra-flow interference, but WCETT has a static view because it only counts the number of channels. Moreover, there is no efficient algorithm which can calculate the minimum

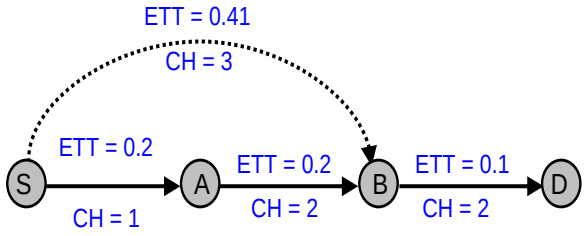


FIGURE 2.4 – *The non-isotonicity of the WCETT metric*

cost WCETT for a wireless multi-hop network because WCETT is non-isotonic. For example, consider figure 2.4. Assuming that with $\beta = 0.5$, we have to find the least-cost path from $S \rightarrow D$. The actual least cost path should have been $S \rightarrow B \rightarrow D$ with cost 0.71 but due to the non-isotonic property of WCETT when using the Dijkstra's algorithm, we will get the path $S \rightarrow A \rightarrow B \rightarrow D$ as the final result with a cost of 1.2. This is because when applying the Dijkstra's algorithm at node S, the least cost path to B would have been selected as $S \rightarrow A \rightarrow B$ and not $S \rightarrow B$ because the ETT of $S \rightarrow B$ is slightly more than that of $S \rightarrow A \rightarrow B$. Hence, $S \rightarrow B$ would have been eliminated and in the next step, the algorithm would select $S \rightarrow A \rightarrow B \rightarrow D$ as the final path which is not the least-cost path. Hence, WCETT is a non-isotonic metric and therefore, efficient algorithms cannot be used to computer the least cost path. Moreover, WCETT does not explicitly capture the *Logical Interference* which can play an important role in the performance of the network.

2.3.4 MIC - Metric of Interference and Channel Switching

Following the WCETT metric, a new metric, the *Metric of Interference and Channel Switching* (MIC) was proposed [Y. Yang 05b]. Formally, the MIC metric for a path p is calculated as :

$$MIC(p) = \frac{1}{N \times min(ETT)} \sum_{link\ \ell \epsilon p} IRU_\ell + \sum_{node\ i \epsilon p} CSC_i \tag{2.6}$$

Here N represents the number of nodes in the network and min(ETT) represents the smallest possible ETT in the network. The min(ETT) is calculated as being equal to the lowest transmission rate of the wireless cards. The MIC metric comprises of two components : IRU (Interference-Aware resource usage) and CSC (Channel Switching Cost). These are defined as :

$$IRU_l = ETT_\ell \times N_\ell \tag{2.7}$$

$$CSC_i = \begin{cases} w_1 & if\ CH(prev(i)) \neq CH(i) \\ w_2 & if\ CH(prev(i)) = CH(i) \end{cases} \quad 0 \leq w_1 \leq w_2 \tag{2.8}$$

Here N_ℓ represents the neighbors which interfere the communication on the link ℓ, and CH(i) represents the channel assigned to the radio at node i for transmission while prev(i) represents the channel used by the node on the previous hop. The IRU component represents the total channel time that the transmission on link ℓ consumes. This is basically the shared channel time for all the neighborhood nodes which operate on the same channel. IRU mainly captures the inter-flow interference since it favors a path that consumes less channel times at its neighboring nodes. The CSC component captures the intra-flow interference because it gives paths with consecutive links using the same channel higher costs than paths that alternate channel assignment per hop, which means that paths with more channel diversity will be preferred. A major limitation [Y. Yang 05a] of the MIC metric is that it is non-isotonic which makes it difficult to use minimum cost finding algorithms for the least cost path. Moreover, the interference estimation is static in that instead of taking into account the actual traffic emitted by neighboring nodes, MIC only considers the size of neighborhood as the criterion for interference estimation.

2.3.5 MCR - Multi Channel Routing metric

The MCR - Multi-Channel Routing metric [P. Kyasanur 05] was proposed to extend the WCETT metric so that it takes into account the cost (delay) of changing channels at radio interfaces in multi-interface multi-channel mesh networks. Let InterfaceUsage(i) be the fraction of time an interface was transmitting on channel i and let ps(j) be the probability that the used interface is on a different channel when we want to send a packet on channel j. If a route chooses to use some channel j, then we estimate the probability ps(j) that the switchable interface will be on a different channel ($i \neq j$) when a packet wants to use channel j to be :

$$p_s(j) = \sum_{\forall\, i \neq j} InterfaceUsage(i) \tag{2.9}$$

The switching cost of using channel j is calculated as :

$$SC(j) = p_s(j) \times Switching\ Delay \tag{2.10}$$

Where *Switching Delay* is the interface switching latency. Taking the switching cost into consideration during route selection makes sure that paths which must require frequent switching are less prioritized. When some flow is already passing through a node, the switching cost of all other channels (except fixed channel) will be high. Therefore, new routes which pass through the node using any other channel will have higher cost, and will not be preferred. To prevent frequent channel switching of the chosen paths, a switching cost is included into the ETT metric so that the resulting MCR metric becomes :

$$MCR = (1-\beta) \sum_{i=1}^{n} (ETT_i + SC(i)) + \beta \max_{1 \leq j \leq k} X_j \tag{2.11}$$

2.3.6 Airtime Link Metric (802.11s Standard Metric)

The working group of the mesh 802.11s mesh standard has proposed the *Airtime Link Metric* as the default routing metric for wireless mesh networks. The metric basically attempts to represent the amount of channel resources used for transmitting a frame over a link. The airtime cost C for each link is calculated according to the following formula :

$$C = \left[O_{ca} + O_p + \frac{B_t}{r}\right] \frac{1}{1 - e_{fr}} \tag{2.12}$$

Where O_{ca} is the channel access overhead. This depends on the modulation and coding scheme, O_p is the overhead of the MAC protocol, B_t are the number of bits in a test frame, r is the transmission rate while e_{fr} represents the frame error rate. The following table lists the constants used in the metric. The path with the smallest sum of airtime link metrics is the best path.

Constant	**802.11a**	**802.11b/g**	**Description**
O_{ca}	$75\mu s$	$335\mu s$	Channel Access Overhead
O_p	$110\mu s$	$364\mu s$	Protocol Overhead
B_t	8192	8192	Bits in Test Frame

TABLE 2.1 – *Constants used for Air Time Metric*

The only variables for the metric are transmission bit rate r and the frame error rate e_{fr}. The mesh standard does not recommend any specific mechanism to measure them and the implementation is left open. The Link Airtime Metric is very similar to the ETT metric and essentially captures physical interference.

2.3.7 Interference-Aware Routing Metric (iAWARE)

The iAWARE routing metric [P. Subramanian 06] considers both inter-flow and intra-flow interference into account for calculating the routing metric. The metric uses the ratio between *Signal to Interference and Noise Ratio* (*SINR*) and *Signal to Noise Ratio* (*SNR*) to continuously capture neighboring interference variations into the metric. The iAWARE metric uses the same path metric formula as WCETT, but replaces ETT with the iAWARE metric. The link metric for link ℓ becomes :

$$iAWARE_\ell = \frac{ETT_\ell}{IR_\ell} \tag{2.13}$$

Where IR_ℓ is the Interference Ratio for link ℓ. The Interference Ratio $IR_\ell(u)$ for a node u on a link $\ell = (u, v)$ (where $0 \leq IR_\ell(u) \leq 1$) is defined as :

$$IR_\ell(u) = \frac{SINR_\ell(u)}{SNR_\ell(u)} \tag{2.14}$$

Where

$$SNR_\ell(u) = \frac{P_u(v)}{N} \tag{2.15}$$

$$SINR_\ell(u) = \frac{P_u(v)}{N + \sum_{w\,\epsilon\,\eta(u)\,-\,v} \tau(w)\, P_u(w)} \tag{2.16}$$

Where $P_u(v)$ represents the signal power of the current packet coming from node u received at v, N is the noise, $\eta(w)$ denotes the set of nodes from which node u can hear (or sense) a packet and $\tau(w)$ is the normalized rate at which node w generates traffic averaged over a period of time. In practice, authors use SINR values from the wireless network card for the metric. For a bidirectional communication link $\ell = (u, v)$ IR_ℓ is defined as :

$$IR_\ell = min\,(IR_\ell(u), IR_\ell(v)) \tag{2.17}$$

The weighted cumulative path metric *iAWARE(p)* becomes :

$$iAWARE(p) = (1 - \alpha) \sum_{\ell=1}^{n} iAWARE_\ell + \alpha \max_{1 \le j \le k} X_j \tag{2.18}$$

The iAWARE metric captures both intra-flow and inter-flow interference. The iAWARE metric explicitly captures the *Physical Interference* since it uses a signal strength based mechanism. However, iAWARE does not capture the *Logical Interference* which occurs due to the MAC protocol. iAWARE also has a static view of channels since the second component simply counts the number of channels and not their relative positions. Moreover, iAWARE is a non-isotonic metric.

2.3.8 MIND - Metric for Interference and Channel Diversity

In the MIND metric [Borges 09], authors argue that the active monitoring mechanism of using probes to measure link quality in existing metrics can cause excessive overhead on the network. They propose the MIND metric which uses *passive measurements*. The MIND metric has two components *INTER_LOAD* which includes both *physical interference* and *logical interference* and the second component is the *Channel Switching Cost*. The MIND metric for a path p is shown in the equation below :

$$MIND(p) = \sum_{link\,\ell\,\epsilon\,p}^{n} INTER\_LOAD_\ell + \sum_{node\,j\,\epsilon\,p}^{m} CSC_j \tag{2.19}$$

The first component captures inter-flow interference. To express the INTER_LOAD component, authors estimate the physical interference and medium load as follows :

$$INTER\_LOAD_i = ((1 - IR_\ell) \times \tau) \times CBT_\ell \tag{2.20}$$

$$where\, 0 \le IR \le 1\, and\, 0 \le CBT \le 1 \tag{2.21}$$

Interference Ratio (IR_ℓ) is the physical interference part while *Channel Busy Time* (CBT) presents the medium load. Authors argue that τ (a configurable parameter) is used to

provide a higher weight to interference in the INTER_LOAD component although it seems like the multiplication operation renders τ as a constant multiplied with both interference and channel busy time. Taking their motivation from iAWARE, authors define IR_ℓ as :

$$IR_\ell = \frac{SINR_\ell}{SNR_\ell} \tag{2.22}$$

However, it must be noted that in iAWARE the IR at both end nodes of a link was considered to calculate the IR of the link but in MIND (because it is passive), IR estimation is done locally. That is, for a link $\ell = (i, j)$ IR_i is used to approximate IR_ℓ. The CBT at a node i is defined as :

$$CBT(i) = \frac{TotalTime - IdleTime}{TotalTime} \tag{2.23}$$

The *Total Time* is the duration which the channel was observed whereas the *Idle Time* represents the time that the medium was free i.e. no communication was taking place. Finally, similar to existing metrics, for capturing intra-flow interference, MIND uses *Channel Switching Cost* to express the channel diversity :

$$CSC_i = \begin{cases} w_1 & if\ CH(prev(i)) \neq CH(i) \\ w_2 & if\ CH(prev(i)) = CH(i) \end{cases} \quad 0 \leq w_1 \leq w_2 \tag{2.24}$$

Overall, the MIND metric provides an interesting approach of integrating physical and Logical Interference and attempts to capture both intra-flow and inter-flow interference components. The IR component in MIND is different from the IR proposed for a link in iAWARE since MIND works locally at a node without considering the link. However the two end nodes may have an asymmetric view of the channel which may introduce inaccuracies. Moreover, the channel busy time calculation includes the transmission time as well which means that a node which is successfully transmitting will be less preferred. Moreover, MIND is basically a non-isotonic metric although authors propose a virtual network based scheme [Borges 09] to resolve this problem.

2.4 Proposed Metric : Expected Link Performance Metric

While a number of routing metrics exist for mesh networks, they have some limitations which must be addressed. Here we describe our motivation for a new metric.

- The first motivation is that most contemporary routing metrics including ETX, ETT, WCETT, MIC and iAWARE use the probe based mechanism proposed in ETX for estimating the expected transmission count (or link delivery probability) and the estimation they offer needs to be adjusted.
- It is important to explicitly take into consideration the *Logical Interference* which stems from the CSMA/CA mechanism in 802.11 based networks. This is important because the *Logical Interference* has a significant influence on how often a station can actually access the channel and transmit.

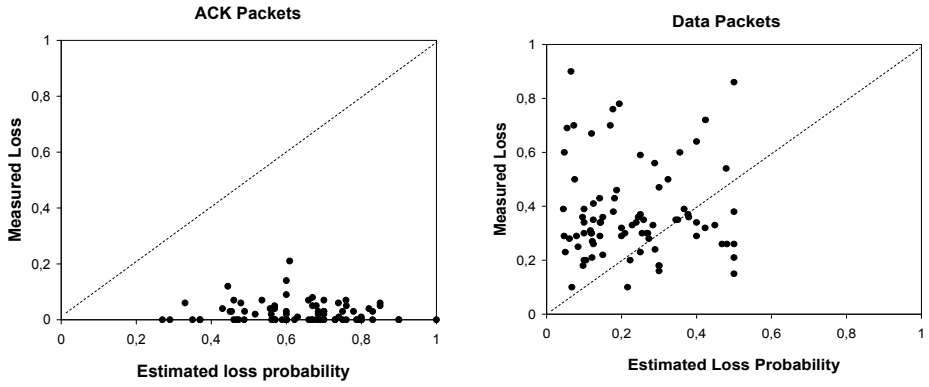


FIGURE 2.5 – *ETX estimation errors*

- The metric should capture both intra-flow and inter-flow interference dynamically as network conditions evolve. Some approaches such as MIC have a static view e.g. using the number of nodes in the neighborhood to estimate interference, regardless of how much traffic (and hence interference) those neighbors are generating.
- Some approaches [Borges 09] use only a passive approach to estimate link quality which does provide an advantage in the sense that the routing packets are reduced compared to active approaches, but some phenomenon such as link loss ratio and interference estimation require active exchange of probes.
- Few existing routing metrics cater to the problems which can be caused by frequently changing routing metrics. This includes excessive routing overhead, frequent route shifting or route oscillations. There must be some mechanism to improve routing stability which can adversely affect performance.

There are four main components of the Expected Link Performance metric. The *Link Loss Ratio* aims at estimating the expected loss ratio of the link. The *Link Interference* explicitly captures the *Logical Interference* present on the link. The *Link Capacity* component integrates the capacity (transmission rate) of the wireless link. Finally, the *Route Stability* component is not directly part of the metric, but aims at dampening the frequent route changes by interacting with the routing protocol. This component aims at stabilizing the route. ELP is an isotonic metric which allows the usage of efficient algorithms for calculating the minimum cost path. Each of these components is discussed in more detail below :

2.4.1 Link Loss Ratio

ETX and a number of contemporary routing metrics including ETT, WCETT, MIC and iAWARE use the probe-based mechanism of ETX to estimate the link loss ratio (also called expected transmission count). In this technique, periodically on a window of time, the ratio of probes successfully delivered from the current node to the neighbor (called the forward delivery ratio (d_f)) and the ratio of probes received from neighbor

to the node itself (called reverse delivery ratio (d_r)) are computed. The node then estimates the expected transmission count (loss ratio) as $\frac{1}{d_f \times d_r}$. There are problems with this technique. The formula assumes that the forward and the reverse links are symmetric i.e. for a link (i, j), the calculated cost is the same for $i \rightarrow j$ and $j \rightarrow i$. In 802.11 wireless networks, a packet transmission is successful over a link if the data packet (relatively large in size) is successfully transmitted in the forward direction *and* subsequently, the corresponding ACK (relatively small) is successfully received in the reverse direction. As the data packet is larger in size than the ACK packet, the communication on the link in the two directions is asymmetric. Moreover, the loss (or delivery) approximation offered by probes is inaccurate because probes are smaller than data packets and therefore underestimate the loss ratio for data packets. Probes are larger than ACK packets and over-estimate the loss ratios. In figure 2.5 we present the results of estimated and measured loss ratios for probe, data and ACK packets for a wireless link in a 50-node mesh network during a window of time. The first graph plots the correlation between the estimated loss probability in the reverse direction $(1 - d_r)$ using probes and the measured ACK loss in the reverse direction. The second graph plots the correlation between estimated loss probability in forward direction $(1 - d_f)$ using probes and the measured loss of data packets in the forward direction. As shown, probes over-estimate loss ratios for ACK packets while under-estimate loss ratios for data packets.

The link loss probability expressed in terms of probe delivery probabilities is equal to sum of the probability that the data transmission fails in the forward direction $(1 - d_f)$ plus the probability that a data transmission is successfully received in the forward direction but the corresponding ACK is lost $d_f * (1 - d_r)$. That is, the probability of loss is :

$$P(loss) = (1 - d_f) + \{d_f * (1 - d_r)\} \tag{2.25}$$

ELP solves the asymmetry and inaccurate probe-approximation problem by introducing a corrective constant in the calculation to bias the estimation in favor of link loss ratios in the forward direction. We can see from the figure that ACK packets are smaller than probe packets and are received successfully almost independent of d_r. However, data packets are much more affected and therefore we bias our calculations to give more importance to d_f than d_r and to scale d_f more than d_r . ELP introduces the following constant :

$$ELP_{LinkLoss} = \alpha \left(1 - d_f\right) + d_f[(1 - \alpha) * (1 - d_r)] \quad 0.5 < \alpha < 1 \tag{2.26}$$

where α represents the corrective term. Similar to the ETX metric, nodes broadcast probes once every second and a moving window of last 10 seconds is used for calculation of the link loss ratios. The probe based loss ratio measurement is the active component of ELP. This active component is important because the probe loss ratio can given an idea about some aspects of the quality of link which could otherwise be

difficult to capture. For example, a very long link may have almost zero interference but actual transmissions on this link will give very poor results as the signal will be very weak at the receiver. This mandates an active component like the probe packets especially if the nodes are not actively exchanging data. The probe loss ratio provides an approximation of the link quality which includes quality of the *propagation channel*, *noise* and *physical interference* as these three factors contribute to the loss of probe packets.

2.4.2 Link Interference

Interference is one of the most significant performance bottleneck for mesh networks [K. Jain 03] [Jitu Padhye 05]. We first describe how existing metrics estimate the interference and then explain how we differentiate between two types of interferences namely *physical interference* and *logical interference*.

Due to lack of a universal agreement on a method to estimate interference in mesh network, we briefly discuss some popular mechanisms of estimating interference specifically for mesh networks and their limitations and then propose our own mechanism. In some approaches [Borges 09] [P. Subramanian 06] [Karol Kowalik 07], signal strength based values are used to estimate the interference. Although, the correlation of signal strength and loss is assumed by a number of metrics, the actual correlation has recently been studied [D. Aguayo 04], and it has been shown that although signal strength values do affect the delivery rates, but the correlation is weak. Moreover, these calculations are sometimes done *per-node* [Borges 09] and not *per-link* which can result in inaccuracies. In general, these approaches primarily capture the *Physical Interference* as they consider physical layer parameters such as *Signal-to-Interference-and-Noise* (*SINR*) or *Received Signal Strength Indicator* (*RSSI*). These approaches seem to neglect the *Logical Interference* which cannot be directly taken into account by observing signal strength.

In other approaches, [K. N. Ramachandran 06] [K. Jain 03], interference in the mesh network is modelled using a conflict-graph approach. The basic idea is that interfering links in the network are modelled using graph theory and the interference on a link is estimated as a function of the traffic on the set of interfering links. In Interference Load Aware (ILA) metric [Devu Manikantan Shila 08], authors advocate considering the traffic load of interfering neighbors and call it *Traffic Interference*. In some approaches [Borges 09] the metric takes into consideration channel load. In general, these approaches capture the *Logical Interference*. Below we explain how ELP captures the *physical* and *logical* interference.

Physical Interference - *Physical Interference* refers to interference at the signal level and occurs *during* the transmission of a packet on the channel as signals from other

concurrent communications affect the original signal which can cause failed transmissions. Since the consequence of physical interference are failed transmissions, we measure physical interference using the probe-based link loss ratio which gives us an estimate of the physical interference on the link.

Logical Interference - As discussed previously, *Logical Interference* refers to the interference arising from the CSMA-CA based MAC which prevents a node from transmitting on the channel because some other node is transmitting in the carrier sense range of this node. We propose a simple mechanism for estimating logical interference. Using the IEEE 802.11 *Network Interface Card* (*NIC*) in promiscuous mode, a node can observe the channel states. Promiscuous listening in 802.11 has been widely used both in simulations and testbeds [Chen 05] [Yang 03] [Kim 06]. We consider the following states that a node can monitor at any given time :

- **Transmit** - presents the time that the node spends in transmitting to other nodes.
- **Receive** - presents the time that the node is receiving packets from other nodes.
- **Occupied** - represents the state that a node senses the medium as busy due to transmission from other nodes. This includes the physical carrier sensing as well as the virtual carrier sensing (a non-zero Network Allocation Vector-NAV).
- **Idle** - this represents the state when the node senses the medium as idle and the node has nothing to transmit.
- **Backoff** - represents the state that the node has some data to send, but cannot because the IEEE 802.11 standard mandates that the node must wait a random time. The backoff is executed if the node finds the medium busy when it tries to transmit and also after every transmission attempt.

We define *Average Interference Ratio* AIR(i) at a node i during a time interval T as :

$$AIR(i) = \frac{T_{Receive} + T_{Occupied} + T_{Backoff}}{T} \tag{2.27}$$

Where $T_{Receive}$, $T_{Occupied}$ and $T_{Backoff}$ are the sums of the duration i.e. the total time the node spent in these states during the time interval. To capture the long-term effects of interference and avoid rapid fluctuations, we use a window of T=10 seconds similar to the interval chosen by ETX [De Couto 03]. *AIR* explicitly captures the *Logical Interference*. $T_{Receive}$, $T_{Occupied}$ and $T_{Backoff}$ all represent the fraction of time that the node is unable to transmit on the channel i.e. the node is *busy unproductively*. *Logical Interference* is the time that the protocol defers the access of the node to the medium because other nodes are transmitting on the shared channel or the node is in backoff. This matches well with the definition of the *Logical Interference* which refers to the phenomenon in which a node is prevented from accessing and transmitting by the

protocol (in our case CSMA/CA) on the channel due to activity of neighboring nodes.

However, the *Average Interference Ratio* observed by a node presents only its local view of link interference. Nodes located at the two ends of a wireless link may have asymmetric views of the channel and it is important to integrate the channel interference information at the other end of the link in the calculation. The *Average Interference Ratio* $AIR(i,j)$ for a link (i,j) is calculated as the maximum of $AIR(i)$ and $AIR(j)$:

$$AIR(i,j) = Max\left(AIR(i), AIR(j)\right) \tag{2.28}$$

The *Logical* Link Interference portion of the ELP metric becomes :

$$ELP_{LogicalLinkInterference} = AIR(i,j) = Max\left(AIR(i), AIR(j)\right) \tag{2.29}$$

Expression for Physical and Logical Interference -The complete expression for the interference must take into account both *physical* and *logical* link interference. Since the *physical* interference part is expressed by link loss ratio, so the complete expression for the link interference is expressed as :

$$ELP_{LinkInterference} = ELP_{LinkLossRatio} \times ELP_{LogicalLinkInterference} \tag{2.30}$$

$$ELP_{LinkInterference} = \alpha\left(1 - d_f\right) + d_f[(1-\alpha) * (1-d_r)] \times Max\left(AIR(i), AIR(j)\right) \tag{2.31}$$

2.4.3 Link Capacity

ELP also takes into consideration the link capacities. This is important because other things being equal, a link with a higher capacity is preferable as it can transmit data at a higher rate and therefore occupy the medium for a shorter period of time compared to the low capacity link which will take longer time and create interference for nodes in vicinity and even for far away nodes (outside carrier sensing range). In ELP, links with higher bandwidth (radio transmission rate) are given a lower link cost :

$$ELP_{LinkCapacityFactor(i,j)} = \frac{1}{Bandwidth(i,j)} \tag{2.32}$$

The bandwidth is expressed in Mega bits per second.

2.4.4 Formula for Expected Link Performance Metric

We define the Expected Link Performance (ELP) metric for a link l and path p as :

$$ELP(l) = ELP_{LinkInterference(l)} \times ELP_{LinkCapacityFactor(l)} \tag{2.33}$$

$$ELP(p) = \sum_{link\ \ell \epsilon p} ELP_{\ell} \tag{2.34}$$

The final aspect of ELP involves routing stability. The problem of routing instability has recently been highlighted [D. Aguayo 05] [K. Ramachandran 07a]. We argue that

frequently changing metrics harm the performance in two ways. First, whenever there is a change in the path costs, proactive routing protocols typically need to disseminate this information throughout the network which introduces a high volume of route update volumes. More routing packets in the network consequently lead to more interference, delays and reduced throughput. Second, frequent path changes cause frequent changes in the end-to-end routes which can degrade the performance and are particularly bad for TCP flows. ELP proposes a simple solution to counter the effects of frequently changing routing metrics. The route to a destination is changed only if the new offered cost brings at least 10 % improvement compared to the previous cost. This takes care of the minor changes in path metrics which would otherwise trigger a huge routing overhead and path shifts. ELP is also isotonic which makes it easy to use efficient algorithm for computing minimum-cost paths.

Table 2.2 shows the comparison of all the routing metrics. As we can see that ELP integrates most of the components. The *physical interference* is approximated by the adjusted link loss ratio of probes while AIR captures the *logical interference*.

Routing Metric	Path Length	Link Delivery or Loss Ratio	Link Capacity	Physical Interference	Logical Interference	Link Asymmetry	Route Stability	Isotonic Property
Hop	✓							✓
ETX	✓	✓		✓				✓
ETT	✓	✓	✓	✓				✓
MIC	✓	✓	✓	✓				
iAWARE	✓	✓	✓	✓				
MIND	✓		✓	✓	✓			✓
ELP	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 2.2 – *Comparison of Routing Metrics*

2.4.5 Performance Evaluation

2.4.5.1 Simulation Environment

Physical and MAC Layers Wireless mesh routers in the simulation are equipped with IEEE 802.11b compliant wireless cards. However, the ns-2 simulator has some limitations in the modelling of the physical and the MAC layer. We therefore enhance ns-2 using a patch [Fiore] which makes simulations more realistic. To model the reception at the wireless card more accurately, the patch uses SINR-BER curves from Intersil for its HFA3861B chip [Int 00]. SINR is calculated using received signal strength, noise and interference. The simulator can now calculate the *Frame Error Rate (FER)* from *Bit Error Rates* (*BER*) and probabilistically drop the frame based on the calculated *FER*. At the MAC layer, the simulator uses the *Distributed Coordination Function(DCF*) compliant with the IEEE 802.11b standard. The following table presents the simulation parameters at the PHY and MAC layers.

Simulation Parameters	Values
MAC Protocol	IEEE 802.11
Data Rate	11 Mbps
Frequency	2.4 GHz
Propagation Model	Ricean Fading
Antenna	Omni-Directional
Transmission Power	281.8 mW
Broadcast Rate	1 Mb
RTS Threshold	3000
Simulation Time	1000 s

TABLE 2.3 – *Simulation Parameters*

Radio Propagation Model We use the Ricean fading model for simulators [Ratish J.Punnoose 00]. This propagation model allows the simulation of time correlated small scale fading, caused by the changing environment around nodes which is typical of outdoor environments, thereby allowing for more realistic tests.

Topology and Traffic Settings We perform all the evaluations in a single-radio single-channel wireless mesh network. The mesh network comprises of 50 mesh routers randomly placed in an area of 1400m by 700m. We have 10 flows assigned to 10 mesh routers at one end of the network and these flows traverse almost the whole width of the network to reach 10 destinations at the other end of the network. This allows for longer available routes, more choices in terms of routes and enables us to have a better evaluation of the quality of the route chosen by different metrics. We generate 10 random topologies and average our results across them. The position of the sources and destinations remains fixed while all other nodes are randomly distributed for each topology. We use *Constant Bit Rate* (CBR) traffic for the flows. The following table presents the topology and traffic parameters. Varying the packet size

(1024-2048 Bytes) is important to see the impact of packet size on the routing metrics.

Traffic and Topology Parameters	Values
Network Area	1.4km * 0.7km
No of Mesh Nodes	50
Random Topologies	10
Traffic Type	CBR
No. of Flows	10
Packet Size	1024,1536,2048 B

TABLE 2.4 – *Simulation Parameters*

Routing and Transport Protocols We have implemented ELP along with other metrics in both AODV and DSDV to enable us to evaluate our metric in both reactive and proactive environments. At the transport layer, we use both UDP and TCP. TCP is considered because it would be interesting to see the impact of the congestion control mechanisms of TCP on the performance of the metrics.

Evaluation Metrics We define some performance evaluation metrics which will be used to compare the performance of ELP to existing metrics. These are the following :

- **Throughput** - The throughput is defined as the aggregate throughput achieved in Kb/s for the whole network i.e. the aggregate throughput for all the flows in the network.
- **End-to-End Delay** - This is the average end-to-end delay for all the network flows in milliseconds. The delay is calculated per packet for all the packets arriving at the destination and the result is the average of all the packets of all the flows.
- **Routing Overhead** - We define routing overhead as the the normalized routing overhead which is the number of routing packets generated per data packet delivered at the destination.

Routing Metrics We have implemented ETX, ETT, iAWARE and the proposed ELP metric. The Hop Count is also included in the performance evaluation.

2.4.5.2 Analysis and Performance Evaluation of ELP

We first perform a sensitivity analysis of α of ELP using AODV to determine the optimal value. Next we present the performance evaluation results using AODV protocol for both UDP and TCP. Next we present the performance evaluation results for DSDV protocol using UDP.

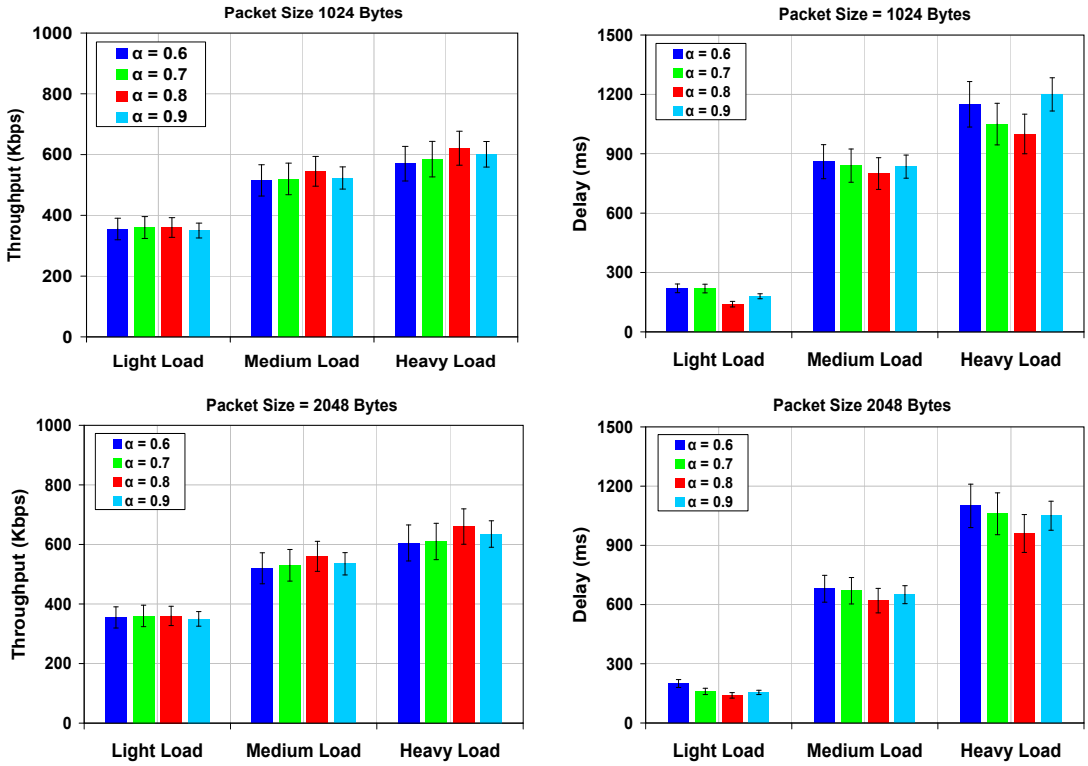


FIGURE 2.6 – *Sensitivity analysis of alpha for ELP*

Sensitivity Analysis of α using AODV The first step in the analysis of ELP is to determine the optimal value of α. As we previously mentioned, the link loss ratio in ELP is calculated as :

$$ELP_{LinkLoss} = \alpha\left(1 - d_f\right) + d_f[(1-\alpha) * (1-d_r)] \qquad 0.5 < \alpha < 1 \tag{2.35}$$

where α represents the corrective term. As discussed previously, probe packets underestimate loss ratios for data packets and over-estimate loss ratios for ACK packets. By using a value $\alpha > 0.5$ the forward loss ratio is given more important and is scaled up compared to the reverse loss ratio which is scaled down. It would be hard to calculate or propose an optimal value of α mathematically which works for all scenarios since there can be a lot of variables including packet size, traffic conditions and network topology. It was necessary to perform a sensitivity analysis of various values of alpha which would yield the best result. We use throughput and end-to-end delay as the criterion for judging the best value of alpha. Figure 2.6 shows the throughput and delay results for a range of α values (0.5 - 0.9) for packet size 1024 and 2048 Bytes. For each scenario, we present throughput and delay results for light, medium and heavy loads in a topology of 50 mesh nodes using ns-2 simulator. As shown in figure 2.6, $\alpha = 0.8$ gives the best performance. We explain the intuition of values of α. Choosing a small value e.g. $\alpha = 0.6$ means that we are only slightly biasing the link loss ratio calculations. This is expected to provide only slight improvements compared to using equal weights for the forward and reverse link i.e. we consider

the forward and reverse loss ratios *almost* equally important. Increasing the value of α increases the weightage in favor of forward links. However, if we use very large values e.g. $\alpha = 0.9$ then it means that we are not giving much importance to the reverse links which may cause problems because even though the reverse link is not as important as the forward link, yet the ACKs are received over this link meaning that we cannot completely ignore the reverse link loss ratios. As figure 2.6 shows, based on our empirical results, a value of $\alpha = 0.8$ seems a decent trade off and we use this value in all our subsequent simulations.

Performance Evaluation for AODV-UDP

There are a number of reasons why we have chosen AODV for the performance evaluation. First, it is an on-demand routing protocol which means that we can study the performance of the metrics with minimal effects of the routing overhead on the evaluation (contrary to the case of proactive routing protocols). Second, the upcoming mesh standard also uses a modified version of the AODV protocol which motivated us to use it as the protocol for performance evaluation. To evaluate ELP, we vary two things : the load on the network and the packet size. Varying the load is important to see its impact of network increased traffic (interference) on the performance of the routing metrics. The packet size is varied because ELP specifically addresses the issue of asymmetry of data and ACK packets and it would be interesting to see how ELP performs when we increase the packet size. We use throughput and delay as evaluation metrics for AODV. The routing overhead for all these metrics is comparable but larger than hop count because these metrics use probe packets in addition to the route discovery packets. In UDP, the sources send the traffic as fast as possible without restrictions which means that there are no restrictions such as congestion-related mechanisms of TCP. Using UDP permits us to test the difference between the performance of the routing metrics without limitations of the transport protocol. Figure 2.7 shows the results for UDP transport protocol for packet size of 1024 Bytes. For throughput, we see that in the beginning all metrics including the hop count have similar performance. This is simply due to the fact that there is minimal interference in the network due to limited load and the choice of any route yields equally favorable results. As the load passes the threshold of $\approx 400Kbps$, we begin to see some difference between the hop count and other metrics which is normal because hop count does not take into consideration any other factor than number of hops. As the load further increases, we begin to see a noticeable difference between various routing metrics. An important thing to notice is that as soon as the load passes a certain threshold $\approx 1200Kbps$, the throughput starts declining. This is because the network is highly loaded and is beyond saturation point. ETX outperforms minimum hop because it considers the link loss ratios which captures qualities of the links (in terms of physical interference as probe losses occur due to physical interference).

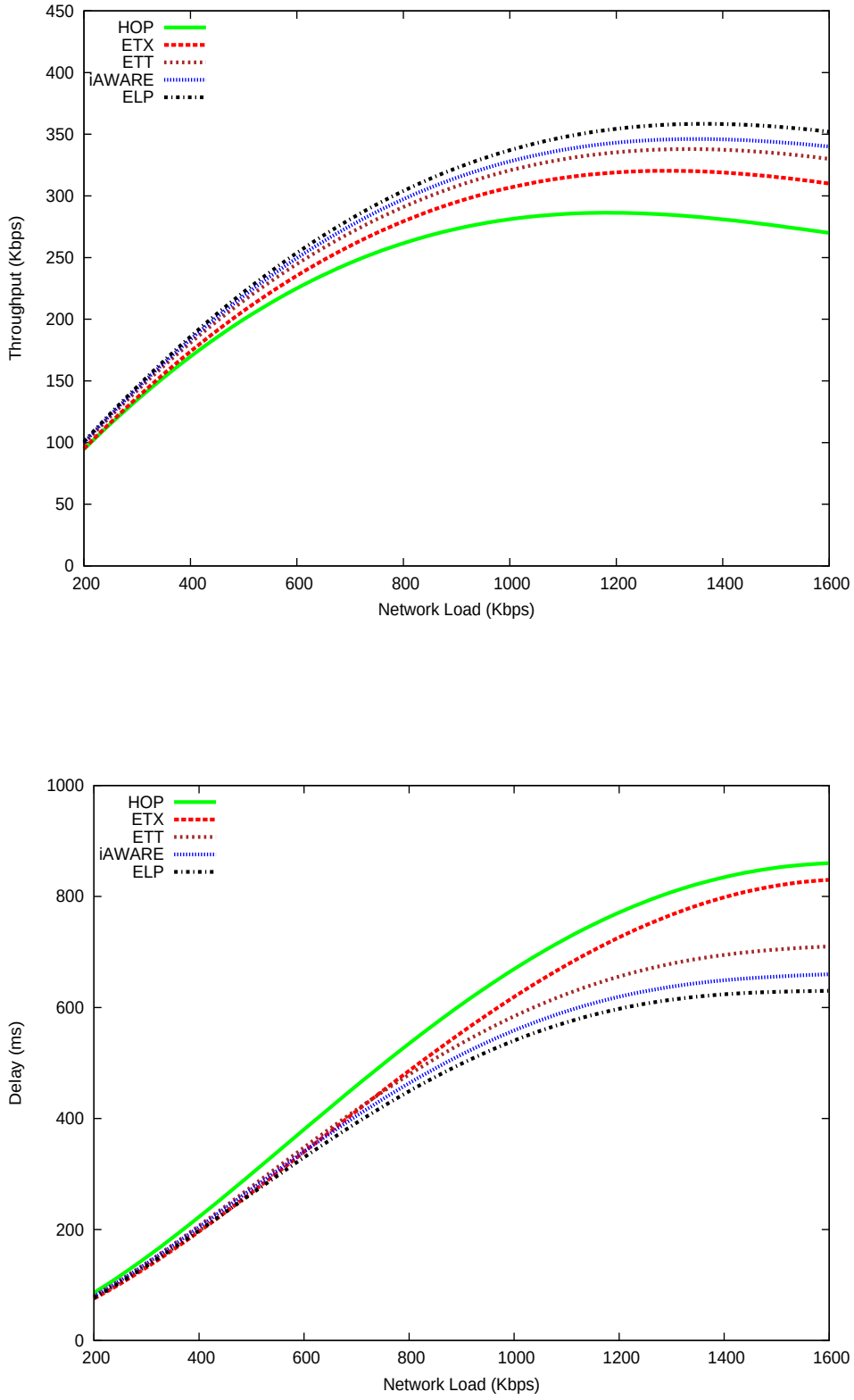
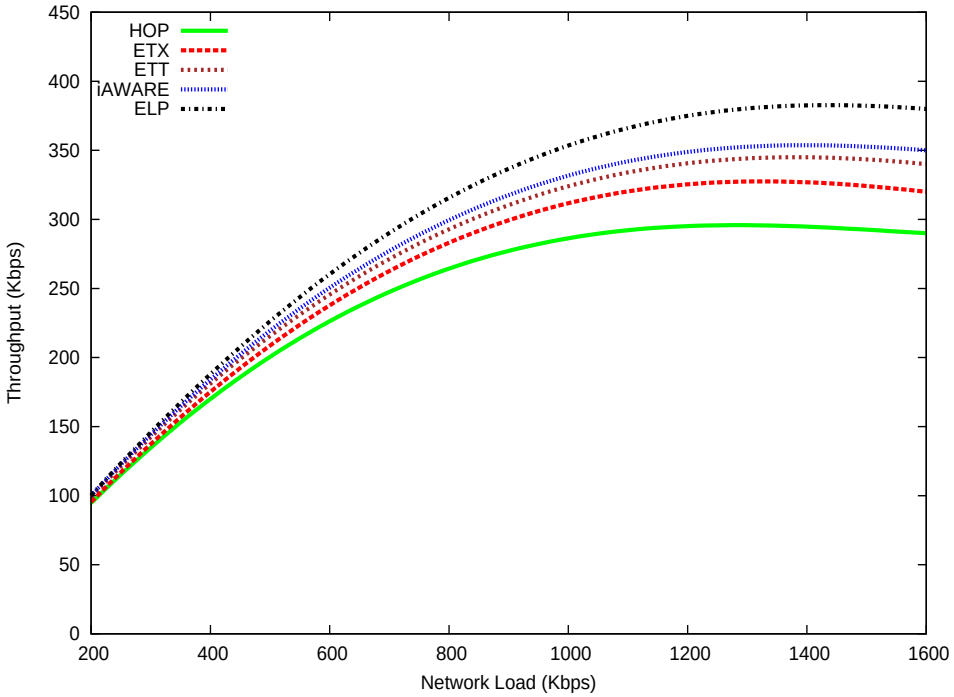


FIGURE 2.7 – *Performance evaluation results for AODV-UDP Packet size 1024 B*

ETT outperforms ETX because it integrates the capacity of links in addition to physical interference of links. iAWARE and ELP outperform all other metrics because they explicitly take into consideration interference present on the network. Based on our extensive simulations, we have observed that *logical interference* plays an important role in determining the performance of the chosen routes. ETX and ETT use the basic probe mechanism of ETX which can give an estimate of the *physical interference* present on the medium i.e. probe losses due to collisions or signal level interference. iAWARE goes one step further and uses SINR to refine the interference estimation and hence outperforms other metrics. However, none of these metrics cater for the *logical interference* which plays an important role in determining how often a node would actually be able to transmit. A metric may select the best possible route but if transmitting nodes on the route are unable to transmit frequently due to deferred access to medium, then performance degrades. ELP uses the *improved* probe loss ratio to approximate the physical interference and also explicitly takes into consideration the *logical interference* present on the route. This is very well reflected in the smallest delay of ELP which means that it chose routes with least latency and high throughput. Compared to the hop count metric, ELP offers a throughput improvement of up to 30% and a reduction in delay of up to 33%. Compared to iAWARE, ELP offers a throughput improvement of up to 5%.

Moving to the case of 2048 Bytes packets (figure 2.8), the first observation we can make is that a large data packet size offers improvement over the 1024 Bytes packet size which seems to present a more efficient utilization of network resources (more data sent per access to medium). From the figure, we can also see that the difference in the performance of ELP and other metrics has become more significant than was with a packet size of 1024 B. It should be noted that ELP uses the asymmetric link loss ratio calculations to mitigate the problem of asymmetry between data and ACK packets. When the size of the data packet increases from 1024 Bytes to 2048 Bytes, the asymmetry between data and ACK packets become even bigger. Due to the larger size, data packets may experience more interference. The greater the difference between data and ACK packets, the more the asymmetric link loss ratio of ELP factors in and improves performance. The delay of ELP is still smaller than other metrics due to the *logical interference* component which ELP takes into account and is neglected by other metrics. Compared to hop count, ELP offers a throughput improvement of up to 35% and a reduction in delay of up to 42%. Compared to iAWARE, ELP offers a throughput improvement of up to 15% and a reduction in delay of up to 10%. Globally, we see more or less similar results as the case for 1024 Bytes and we can conclude that ELP outperforms other metrics.



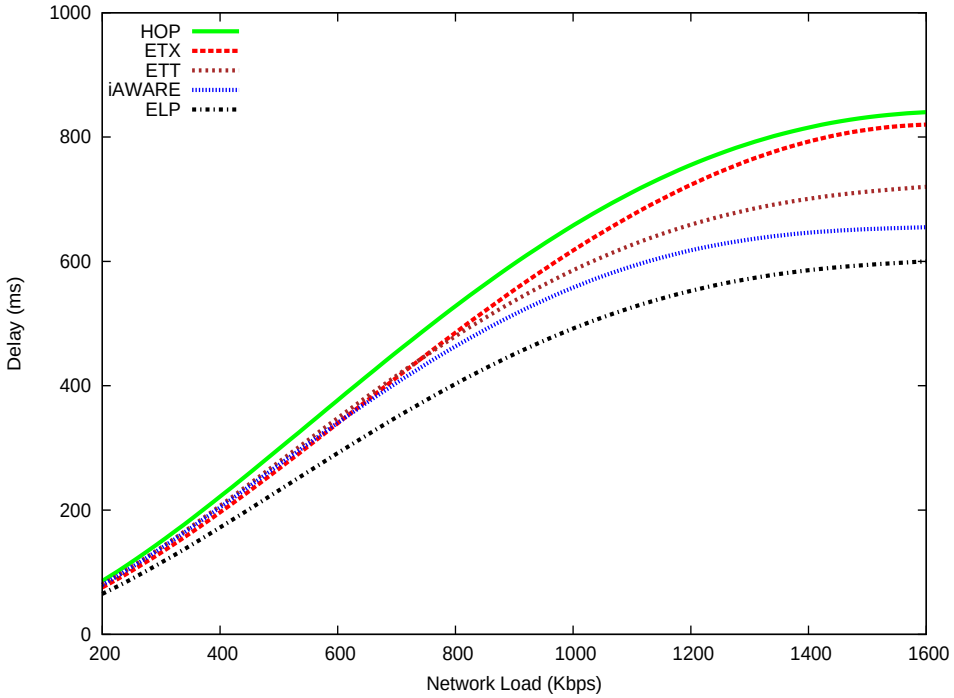


FIGURE 2.8 – *Performance evaluation results for AODV-UDP Packet size 2048 B*

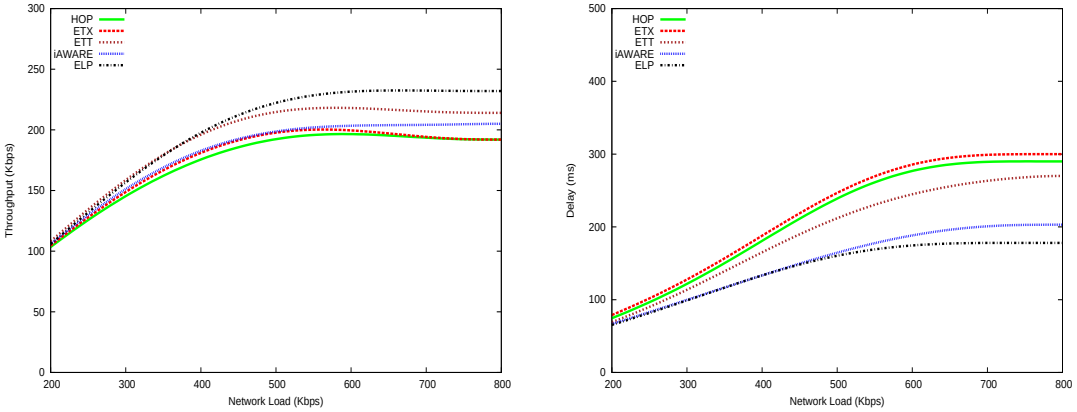


FIGURE 2.9 – *Performance evaluation results for AODV-TCP packet size 1024 B*

Performance Evaluation for AODV-TCP

Figure 2.9 and 2.10 present the results for AODV using TCP as the transport protocol. Classically UDP is used to evaluate routing metrics however, inline with some existing solutions [De Couto 03], it would be interesting to see how the metrics perform under the congestion-control mechanism of TCP. The first main difference is that TCP provides a much smaller throughput than UDP which is normal due to the slow-start and congestion-control mechanisms of TCP. Once the network reaches the saturation point, the throughput becomes constant as TCP does not permit overburdening the network. From the results we see that other metrics do not take into account the *logical interference* which actually determines the latency in transmissions. Therefore, we see that ELP chooses router with smaller end-to-end delay. The minimal delay of ELP reflects the fact that the *logical interference* component of ELP selects routes with less delay as each node will have more frequent access to the medium. Compared to the UDP case, iAWARE seems to perform well below its performance in the UDP case. One plausible explanation can be that in the case of TCP, *logical interference* can dampen the multiplicative increase of the TCP and iAWARE does not explicitly takes into consideration the *logical interference*. This means that if a node has too many contending flows within its carrier sensing range, those flows may cause deferred

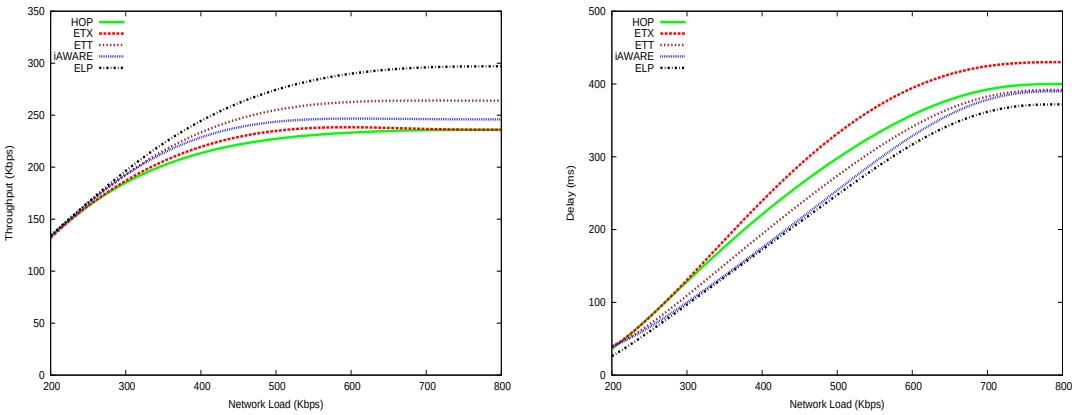


FIGURE 2.10 – *Performance evaluation results for AODV-TCP packet size 2048 B*

access to the medium for the node resulting in slowing down the multiplicative increase of the TCP. Moving from packet size 1024 Bytes to 2048 Bytes, we observe that the difference between ELP and other metrics becomes more visible in terms of throughput. This is due to the asymmetric link loss calculations. For the case of packet size of 1024 Bytes, compared to the hop count metric, ELP offers a throughput improvement of up to 30% and a reduction in delay of up to 40%. Compared to iAWARE, ELP offers a throughput improvement of up to 15% and a reduction in delay of up to 10%. For the case of packet size of 2048 Bytes, compared to iAWARE, ELP offers a throughput improvement of up to 15% and a reduction in delay of up to 5%. Globally, ELP outperforms all other metrics.

Performance Evaluation for DSDV-UDP

DSDV is a popular distance vector routing protocol for wireless multi-hop networks. We have evaluated our routing metric in DSDV in addition to AODV so that we can have a comprehensive performance evaluation of ELP. The ETX metric was originally evaluated using the DSDV routing protocol [De Couto 03]. It should be noted that the proactive routing mechanism of DSDV results in excessive routing packets which can introduce an unforeseeable and non-negligible affect on the performance of routing metrics and also DSDV is known to perform well-below AODV.

For DSDV, we performed performance evaluation for both UDP and TCP. Apart from the expected reduction in the throughput offered, results for metrics using TCP showed somewhat similar trend. Here, we only present results for UDP transport protocol. Figure 2.11 shows the performance results for throughput, end-to-end delay and routing overhead for packet sizes of 1024 and 2048 Bytes. Overall, we see that ELP and iAWARE remain the best choices. In terms of throughput, ELP outperforms all other routing metrics for both packet sizes under medium and high load. However, for very light load, we see that ELP performs worse than most metrics. It seems that ELP generated a relatively larger number of routing packets for light load situations. However, this can be explained by the fact that there are multiple factors in ELP such as the AIR which can change relatively frequently, triggering the route broadcast mechanism of DSDV. In our simulations, we came to the conclusion that the route update mechanism of DSDV has a non-negligible impact on the performance of the routing metric. For medium and high load situations, the benefits of considering a diverse set of components seems to outweigh the problem of routing overhead resulting in an overall performance improvement. The delay offered by ELP is comparable to iAWARE. In terms of routing overhead, ELP has a higher overhead than other metrics for light load scenarios. Nevertheless, if we see the results globally, we see that in DSDV ELP outperforms other metrics.

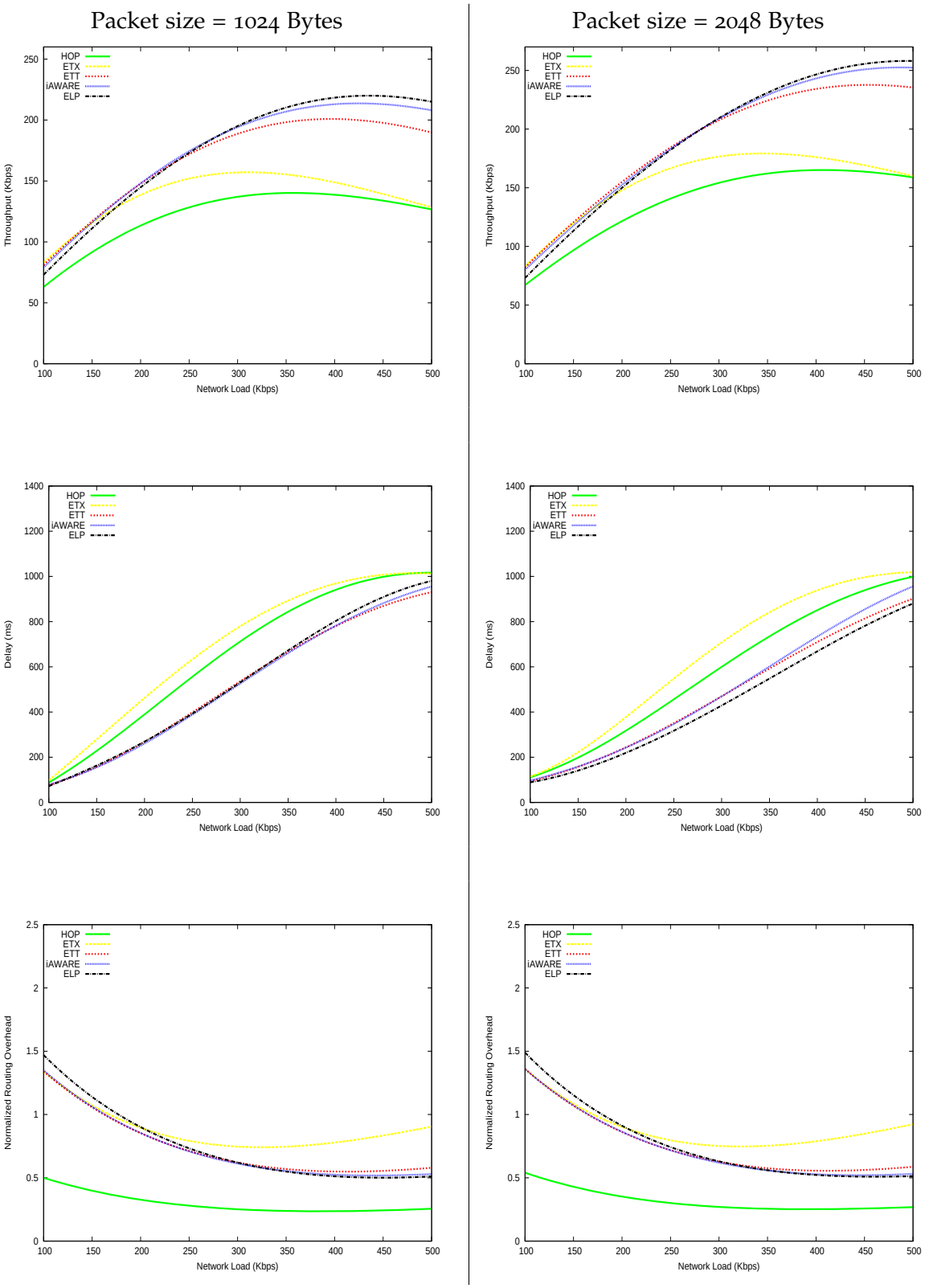


FIGURE 2.11 – *Performance evaluation results for DSDV-UDP Packet size 1024 and 2048 B*

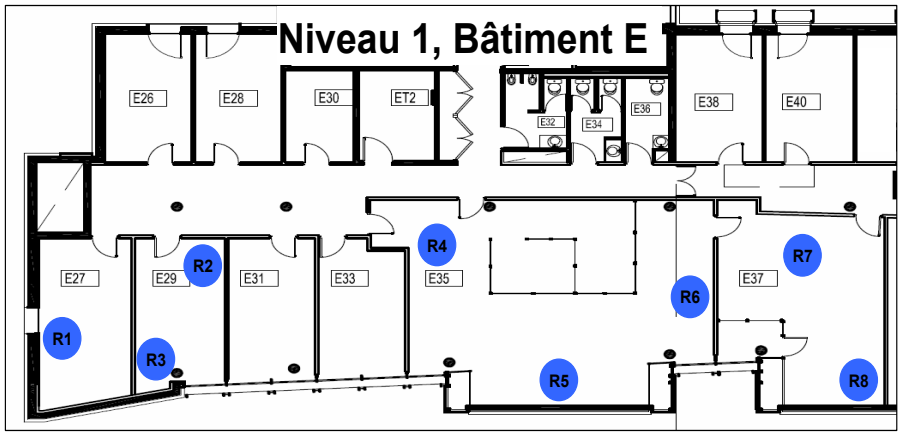


FIGURE 2.12 – *Distribution of mesh nodes of the LAAS-MESH*

2.4.6 Experimental Wireless Mesh Testbed

In order to evaluate parts of the proposed ELP routing metric, a wireless mesh testbed named LAAS-MESH was deployed at our laboratory LAAS-CNRS (Toulouse, France). The wireless mesh testbed consists of 8 mesh nodes deployed on the first floor in the offices of our research group (Tools and Software for Communication) as shown in figure 2.12. Each node of the testbed is an Avila Gateworks 2348-4 board (IPX425 architecture, 533 MHz processor) equipped with 2 mini-PCI Atheros wireless cards which are connected to small 5dB omni-directional antennas. Figure 2.13 shows the Avila 2348-4 card as well as the indoor Avila enclosure used for the mesh nodes. Each router runs the OpenWRT operating system (Kamikaze version). The wireless card uses Mad Wi-Fi drivers (version 0.10.5.6). The OLSR routing daemon version 0.5.6-r8 with ETX extension is used. At this stage, we have experimented with one component of the ELP metric, which is the asymmetry component. We modified the source code of the OLSR daemon to integrate the *Link Loss Asymmetry* aspect of ELP. We used an alpha of 0.8. The choice of 0.8 was mainly motivated by simulation results. A more comprehensive comparison between alpha values is a future direction. To maintain the comportment of the OLSR routing protocol implementation, the asymmetry aspect was integrated using some simplifications, but the main concept remains the same i.e. giving more importance to the forward loss component. The resulting package was then cross-compiled to create a modified OLSR daemon.

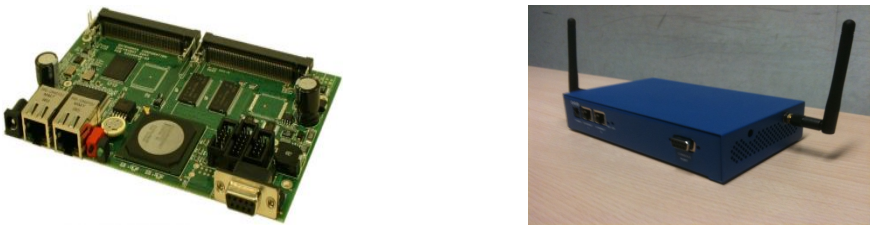


FIGURE 2.13 – *The Avila Gateworks 2348-4 card and the node outlook*

A number of measures were taken to minimize the impact of interference from other 802.11 wireless networks. The experiments were run late at night after office hours, often running throughout the night until early morning hours. We used a channel other than the one used by the WLANs in the lab. There are two background UDP flows of 100 Kbps each from R2→R4 and R6→R5. The flow that was used to compute the results was the end-to-end UDP flow from R1→R8. A packet size of 1500 Bytes was used. The measurement tool Iperf was used to take all the readings. Multiple runs of the experiment were made over a period of one week. A total of 20 hours of experiments were run for OLSR+ETX and another 20 hours for OLSR+ELP(Asymmetry) and the results are the averaged values for all the results obtained. For the flow R1→R8, we used traceroute and also observed the routing tables which revealed that typically two hops were required to reach the destination node R8 from the source node R1 . It should be noted that when the source changes the intermediate node that it uses to arrive at the destination, the actual effect is the change of two wireless links till the destination. To evaluate the difference between the two metrics, the data rate of the flow was increased and the performance of the two solutions was observed in terms of throughput, delay and packet loss percentage.

Figure 2.14 on the next page shows the results of the experimental performance evaluation. We see that when the load is light, both metrics perform more or less the same which is understandable because under light load, there is not much interference generated to cause problems. However, we see a significant difference between the performance of the two metrics under high load. The intuition for the performance improvement is that the asymmetry component gives more importance to the link loss ratios of data packets compared to the ACK packets and therefore better captures the asymmetric nature of communication of IEEE 802.11. This results in a selection of better end-to-end routes, resulting in higher throughput, low delay and low packet loss ratios. The results of the experimentation generally conform to the improvement observed through simulations [Ashraf 08a] as well in which we observed that integrating the asymmetry component into ETX improves the performance of ETX. However, the gains observed in the experimental results are significantly larger than were observed through simulations. A more thorough comparison spread over multiple weeks is envisaged to be carried out. Preliminary results as presented here show a promising direction. What is important to note is that most contemporary metrics including ETX, ETT, MIC and iAWARE use the same probe based loss ratio estimation and if our asymmetric component can improve performance for ETX then it is only logical that the performance of all these contemporary metrics is very likely to improve as well if we integrate the proposed asymmetry mechanism.

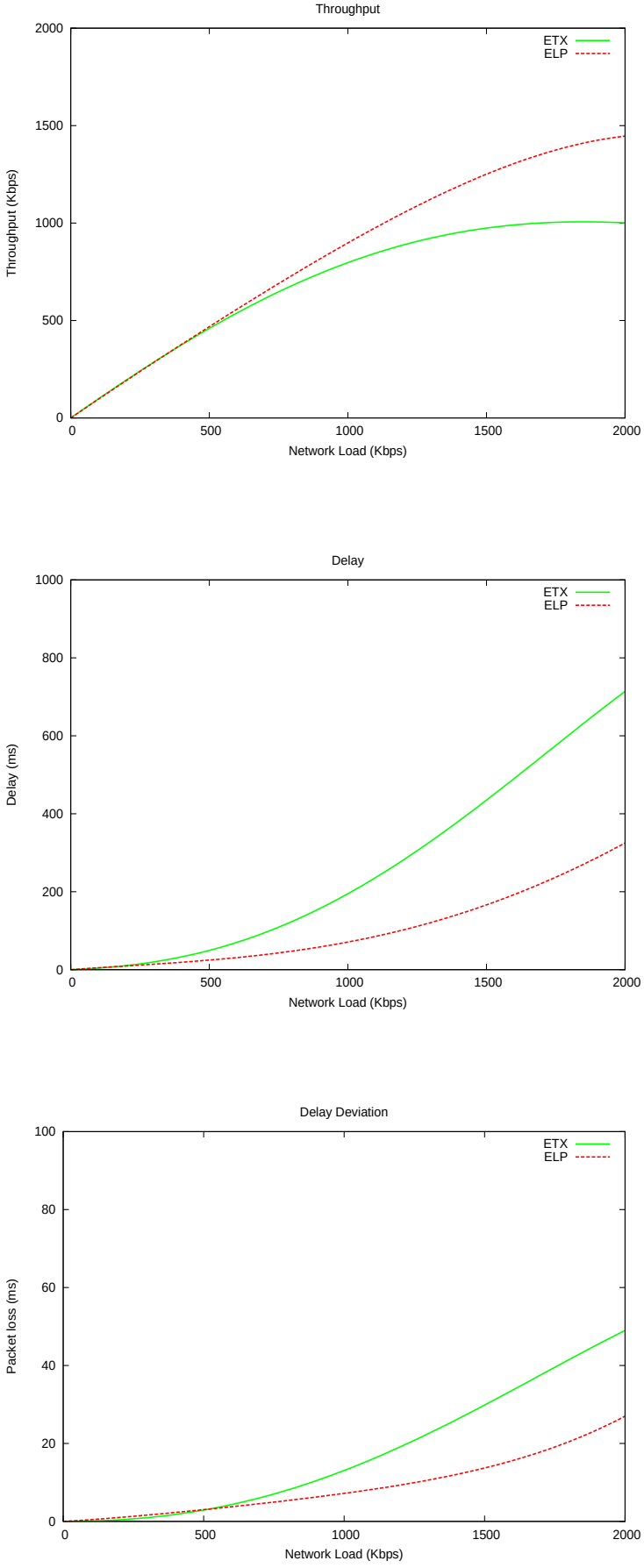


FIGURE 2.14 – *Performance evaluation of ETX and ELP (Asymmetry)*

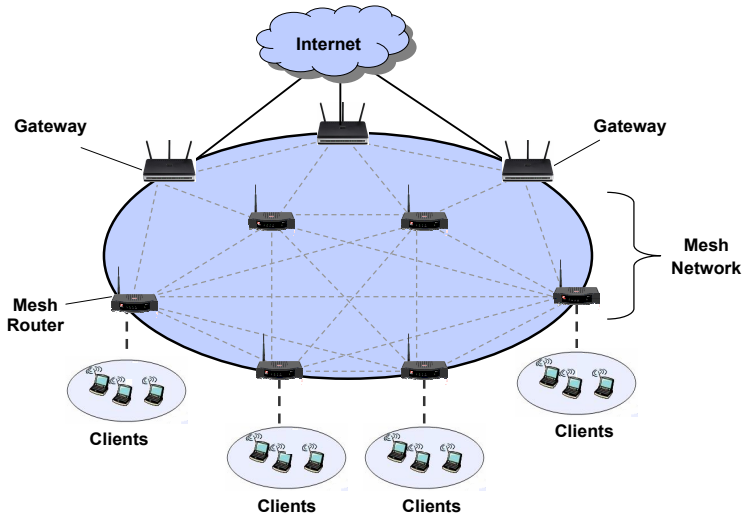


FIGURE 2.15 – *A Wireless Mesh Network with Gateway Nodes*

2.5 Extension of ELP Metric for Gateway-Oriented Traffic

In the previous section, we proposed the ELP routing metric for route selection between mesh routers. In this section, we propose an extension of the ELP metric (*ELP-GS*) which acts as a routing metric for gateway-oriented traffic in mesh networks. The metric considers both the gateway load and the quality of the route to the gateway. However, before the mesh routers can send traffic to gateway nodes, they must be aware of the identities of the gateways present and the route to them. Since the announcement of the presence of gateways is typically done through gateway advertisement messages, we also propose a *Gateway Discovery* protocol which also integrates the dissemination of the metric to mesh nodes.

In general, *Gateways* can be considered as specialized mesh routers which provide connectivity between the wireless mesh domain and the wired Internet as shown in figure 2.15. Mesh networks which have a connection to the Internet are likely to have a significant volume of traffic directed towards gateways, increasing the likelihood of congested nodes and regions near the gateway. The gateway selection problem is straightforward when we have a single gateway, but a single gateway can get congested and become a bottleneck for the entire network [J. Jun 03]. To mitigate this problem, multiple gateway nodes are typically installed to distribute load and improve performance. However simply adding more gateway nodes does not necessarily mean a proportional increase in the nominal capacity of the network. Efficient gateway and route selection is required when we have multiple gateways with multiple possible routes to these gateways. In this section, we briefly discuss the existing solutions proposed for gateway selection, the design considerations for developing a routing metric for gateway-oriented traffic and finally the proposed extension of ELP along with a gateway discovery protocol.

2.5.1 Review of Related Work

Most existing gateway selection schemes in ad hoc networks select the nearest gateway. However, nearest gateway selection (hop count) is a poor choice in multi-hop wireless networks [Couto 02]. A number of solutions [C-F Huang 04],[K. Yonggyu 07],[J. Shin 05],[R. Kumar 07],[D. Nandiraju 06] propose using the gateway load (often measured as the average queue occupancy) as the metric for gateway selection. Gateway-load based gateway selection can help distribute the traffic more evenly over the network rather than creating a few hot-spots making it a better alternate to the traditional hop count metric. The remaining energy at the gateway node and its mobility are sometimes used as metrics [F.P. Setiawan 08] for mobile gateways. Some approaches [S. Tajima 06] propose solutions for gateway selection which aims at minimizing the total traffic transmitted between the mesh routers. However, this solution has been proposed for mobile mesh client networks and the cost function of minimizing the traffic between APs encourages the selection of shorter routes which is similar to the hop count metric. Some researchers [S. Das 07] argue that the efficiency of the mesh network can be increased if multiple frequencies are used at the gateways and the nodes are partitioned among these frequencies. The main idea is interference reduction by using channel diversity. Some approaches [L. Luo 08] use existing metrics (ETT) for selecting gateways in the mesh backhaul.

The upcoming IEEE 802.11s draft standard proposes the *Hybrid Wireless Mesh Protocol* (HWMP) as the default routing protocol for mesh networks. HWMP uses a proactive routing approach for gateway discovery in mesh networks. Gateways periodically broadcast special advertisement packets which are flooded throughout the network and mesh routers select the best gateway based upon a routing metric. While 802.11s proposes using the *Airtime* metric for routing within the mesh network, the choice of a routing metric for gateway selection is left open. Alternatively, the ETX metric can be used which has been shown [R. Draves 04b] to work well for static mesh networks. However, we believe that the problem of gateway and route selection can be handled more efficiently if multiple gateway-dependant and route quality metrics are jointly used to give the "*best*" choice of gateway and the route to it.

2.5.2 Design Considerations of metric for Gateway-Oriented Traffic

We identify some important design considerations for developing gateway and route-to-gateway selection metric for mesh networks :

- The selection of a gateway can be considered as a joint decision which also includes selection of the route to that gateway. The solution should strive for load balancing among multiple available gateways which could help achieve a more efficient use of the available network resources. Moreover, reducing interference is a primary concern in mesh networks. Therefore, the proposed solution

should minimize interference between flows. Among a set of available routes, high quality (in terms of less interference, less link loss ratio etc) routes should be selected to the gateway.

- Route selection should be dynamic in the sense that the network should react to changing traffic patterns and changing load at the gateways. In reactive gateway selection approaches [Josh Broch 99], the route/gateway selection can sometimes become "*stale*" in the sense that once a route/gateway has been selected, it is used until the route breaks regardless of whether better routes or less loaded gateways have become available. The proposed solution should have an active component which periodically informs the mesh routers of the load at the gateways as well as the cost to reach those gateways.

2.5.3 ELP Metric for Gateway Selection (ELP-GS)

In this section, we describe the components of the proposed *ELP-GS* metric.

1. Expected Link Performance - To incorporate the quality of the route, we use the *Expected Link Performance* metric developed in previous section. This includes three components i.e. *Link Loss Ratio*, *Link Capacity* and *Link Interference*.

$$ELP(l) = ELP_{LinkLossRatio(l)} \times ELP_{LinkInterference(l)} \times ELP_{LinkCapacityFactor(l)} \tag{2.36}$$

2. Gateway load - The gateway load is defined as the average queue occupancy at the network interface of the gateway with the mesh network. There may be delay problems especially for the high speed downlink traffic if the gateway is overloaded. It is also much more efficient to uniformly distribute the load over multiple gateways instead of overloading a few gateways. To estimate the gateway load, the long-term average queue occupancy Q at the gateway interface servicing the mesh network is considered. We assume that there is a single queue which services all classes of traffic. To smooth out variations, an exponentially weighted moving average is used as shown in the formula below.

$$QLength_{t+1} = \alpha\, QLength_t + (1-\alpha)\, QLength_{t-1} \tag{2.37}$$

Together these two elements help in the selection of both the gateway and route to the gateway. The final expression of the path metric for Gateway Selection Metric for accessing the gateway g over path p becomes :

$$ELP\_GS(g,p) = (\sum_{link\ \ell \epsilon p} ELP_\ell) \times QLength(g) \tag{2.38}$$

ELP-GS is an isotonic metric.

2.5.4 The Proposed Gateway Discovery Protocol

Here, we present our gateway discovery and routing protocol based on AODV (and similar to gateway-based version of HWMP), which handles gateway discovery and also disseminates the gateway reachability information along with the metric cost to reach that gateway.

The gateway nodes periodically broadcast small *Gateway Advertisement* packets (*GWADVs*). The format of the *GWADV* message is a modification of the *Route Request* packet of the AODV protocol with some additional fields and is shown in figure 2.16. The advertisement contains *i)* the ID of the Gateway (typically the IP address), *ii)* the unique ID for this advertisement packet (GWADV ID), *iii)* the load at the Gateway, and *iv)* fields for the route metric (ELP). The gateway periodically creates a GWADV packet, puts its ID and load in it and broadcasts it. Each node which receives a *GWADV* checks its local table to see it has already broadcast this packet. A previously seen *GWADV* is rebroadcast again only if it has followed a better route to this node than the last advertisement of the same ID. If it is a new advertisement (or the same *GWADV* but with smaller metric cost), the router creates or updates a new routing entry with the corresponding gateway as the destination and the next-hop as the node from which the request was received. The router stores the information including the load at that gateway, the unique advertisement ID and the route metric (link loss ratio, link interference and link capacity). The fields for the route metric in the packet are updated by adding to it the link metric for the link on which the *GWADV* is received. Eventually, the gateway identity, gateway load and gateway reachability information are distributed throughout the network and the mesh routers can make an informed decision to select the *best* gateway and route based on ELP-GS.

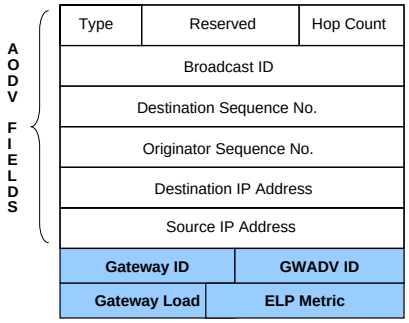


FIGURE 2.16 – *Format of the GWADV packet of Gateway Selection Scheme*

2.5.5 Performance Evaluation

Simulation Environment

The simulation setup remains as described in the previous section except for the elements described below :

- There are ten flows originating from mesh routers located at the perimeter of the network (to simulate users connected to edge routers) and the destinations of the flows are three gateways nodes (located equidistant) at the top. Ten random topologies are generated and results averaged across them. The position of all other nodes is random except the source nodes and the gateway nodes. The simulation is run for 100 seconds.

- We modify the AODV protocol to incorporate our scheme. The gateway nodes periodically broadcast GWADV messages just as a source node does in the classical AODV protocol. The interval of these advertisement messages is a design parameter. A very short period would incur a large routing overhead and strain on the network as every advertisement is subsequently broadcast by intermediate nodes. On the contrary, choosing a very long interval will result in stale information as the routing metric and load to the gateway are dynamic. For our performance evaluation we choose the interval of 5 seconds which seems a reasonable trade-off.

- We evaluate four possible approaches for selection of gateway and route-to-gateway : i) selection based on nearest gateway, ii) selection based on gateway load only, iii) selection based on ETX iv) selection based on gateway load and route quality (ELP-GS).

Simulation Results

Figure 2.17 presents the results for throughput, end-to-end delay, delay deviation and routing overhead for the four schemes discussed above. The first observation we make is that using only the gateway-load to select the gateway and the route gives the worst performance in terms of the throughput and the end-to-end delay. This is normal because there is absolutely no consideration of which route the flow will flow and the choice is done merely on the least loaded gateway. Imagine that the least loaded gateway is located the furthest away from the mesh router, the mesh router will select the first available route to that gateway without considering the length or the quality of that route. This could result in choosing a very long and poor quality (e.g. high interference, high link loss ratio etc) route which explains the low throughput and the high end-to-end delays. The next best option is to select the gateway which is the nearest. This provides some improvement over the load-based selection as at least it strives to choose routes and gateway located near to it. But hop count is a very rudimentary metric which does not take into account interference and other important factors and therefore performs less well than other possible schemes. For example, the nearest gateway (in terms of hops) may be the most congested gateway and the route to it (while being shortest) may have high interference. ETX outperforms both load-based selection and nearest-gateway selection, however, it does not incorporate other important factors such as *logical interference*, or asymmetry of the link or the capacity of the links. Next, we use the ELP-GS metric. ELP-GS integrates multiple

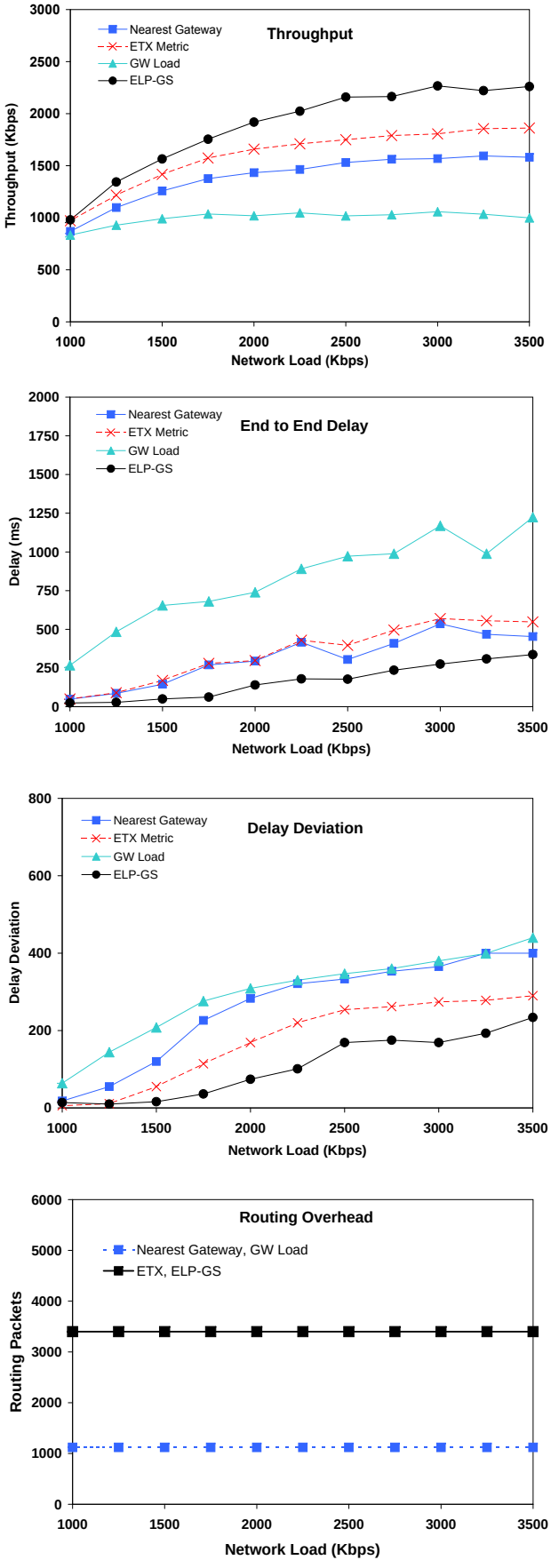


FIGURE 2.17 – *Performance evaluation results for ELP-GS*

factors including a component for adjusted link loss ratio (to capture physical interference), a component to capture logical interference, a component for link capacity and a component to integrate gateway load. ELP-GS outperforms all other metrics for most evaluation metrics considered. As explained before, the ELP part of ELP-GS captures multiple factors pertaining to link quality (and therefore route quality). ELP-GS additionally integrates the load at the gateways. This helps achieve a better load-balancing for the network as a whole. For gateway-oriented traffic, we can visualize the gateways as the roots of a tree towards which most traffic is directed, resulting in congestion regions and hot-spots near the gateways. A simple and efficient way to achieve a better distribution of load over the network is by spreading the load more equitably on multiple gateways instead of overloading a single gateway. Owing to selection of "*best*" routes to the gateway along with the least loaded gateway, overall ELP-GS provides better throughput, lower end-to-end delay and lower delay-deviation. The routing overhead is the lowest for nearest gateway selection and selection based on gateway load. This is because for these schemes, we only have the periodic GWADV messages and no other routing overhead. The routing overhead is higher for both ETX and ELP-GS since both schemes require periodic exchange of probe packets for metric calculation. However, this is a small trade-off compared to substantial performance gains in throughput and delay. Overall, we see that ELP-GS outperforms other metrics and the gains obtained are significant.

2.6 Conclusion

Selecting efficient end-to-end routes in wireless mesh networks is an important problem because interference plays a significant role in limiting the performance of the network. In this chapter, we presented the *Expected Link Performance* (ELP) metric for routing between mesh routers. The first component of ELP metric is that it considers the link loss ratios on the links to estimate the first component of link quality. An important contribution here is that ELP introduces the notion of link asymmetry in which we show that the forward loss ratios have a more important role than reverse link loss ratios because the forward direction is meant for the large data packets while the reverse is for small ACK packets. ELP mitigates this problem by introducing corrective terms which bias the overall link-loss ratio in favor of forward link-loss ratios. The second component of ELP introduces the link capacity i.e. the transmission rate of the transmitting radio on the link which has a significant impact on performance. The third component of ELP proposes the *Average Interference Ratio* (AIR) which captures the *logical interference* present on the medium. Most metrics do not explicitly take the contention or the deferred access caused by the CSMA-CA MAC of IEEE 802.11. Finally, we propose an extension of the ELP metric for gateway-oriented flows which considers the load at the gateway in addition to performance of links on the route. We are investigating the possibility of testing parts of the basic ELP metric on a wireless mesh testbed.

Route Maintenance in Wireless Mesh Networks

3

Contents

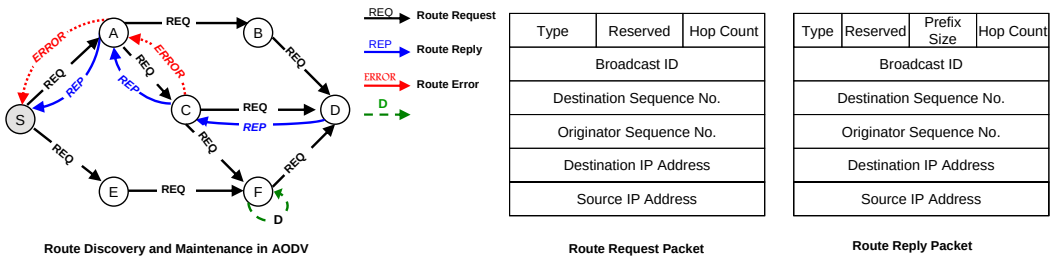
3.1 Introduction

Routing in mesh networks has been heavily influenced by ad hoc routing protocols. There are two broad families of ad hoc routing protocols : *proactive* (table-driven) and *reactive* (on-demand). A major attraction of on-demand routing protocols is their good reactivity to network conditions and generally, a much smaller routing overhead than their proactive counterparts. Ad hoc on-demand routing protocols such as DSR and AODV have been very popular for ad hoc networks and have undergone rigorous testing and enjoy numerous optimizations and implementations. Motivated by the popularity of these on-demand routing protocols, many testbed and real-world deployments of mesh networks use these on-demand routing protocols and a number of protocols developed specifically for mesh networks, such as SrcRR [D. Aguayo 05], AODV-MR [A. A. Pirzada 06], AODV-ST [K. Ramachandran 05a] are variations of DSR and AODV. More importantly, the *Hybrid Wireless Mesh Protocol* (*HWMP*) in the draft mesh standard 802.11s [802 08] also adopts a modified version of AODV. It is therefore interesting to investigate the performance of on-demand routing protocols in mesh networks.

Research reveals that despite lack of mobility in IEEE 802.11-based wireless mesh networks, on-demand routing protocols in particular, such as AODV and DSR surprisingly suffer from route instability due to frequent route breakages in these networks, resulting in significant performance degradation. A *route breakage* is defined as the condition when the routing protocol considers that the current route is "*broken*" because an intermediate node has detected a "*broken*" link in the route. Routing in 802.11-based wireless multi-hop networks generally works on the principle of *hop-by-hop* routing in which each intermediate node is responsible for delivering the data to the *next-hop* node. Each node transmits the frame to the *next-hop* node and waits for an ACK packet. If the ACK timer expires and there is no ACK received, the node assumes that it was a *transmission failure* and the link-layer retransmits the frame. In IEEE 802.11 based networks, there is a retry limit of 7 (or 4 for large packets), as mentioned in the standard [IEE 99]. If there are eight consecutive (one try and seven retries) failed transmission attempts to the *next-hop* node, then the link layer sends a failure notification to the network layer, we refer to this as *link failure notification*. In reactive routing protocols, this is interpreted as a *link breakage* at network layer. Protocols such as AODV systematically translate a *link breakage* into a *route breakage* and the intermediate node notifies the source node to find new routes. Frequent route breakages result in route request broadcast storms, poor performance and significant route instability. Although there are optimizations available [Yu 07] [C.M. Chung 01] [Lee 00] [P.C. Ng 04] which rely on alternate backup routes (local or end-to-end), but this depends upon the availability of alternate routes in the cache of intermediate nodes and still introduce delays and degrade performance.

The underlying assumption that in IEEE 802.11 networks, the *link failure notification* sent by link layer after 8 (or 4) *transmission failures* represents actually broken links is not accurate. The *transmission failures* may have been caused by a number of factors e.g. interference or noise and more importantly, *transmission failures* may be a transient phenomenon and links considered "*broken*" by the routing protocol at network layer have sometimes been observed to become "*connected*" immediately afterwards (more details in next section). It is pertinent to distinguish "*good*" links experiencing temporary transmission problems but are otherwise performing well from "*bad*" links with sustained transmission problems over a long time so that false link (and therefore route) breakages due to transient transmission failures are avoided. We propose a new route maintenance mechanism which improves the link breakage detection for on-demand routing protocols in 802.11-mesh networks. The proposed mechanism considers multiple factors to distinguish links with transient transmission problems which can be expected to improve shortly from those which have sustained transmission problems. Based on this information about link quality, the proposed mechanism takes a coherent decision on link breakage. The proposed mechanism can be incorporated in existing reactive routing protocols to increase route stability for both *single-radio single-channel* and *multi-radio multi-channel* mesh networks. The proposed solution complements existing approaches which aim at discovering alternate routes with reduced routing overhead. This chapter is divided into six sections :

- The first section describes the basic routing mechanism of reactive routing protocols namely, *Route Discovery* and *Route Maintenance* using AODV as example.
- The second section presents the problem of route instability for reactive routing protocols in wireless mesh networks. We first present the causes of the route instability and next we explain the effect of route instability (frequent route breakages) on the performance of the network using AODV as an example.
- In the third section, we review existing solutions for mitigating the problem of route instability and explain how our contribution is different.
- The fourth section presents our proposed solution - *Efficient Route Maintenance (ERM)* which has two main components : *Link Quality Assessment* and *Link Breakage Decision*. For *Link Quality Assessment*, ERM proposes two complementary solutions : a passive and an active solution. Moreover, we present an extension of the ERM mechanism to multi-radio multi-channel case to show that the proposed solution works in multi-radio multi-channel scenarios as well.
- The fifth Section deals with extensive performance evaluation of the proposed ERM mechanism and the two link quality assessment mechanisms that we proposed within ERM. The section concludes with the performance evaluation of ERM in multi-radio multi-channel scenarios.
- The final section concludes the chapter with possible future directions.



❑ **Destination Sequence No.** indicates the sequence no. the nodes has for the destination. An intermediate node can send reply to the source if its Destination Sequence No. is greater or equal to the one in the RREQ packet.

❑ **Originator Sequence No.** is the current sequence number to be used in the route entry pointing towards the originator of the route request

FIGURE 3.1 – *Route Discovery and Maintenance and AODV packet types*

3.2 REACTIVE ROUTING PROTOCOLS

3.2.1 Route Discovery and Route Maintenance in Reactive Routing Protocols

We describe the routing mechanism of reactive approaches in multi-hop wireless networks using AODV over a IEEE 802.11 network as example. There are two main phases in AODV : *Route Discovery* and *Route Maintenance*. Figure 3.1 presents the two main phases of AODV and the packet formats.

A. Route Discovery

A source node (S) which needs to send data to a destination (D) first checks its cache and if there is no route available, it broadcasts the route request packet - ROUTE_REQ (denoted by "*REQ*" in figure 3.1). The ROUTE_REQ packet contains a destination sequence number to measure freshness of the route request. Every intermediate node which receives the route request checks to see if it has already seen the sequence number. If it is a new request, the node creates or updates a new routing entry with the source node as the destination and the next hop as the node from which the request was received. This establishes a "*reverse*" route at each intermediate node towards the source. If the node observes that the route request has a previously seen sequence number, it drops the route request packet (denoted by "*D*") and does not rebroadcast it. Assuming that node F has already received a route request packet from E and node C later sends the same route request packet to node F, node F will drop it. If it is a new route request, the node rebroadcasts the route request. This process is repeated until the request reaches the destination. The destination node creates a ROUTE_REPLY packet (denoted by "*REP*" in figure 3.1) and sends it to next-hop node on the route to source. Each intermediate node receives the reply packet, creates an entry for the next-hop node to the destination node and forwards the reply. Thus, the "*forward*" route from destination to the source is created. Eventually, the source receives the reply packet, creates an entry of next-hop for the destination node and route discovery is complete. The route from source to destination has been created and the source can start sending data.

B. Route Maintenance

Route Maintenance comes into play during the use of the data path which was established during the *Route Discovery*. Route maintenance mainly deals with detecting broken links and reporting them to the source node. All intermediate nodes on the route to the destination are responsible for detecting if the wireless link to the next hop node is "broken". For IEEE 802.11 based networks, link breakage declaration relies on link-layer *link failure notification* which is generated after a certain number (4 or 7) of unsuccessful frame retransmissions. The routing protocol concludes that the link is broken (*link breakage*) and that the route to the destination is broken. AODV then sends a unicast Route Error message (ROUTE_ERROR, denoted by *"ERROR"* in figure 3.1) to the source node upstream (from node C in figure 3.1). When the source node receives the error message, it concludes that the route is no longer valid and starts another route discovery.

3.3 Route Instability : Causes and Consequences

3.3.1 The problem of Route Instability

In this section we explore how changing network conditions contribute to route breakages in mesh networks. IEEE 802.11 standard specifies that the link layer report transmission problems to higher layers if it fails to transmit a frame successfully to the next hop node after a certain number of transmission attempts at the link layer. As discussed previously, the standard limit is that of 8 attempts (one transmission and seven subsequent retransmission attempts) or 4 for frames greater than a threshold. In multi-hop wireless networks, data packets traverse from source to the destination node over multiple wireless hops and it is not uncommon that some packets experience transmission problems over some wireless links. However, whether those transmissions problem actually represents a broken link or just a temporary problem is a different matter. Routing protocols for multi-hop wireless networks have an inherent vulnerability that they are dependant upon intermediate nodes to detect and report (or repair) broken links. It is the responsibility of each intermediate node to ensure that the data packets are transmitted to the next hop. For reactive routing approaches, if an intermediate node fails to transmit data to the next hop, it is expected to inform the source that the link to the next hop is broken, or launch local route recovery if such a mechanism is available.

Consider the chain mesh topology shown in figure 3.2. Interference between conflicting links in a network can be explained as interference between the flows (inter-flow interference) and within a flow traversing multiple hops (*intra-flow interference*). In figure 3.2, flow 1 $(A \rightarrow F)$ experiences *intra-flow interference* between hops $A \rightarrow B$ and $B \rightarrow C$, $B \rightarrow C$ and $C \rightarrow D$ and so on. Depending upon the transmission power and the carrier sensing range, the *intra-flow interference* can also be between links two

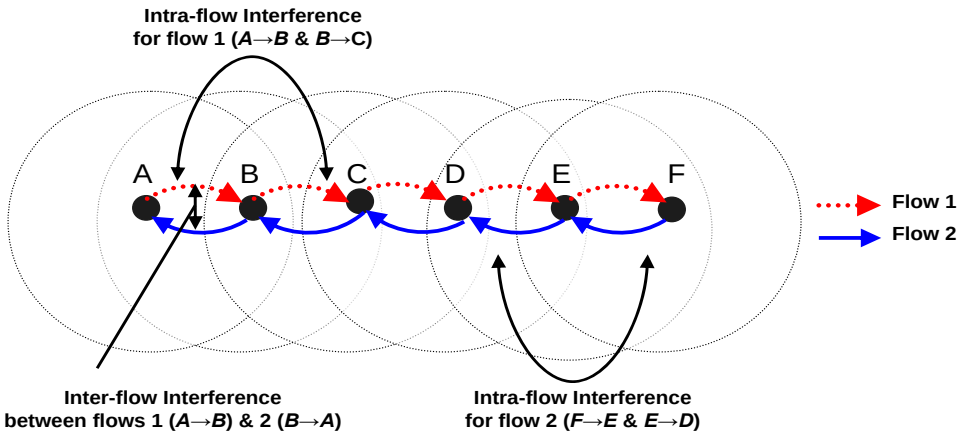


FIGURE 3.2 – *Inter and intra-flow interference in a single-channel mesh network*

or more hops away. *Inter-flow interference* exists between flows on the same frequency channel such as between flow 1 ($A \rightarrow F$) and flow 2 ($F \rightarrow A$). Both intra-flow and inter-flow interference can significantly degrade the performance of the network and can cause interference-related *transmission failures* resulting in *link failure notification* by link-layer which is interpreted as link (and therefore route) breakage. In multi-hop networks, it is likely that occasionally a packet would be dropped (8 tries at link-layer) from time to time for flows traversing multiple hops, especially if there is high interference present on the wireless medium.

3.3.2 Consequences

In this section, we show the consequences of these route breakages. When an intermediate node on the data path between the source and destination detects a *link breakage* (and consequently *route breakage*), it generates a route error message. The route error message generated by an intermediate node traverses the reverse path to the source node and all the intermediate nodes which receive this message delete the routing entry for that particular destination. Moreover, each route error is subsequently followed by a route discovery phase launched by the source node which introduces more packets in the network. For the six node chain topology shown in figure 3.2 we observed the routing messages generated due to link breakages and the throughput and delay variation for a UDP flow traversing multiple hops ($A \rightarrow F$) using AODV. There is another UDP flow in the opposite direction ($F \rightarrow A$) with the same data rate of 1000Kbps and a packet size of 1000 Bytes. Figure 3.3 (a, b & c) show the variation of routing packets, and throughput and delay variation for the flow from $A \rightarrow F$ over time. The route breakage instances are shown by asterisk in the top bar in each figure. We see that there are frequency peaks of route error and route request packets over time indicating frequent route breakages and subsequent route discovery packets introduced in the network. Due to frequent route breakages there is a high variation of throughput over time which occurs due to route breakages and due to the fact that

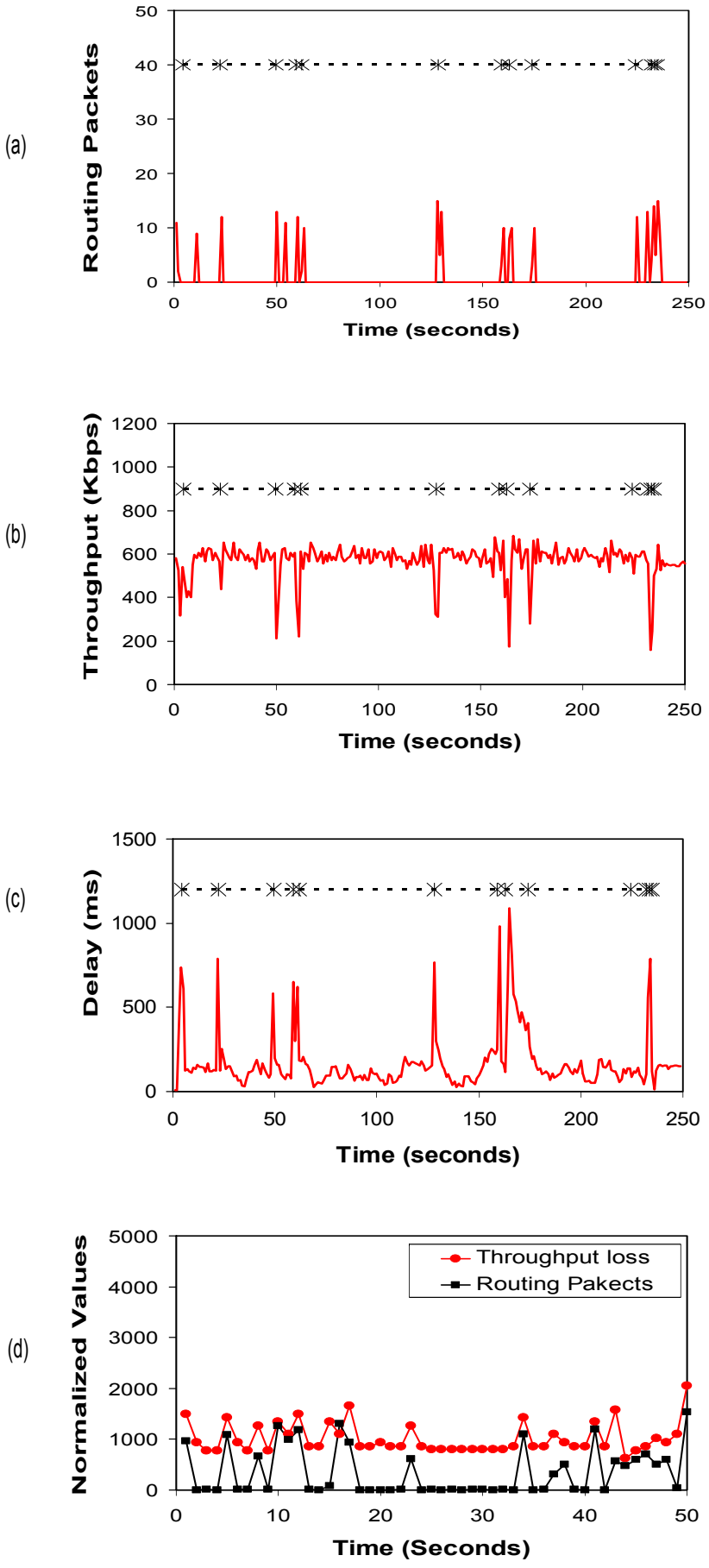


FIGURE 3.3 – *Correlation of route breaks with routing packets, throughput and delay*

each route breakage introduces more routing packets in the network which create more interference and cause further interference related route breakages. Each route breakage implies that the source must start another route discovery phase and during the route establishment phase, data packets must wait. Due to this, there is high variation of end-to-end delays in the network as shown in the figure.

In figure 3.3 (d), we show the correlation between throughput loss and routing packets. The throughput-loss is simply the observed throughput subtracted from a theoretical maximum achievable throughput (this is simply a constant) for the flow. We plot scaled values of throughput-loss and routing packets since the values cannot be directly plotted and we are interested in only the correlation between the two curves. The peaks in the throughput-loss curve represent instances of high throughput degradation. We see a strong correlation between throughput-loss and route breakage (Route Error, Request and Reply) packets because after route breakage route error, route request and route reply messages are introduced in the network which creates further interference causing more route breakages and degrade the throughput.

3.4 Review of Existing Works

Reactive routing protocols have two phases as described in the previous section : *Route Discovery* and *Route Maintenance*. ***Most existing works focus on optimizing Route Discovery. Our main motivation is that there has been little research on making Route Maintenance more efficient by avoiding frequent link breakages due to transient transmission problems on the wireless links.*** Most existing approaches rely upon the IEEE 802.11 link layer based feedback to declare link breakages. While there are a number of solutions on how to cope with route breakages, including local route recovery and using alternate routes [Yu 07] [C.M. Chung 01] [Lee 00] [P.C. Ng 04] [Haas 98] [M. R. Pearlman 00] [S.L. Wu 01] [Qin 02], the fact that many link breakages are transient and route maintenance can be optimized has been neglected. The first class of solutions employs backup routes in case the original fails. Some approaches [C.M. Chung 01] [Lee 00] propose maintaining backup routes so that if the primary route fails, an alternative route can be used instead of launching new request broadcasts. There are at least two problems with these kinds of solutions. First, backup routes are typically created in the same phase as the route discovery for the primary route. Hence, after the data has been routed over the primary route for some time, the backup routes may be stale and may not necessarily represent valid or optimal routes as network conditions may have changed and routes which were previously viable may not be so. Hence, alternate routes may actually be routes which are either broken or inefficient. Second, the assumption that *link failure notification* reported by the link layer represents actual link breakages may not be true due to a number of other factors e.g. interference, noise etc.

The second class of solutions proposes local route discovery and maintenance solutions. In the *Zone Routing Protocol (ZRP)* [Haas 98] [M. R. Pearlman 00], authors propose creating alternate local routes if a route breaks, so that data can be rerouted using links passing through a different zone. In another approach, [Yu 07] authors propose a solution where when an intermediate node detects a link as broken, it launches a local Route Discovery process and neighboring nodes reply if they have alternate links to reach the destination by bypassing the failed link. This can help route around failed links. However, the Route Maintenance phase still suffers from unnecessary link breakages and therefore unnecessary local route request broadcasts. An optimization of AODV called AODV with *Local Route Repair* (AODV-LRR) and similar works [S.L. Wu 01] [Qin 02] also propose local route recovery procedures which can minimize the adverse effects of route failures. A different solution [P.C. Ng 04] can be that nodes in the network try to establish routes if the current next-hop link is likely to break. It is a *don't-break-before-you-can-make* approach.

Recently, the problem of route instability in multi-hop wireless networks was studied [K. Ramachandran 07b] and authors describe route flapping i.e. frequent route switching due to changing route metrics as the main cause of route instability. They propose an algorithm for route stability by switching a route only if the new route provides a difference in quality greater than a threshold. However, they do not consider route instability due to frequent route breakages and moreover, their approach works at the source node only which decides whether to switch routes. However we argue that in all these solutions, the basic assumption that *link failure notification* by link layer is due to an actual link breakage may not necessarily be true.

3.5 Motivation

While route instability is problematic for multi-hop wireless networks in general, it is a particularly serious problem for wireless mesh networks which must act as a high-speed wireless backbone for user networks. Frequent route breakages can seriously degrade performance (see section 3.3.2). Therefore, we must have a solution to deal with the problem of false and frequent route breakages. In the next paragraphs, we first show and explain how some route breakages may be false. Next we briefly outline how our approach differs from existing works.

The main motivation for this contribution is that the *link breakage* detection mechanism of reactive routing protocol based on IEEE 802.11 networks has some limitations in that transient factors such as interference, channel load or a burst of channel errors can lead to consecutive *transmission failures* at link layer resulting in a *link failure notification* by link-layer to the network layer. On-demand routing protocols consider the *link failure notification* systematically as an actually "broken" link (*link breakage*) and therefore consider the route to be broken (*route breakage*). We show that most *link*

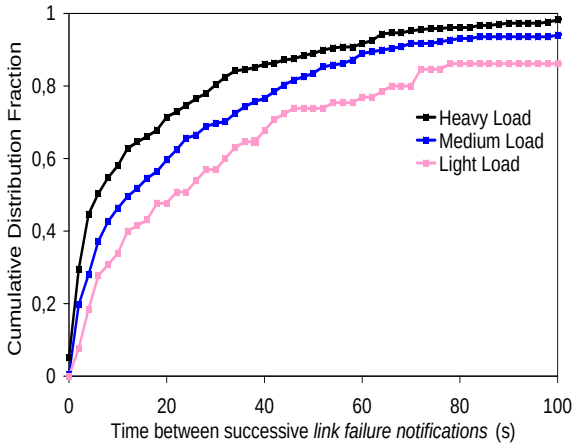


FIGURE 3.4 – *Average time between successive link-layer link failure notifications*

failure notifications from link layer do not necessarily represent actual link breaks and should not be interpreted as such at the network layer.

In figure 3.4, we study the system in conditions which allow us to view the phenomenon of "*transient*" nature of link breakages. We do not consider the *link failure notification* as representative of *link breakage* (and *route breakage*) and instead continue using the link to see how it behaves. For each link studied, the routing protocol at the network layer is made to continue using the link (i.e. not consider it as *link breakage* despite the *link failure notification*). The *x-axis* represents the average time between *link failure notification* for each particular link. Theoretically, once a link is reported "broken" by link-layer, the network layer should continuously receive *link failure notifications* from link-layer for every packet it tries to send over that link. The *y-axis* represents the cumulative distribution function of all the links. As we see in figure 3.4, the average duration between a *link failure notification* by link-layer and the next notification for that same link (which is still being used due to our ignoring of link layer notifications) is on the order of seconds which proves that the *link failure notification* by the link-layer does not represent actually broken links (*link breakage*) as is classically interpreted by reactive routing protocols. All three curves for light, medium and high network load are plotted which clearly indicate that despite receiving a link-layer *link failure notification* for a link, the links were reusable for a large amount of time before the next notification and so on. This proves that interpreting the *link failure notification* as *link breakage* is incorrect as transient interference or a burst of channel errors may result in consecutive *transmission failures* which lead to a *link failure notification* from link-layer. In reality, the links are usable even after the assumed broken by the protocol.

Few approaches optimize *Route Maintenance* by incorporating link failure differentiation which can avoid unnecessary route breakages. We argue that performance can be significantly improved by avoiding unnecessary route breakages rather than

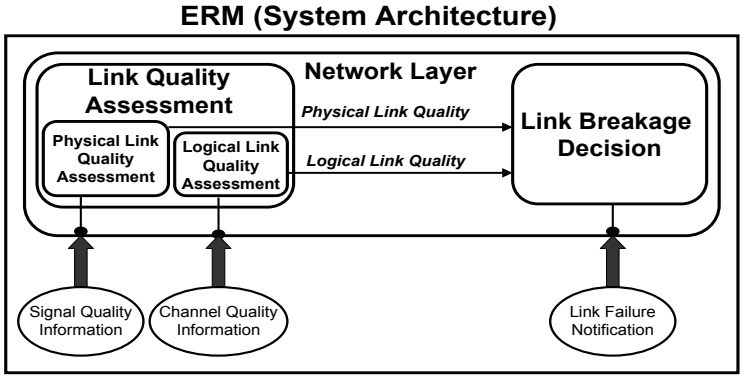


FIGURE 3.5 – *ERM System Architecture*

utilizing mechanisms to recover from these route breakages. We aim to develop a mechanism which can improve the link breakage detection for reactive routing protocol in 802.11 mesh networks and integrate it in Route Maintenance so that we can distinguish between links which are performing poorly for a long time from those experiencing transient transmission problems. Rather than systematically trying to recover from doubtful route breakages, we concentrate on introducing resilience in the network against route breakages due to transient network conditions on the link. We extend our preliminary work [U. Ashraf 08] for improving route maintenance in wireless mesh networks. The focus of our contribution is on Route Maintenance and in particular improvement of the link breakage detection mechanism and its incorporation in the Route Maintenance mechanism so that accurate decisions about link breakage and consequently route breakage can be made. Efficient Route Maintenance procedures are proposed which can significantly improve the performance of reactive routing protocols. It is important to note that the proposed mechanism is not meant as a replacement, but as a complementary mechanism in addition to approaches that aim at discovering alternate routes or using other mechanisms such as local route repair.

3.6 Proposed Solution : Efficient Route Maintenance (ERM)

In this section, we describe the proposed route maintenance scheme - *Efficient Route Maintenance* (*ERM*) for on-demand routing protocols in 802.11-based wireless mesh networks. ERM is a cross-layered solution in which the network layer uses information available at the MAC and physical layers to make a coherent decision about link breakage. The main job of ERM is to decide which links to declare as broken and more importantly when to declare them broken. With this objective in mind, ERM makes distinction between two types of links :

- *"Good"* quality links which are assumed to have transient transmission problems
- *"Bad"* quality links which are assumed to have sustained transmission problems

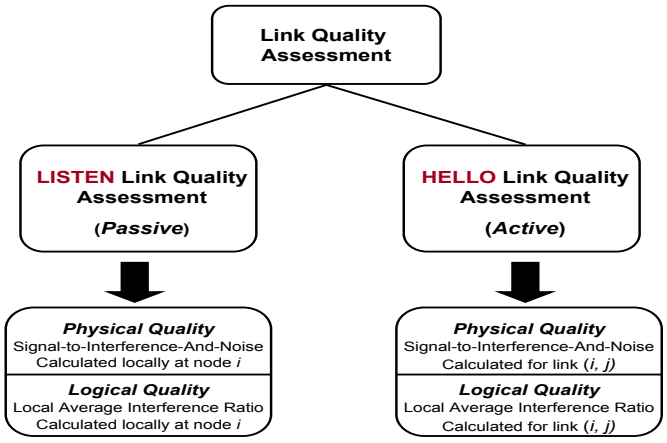


FIGURE 3.6 – *Two possible solutions to Link Quality Assessment*

Figure 3.5 shows the components of ERM at a node. There are two main components of ERM : 1) ***Link Quality Assessment*** and 2) ***Link Breakage Decision***. The *Link Quality Assessment* component is assigned the task of estimating the long-term quality of the link at two levels : the *physical link quality* and the *logical link quality*. The estimated long-term link quality is then passed to the *Link Breakage Decision* component. When the MAC layer fails to transmit a data packet to the next hop node, it reports the transmission problem to the *Link Breakage Decision* component. Traditionally, the routing protocol residing at the network layer systematically considers this as a route breakage [C. Perkins 03]. However, the *Link Breakage Decision* component in ERM uses the long-term link-quality information delivered to it by the *Link Quality Assessment* component to make a coherent decision.

3.6.1 Link Quality Assessment in ERM

ERM offers two complementary mechanisms for link-quality assessment (figure 3.6).

1. A *Passive*, measurement-based mechanism - the *Listen Link Quality Assessment*
2. An *Active*, measurement-based mechanism : *Hello Link Quality Assessment*

3.6.1.1 *Listen* Link Quality Assessment

This mechanism is called *Listen* because it is a passive approach and estimates the link quality by either "*listening*" to the medium or using information locally available at the node. This means that there is no active component or extra packets generated by the mechanism. ERM tackles the problem of link quality estimation by dividing the problem into two parts : a mechanism for determining the *physical* quality of the link and a separate mechanism for determining the *logical* quality of the link. For estimating the physical quality of the link we base ourselves on the classical signal-strength based mechanisms for estimating the physical quality of the link. *Signal-to-Interference-and-Noise Ratio* (*SINR*) is widely considered as a good indicator of link

quality as it provides measurements from physical layer. SINR at a node is calculated as :

$$\frac{P_o}{P_N + \sum_{r=1}^{n} P_r} \tag{3.1}$$

Where P_o is the power of the signal for the current packet being received at the receiver, P_N is the noise level and $\sum P_r$ is the sum of signal power from interfering transmissions. Since *Listen* is a passive mechanism, it can only use the locally available information. For a link (i, j) we denote the SINR measured at node i for data received from node j as $SINR(i)$. This is an approximation in which it is assumed that the link has the same quality in both the directions. In order to get an idea of the long-term performance of the link, node i maintains the average SINR of all the frames received from node j for a sliding window of time.

The *logical* quality aims at capturing the link quality in terms of contention on the link. This is the *Logical Interference* which is captured using the *Average Interference Ratio* at node i (*AIR(i)*) - as explained in chapter 2. High *AIR(i)* means that there is less time available on the medium to transmit and that there is high contention on the channel. This introduces delays in accessing the channel and intuitively this can also be used as an indication of the probability of transmission failures. The *Average Interference Ratio* AIR(i) at a node i during a time interval T is calculated as :

$$AIR(i) = \frac{T_{Receive} + T_{Occupied} + T_{Backoff}}{T} \tag{3.2}$$

To capture the long-term quality of the link, both the *physical* and *logical* quality of the link is calculated over a moving window of 10 seconds for each outgoing link at a node. This reduces the problem of transient problems and gives an idea of the long-term performance of the link. Selecting an interval too short would result in too frequent route breakages as even transient link quality problems would result in link breakages. Selecting an interval too long would result in a very slow responding route maintenance mechanism which may force the protocol to continue using poor quality links for a long time. Ten seconds seems to be a good trade-off and results from ETX [De Couto 03] validate the fact that a moving window of 10 seconds is a good choice for mesh networks.

3.6.1.2 *Hello* Link Quality Assessment

This mechanism is called *Hello* because it has an active component whereby information is exchanged between nodes using extra packets. Similar to the *Listen* Link Quality Assessment, the *Hello* mechanism estimates both the *physical* and *logical* quality of the link. For estimating the physical quality of the link we again use SINR, but the difference this time is that we consider the link SINR in contrast to the local SINR of the *Listen* mechanism. The *Listen* mechanism supposes that the link quality is the same in the two directions which is not necessarily always true as the link

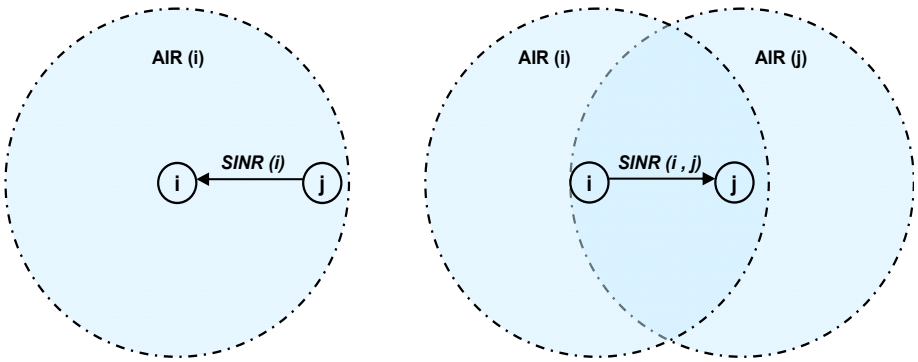


FIGURE 3.7 – *Listen and Hello Link Quality Assessments*

quality in the two directions can be very different. In reality, for a link (i, j), we have data flowing from i to j which is the key criterion. Similar to the receiver-based measuring of signal-strength [G. Holland 01] [B. Sadeghi 02], we use receiver-based link quality estimation based on *SINR* at the receiver. For a link (i, j) we denote the SINR measured at node j for data received from node i as $SINR(i, j)$. Consider the example as shown in figure 3.7 for a link (i, j), the receiver j maintains the SINR of frames received from node i for a sliding window of time. Periodically, node j unicasts small packets to the node i which contain the average SINR of the frames received from node i. This mechanism will be more precise and accurate because we capture the SINR of frames in the correct direction.

In *Hello* Link Quality Assessment, the *Average Interference Ratio* at the two ends of the link is jointly considered to estimate the logical interference present on the link. Both the nodes at the two ends of the link keep track of the *Average Interference Ratio*. Periodically (once every second), nodes exchange their AIR values in tiny packets. This does not necessarily entail routing overhead as some protocols such as AODV require periodic exchange of *Hello* packets between nodes active in the data path and the AIR values can be piggy-backed on them without incurring any extra overhead. The *Average Interference Ratio* $AIR(i, j)$ for the link (i, j) at a node i during a time interval T is calculated as the maximum of the AIR at the two end nodes because a transmission over the link experiences logical interference in the carrier sensing range of both nodes i and j :

$$AIR(i, j) = Max\,(AIR(i), AIR(j)) \tag{3.3}$$

To capture the long-term quality of the link, the *Hello Link Quality Assessment* is done for a moving window of 10 seconds for each link. This means that both the physical and logical parts of the link quality are calculated for a window of 10 seconds. This reduces the problem of transient problems and gives an idea of the long-term performance of the link.

3.6.2 Link Breakage Decision

The *Link Breakage Decision* (*LBD*) comes into action when a *link failure notification* (8 failed transmission attempts in total without ACK) is reported by the link layer. The key decision that the *Link Breakage Decision* component must make is to decide whether the link is broken and declare a route breakage or not. The *Link Quality Assessment* component periodically delivers the estimated link quality (both physical and logical) to the *Link Breakage Decision* component for all the outgoing links. The focus of this component is on improved link breakage decision making based on a relatively long-term performance of the link. As discussed previously, both the *Listen* and *Hello* mechanisms estimate the link quality over a relatively large moving window of time i.e. 10 seconds. A link which has few and transient transmission problems and has good physical and logical link quality represents a "*stable*" (or "*good*") link whereas a link with persistent transmission problems over a long period of time along with poor physical and logical link quality represents an "*unstable*" or "*poor*" link.

For the physical link quality, the decision is simple because we reply on pre-specified SINR threshold values against data rates (e.g. 10dB for 11 Mbps). If the long-term SINR value is below the minimum threshold required for maintaining that specific data rate, we can consider the physical quality of the link as poor. For the logical link-quality component, there cannot be a universally accepted optimal value and therefore we present our results for various values of AIR. The logical link quality component varies as $0 \leq AIR \leq 1$. We suppose that β is the threshold for considering AIR as too high. The appropriate threshold β for distinguishing "*poor*" quality links with permanent transmission problems from "*good*" links with transient transmission problems are a design parameter. We do an extensive performance evaluation for β. The algorithm below describes the pseudo code for ERM including the link quality estimation and the link breakage decision components.

ERM significantly improves the *link breakage* (and therefore *route breakage*) mechanism by not considering every *link failure notification* systematically as a *link breakage*. The long-term performance of the link (in terms of physical and logical link qualities) is evaluated to make a coherent decision. ERM brings more stability to the routing protocols and protects them against the negative effect of transient changes in network conditions. This improves the lifetime of routes and provides a more stable routing in the wireless mesh networks.

Algorithm 1: Efficient Route Maintenance at node i

```
1  begin
2      while Outgoing links at node i ≠ ∅ do
3          foreach Outgoing link j do
4              Quality_Physical, Quality_logical ← LinkQualityEstimation(link(i, j))
5              LinkBreakageDecision( Quality_Physical, Quality_logical)
6          end
7      end
8  end
```

Algorithm 2: LinkQualityEstimation

Preconditions: Mode ∈ {Listen, Hello}
Input: $link(i, j)$
Output: Physical and Logical Link Quality

```
1  begin
2      if Mode = Listen then
3          SINR(i) ← SINR observed at i for packets from j → i
4          AIR(i) = (Time(i)_Receive + Time(i)_Busy + Time(i)_Backoff) / TotalTime
5          Quality_Physical ← SINR(i)
6          Quality_Logical ← AIR(i)
7      end
8      if Mode = Hello then
9          SINR(i,j) ← SINR sent from j to i for packets from i → j
10         AIR(i,j) = Max{AIR(i), AIR(j)}
11         Quality_Physical ← SINR(i,j)
12         Quality_Logical ← AIR(i,j)
13     end
14     return Quality_Physical (i, j) & Quality_Logical (i, j)
15 end
```

Algorithm 3: LinkBreakageDecision

Preconditions: Link Failure notification, $\alpha \leftarrow SINRThreshold$, $\beta \leftarrow AIRThreshold$
Input: $link(i, j)$, $\text{Quality}_{\text{Physical}}$, $\text{Quality}_{\text{Logical}}$
Output: Link Breakage Decision for link (i, j)

```
1  begin
2      BreakStatus ← False
3      if Quality_Physical ≤ α   OR   Quality_Logical ≥ β then
4          BreakStatus ← True
5      end
6      return BreakStatus
7  end
```

3.6.3 ERM in multi-radio multi-channel mesh networks

The problem of interference-related false route breakages is severe for single radio, single channel wireless mesh networks. Wireless mesh networks have evolved over the years and today multi-radio, multi-channel wireless mesh networks are common. We explore multi-radio extensions of AODV which can exploit multiple available channels between neighboring nodes to increase route stability. Multi-radio mesh networks have a better capability to reduce the effects of false link breakages as there are usually multiple redundant links between neighboring nodes and if a link "breaks", traffic can be re-routed on these alternate links. We implement the multi-radio extension AODV-MR [A. A. Pirzada 06] for evaluating the performance of AODV in multi-radio multi-channel environments. The basic idea is that in the Route Discovery phase, the route request is broadcast over all the available interfaces and the source node, the intermediate nodes and the destination node create routing entries with interface information as well. The same authors propose the multi-link extension to AODV (AODV-ML) [AA Pirzada 07b] for multi-radio multi-channel networks. In the route discovery phase, the information about the multiple wireless links between neighboring nodes (on different channels) is also incorporated and each intermediate node creates these multiple links to each next-hop node during the Route Request and Route Reply phases. The basic idea is that during the route discovery phase, multiple links to the next hop node are created depending upon the number of radios on each node and upon the channels to which they are configured.

In many cases, we have multiple-link connectivity between neighboring nodes which can be exploited for improved connectivity. However, the multi-radio extension [A. A. Pirzada 06] does not specify how to exploit multi-link availability for Route Discovery or Route Maintenance in case of broken links. Typically, a route breakage would entail the same route error message by an intermediate node to the source which can then use an alternate route since it does not exploit the multi-link availability. However, we argue that route maintenance in AODV-ML can be improved through a number of ways. Since there is no standardized version of AODV for multi-radio multi-channel mesh networks, we choose to integrate our proposed mechanism in AODV-ML. We aim to show that even in the presence of multiple links and even with reduction of link breakage problems (by using alternate redundant links), ERM still provides improved performance. More specifically, we perform the evaluation of ERM in AODV-ML to show that ERM works well even for this case. We have implemented three different versions of AODV-ML :

- AODV-ML
- AODV-ML with link switching
- AODV-ML with link switching and ERM

In the basic AODV-ML protocol, a link breakage is reported to the source and the source can then either use an alternate route or launch another route discovery process. In AODV-ML with link switching, if the primary link breaks, the data is re-routed to alternate links to the next-hop neighbor without reporting the link breakage to the source. This can reduce the problem of route instabilities as nodes can continue to route traffic to their next-hop neighbor over alternate links. If however, all the links become broken, the node resorts to the conventional behavior of AODV and notifies the source which may launch another route request for multi-radio route discovery. In figure 3.8 we provide results for a link from the same 6-node scenario of the previous section. Each node is equipped with two radios tuned to non-overlapping channels.

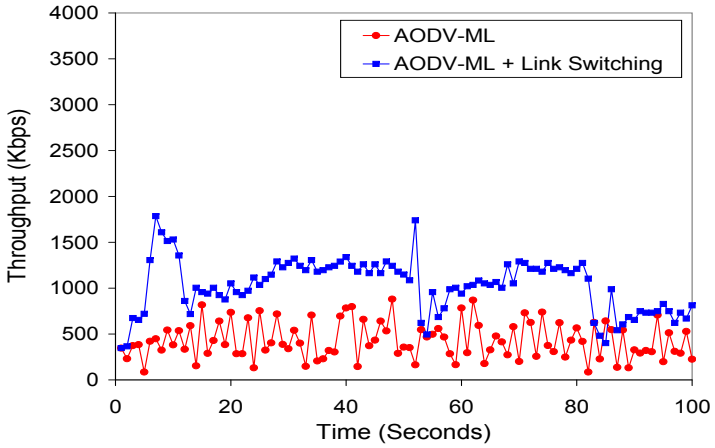


FIGURE 3.8 – *Comparison of AODV-ML with AODV-ML with Link Switching*

Figure 3.8 shows the comparison between *AODV-ML* and (*AODV-ML with link switching*). As the results show, link switching provides more route stability shown by less throughput variation. However, switching to alternate links creates an oscillating effect as shifting the complete load to the alternate link creates burden on that link causing interference-related link breakages and consequently throughput variation. Therefore even though AODV-ML with link switching provides increased route stability, the basic link breakage detection mechanism is still flawed and performance can further be improved. We also implement a final version of AODV-ML which has link switching along with ERM which means that each link breakage decision would be handled by ERM and if ERM declares a link as broken, data is re-routed to a randomly selected alternate link. The basic idea is that despite the availability of alternate links, the inaccurate link breakage detection mechanism of 802.11 still creates problems and ERM can provide improved performance despite the availability of alternate links. This means that ERM will help avoid frequent link (and therefore) route breakages. We implement a simple version in which each node is equipped with two radios operating on two different non-overlapping channels and that the two radios on all nodes are configured to the same two non-overlapping channels to ensure optimal connectivity of the network. The link qualities (physical and logical)

are maintained for each of the outgoing links on the different channels by each node. We implement the Hello *Estimation* version of the ERM mechanism for AODV-ML.

3.7 Analysis and Performance Evaluation of ERM using AODV

3.7.1 Simulation Environment

Physical and MAC Layers Wireless mesh routers in the simulation are equipped one or more IEEE 802.11b compliant wireless cards. We use the enhanced version of ns-2 as described in the simulation settings of chapter 2. The following table presents the simulation parameters at the PHY and MAC layers.

Simulation Parameters	Values
MAC Protocol	IEEE 802.11
Data Rate	11 Mbps
Frequency	2.4 GHz
Propagation Model	Ricean Fading
Antenna	Omni-Directional
Transmission Power	281.8 mW
Broadcast Rate	1 Mb
RTS Threshold	3000
Simulation Time	100 s

Table 3.1 – *Simulation Parameters*

Radio Propagation Model We use the Ricean fading model [Ratish J.Punnoose 00]. This model allows the simulation of time correlated small scale fading, typically caused by the changing environment around nodes which is typical of outdoor environments, thereby allowing for more realistic tests.

Topology and Traffic Settings We carry out the performance evaluation in both *single-radio single-channel* and *dual-radio dual-channel* wireless mesh networks. The mesh network comprises of 50 mesh routers randomly placed in an area of 1400m by 700m. We have 10 flows assigned to 10 mesh routers at one end of the network and these flows traverse almost the whole width of the network to reach 10 destinations at the other end of the network. This allows for longer available routes. We generate 10 random topologies and average our results across them. The position of the sources and destinations remains fixed while all other nodes are randomly distributed for each topology. We use *Constant Bit Rate* (CBR) traffic for the flows. The following table presents the topology and traffic parameters.

Routing and Transport Protocols For the *single-radio single-channel* case, we have implemented ERM in the AODV routing protocol. For the multi-radio extension of ERM, we first implemented a *dual-radio dual-channel* version of AODV in the ns-2 simulator and then integrated the proposed ERM extension in that. For the transport

Traffic and Topology Parameters	Values
Network Area	1.4km * 0.7km
No of Mesh Nodes	50
Random Topologies	10
Traffic Type	CBR
No. of Flows	10
Packet Size	1024 Bytes

TABLE 3.2 – *Simulation Parameters*

protocol, we have used TCP because it is most affected by route breakages due to its slow-start and multiplicative decrease mechanism.

Evaluation Metrics We define some performance evaluation metrics which will be used to assess the performance of ERM. These are the following :

- **Throughput** The throughput is defined as the aggregate throughput achieved in Kb/s at the destination nodes for the whole network i.e. for all the flows.
- **End-to-End Delay** This is the average end-to-end delay for all the network flows in milliseconds. The delay is calculated per packet for all the packets arriving at the destinations and the result is the average of all the packets of all the flows.
- **Routing Overhead** We consider routing overhead as the total number of non-data and non-ACK packets that are generated in the network. These include the routing packets of the protocol and the probe packets used by the ERM (*Hello* mechanism).
- **Route Lifetime** We define route lifetime as average duration for which a route remains intact i.e. without a breakage. The obtained result is an average of the route lifetimes for all the flows traversing the network. This metric would give an idea about the route stability.
- **Route Breakages** Route breakages are directly related to the route lifetime metric. The route breakages are the average route breakages that a flow experiences during the simulation. The result is the average number of route breakages for all the flows. This metric would give an idea about how often flows experienced route breakages.
- **Standard Delay Deviation** The standard delay deviation is calculated as the standard delay deviation for all the flows traversing the network.

Solutions Evaluated

Single-Radio Single-Channel Case : We implement ERM-Listen and ERM-Hello in AODV. These solutions are compared against the standard AODV and AODV

with Local Route Repair (AODV-LRR), an optimization which allows an intermediate node to launch a route request broadcast to locally establish a alternate route. This avoids the complete route discovery by the source node.

Dual-Radio Dual-Channel Case : We implement the multi-radio multi-channel extension of ERM in AODV-ML with link-switching. We use the ERM-Hello version to evaluate how ERM would perform if we have the luxury of alternate links at some (or all) intermediate hops.

Here we provide a brief outline of how the performance evaluation results are organized. As was discussed previously, the link breakage decision depends upon two thresholds. For the logical link quality, there will be no optimal value of the threshold limit which performs the best for all traffic and topology scenarios. The logical solution is to provide evaluation results across a range of values which we do in the next step. Therefore, first, we provide sensitivity analysis of β the threshold of logical link-quality to assess the optimal value of β. Next, we provide performance comparison of *Listen* and *Hello* with using the optimal threshold that we obtained through empirical testing. Next we provide comprehensive performance comparison of *ERM-Hello* against classical *AODV* and *AODV-LRR*. Finally, we present the performance evaluation results for ERM in a multi-radio environment.

3.7.2 Analysis of ERM in single-radio single-channel scenario using AODV

A. Sensitivity Analysis of Threshold (β) for Logical Link Quality

The first step in our performance evaluation is to evaluate different threshold values for β. As discussed previously, there will be no optimal value of the threshold limit which performs the best for all traffic and topology scenarios. The logical solution is to provide evaluation results across a range of values. We have identified the range of threshold values and therefore we present results for $0.60 \leq AIR \leq 0.90$. Figure 3.9 shows the performance of selecting various values of β for the Hello link quality assessment. For clarity, we only present the sensitivity analysis for the Hello mechanism. Results for the Listen mechanism show the same tendency for the various values of β. Starting from $\beta = 0.60$ we first explain the correlation between the threshold and the route lifetime. We see from results that the higher the threshold is, the higher is the route lifetime. Using a higher limit means that we keep on ignoring transmission problems on the link until the *logical interference* (AIR) reaches a very high level. This means that in general, we will experience less link (and therefore route) breakages as we increase the threshold. Most *link failure notifications* from the link-layer will therefore not result in actual link breakages unless the logical interference becomes very high. Less route breakages automatically means that the route lifetime increases i.e. the average duration that a route remains intact increases as the threshold increases as shown in the figure.

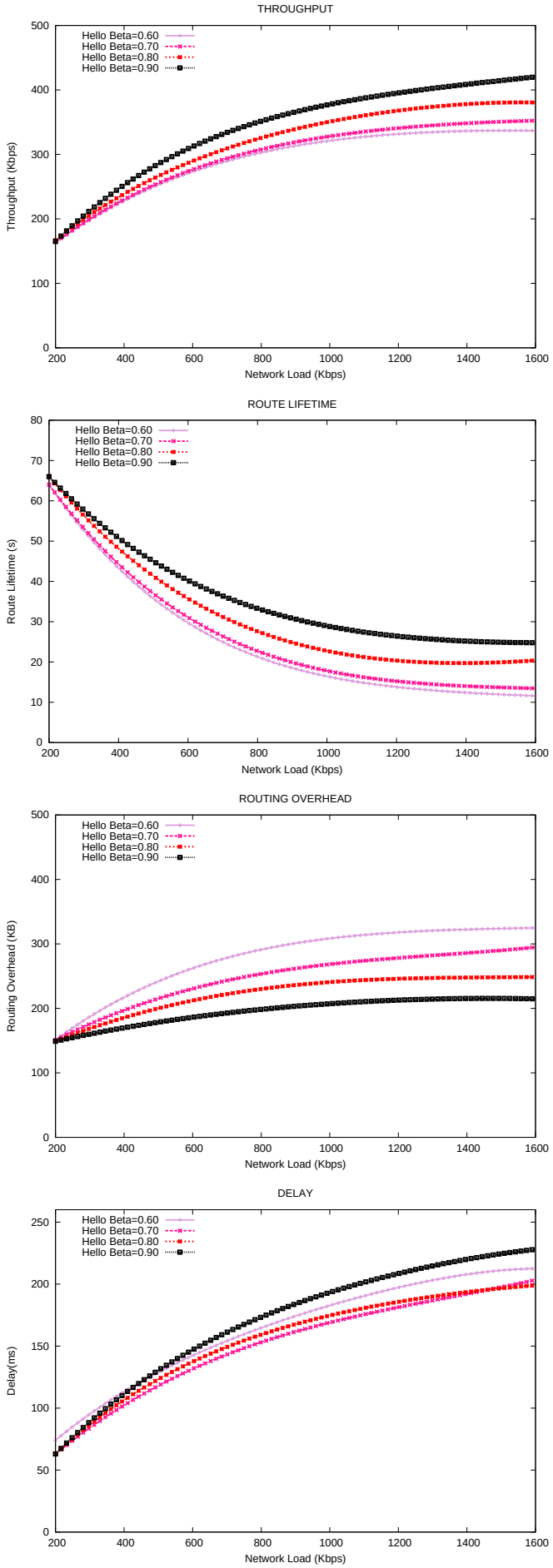


FIGURE 3.9 – *Sensitivity results for β in single-radio single-channel scenario using AODV*

Next, we explain the correlation between higher threshold and routing overhead. Higher threshold values also means smaller routing overhead as we have less route breakages which means that there will be less route discovery packets for finding new routes in place of the broken routes. Next we explain the correlation between threshold values and the throughput obtained. Higher threshold values result in higher throughput for two reasons. First, less route breakages and increased route lifetime means that we will have more stable routes which means a higher throughput. Second, less route breakages means that fewer extra routing packets would be introduced in the network. It is a well known fact that more routing packets introduce excessive load on the network and degrade performance. Thus, higher threshold means fewer routing packets and therefore a higher throughput.

We have observed that using higher threshold improves performance in terms of throughput, route lifetime and routing overhead. However, all is not well because when using a higher threshold, we face a tradeoff. As figure 3.9 shows, increasing the threshold also increases the overall end-to-end delay. This may be explained by the fact that sometimes a route becomes very congested (high interference on the medium) and should be changed, but we keep on using it due to a high threshold before we can declare it as broken. This is shown in figure 3.9 in which higher thresholds cost higher end-to-end delays. Therefore, we may benefit in terms of other parameters, but the end-to-end delay increases. However, we can argue that the overall benefits provided in terms of throughput, route lifetime and routing overhead outweigh the small tradeoff in terms of end-to-end delay which we argue is still within reasonable bounds. Increasing the threshold beyond 0.90 (e.g. $\beta = 0.95$) shows a start in decrease in the throughput and a non-negligible increase in the delay. Values below $\beta = 0.60$ show limited throughput. Therefore, based on our empirical testing, we will use a value of $\beta = 0.90$ for our subsequent experiments. Results for the *Listen* show similar trend for threshold values and we will therefore use the same threshold value for both *Listen* and *Hello* mechanisms.

B. Comparison of Listen and Hello in single-radio single-channel using AODV

The next logical step is to compare the performance of *Listen* and *Hello* mechanisms so that we can identify which mechanism provides the best results. We will subsequently use that mechanism for comparison with AODV and AODV-LRR. As previously mentioned, a threshold value of $\beta = 0.90$ is used for both *Listen* and *Hello* mechanisms. Figure 3.10 shows the throughput, delay, route breakages, route lifetime, routing overhead and delay deviation results for both the schemes.

As figure 3.10 shows, overall, *Hello* outperforms the *Listen* mechanism in all respects. This is due to the simple fact that *Listen* makes some unrealistic assumptions during the link-quality assessment phase which fail to accurately capture the link quality. As was discussed in the previous sections, the major difference between the *Listen*

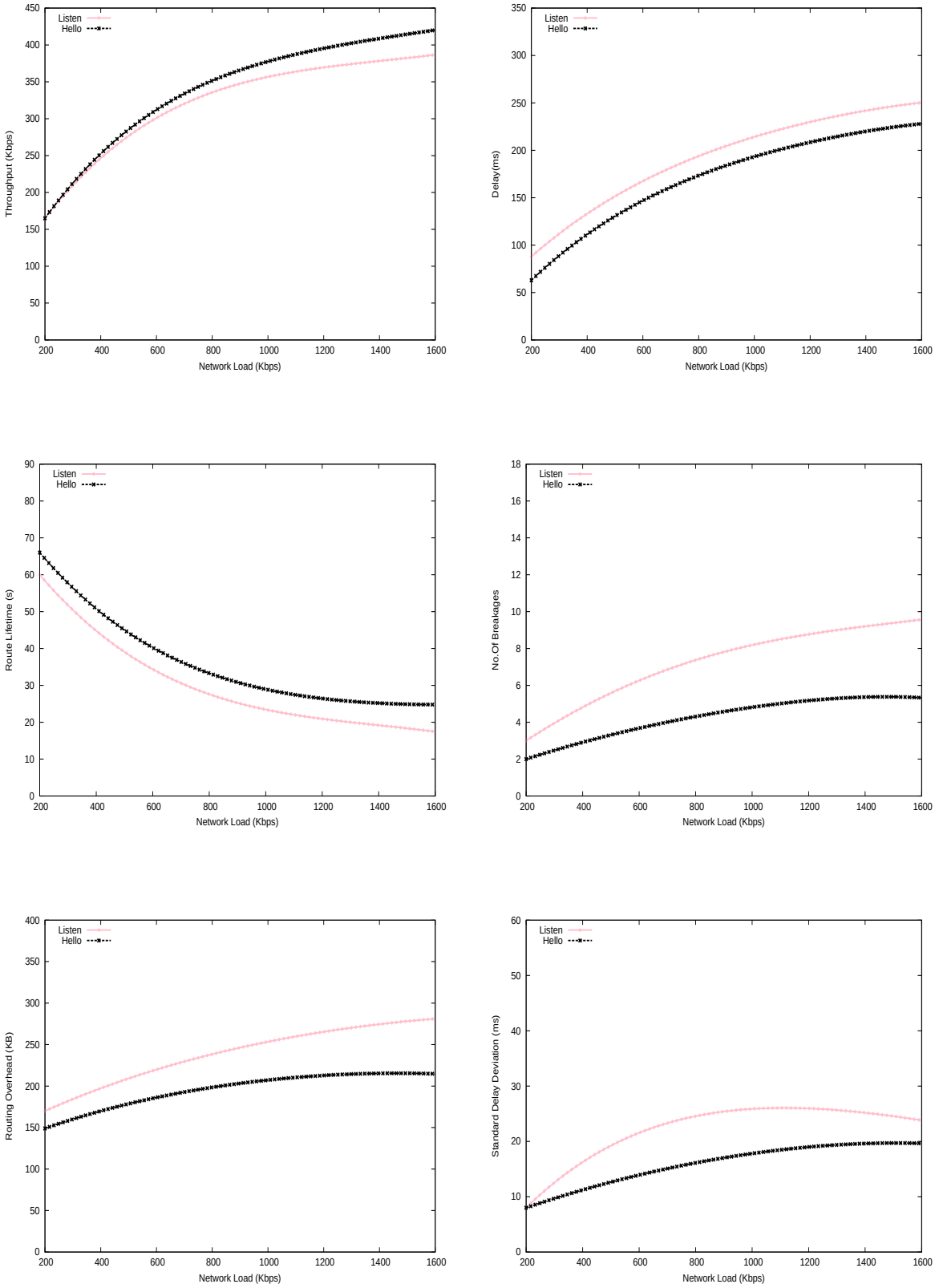


FIGURE 3.10 – *Comparison of Listen and Hello in single-radio single-channel scenario using AODV*

and the *Hello* mechanism is that the *Listen* mechanism estimates the link quality for a link (i, j) by using local information only available at node i. The advantage of this approach is that it is a passive mechanism which does not incur any routing overhead and we know that routing overhead is harmful for the network performance. The downside of this approach is that the link quality assessment is not accurate. For example, for estimating the physical link quality of link (i, j) only packet received at node i from node j are used for SINR. In reality, in IEEE 802.11 we know that for any given flow, data packets travel in the forward direction and the *Listen* approach therefore assumes that the link quality will be the same in both the directions which is not very accurate (although it does capture the problems that ACK packets may experience on the reverse link).

Second, for the logical link quality, the node only estimates the *Average Interference Ratio* within its CS range only without considering the interference in the CS range of the receiving node i.e. j. The Hello approach solves this problem by calculating the physical link quality as SINR of packets from i to j and the logical link quality as the maximum of AIR in the CS ranges of two nodes. As results show, *Hello* achieves a higher throughput than the *Listen* mechanism. This can be attributed to the fact that the link breakage decisions by *Listen* can be somewhat arbitrary because node i has only a limited view of the link and because the SINR of the reverse link may have no correlation with the forward link leading to somewhat random link breakage decisions. In our opinion, these problems lead to more frequent link breakages than necessary and sometimes link breakages at the wrong time. Frequent route breakages result in smaller route lifetime and more routing packets in the network resulting in lowered throughput. Moreover, the end-to-end delays also seem to be slightly bigger for the *Listen* mechanism. We conclude that the *Hello* mechanism is more accurate than its *Listen* counterpart and provides a more interesting gain in terms of throughput. However, this does not mean that *Listen* does not bring any improvement. *Listen* still outperforms both AODV and AODV-LRR, though, the performance improvement offered by Hello is more substantive.

3.7.3 Performance Evaluation of AODV, AODV-LRR and ERM-Hello in Single-Radio Single-Channel Scenario

We now provide comprehensive performance comparison of *ERM-Hello* with AODV and AODV-LRR using $\beta = 0.90$ as the threshold value. Figure 3.11 shows the simulation results for AODV, AODV-LRR, and ERM-Hello. We see that AODV with local link repair improves performance compared to the classical AODV protocol. For each route breakage encountered, AODV-LRR locally launches a route request locally. The first advantage is that we avoid global route discoveries from the source and route breakages are recovered locally with significantly smaller routing overhead as shown in the routing overhead graph. This results in less route breakages than AODV,

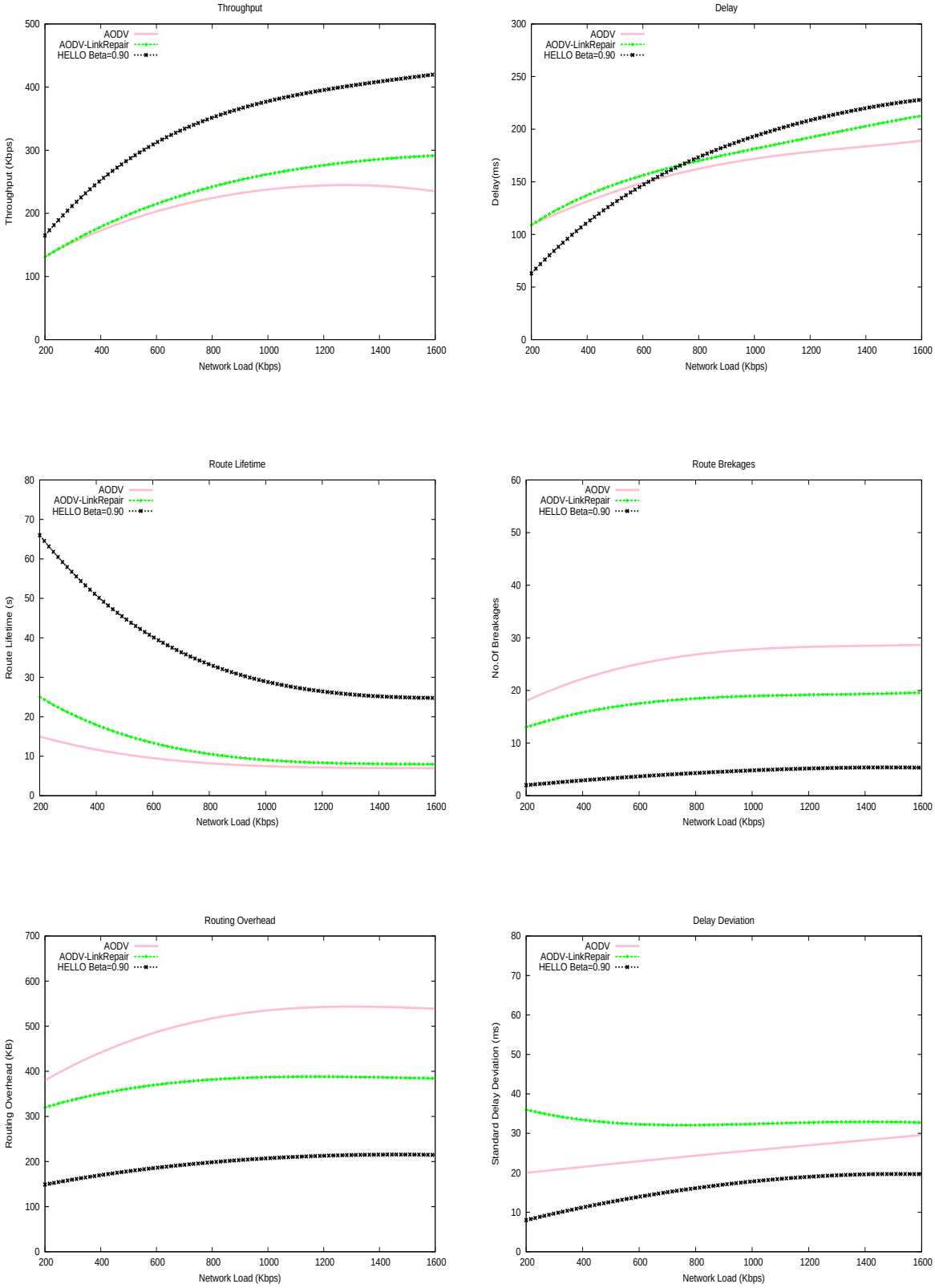


FIGURE 3.11 – *Performance evaluation results for the Hello Mechanism*

higher route lifetime and consequently higher throughput. However, the end-to-end delay is slightly higher than AODV which can be explained as the data must wait at intermediate nodes for every local route repair and if the local route repairs are too frequent, the end-to-end delay becomes higher. Moreover, due to the same reason of local link repair, AODV with link repair has higher standard delay deviation than AODV. However, overall AODV-LRR outperforms AODV.

The main observation we make for *ERM-Hello* is that it outperforms both AODV and AODV-LRR in almost all respects. We explain results for each performance metric turn by turn. We see from the results that *ERM-Hello* has fewer route breakages than both AODV and AODV-LRR. This is because ERM makes link breakage (and hence route breakage) decisions more coherently by considering the long-term performance of the link instead of systematically declaring a link breakage every time the link-layer reports a problem. This is why AODV and AODV-LRR have a significantly higher number of route breakages than *ERM-Hello*. Following the same logic, *ERM-Hello* has a higher average route lifetime due to a smaller number of route breakages. Due to the reduced number of route breakages, we have a significantly smaller routing overhead which also explains why *ERM-Hello* has the highest throughput (more overhead in AODV and AODV-LRR leads to poor performance). Similarly, the standard delay deviation is smallest for *ERM-Hello* because it does not suffer from frequent route breakages. The only metric where *ERM-Hello* performs slightly less well is the end-to-end delay. Intuitively, we can argue that although ignoring transient transmission problems can provide higher throughput, but we also risk of keeping on using a relatively more congested (in terms of interference) in which case more retransmissions maybe required at each wireless hop resulting in larger end-to-end delays. However, our approach proves beneficial from a throughput perspective since a route change is costly (traffic is blocked waiting for route establishment).

We argue that the benefits in terms of throughput (almost 150% improvement), routing overhead (reduced to almost one fourth), route lifetime and other metrics far outweigh the slight increase in the delay. Moreover, the delay is within reasonable bounds (less than 250 ms). In certain cases, delay may be of prime importance and in those cases, we would recommend using a lower value of β. For example, $\beta = 0.8$ would provide a smaller delay than both AODV and AODV-LRR but obviously at the cost of less gains in throughput than $\beta = 0.90$. Based on our performance evaluation results, we would suggest a value of $\beta = 0.90$.

3.7.4 Performance evaluation of ERM-Hello in multi-radio multi-channel scenario

In this section, we present and discuss simulation results for the extension of ERM to multi-radio multi-channel case. For simplification, we assumed a dual-radio dual-

channel mesh network. The basic idea was to evaluate whether ERM works well if we have multiple available links available between neighboring nodes which we can use as backup in case the primary link fails. We have implemented three schemes. In the basic AODV-ML protocol, a link breakage is reported to the source and the source can then either use an alternate route or launch another route discovery process. In the AODV-ML with link switching, if the primary link breaks, the intermediate node re-routes the data to an alternate available link to the next-hop node. We have used the Hello mechanism.

Figure 3.12 shows the results for the three schemes. As we see from the results, the simple AODV-ML performs the worst which is expected because it does not exploit the availability of multiple available links between nodes. The next best performer is AODV-ML with link-switching which instead of declaring a route as broken for every link failure, switches the link to the next neighbor and provides increased route lifetime and reduced route breakages as shown in the figure. Throughput increases due to increased route lifetime. The delays however are higher than AODV-ML because while link switching provide route stability, it also poses some problems as there may already be traffic present on the alternate links and the newly switched traffic creates a burden on that link, causing more collisions, retransmissions and hence larger end-to-end delays. However, since delays remain acceptable, the throughput can be considered as the more important criteria. AODV-ML with ERM outperforms the two other schemes which proves that despite the availability of multiple links, ERM brings some additional stability to the network. However the performance improvement are understandably lower than the case of single-radio single-channel mesh networks which have the highest level of interference and suffer the most from route breakages.

3.8 Conclusion

Wireless Mesh Networks are expected to play an important role in the future due to their promising capability to provide last-mile broadband wireless Internet access to communities and regions. However in reality, real world deployments of mesh networks need improvements before they can fulfil the promise of true wireless broadband as performance degrades significantly as the network size increases and data has to traverse multiple wireless hops before reaching the destination. In this paper, we presented the problem of route instability in wireless mesh networks for reactive routing protocols which leads to poor performance. Reactive routing protocols in wireless multi-hop networks depend upon intermediate nodes on the multi-hop path to detect and report broken links. Each node uses IEEE 802.11's classical link-layer feedback mechanism based on 8 consecutive transmission failures to detect and report broken links. This mechanism of on-demand protocols has flaws as it cannot distinguish between actual link breakages and breakages induced by

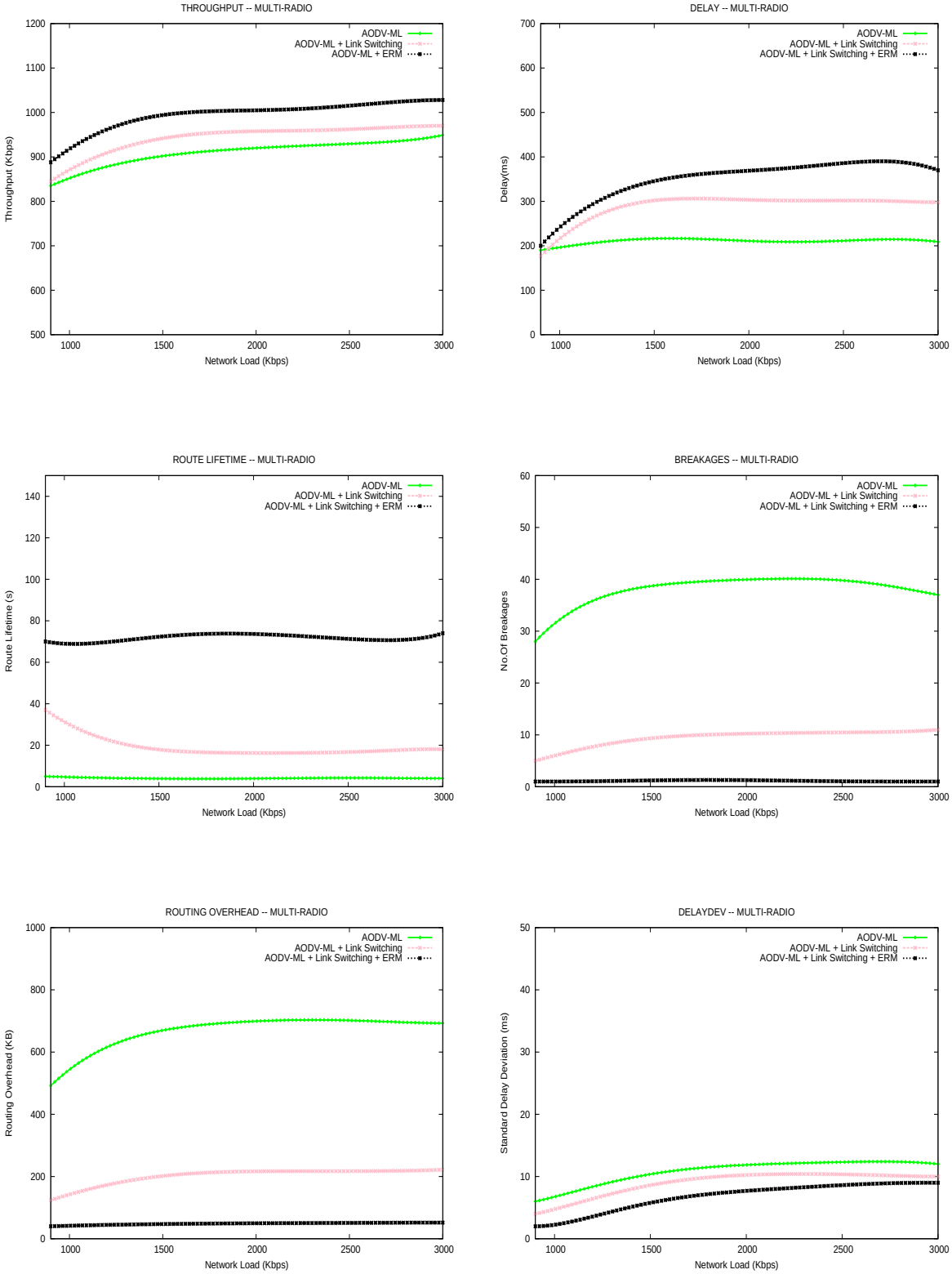


FIGURE 3.12 – *Performance evaluation results for Multi-Radio Multi-Channel Scenarios*

transient transmission problems due to any reason including interference present on

the wireless link. While significant research exists on recovering from link failures in multi-hop wireless networks for reactive routing protocols, there has been little research on improving route maintenance of reactive protocols by avoiding unnecessary link breakages.

We proposed a new route stability mechanism for wireless mesh networks aimed at reducing false route breakages. ERM exploits MAC and physical layer information to estimate the long-term performance of the link. If the link-layer reports a link failure, ERM examines the long-term link-quality to distinguish between links with transient problems and those which have poor long-term quality. By not treating every *link failure notification* from link-layer systematically as *link breakage* (and therefore *route breakage*), ERM can ignore transmission problems if they are temporary and transient. Our mechanism is flexible and can be easily implemented in existing reactive routing protocols for mesh networks. It introduces intelligence in the route maintenance mechanism of routing protocols so that a more coherent decision about link breakage detection can be made instead of relying on the systematic logic of declaring a link breakage followed by contemporary on-demand routing protocols. We proposed two different mechanisms for estimating link quality namely *Listen* and *Hello* link-quality assessment. Extensive simulation results show that ERM can provide substantial performance improvements for both single-radio single-channel and multi-radio multi-channel mesh networks. Compared to AODV for single-radio single-channel scenario, we observed an average 100% improvement in throughput, 3 times longer route lifetime, almost 10 times less route breakages and 50% smaller routing overhead for ERM. The chapter also makes a contribution by proposing an improvement of AODV-ML which involves switching to another alternate link between neighboring nodes if the primary fails. We also show that ERM works well even in multi-radio environments despite using link-switching. Compared to the AODV-ML with link-switching in multi-radio multi-channel scenarios, ERM offers an improvement of about 10% in throughput, about 2.5 times longer route lifetime and one tenth the routing overhead. Overall, results show that ERM provides substantial performance improvements for both single-radio and multi-radio wireless mesh networks in terms of throughput, route lifetime, routing overhead and delay deviation.

4 Framework for QoS Guarantees in Wireless Mesh Networks

Contents

4.1 Introduction

An important research problem for mesh networks is providing Quality of Service guarantees. Over the years, user application requirements have moved beyond *best-effort* services and today, a number of applications require QoS guarantees such as end-to-end delay and/or end-to-end throughput. QoS is especially important for users who use the mesh backbone as the *last-mile wireless hop* to access the Internet because many Internet-based applications require certain QoS. Providing QoS in wireless networks is challenging in general because the wireless medium is unpredictable (random packet losses, noise etc) and shared. For mesh networks, a number of challenges arise. First, a significant portion of traffic in mesh networks is between users connected to mesh routers and gateway nodes, resulting in congested regions near the gateways. Moreover, interference (both *inter-flow* and *intra-flow*) between a large number of mesh routers sharing the same wireless medium significantly limits the network performance (throughput, end-to-end delay, reliability) and capturing the effects of interference is fundamental for QoS provisioning. These factors make resource availability unpredictable and render QoS-provisioning difficult.

Providing QoS guarantees has been extensively explored for wireless multi-hop networks including MANETs and WSNs. Mesh networks differ significantly from existing wireless multi-hop networks (architecture, traffic patterns, user requirements etc). Moreover, mesh networks are a recent phenomenon and few mesh-specific QoS solutions have been proposed. A literature review of mesh-specific QoS solutions shows that most existing solutions focus on QoS guarantees in single-radio single-channel mesh networks [V. Kone 08], [X. Cheng 08] [Xue Q 02] [B. Wang 08a] and only a few solutions consider multi-radio multi-channel mesh networks [M.A. Ergin 08a]. Recently, multi-radio multi-channel mesh networks have become more common and it is necessary to develop solutions for these networks.

This chapter proposes a novel solution for providing QoS guarantees (per-flow end-to-end bandwidth guarantees) to flows in multi-radio multi-channel mesh networks. First, the solution proposes a mechanism to capture interference (*inter-flow* and *intra-flow*) in multi-radio multi-channel mesh networks. The solution also explicitly captures *intra-flow* interference that the incoming flow will experience with itself, something which is important but sometimes ignored [X. Cheng 08]. Moreover, in multi-radio multi-channel mesh networks, neighboring nodes are often connected through multiple links (i.e. multiple radio operating over non-overlapping channels) and this provides *link-diversity*. The proposed solution exploits *link-diversity* to : 1) Improve admissibility as sometimes a single link between two nodes may not have sufficient bandwidth to support the incoming flow and using multiple links concurrently can provide higher flow admission ratio 2) Perform load-balancing by distributing the load between neighboring nodes on multiple concurrent links

instead of putting all the load on a single link.

The rest of the chapter is organized as follows. First we review existing QoS solutions for wireless mesh networks and explain the basic QoS framework typically used by existing solutions to provide QoS guarantees in wireless mesh networks. Next, we elaborate on the motivation behind this contribution. Subsequently, we state our assumptions and present our network model. We then present the proposed QoS solution which exploits link diversity to achieve more efficient admission control and load-balancing in multi-radio multi-channel wireless mesh networks. Finally, we show how the proposed QoS approach works on a sample topology.

4.2 Review of Existing Work

4.2.1 General Framework for QoS Guarantees in Wireless Multi-hop Networks

We describe the general principle on how existing QoS approaches work. Almost all QoS guarantee solutions for wireless mesh networks use an on-demand routing protocol (typically AODV) as the base. The admission control mechanism is combined with the route discovery phase of the on-demand routing protocol. When a mesh router has an incoming flow demanding a certain bandwidth to a certain destination, the mesh router launches the route request phase of the on-demand protocol for the requested destination. In the *Route Discovery* phase, the route request packet now also contains the required bandwidth for the incoming flow. At each intermediate node, admission control is performed to see whether the current node has enough available bandwidth to support the incoming flow bandwidth. The precise mechanism of available bandwidth estimation varies [X. Cheng 08] [Xue Q 02] [Chen 05] . If the node cannot support the requested bandwidth, the request is dropped. If however, the node can support the required bandwidth, the node updates the route request packet (by adding information), makes a temporary bandwidth reservation for the incoming flow and rebroadcasts the route request. This process is repeated until the route request arrives at the destination. The destination sends back a *Route Reply* packet along the same path and on the reverse path, each intermediate node makes the bandwidth reservation permanent. The source finally receives the reply packet and starts sending data. Obviously, there are a number of things which can go wrong. To counter these problems, a QoS violation detection mechanism is used after admission control and during data transfer. In this mechanism, if the source or the destination or any intermediate node detects that the QoS guarantees are not being met, they can send a message telling other nodes on the path to relinquish the reserved resources and tell the source node to start another route discovery and admission control phase. There are obviously variations and optimizations available to these basis mechanisms of QoS guarantees, but most approaches work more or less on this principle. The existing approaches mainly differ on how each they estimate the available bandwidth.

4.2.2 QoS Solutions for Single-Radio Single-Channel Mesh Networks

Wireless Mesh Routing (WMR) protocol [Xue Q 02] is a QoS-solution for wireless mesh networks which provides bandwidth guarantees and is based upon the *Ad hoc QoS On-demand Routing* (AQOR) protocol [Xue Q 03] originally developed for *Mobile Ad hoc Networks* (*MANETs*). In the *Topology Discovery* phase of WMR, nodes periodically broadcast a *HELLO* packet containing a distance tag which contains the distance from the nearest gateway node in terms of hops. So each network node has information about its neighborhood and the distance (in terms of hops) to the nearest gateway. *WMR* estimates the available bandwidth by measuring self-traffic and that of its neighbors. Admission control with required bandwidth is performed jointly with route discovery. At each intermediate node in the discovery process, if the available bandwidth is greater than the required bandwidth, route-reservation is performed or else, the route request is dropped at that node. The *Route Recovery* mechanism of *WMR* (during data transfer) deals with recovering from QoS violations. This usually involves delay or bandwidth violation detected at the destination. If such a violation is detected, the source node is informed of the violation (usually by the destination node) and another *QoS-Route Discovery* phase is launched. The accuracy of the bandwidth estimation approach is not evaluated in the paper.

QUORUM [V. Kone 08] is another QoS-aware routing protocol proposed for wireless mesh networks which provides delay guarantees. The authors argue that both *WMR* and *AQOR* (its counterpart protocol proposed for ad hoc networks) do not estimate the expected delay accurately. The authors argue and show through experimentation that *WMR* and *AQOR* use *Route Request* (*RREQ*) and *Route Reply* packets to calculate the delay which can lead to incorrect delay estimations because route request and reply packets are smaller than actual data packets and therefore experience different delays and loss rates. *QUORUM* uses the concept of "*dummy*" packets i.e. after the source has received the route reply at the end of Route Discovery phase, it stores the route in a table and sends a stream of dummy packets along the route which have the same size and priority as the data packets, thus effectively emulating real data. The destination then notes down the delay of these packets and informs the source of the delay. The delay estimation through this mechanism is fairly accurate but the drawbacks include the latency in setting up a route (i.e. first we have the route discovery phase and then the dummy packet phase and secondly the extra interference that the dummy packets may introduce in the network). The solution only provides delay guarantees without providing bandwidth guarantees.

MARIA : *Interference-Aware Admission Control and QoS Routing* [X. Cheng 08] is another solution which provides bandwidth guarantees in wireless mesh networks. MARIA captures interference by using the *conflict graph* [K. Jain 03]. The *conflict graph* is a model to capture interference in wireless multi-hop networks by identifying groups

of mutually interfering links. To create the conflict graph, nodes periodically exchange small HELLO packets which contain the information of flows traversing these nodes. The HELLO messages convey the interference information (traffic flows traversing the nodes) within an "interference neighborhood". To ensure that HELLO packets reach all the nodes within the "interference neighborhood", each node transmits the HELLO message with an increased transmission power. From the constructed clique graph, each node can decide whether it can admit the incoming flow. *Quality-of-service Aware Fair Rate Allocation* (*QUOTA*) is a framework [B. Wang 08b] that combines QoS and fair-rate allocation for wireless mesh networks. The basic idea behind *QUOTA* is that real-time flows are guaranteed the required bandwidth while the remaining bandwidth is fairly distributed between non real-time flows or flows without specific QoS requirements.

4.2.3 QoS Solutions for Multi-Radio Multi-Channel Mesh Networks

Liu et al. [M.A. Ergin 08a] propose an admission control algorithm for multi-radio multi-channel wireless mesh networks which provides bandwidth guarantees. Their main contribution is proposing two new mechanisms for available bandwidth estimation at a node. The first mechanism introduces the mechanism of increasing the carrier sensing range so that interference from far off flows near the boundary of the carrier sensing range can also be taken into account for bandwidth estimation. This is something which has previously been neglected and when nodes only consider flows in their CS range and not the extended range, they risk admitting flows which can violate the QoS. The second mechanism that they propose is to use the classical concept of back-to-back packet probes on a link and then using mathematical models to estimate the available bandwidth using the probe dispersion observed. They integrate the bandwidth estimation and admission control with the on-demand *LUNAR* routing protocol (somewhat similar to AODV) in which admission control is done during the *Route Discovery* phase.

4.2.4 QoS Solutions for TDMA-based Wireless Mesh Networks

Some solutions have been proposed for TDMA mesh networks. *Distributed Call Admission Control* (*DCAC*) [Yi Hu 07] is a protocol for TDMA based multi-channel multi-radio wireless mesh networks. In another work [S. Lee 06b], a QoS admission control is proposed for backhaul WiMax Wireless Mesh Networks. However, it is very difficult to achieve synchronization for TDMA for large multi-hop wireless networks.

4.3 Motivation

- An overwhelming majority of existing QoS solutions focus on single-radio single-channel mesh networks [Xue Q 02] [V. Kone 08], [X. Cheng 08] [B. Wang 08a]. However, due to the reduced cost of hardware, multi-radio multi-channel mesh networks have become common and it is therefore interesting to propose a QoS solution for multi-radio multi-channel mesh networks.
- Few QoS solutions for multi-radio multi-channel mesh networks exploit *link-diversity* (the availability of multiple links between neighboring nodes). Our QoS solution explicitly exploits *link-diversity* in multi-radio multi-channel mesh networks in two ways :
  1. First, sometimes a single link cannot support the required bandwidth over a wireless hop. Our proposed solution considers all the available links between two nodes over a wireless hop as one logical link whose bandwidth is equal to the sum of the bandwidths of all the comprising links. This helps achieve a much higher flow admittance percentage.
  2. Second, the solution does not simply distribute the load of the incoming flow equally on all the available links between two nodes. Load-balancing is performed according to the load (interference) already present on the links hence achieving a more efficient distribution of load.
- The proposed solution provides an elegant mechanism to capture interference (both *intra-flow* and *inter-flow*) for the existing flows in the network. The solution explicitly takes into account the *intra-flow interference* that the incoming flow will create with itself, which is something often ignored by existing approaches [X. Cheng 08].

4.4 Network Model

To define and study interference in wireless mesh networks, we apply the *protocol model* [Gupta 00]. The protocol model was subsequently modified [Alicherry 05] [Brar 06] to reflect IEEE 802.11 based communications. We elaborate upon different aspects of our network model below :

4.4.1 Concept of Connectivity Graph

We assume that we have a given wireless network topology (topology here refers to a spatial distribution of wireless nodes within a certain region). We model it as an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ such that $\mathcal{V}$ represents the wireless mesh nodes (vertices), the set of edges $\mathcal{E}$ represents the set of bidirectional wireless links. In this graph, the edge (i_k, j_k) $i, j \in \mathcal{V}$ represents a bidirectional wireless link between nodes i and j on channel k in the network. The graph $\mathcal{G}$ actually represents the *connectivity graph*. Figure 4.1

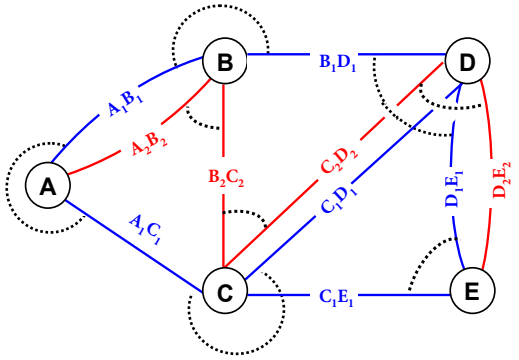


FIGURE 4.1 – *The connectivity graph of a wireless mesh network*

shows the connectivity graph for a *dual-radio dual-channel* wireless mesh network topology comprising of five wireless nodes $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ *and* E. In the connectivity graph, the link $\mathcal{A}_1\mathcal{B}_1$ represents a bidirectional wireless link between nodes $\mathcal{A}$ and $\mathcal{B}$ on channel 1. Similarly, $\mathcal{A}_2\mathcal{B}_2$ represents the wireless link between nodes $\mathcal{A}$ and $\mathcal{B}$ over channel 2. Channel 1 and 2 are two non-overlapping channels. These bidirectional wireless links are represented by solid lines in figure 4.1. The dotted lines connecting the wireless links represent the interferences between these links. For example, around node $\mathcal{C}$, links $\mathcal{A}_1\mathcal{C}_1$, $\mathcal{C}_1E_1$ and $\mathcal{C}_1\mathcal{D}_1$ mutually interfere on channel 1 and links $\mathcal{B}_2\mathcal{C}_2$ and $\mathcal{C}_2\mathcal{D}_2$ mutually interfere on channel 2.

4.4.2 Concept of Conflict Graph

The conflict graph is a graph developed on the basis of the connectivity graph and which deals with a single channel at one time. In our example, the connectivity graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ gives two conflict graphs (one for channel 1 and the other for channel 2). For each channel, each wireless link in the original connectivity graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is represented by a node $v' \in \mathcal{V}_c$ in the corresponding conflict graph $\mathcal{G}_c = (\mathcal{V}_c, \mathcal{E}_c)$. A link $e' \in \mathcal{E}_c$ exists in the conflict graph $\mathcal{G}_c$ if two links in the original connectivity graph G interfere with each other on the given channel. For a given channel, the conflict graph *"visualizes"* the interferences which can occur between links. Figure 4.2 shows the conflict graphs relative to channel 1 and channel 2 for the given connectivity graph.

From the conflict graph, we can extract *"cliques"*. A *"clique"* is a complete subgraph from the original conflict graph such that all nodes in a clique are connected pairwise implying that all links represented by these nodes interfere with each other. A maximal clique is a clique not contained in any other clique i.e. we cannot add any more vertices to it. This is denoted by shaded regions in figure 4.2 for both channel 1 and channel 2. No two links belonging to the same maximal clique can simultaneously be active. For example, from figure 4.2, we see that for channel 1,

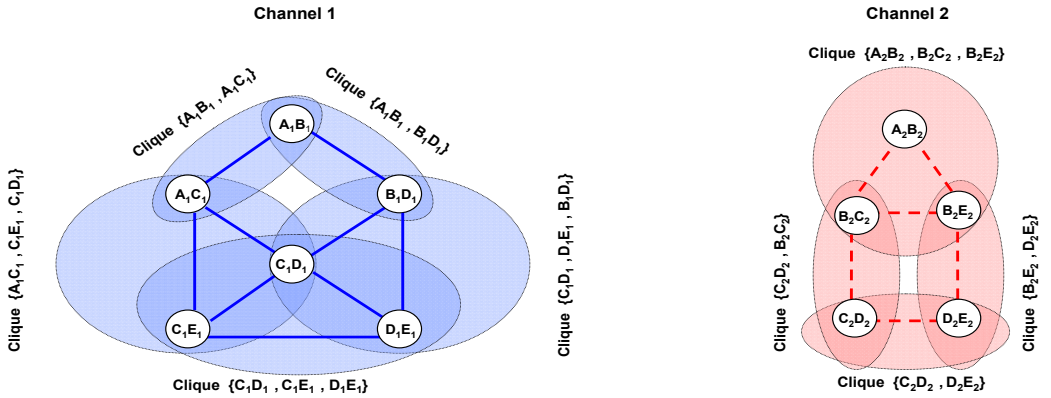


FIGURE 4.2 – *Conflict graph for channel 1 and channel 2*

we have the following maximal cliques $\c{C}_1 = \{\mathcal{A}_1\mathcal{B}_1\,,\,\mathcal{A}_1\mathcal{C}_1\}$, $\c{C}_2 = \{\mathcal{A}_1\mathcal{B}_1\,,\,\mathcal{B}_1\mathcal{D}_1\}$, $\c{C}_3 = \{\mathcal{A}_1\mathcal{C}_1\,,\,\mathcal{C}_1\mathcal{D}_1\,,\,\mathcal{C}_1E_1\}$, $\c{C}_4 = \{\mathcal{C}_1\mathcal{D}_1\,,\,\mathcal{C}_1E_1\,,\,\mathcal{D}_1E_1\}$ $\c{C}_5 = \{\mathcal{C}_1\mathcal{D}_1\,,\,\mathcal{D}_1E_1\,,\,\mathcal{B}_1\mathcal{D}_1\}$. For channel 2, we have the following maximal cliques $\c{C}_6 = \{\mathcal{A}_2\mathcal{B}_2\,,\,\mathcal{B}_2\mathcal{C}_2\,,\,\mathcal{B}_2E_2\}$, $\c{C}_7 = \{\mathcal{B}_2\mathcal{C}_2\,,\,\mathcal{C}_2\mathcal{D}_2\}$,$\c{C}_8 = \{\mathcal{C}_2\mathcal{D}_2\,,\,\mathcal{D}_2E_2\}$, $\c{C}_9 = \{\mathcal{B}_2E_2\,,\,\mathcal{D}_2E_2\}$.

From the notion of maximal cliques, we can get the constraints on the aggregate rates of flows on the links of the wireless network (i.e. the nodes in the conflict graph).

4.4.3 Specifying Clique Constraints

lemma 1 - *Let $S_\mathcal{K}$ represent a maximal clique (set of mutually conflicting links) and let $\mathcal{F}$ be a link flow vector where $\mathcal{F}_e$ represents the aggregate rate of flows on link e. $\Re(e)$ is the capacity of the channel on which link e operates. The flow vector $\mathcal{F}_e$ is schedulable if it satisfies the following constraint :*

$$\sum_{e \in S_\mathcal{K}} \mathcal{F}_e \leq \Re(e) \quad \forall \kappa \tag{4.1}$$

In simple words, the aggregate rate of flows on all the links in a maximal clique will always be less than or equal to the capacity of the channel on which the links operate. The cliques constraints have been previously explained in detail in existing works [K. Jain 03] [R. Gupta 05]. For the conflict graph of figure 4.2, we obtain the following clique constraints for the link $\mathcal{A}_1\mathcal{C}_1$ from the conflict graph :

$$\begin{aligned} \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{C}_1E_1} \leq \Re(1) \\ \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} \leq \Re(1) \end{aligned} \tag{4.2}$$

Where $\mathcal{F}_{\mathcal{A}_1\mathcal{C}_1}, \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1}, \mathcal{F}_{\mathcal{C}_1E_1}$ are the aggregate flow rates on links $\mathcal{A}_1\mathcal{C}_1$, $\mathcal{C}_1\mathcal{D}_1$ and $\mathcal{C}_1E_1$ and $\Re(1)$ is the capacity of channel 1. If a link is part of more than one maximal clique, then the clique constraints must be met for all the maximal cliques. For example, if we want to admit a flow on link $\mathcal{A}_1\mathcal{C}_1$, then the additional flow rate introduced by the flow must meet all the maximal clique constraints to which link $\mathcal{A}_1\mathcal{C}_1$ belongs. In section 4.5.3.2, we will describe how we can estimate the available bandwidth on each

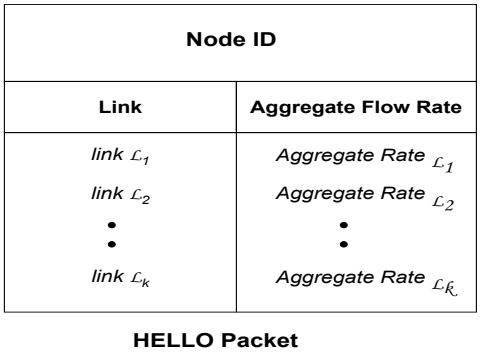


FIGURE 4.3 – *Possible format of the HELLO packet*

link using the clique constraints and how the bandwidth of a hop can be expressed as the sum of the available bandwidths on individual links.

4.4.4 Computation of the Conflict Graph and Clique Constraints

In order for each node to build its local conflict graph and derive local maximal cliques, it needs to be aware of the conflicting flows within a "*region of interference*" [X. Cheng 08] [J. Tang 05] along with the aggregate flow rates on these links. We assume that using an existing method [X. Cheng 08], the aggregate flow information on links is exchanged between nodes in an interference region using *CONFLICT-HELLO* packets. Basically, each node keeps track of the transmission rate of each flow during a sliding window of time along with the link on which the flow is being transmitted. Periodically, this information is broadcast in small *CONFLICT-HELLO* packets. Since the "*region of interference*" is larger than the transmission range, therefore each node broadcasts the *CONFLICT-HELLO* message with an extended transmission range to cover all nodes within this region. Figure 4.3 shows the possible structure of the *CONFLICT-HELLO* packet. Finding maximal cliques in a network is an NP complete problem [Garey 79] and therefore approximations [Gupta 04] are used. Regardless of the mechanism used for computing the conflict graph and the clique constraints, for our proposed solution to work, it suffices that each node can compute its local conflict graph and derive clique constraints using whatever method. The focus of this contribution is not on the specifics of the conflict graph and any existing solution to compute the conflict graph and clique constraints [X. Cheng 08] [K. N. Ramachandran 06] can be used.

4.5 The Proposed QoS Framework

In this section, we present our QoS framework for providing resource-reservation based bandwidth guarantees in multi-radio multi-channel wireless mesh networks.

4.5.1 Assumptions

- Each node is equipped with one or more radios. Each radio is a separate wireless *Network Interface Card (NIC)* with separate MAC and physical layers. The same network layer interfaces with all the radios on a node.
- We assume that the channel assignment is static and handled by some outside agency. The channel assignment is understood to be already done using an efficient channel-assignment scheme [Alicherry 05] [K. N. Ramachandran 06]. The channels on the radios of a node are assigned on non-overlapping channels to reduce interference. We assume that the channel assignment is done to provide optimal connectivity within the network.

4.5.2 Overview of Phases of the QoS Framework

We make a choice of selecting an on-demand routing protocol for our proposed mechanism to work. For the conflict graph model to work, we need two information components : the local conflict graph at each node and the aggregate flow rates on conflicting links. This can be achieved by using any mechanism such as mentioned in section 4.4.4. The QoS framework has three important phases :

1. **Phase 1 : *Neighbor Discovery***
   In the *Neighbor Discovery* phase, nodes discover their neighbors on all of their available radio interfaces to create a neighborhood table.

2. **Phase 2 : *QoS-Aware Route Discovery and Admission Control***
   There are four sub-phases of *QoS-Aware Route Discovery and Admission Control*. A node wishing to find a route for an incoming flow specifying certain QoS (bandwidth in our case) broadcasts the route request and these procedures are performed during the route discovery phase.

   Bandwidth Estimation In this phase, first, every node estimates the available bandwidth for all its outgoing links using locally constructed conflict graphs by taking into account the interference from the existing flows. Next, the intra-flow interference that the new incoming flow will generate with itself is taken into consideration. Finally, the available bandwidths of multiple links on a "wireless hop" are summed up to estimate the bandwidth that each outgoing "*wireless hop*" can support for the incoming flow.

   Admission Decision In this phase, it is checked at the current node whether any of the hops can support the required bandwidth. If yes, then the route request packet is re-broadcast. If no, then the packet is simply dropped.

   Load Balancing Load balancing is also performed in the proposed QoS solution. In this phase, the load of the flow which will come after admission

control is distributed on multiple links for a wireless hop. The distribution of traffic for the incoming flow is done inversely in proportion to the interference present on each of the links.

Resource Reservation In this phase, resources reservation is finalized when the nodes receive the route reply message coming from the destination.

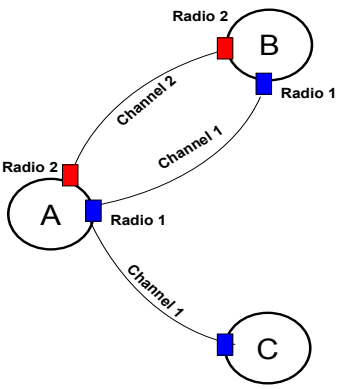
3. **Phase 3 : *QoS Violation Detection and Recovery***
   Once admission control and resource reservation phases are over, the source can start sending traffic to the destination. But, in order to protect against the possibility of QoS violation (e.g. if the end-to-end bandwidth guarantee is no longer being met), any violation of the guaranteed bandwidth is detected and reported to the source. The recovery usually involves another phase of route request to find an alternate route fulfilling QoS requirements.

4.5.3 Details of the Phases of the QoS Framework

Here we will describe the various components of each of these phases. We will apply the proposed solution on an example to explain how the algorithm works.

4.5.3.1 Phase 1 : *Neighbor Discovery*

The first step is neighbor discovery i.e. each node must build what is called a *neighborhood table*. Every node is equipped with multiple radios tuned to non-overlapping channels and the node must discover neighbors on all its radio interfaces. To achieve this, nodes periodically broadcast a small *HELLO* packet. The *HELLO* packet is small in size, contains the node ID, and is broadcast over all the available radio interfaces of a node. All neighbor nodes (i.e. nodes within the communication range of the transmitting node) which receive the *HELLO* make note of the neighbor ID, the interface over which the *HELLO* was received and the channel assigned to that interface. By



Neighbor Table of Node A

Neighbor ID	Radio ID	Channel ID
B	1	1
B	2	2
C	1	1

FIGURE 4.4 – *The neighbor discovery phase*

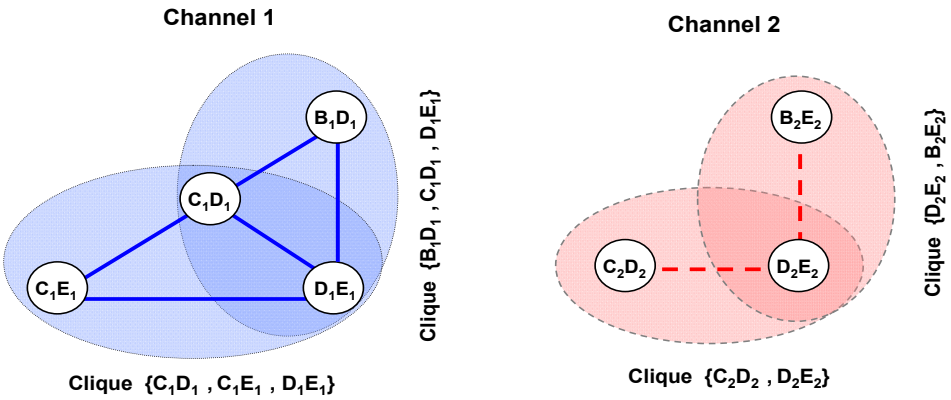


FIGURE 4.5 – *Conflict graphs for link (D, E) on channel 1 and channel 2*

considering the example of the network represented in figure 4.1 ; we represent in figure 4.4 the neighborhood table for node A. Note that as shown for node A, the neighbor discovery mechanism enables the node to identify *multi-link* neighbors (node B) which are connected to the node through more than one interface (and consequently over multiple channels). Since topology changes are few in wireless mesh networks, we propose using a large time interval for the periodic *HELLO* messages.

4.5.3.2 Phase 2 : *Route Discovery and Admission Control*

A. Bandwidth Estimation

We use the conflict graph approach to estimate the available bandwidth on a "wireless hop". In this section, there are three important steps. First, we estimate the available bandwidth on each outgoing link at a node considering only the interference caused by existing flows. Second, we take into account the *intra-flow* interference that the incoming flow will experience with itself and update the estimated bandwidth. Finally, we estimate the total bandwidth available on each outgoing hop (by combining the estimated bandwidths of links which comprise those hops) :

1. Bandwidth Estimation Considering Existing Flows - From the example topology presented in the previous section, we will show how we will calculate the available bandwidth on the wireless hop DE (figure 4.1) comprising of links $\mathcal{D}_1E_1$ and $\mathcal{D}_2E_2$. Figure 4.5 shows the relevant portions of conflict graph for links $\mathcal{D}_1E_1$ and $\mathcal{D}_2E_2$ taken from the conflict graph of figure 4.2 in the previous section.We first estimate the bandwidth available on link $\mathcal{D}_1E_1$. From figure 4.5, we can see that the maximal cliques constraints for link $\mathcal{D}_1E_1$ are :

$$\begin{aligned} \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{C}_1E_1} + \mathcal{F}_{\mathcal{D}_1E_1} \leq \Re(1) \\ \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{D}_1E_1} \leq \Re(1) \end{aligned} \tag{4.3}$$

To calculate the aggregate flow rates on links within a maximal clique, nodes can use techniques similar to those [X. Cheng 08] explained in section 4.4.4. The link $\mathcal{D}_1E_1$ is part of two maximal cliques $Clique_1 = \{\mathcal{C}_1\mathcal{D}_1, \mathcal{C}_1E_1, \mathcal{D}_1E_1\}$ and $Clique_2 =$

$\{\mathcal{B}_1\mathcal{D}_1, \mathcal{C}_1\mathcal{D}_1, \mathcal{D}_1E_1\}$. Clique constraints dictate that we cannot have two links simultaneously active neither in $Clique_1$ or $Clique_2$. To estimate the available bandwidth on link $\mathcal{D}_1E_1$, one approach [J. Tang 05] is that it is the residual bandwidth after removing traffic from all interfering links belonging to all maximal cliques for that link and the traffic on the link itself. This definition is the worst case computation because two links belonging to two different maximal cliques may interfere with a given link but they may not be mutually interfering and may be active simultaneously. This definition however assumes that the activity of these links is completely non-overlapping and blocks the given link the maximum possible. For example, for link $\mathcal{D}_1E_1$ from figure 4.5, links $\mathcal{C}_1E_1$ and $\mathcal{B}_1\mathcal{D}_1$ interfere with link $\mathcal{D}_1E_1$, but they can be active simultaneously as they do not mutually interfere. The worst case is when they block link $\mathcal{D}_1E_1$ by transmitting at completely non-overlapping times. For link $\mathcal{D}_1E_1$, let $(Av.BW)_{\mathcal{D}_1E_1}$ represent the available bandwidth on link $\mathcal{D}_1E_1$. Here, the load on the links interfering with link $\mathcal{D}_1E_1$ is equal to $\{\mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{C}_1E_1} + \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1}\}$ and the load on the link itself is equal to $\mathcal{F}_{\mathcal{D}_1E_1}$. Therefore, we have :

$$(Av.BW)_{D_1E_1} = \Re(1) - \{\mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{C}_1E_1} + \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{D}_1E_1}\} \tag{4.4}$$

For link $\mathcal{D}_2E_2$, we can calculate the Available Bandwidth $(Av.BW)_{\mathcal{D}_2E_2}$ as follows :

$$(Av.BW)_{\mathcal{D}_2E_2} = \Re(2) - \{\mathcal{F}_{\mathcal{C}_2\mathcal{D}_2} + \mathcal{F}_{\mathcal{B}_2E_2} + \mathcal{F}_{\mathcal{D}_2E_2}\} \tag{4.5}$$

Until this point, we have presented how this definition captures interference (*intra-flow* and *inter-flow*) between existing flows. We now explain how we capture the interference (*intra-flow*) of the incoming flow with itself.

2. Considering the effect of interference of the incoming flow on Bandwidth - An important part of our contribution is that we explicitly take into account the intra-flow interference that the new incoming flow will create with itself. This is an important problem which is sometimes neglected [X. Cheng 08]. *In our proposed approach, we again use the conflict graph to know which links are interfering with each other and use it for estimating intra-flow interference of the incoming flow*. We explain this using the same connectivity and conflict graph as example. Suppose that we have a route request which originated at node $\mathcal{C}$ and has now reached node $\mathcal{D}$. The last node i.e. node $\mathcal{C}$ computed the clique constraints and decided that when the incoming flow starts, it will put $X_{\mathcal{C}_1\mathcal{D}_1}$ amount of traffic of the flow on the link $\mathcal{C}_1\mathcal{D}_1$ and $\mathcal{Y}_{\mathcal{C}_2\mathcal{D}_2}$ amount of traffic of the flow on the link $\mathcal{C}_2\mathcal{D}_2$ ($BW_Required$ = $X_{\mathcal{C}_1\mathcal{D}_1}$ + $\mathcal{Y}_{\mathcal{C}_2\mathcal{D}_2}$). Then from the conflict graph we can see that links $\mathcal{C}_1\mathcal{D}_1$ and $\mathcal{D}_1E_1$ interfere with each other since they belong to the same maximal clique. Similarly, $\mathcal{C}_2\mathcal{D}_2$ and $\mathcal{D}_2E_2$ interfere with each other. We integrate the *expected* interference (traffic represented by $X_{\mathcal{C}_1\mathcal{D}_1}$ and $\mathcal{Y}_{\mathcal{C}_2\mathcal{D}_2}$) in our calculations. Equations 4.4 and 4.5 become :

$$(Av.BW)_{D_1E_1} = \Re(1) - \{F_{C_1D_1} + F_{C_1E_1} + F_{D_1E_1} + F_{B_1D_1} + X_{\mathcal{C}_1\mathcal{D}_1}\} \tag{4.6}$$

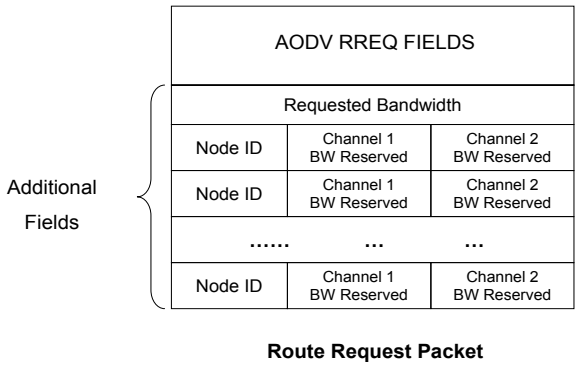


FIGURE 4.6 – *Possible format of the Route Request packet*

$$(Av.BW)_{D_2E_2} = \Re(2) - \{F_{C_2D_2} + F_{B_2E_2} + F_{D_2E_2} + \mathcal{Y}_{\mathcal{C}_2\mathcal{D}_2}\} \tag{4.7}$$

The information about how much traffic share of the incoming flow is reserved on which links of the previous hops for the current route is transported in the route request packet of the protocol. Each intermediate node puts this information when the packet reaches it as shown in figure 4.6. Each node gets the values of the terms such as $X_{\mathcal{C}_1\mathcal{D}_1}$ and $\mathcal{Y}_{\mathcal{C}_2\mathcal{D}_2}$ by looking at the route request packet.

3. Available Bandwidth on a Hop

Definition *: (Available Hop Bandwidth) - Let $\mathcal{L}(u,v) = \{\ell_1, \ell_2 .... \ell_K\}$ represent the set of links on non-overlapping channels which constitute a wireless hop between nodes u and v. The Hop Bandwidth of a hop between nodes u, v and denoted by $(Av.BW)_{Hop\ (u,v)}$ is the sum of the individual bandwidths of all the links on the wireless hop (u,v) :*

$$(Av.BW)_{Hop\ (u,v)} = \sum_{\ell \in \mathcal{L}(u,v)} (Av.BW)_{\ell} \tag{4.8}$$

For example, the aggregate bandwidth that the wireless hop $\mathcal{D}E$ can support is the sum of individual bandwidths available on all the links between nodes $\mathcal{D}$ and E : $(Av.BW)_{\mathcal{D}_1E_1} + (Av.BW)_{\mathcal{D}_2E_2}$. In our approach, the bandwidth requirements of an incoming flow can be met by splitting its traffic between multiple links at each wireless hop. How the traffic is actually split is the problematic of load-balancing.

B. Admission Decision

In this step, we only check whether any of the outgoing wireless hops has enough bandwidth available. For example, for hop $\mathcal{D}E$, we perform the following check :

$$\begin{aligned} &If((Av.BW)_{Hop\ \mathcal{D}E} \geq BW_{required}) \qquad Proceed \\ &\qquad Else \quad Stop \end{aligned} \tag{4.9}$$

C. Load Balancing

When the route request packet for an incoming flow reaches a node, the node first estimates the available bandwidth on each wireless link (and wireless hop). In existing approaches, for any given flow, only one link is used between neighboring nodes

which we argue can seriously limit both performance and flow admissibility. In its simplest form, the load-balancing can be to split the incoming traffic equally between multiple available links on a wireless hop. However, a more efficient load balancing can be achieved by splitting the traffic on multiple links between neighboring nodes using the existing interference on those links as a heuristic. Conversely, the available bandwidth is the remaining bandwidth after removing all the interferences. We split traffic for the incoming flow on links of a wireless hop according to the proportion of bandwidth that they have available. Formally, for a flow requiring bandwidth $BW_{Required}$ on wireless hop $\mathcal{L}(u,v) = \{\ell_1, \ell_2 .... \ell_K\}$ the bandwidth reserved $\mathcal{B}_\ell$ on link $\ell \in \mathcal{L}(u,v)$ which has available bandwidth $(Av.BW)_\ell$ will be :

$$\mathcal{B}_\ell = \frac{(Av.BW)_\ell}{(Av.BW)_{Hop\ (u,v)}} \times BW_{Required} \tag{4.10}$$

C. Resource Reservation

When the route request packet was traversing the network, intermediate nodes which could support the required bandwidth (and including the intra-flow interference) make a temporary reservation and rebroadcast the route request packet. Once the route request packet has reached the destination node, the destination sends back a route reply and all intermediate nodes finalize the reservation.

4.5.3.3 Phase 3 : *QoS Violation Detection and Recovery*

The phase of QoS violation detection and Recovery comes into action once admission control and resource reservation phases are over and the source has actually started sending data to the destination node. QoS violations can occur due to a number of reasons. First, since the mesh network represents a distributed system, network conditions may change during the route discovery phase, rendering the bandwidth estimations and reservations invalid. For example, the bandwidth estimation of a link at a node is done based on the information received from nodes within a *region of interference* periodically and the node may admit a flow assuming that there is enough bandwidth available whereas it comes to know in the next periodic update from its neighbors that this may not be the case. Such violations cannot be avoided since every node cannot have a complete and perfectly synchronized image of the network at all times. For example, the periodic exchange of aggregate flow information may be done every 2 seconds [X. Cheng 08] and things may change between two successive updates. Moreover, a flow may start sending more data than it reserved. To counter these violations, each node periodically checks whether the bandwidth guarantees are met and if the flow is sending more than its share. This can be done by e.g. keeping track of the dynamic transmission rate of each flow in the queues of each node. If any node detects any violation of the guaranteed bandwidth, it reports the problem to the source. The recovery usually involves another phase of route request to find an alternate route fulfilling QoS requirements. The node may additionally inform other nodes on the route to relinquish the reserved resources for that flow.

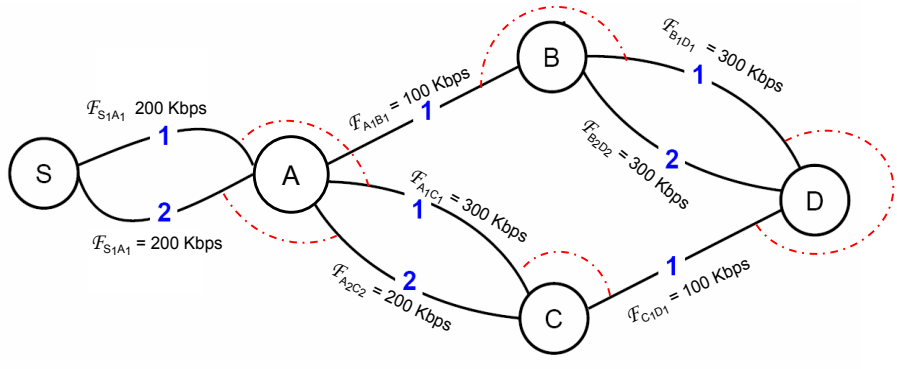


FIGURE 4.7 – *Connectivity graph with load distribution*

4.6 An Example

QoS provisioning in a multi-radio multi-channel network by exploiting link-diversity is a complex problem as there are a number of considerations which must be accounted for. Next, we will show how this works on a sample connectivity graph. We assume that we have an incoming flow at node $\mathcal{S}$ which requires $BW_{Required} = 100\,Kbps$ end-to-end bandwidth to node $\mathcal{D}$. We assume that the channel bandwidth of channel 1 and channel 2 is 1 Mbps i.e $\Re(1) = \Re(2) = 1\,Mbps$. We will show the evolution of our proposed solution from node $\mathcal{S}$ to node $\mathcal{D}$.

Figure4.7 shows the connectivity graph along with load distribution for a 6-node dual-radio dual-channel wireless mesh network. For simplicity, we present the global conflict graph derived from the connectivity graph here just once instead of presenting the local conflict graph that each node will generate. Each node will "see" only its portion of the global conflict (node's local conflict graph). In reality, instead of one global conflict graph, each node will actually derive its local conflict graph. However, this is just a simplification and does not change results. Figure 4.8 shows the global conflict graph created assuming the connectivity graph and conflicting links shown in figure 4.7. From here on, we explain how our proposed solution works at each node. We will also indicate the load distribution i.e. the reserved bandwidth that each node makes for the incoming flow on its outgoing links.

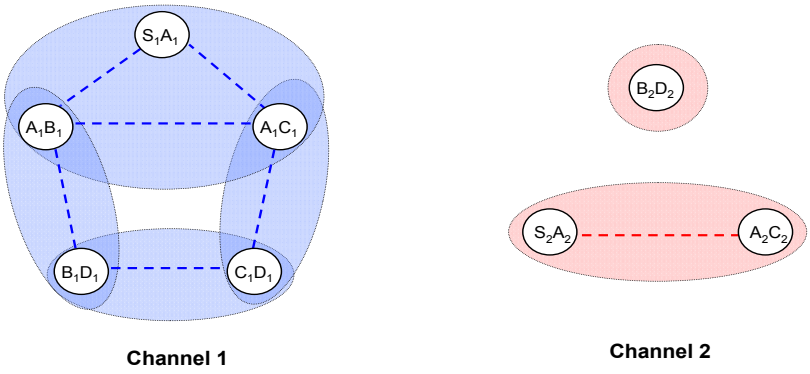


FIGURE 4.8 – *The global conflict graph*

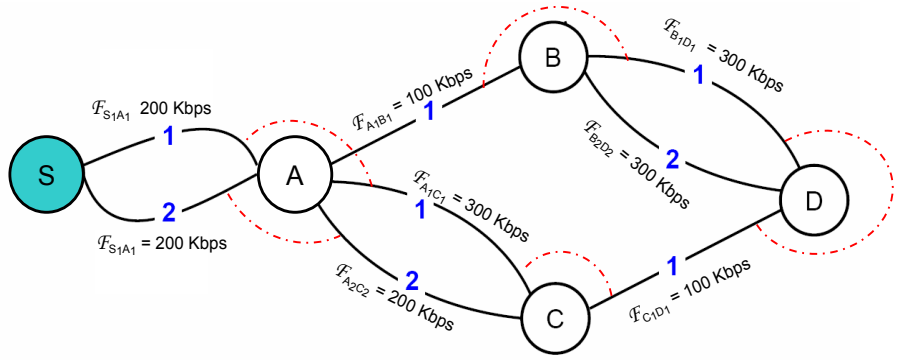


FIGURE 4.9 – *Connectivity graph for the network with load distribution when request is at node S*

4.6.1 Analysis at Node S

A) Compute Bandwidth Available on Links and Hops

Hop $\mathcal{SA}$: - Hop $\mathcal{SA}$ has two links $\mathcal{S}_1\mathcal{A}_1$ and $\mathcal{S}_2\mathcal{A}_2$, so we calculate the bandwidths for both and then sum them together to get the bandwidth of the hop $\mathcal{SA}$. The link $\mathcal{S}_1\mathcal{A}_1$ is part of a single maximal clique constraint. The maximal clique constraint related to link $\mathcal{S}_1\mathcal{A}_1$ is the following :

$$\mathcal{F}_{\mathcal{S}_1\mathcal{A}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} \leq \Re(1) \tag{4.11}$$

Link $\mathcal{S}_2\mathcal{A}_2$ is also part of a single maximal clique constraint :

$$\mathcal{F}_{\mathcal{S}_2\mathcal{A}_2} + \mathcal{F}_{\mathcal{A}_2\mathcal{C}_2} \leq \Re(2) \tag{4.12}$$

$$\begin{aligned} (Av.BW)_{\mathcal{S}_1\mathcal{A}_1} &= \Re(1) - \{\mathcal{F}_{\mathcal{S}_1\mathcal{A}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1}\} \\ (Av.BW)_{\mathcal{S}_1\mathcal{A}_1} &= 1000 - \{200 + 100 + 300\} = 400\,Kbps \\ (Av.BW)_{\mathcal{S}_2\mathcal{A}_2} &= \Re(2) - \{\mathcal{F}_{\mathcal{S}_2\mathcal{A}_2} + \mathcal{F}_{\mathcal{A}_2\mathcal{C}_2}\} \\ (Av.BW)_{\mathcal{S}_2\mathcal{A}_2} &= 1000 - \{200 + 200\} = 600\,Kbps \end{aligned} \tag{4.13}$$

$$(Av.BW)_{Hop\ \mathcal{SA}} = (Av.BW)_{\mathcal{S}_1\mathcal{A}_1} + (Av.BW)_{\mathcal{S}_2\mathcal{A}_2} = 400 + 600 = 1000\,Kbps \tag{4.14}$$

B) Enough Bandwidth Available on any hop ?

We now check whether any of the next hops can support the required bandwidth or not. We find the following inequalities :

$$\begin{aligned} (Av.BW)_{Hop\ \mathcal{SA}} &\geq BW_{required} \quad ? \\ 1000\,Kbps &\geq 100\,Kbps \end{aligned} \tag{4.15}$$

The required bandwidth is met for hop $\mathcal{SA}$ therefore, a temporary reservation is made at the node.

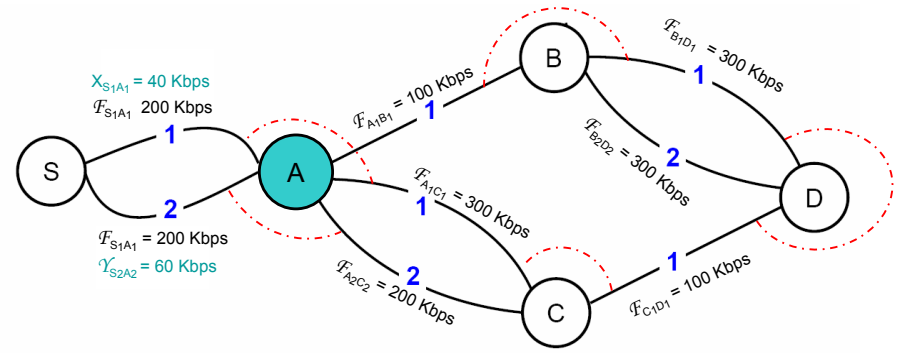


FIGURE 4.10 – *Connectivity graph with load distribution when request is at node A*

C) Load Balancing

We next perform load-balancing using the technique described in the previous section. The traffic of the incoming flow will be distributed proportional to the bandwidth available on these links.

$$\begin{aligned} \mathbf{X_{S_1A_1}} &= \frac{(Av.BW)_{\mathcal{S}_1\mathcal{A}_1}}{(Av.BW)_{Hop\,\mathcal{SA}}} \times BW_{required} = \frac{400}{1000} \times 100 = 40\,Kbps \\ \mathbf{Y_{S_2A_2}} &= \frac{(Av.BW)_{\mathcal{S}_2\mathcal{A}_2}}{(Av.BW)_{Hop\,\mathcal{AC}}} \times BW_{required} = \frac{600}{1000} \times 100 = 60\,Kbps \end{aligned} \tag{4.16}$$

4.6.2 Analysis at Node A

A) Compute Bandwidth Available on Links and Hops

Hop $\mathcal{AB}$: - Hop $\mathcal{AB}$ has only one link, so the bandwidth of the hop will be the bandwidth of the link $\mathcal{A}_1\mathcal{B}_1$. We note that link $\mathcal{A}_1\mathcal{B}_1$ is part of two maximal cliques :

$$\begin{aligned} \mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{S}_1\mathcal{A}_1} + \mathbf{X_{S_1A_1}} &\leq \Re(1) \\ \mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1} &\leq \Re(1) \end{aligned} \tag{4.17}$$

In these constraints, $\{\mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{S}_1\mathcal{A}_1}\}$ and $\{\mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1}\}$ represent the interference from existing flows. Whereas, $\mathbf{X_{S_1A_1}}$ has been included as part of clique constraint because we will have this much amount of traffic of the incoming flow already passing through the link $\mathcal{S}_1\mathcal{A}_1$. This is the *intra-flow interference* that the incoming flow will generate from the previous link. As explained in the previous section, we can calculate the available bandwidth $(Av.BW)_{\mathcal{A}_1\mathcal{B}_1}$ for link A_1B_1 as :

$$\begin{aligned} (Av.BW)_{\mathcal{A}_1\mathcal{B}_1} &= \Re(1) - \{\mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{S}_1\mathcal{A}_1} + \mathbf{X_{S_1A_1}} + \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1}\} \\ (Av.BW)_{\mathcal{A}_1\mathcal{B}_1} &= 1000 - \{100 + 300 + 200 + 40 + 300\} = 60\,Kbps \\ (Av.BW)_{Hop\ \mathcal{AB}} &= (Av.BW)_{\mathcal{A}_1\mathcal{B}_1} = 60\,Kbps \end{aligned} \tag{4.18}$$

Hop $\mathcal{AC}$: - Hop $\mathcal{AC}$ has two links $\mathcal{A}_1\mathcal{C}_1$ and $\mathcal{A}_2\mathcal{C}_2$, so we calculate the bandwidths for both and then sum them together to get the bandwidth of the hop $\mathcal{AC}$. The maximal cliques for link $\mathcal{A}_1\mathcal{C}_1$ are the following :

$$\begin{aligned} \mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{S}_1\mathcal{A}_1} + \mathbf{X}_{\mathbf{S}_1\mathbf{A}_1} &\leq \Re(1) \\ \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} &\leq \Re(1) \end{aligned} \tag{4.19}$$

The maximal cliques for link $\mathcal{A}_2\mathcal{C}_2$ are :

$$\mathcal{F}_{\mathcal{A}_2\mathcal{C}_2} + \mathcal{F}_{\mathcal{S}_2\mathcal{A}_2} + \mathbf{Y}_{\mathbf{S}_2\mathbf{A}_2} \leq \Re(2) \tag{4.20}$$

Once again $\mathbf{X}_{\mathbf{S}_1\mathbf{A}_1}$ and $\mathbf{Y}_{\mathbf{S}_2\mathbf{A}_2}$ are included in the clique constraints as they represent the *intra-flow interference* that the incoming flow will experience with itself on channel 1 and channel 2 respectively. The bandwidths are calculated as :

$$\begin{aligned} (Av.BW)_{\mathcal{A}_1\mathcal{C}_1} &= \Re(1) - \{\mathcal{F}_{\mathcal{A}_1\mathcal{B}_1} + \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{S}_1\mathcal{A}_1} + \mathbf{X}_{\mathbf{S}_1\mathbf{A}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1}\} \\ (Av.BW)_{\mathcal{A}_1\mathcal{C}_1} &= 1000 - \{100 + 300 + 200 + 40 + 100\} = 260\,Kbps \\ (Av.BW)_{\mathcal{A}_2\mathcal{C}_2} &= \Re(2) - \{\mathcal{F}_{\mathcal{A}_2\mathcal{C}_2} + \mathcal{F}_{\mathcal{S}_2\mathcal{A}_2} + \mathbf{Y}_{\mathbf{S}_2\mathbf{A}_2}\} \\ (Av.BW)_{\mathcal{A}_2\mathcal{C}_2} &= 1000 - \{200 + 200 + 60\} = 540\,Kbps \end{aligned} \tag{4.21}$$

$$(Av.BW)_{Hop\ \mathcal{AC}} = (Av.BW)_{\mathcal{A}_1\mathcal{C}_1} + (Av.BW)_{\mathcal{A}_2\mathcal{C}_2} = 260 + 540 = 800\,Kbps \tag{4.22}$$

B) Enough Bandwidth Available on any hop ?

We now check whether any of the next hops can support the required bandwidth or not. We find the following inequalities :

$$\begin{aligned} (Av.BW)_{Hop\ \mathcal{AB}} \geq BW_{required} \quad ? \\ 60\,Kbps \ngeq 100\,Kbps \\ (Av.BW)_{Hop\ \mathcal{AC}} \geq BW_{required} \quad ? \\ 800\,Kbps \geq 100\,Kbps \end{aligned} \tag{4.23}$$

The node will decide that hop $\mathcal{AB}$ does not pass the first check, so this option will be eliminated. The required bandwidth is met for hop $\mathcal{AC}$ therefore, a temporary reservation is made at the node.

C) Load Balancing

We next perform load-balancing using the technique described in the previous section. The traffic of the incoming flow will be distributed proportional to the bandwidth available on these links.

$$\begin{aligned} \mathbf{X}_{\mathbf{A}_1\mathbf{C}_1} &= \frac{(Av.BW)_{\mathcal{A}_1\mathcal{C}_1}}{(Av.BW)_{Hop\,\mathcal{AC}}} \times BW_{required} = \frac{260}{800} \times 100 = 32\,Kbps \\ \mathbf{X}_{\mathbf{A}_2\mathbf{C}_2} &= \frac{(Av.BW)_{\mathcal{A}_2\mathcal{C}_2}}{(Av.BW)_{Hop\,\mathcal{AC}}} \times BW_{required} = \frac{260}{800} \times 100 = 68\,Kbps \end{aligned} \tag{4.24}$$

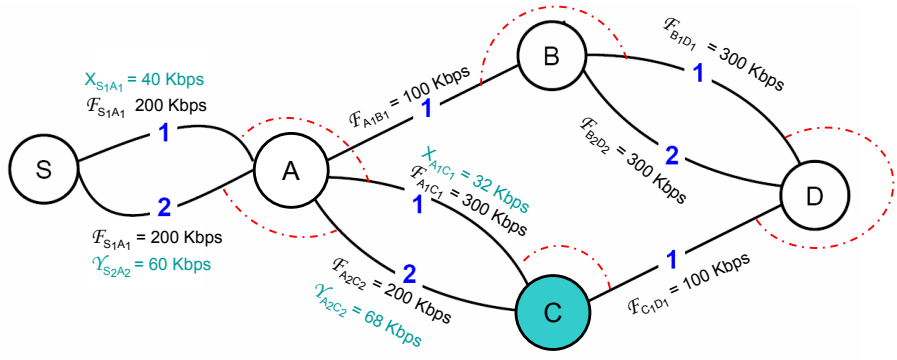


FIGURE 4.11 – *Connectivity graph with load distribution when request is at node C*

4.6.3 Analysis at Node C

A) Compute Bandwidth Available on Links and Hops

Hop $\mathcal{CD}$: - Hop $\mathcal{CD}$ has only one link, so the bandwidth of the hop will be the bandwidth of the link $\mathcal{C}_1\mathcal{D}_1$. We note that link $\mathcal{C}_1\mathcal{D}_1$ is part of two maximal cliques :

$$\begin{aligned} \mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathbf{X}_{\mathbf{A_1C_1}} &\leq \Re(1) \\ \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} &\leq \Re(1) \end{aligned} \tag{4.25}$$

We can calculate the available bandwidth $(Av.BW)_{\mathcal{C}_1\mathcal{D}_1}$ for link C_1D_1 as :

$$\begin{aligned} (Av.BW)_{\mathcal{C}_1\mathcal{D}_1} &= \Re(1) - \{\mathcal{F}_{\mathcal{A}_1\mathcal{C}_1} + \mathcal{F}_{\mathcal{C}_1\mathcal{D}_1} + \mathbf{X}_{\mathbf{A_1C_1}} + \mathcal{F}_{\mathcal{B}_1\mathcal{D}_1}\} \\ (Av.BW)_{\mathcal{C}_1\mathcal{D}_1} &= 1000 - \{300 + 100 + 32 + 300\} = 268\,Kbps \\ (Av.BW)_{Hop\ \mathcal{AB}} &= (Av.BW)_{\mathcal{C}_1\mathcal{D}_1} = 268\,Kbps \end{aligned} \tag{4.26}$$

B) Enough Bandwidth Available on any hop ?

We now check whether any of the next hops can support the required bandwidth or not. We find the following inequalities :

$$\begin{aligned} (Av.BW)_{Hop\ \mathcal{CD}} \geq BW_{required} \quad ? \\ 268\,Kbps \geq 100\,Kbps \end{aligned} \tag{4.27}$$

The required bandwidth is met for hop $\mathcal{CD}$ therefore, a temporary reservation is made at node $\mathcal{C}$.

C) Load Balancing

Since there is only one link in this hop, all the load is put on it.

Node $\mathcal{C}$ re-broadcasts the route request and the request arrives at the destination node $\mathcal{D}$. Figure 4.12 shows the load distribution for the incoming flow including the hop $\mathcal{CD}$. Node $\mathcal{D}$ sends back the route reply packet and the reservation is finalized at the intermediate nodes.

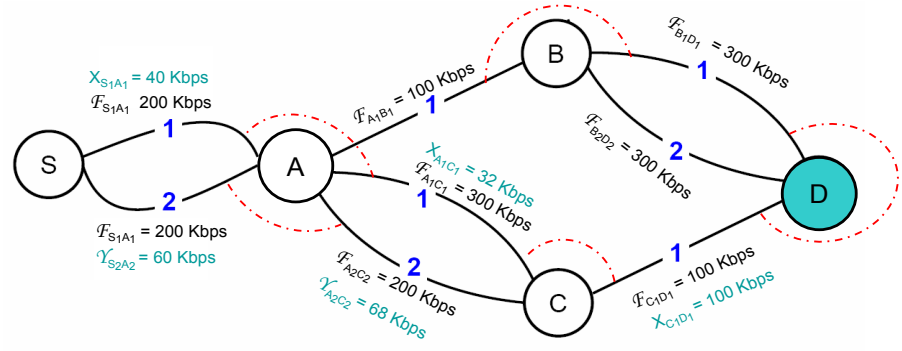


FIGURE 4.12 – *Connectivity graph with load distribution when request is at node D*

4.7 CONCLUSION

This chapter addresses the problem of providing end-to-end bandwidth guarantees to flows in multi-radio multi-channel wireless mesh networks. The focus has been on the problem of interference (*inter-flow* and *intra-flow*) which has been captured by means of the conflict graph and clique constraints. The main contribution of this chapter is to capture *inter-flow* and *intra-flow* interference in the multi-channel, multi-hop route and to exploit link diversity to both, improve flow admissibility and perform better load-balancing. Our motivation for future is to evaluate the performance of the proposed QoS scheme through simulations.

Conclusion

The aim of this dissertation is to contribute to performance improvement and QoS provisioning in wireless mesh networks, the two principle challenges faced by mesh networks today. The dissertation contributes in the following fundamental areas for IEEE 802.11-based wireless mesh networks : *route selection*, *route maintenance* and *conceptual framework for providing per-flow QoS guarantees*. Figure 4.13 presents the main components of the contribution.

The first contribution, *route selection*, encompasses two scenarios in mesh networks. The first scenario concerns the definition and selection of a route to provide high performance for *peer-to-peer* communication between mesh routers. The "*metric*" to select the route called *Expected Link Performance Metric* (ELP) captures several fundamental link quality components of intermediate links to define the quality of the end-to-end route. The first component is the influence of *logical interference* which is the interference arising from CSMA-CA based MAC protocol which prevents a node from transmitting on the channel because some other node is transmitting in the carrier-sensing range of the node. This is captured by the *Average Interference Ratio* (AIR) which is essentially the ratio of time that the node is blocked from transmitting to the total available time during a window of time. The second component is the *link loss ratio* which results from *physical interference* (interference at signal level which can occur during the transmission of a packet) and *noise* present on the channel. The third component is the *link capacity*, which is essentially the transmission rate of the radio on the link. The ELP metric has been compared through simulations with several existing metrics (ETX, ETT, iAWARE) and the results show performance improvement. The second scenario concerns an extension of the ELP metric - *ELP-GS* for *gateway-oriented* traffic. The extended metric integrates the gateway load in addition to the basic components of the ELP route metric. Simulation based performance comparison of ELP-GS with existing gateway and route-to-gateway selection schemes show interesting results.

The second contribution was motivated from the observation that in IEEE 802.11-based mesh networks, on-demand routing protocols suffer from route instability due to frequent route breakages resulting in poor performance. Routing protocols, rely on IEEE 802.11 link-layer feedback to detect broken links between intermediate nodes in a path. Transmission attempts from one node to another sometimes fail due to a number of reasons including poor signal quality or collisions on the shared

wireless medium. The IEEE 802.11 link-layer reports these problems as a *link failure notification* message to the routing protocol at network layer after 7 consecutive failed transmissions (4 for large packets). Routing protocols systematically interpret this as *link breakage* and declare a *route breakage*. In reality, the transmission failures (and the resulting *link failure notification*) are sometimes "*transient*" in nature, resulting from temporary transmission problems and do not actually represent broken links. We propose a novel route maintenance mechanism *Efficient Route Maintenance (ERM)* which evaluates the *physical link quality* (Signal-to-Interference-plus-Noise Ratio - SINR) and the *logical link quality* (AIR) to distinguish between *"good"* quality links which are assumed to have transient transmission problems and *"bad"* quality links with sustained transmission problems and which must be declared broken. When the routing protocol (network layer) receives a *link failure notification*, the long-term performance of the link (based on the physical and logical link quality) is assessed to make a coherent link-breakage decision. To assess the link quality (both physical and logical), ERM uses two mechanisms : *Listen* (based on passive measurements) and a *Hello* (based on active measurements). The *Listen* mechanism uses local SINR and local AIR to estimate the link quality whereas the *Hello* mechanism uses active exchange of Hello packets between nodes on a link to jointly estimate the physical and logical link quality. Simulation based performance comparison of ERM with the standard AODV and AODV with local route repair optimization shows substantial performance improvements (up to 100%) in both single-radio single-channel mesh networks and multi-radio multi-channel mesh networks.

The final contribution proposes a conceptual framework for providing per-flow QoS guarantees in multi-radio multi-channel wireless mesh networks. The proposed solution models the fundamental problematic of interference (*inter-flow* and *intra-flow*) and exploits link-diversity (availability of multiple links between neighboring nodes) offered in multi-radio multi-channel mesh networks. The solution is based on the concepts of conflict-graph, maximal cliques and clique constraints to model interference in the network. From the clique constraints, we derive the constraints on the aggregate rates of existing flows on the link relative to each channel. Based on the flow-rate constraints, the solution performs admission control for an incoming flow while taking into consideration the *inter-flow* interference of existing flows as well as the *intra-flow* interference that the incoming flow will generate with itself. Moreover, the solution also exploits link-diversity to perform load-balancing at each wireless hop by spreading the traffic load of the incoming flow on multiple concurrent links in inverse proportion to the interference already present on them to achieve better load-balancing and higher flow admittance rate. An example of the application of the solution is also presented.

Finally, we believe that wireless mesh networks are expected to remain the center of attention in the coming years. With increasing user requirements for performance,

we need efficient solutions which push the capacity of the mesh networks to limits. For the future, there are a number of possible directions. An interesting direction of work can be to further enhance the *logical interference* estimation component since we observed that it is one of the most important aspects for a routing metric. The QoS framework proposed is conceptual in nature and it would be interesting to evaluate its performance using simulations to contrast it against traditional approaches. Moreover, some aspects of the QoS framework can be further improved. The load-balancing component of the QoS framework (allocating the traffic of the incoming flow based on interference present on the link) can be used independently for dynamically splitting traffic between neighboring nodes without the QoS guarantees context. This can provide better load-balancing in the network. Another possible direction of research can be to propose solutions for providing end-to-end delay guarantees for real-time applications.

Currently, we have deployed a small 8-node wireless mesh testbed - LAAS-MESH at our laboratory. Experimental work is in progress to investigate different aspects of mesh networks including the various components of the routing metric. It would be interesting to evaluate some parts of the contributions of this dissertation. We are mainly interested in validating some aspects of the routing metric on the testbed. The experimental results for the asymmetry component have already been presented in chapter 2. In the long-term, we aim at developing a unified software which integrates route selection, route maintenance and QoS guarantees for mesh networks.

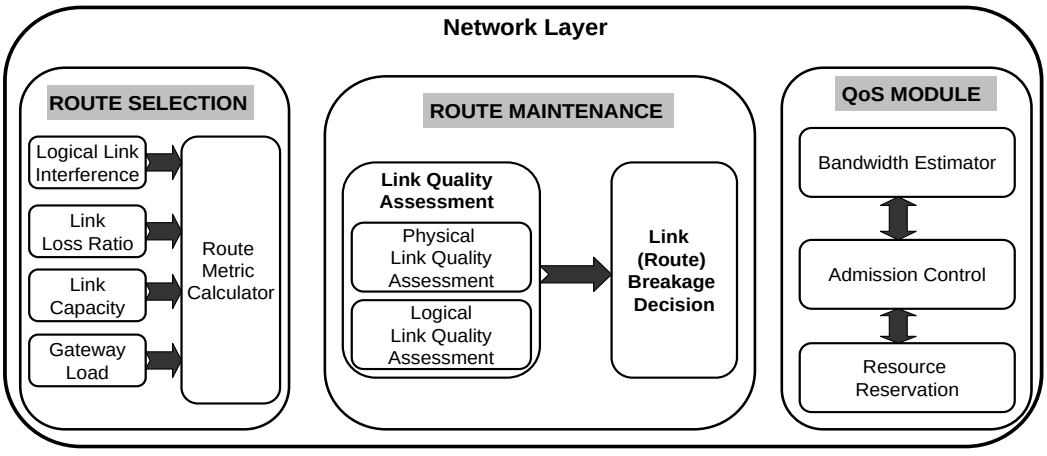


FIGURE 4.13 – *Logical Framework of the dissertation contributions*

Sommaire en Français

A

Introduction

De nos jours, les réseaux locaux sans fil connaissent un succès certain. Ils sont désormais omniprésents et sont déployés dans les bureaux, les cafés, les universités et les aéroports. Ils offrent également plusieurs perspectives d'application liées notamment à la mobilité des personnes, à la sécurité des personnes, etc.

Les réseaux locaux sans fil conventionnels ont néanmoins quelques limitations, notamment, le besoin d'une infrastructure filaire (généralement Ethernet) reliant chaque Point d'Accès (PA). En effet, l'extension de leur couverture devient coûteuse et peu pratique. Les réseaux maillés sans fil ont dernièrement été proposé afin de répondre à cette limitation. Libre de toute exigence d'infrastructure, les routeurs peuvent être ajoutés comme la situation le demande, offrant une excellente flexibilité. Le réseau peutainsi se prolonger sur plusieurs kilomètres, et offrir un accès sans fil à Internet.

Les réseaux maillés sans fil sont un cas particulier de réseaux multi-sauts sans fil. Ils se distinguent par la présence d'un coeur de réseau (dit fédérateur ou backbone) constitué de routeurs fixes et alimentés . Les routeurs dans un réseau maillé se connectent entre eux afin de créer une topologie avec un maillage fort. Les routeurs agissent en tant que points d'accès sans fil auxquelles d'autres utilisateurs et des réseaux d'utilisateurs se connectent. Des routeurs (appelé passerelles) permettent la connexion filaire à l'Internet. Plusieurs technologies de communication ont été proposées pour les réseaux maillés, principalement, IEEE 802.11 (Wi-Fi) et le 802.16 (Wimax). En raison du coût relativement faible des équipements et leur disponibilité sur le marché , les réseaux maillés basés sur IEEE 802.11 sont les plus populaires.

Le but de cette dissertation est de contribuer à plusieurs aspects de la Qualité de Service et du routage dans les réseaux maillés sans fil basés sur IEEE 802.11. La première contribution définit une métrique de routage afin de sélectionner un chemin performant entre deux routeurs en prenant compte plusieurs aspects de la qualité des liens, à savoir le taux de pertes, l'interférence et la capacité du lien. L'évaluation de performances de cette métrique en comparaison aux métriques usuelles montre une amélioration de performance en termes de débit et de délai. La deuxième contribution concerne l'amélioration du mécanisme de maintenance des routes pour les

protocoles de routage réactifs. Les protocoles réactifs considèrent qu'un lien (et par conséquence une route) est coupé si la couche liaison observe plusieurs tentatives consécutives d'échec de transmission . Ces échecs sont souvent dues à des problèmes temporaires sur le lien (présence de bruit, interférences etc.) et les coupures de routes qu'ils peuvent occasionner dégradent fortement les performances du réseau. Le mécanisme que nous proposons considère la qualité du lien sur le long terme afin de prendre une décision cohérente sur la coupure du lien (et de la route). Les résultats de simulation montrent une amélioration conséquente des performances du résau. La dernière contribution propose un cadre pour la foruniture de la Qualité de Service (garantie de bande passante) dans les réseaux maillés multi-interfaces et multi-canaux. Ce cadre cherche à tirer partie de la diversité des liens entres les routeurs adjacents du réseau afin d'améliorer le taux d'admission des flux avec garantie de bande passante et mieux répartir la charge.

A.1 Chapitre 1 : L'Etat de l'art

A.1.1 L'Architecture

Un réseau maillé sans fil est divisé en deux parties : le réseau fédérateur (ou l'infrastructure) et les réseaux maillés clients. Le réseau maillé fédérateur se compose de routeurs sans fil statiques qui maintiennent la connectivité, effectuent le routage et constituent l'épine dorsale sans fil. Ces routeurs constituent une infrastructure sans fil de routeurs interconnectés qui fournissent des services aux utilisateurs et aux réseaux. Ces routeurs sont équipés, en général, de plusieurs interfaces radios pour le maillage et une interface radio pour la connexion avec les terminaux et les réseaux. Généralement, un ou plusieurs de ces routeurs fournissent la connectivité filaire à l'Internet. Les réseaux maillés clients sont souvent mobiles et comportent des machines qui ont des contraintes d'énergie. Les réseaux maillés sont aussi classés en fonction du nombre d'interfaces radio et des canaux dont ils disposent. Le plus basique repose sur une interface radio par noeud et un unqiue canal de communication. ce type de réseau souffre des problèmes de performance à cause de l'utilisation d'un seul canal et des fortes interférences entre les routeurs. Dans le deuxième type de réseau, un noeud possède plusieurs interfaces radio qui peuvent opérer sur différents canaux de communication. Dans la suite, nous présentons les différences principales entre les réseaux maillés sans fil et les réseaux multi-saut sans fil conventionnels.

A.1.2 Différences entre les réseaux maillés sans fil et les réseaux multi-sauts sans fil conventionnels

Classiquement, les réseaux multi-sauts sans fil sont sans structure et plutôt ad hoc, mais dans les réseaux maillés, les clients sont souvent présents à la périphérie du réseau, alors que les routeurs passerelles se trouvent au coeur du réseau. Entre ces deux types de noeuds, des routeurs maillés s'intercalent assurant l'acheminement depuis

les clients jusqu'aux passerelles. Les réseaux maillés introduisent donc une organisation matérialisée par la présence de l'infrastructure sans fil (réseau fédérateur).. Plus important encore, la plupart des flux sont entre les clients et les noeuds passerelle ce qui crée des zones de surcharge dans le réseau. Enfin, les réseaux maillés sans fil doivent pour fournir des garanties la bande passante et de performance beaucoup plus contraignantes.

A.1.3 Solutions de Qualité de Service pour les réseaux multi-sauts et pour les réseaux maillés

La fourniture de la Qualité de Service et le routage sont deux problèmes fondamentaux pour les réseaux maillés sans fil. Plusieurs travaux qui traitent de ces deux challenges ont dernièrement été proposés dans la littérature scientifique. Cette section décrit les principaux résultats obtenus pour les réseaux multi-sauts sans fil basées sur la technologie IEEE 802.11. Cette dernière elle repose sur une technique d'accès de type "Carrier Sense Multiple Access (CSMA)" qui souffre des problèmes de stations cachées, stations exposées, collisions etc. Fournir de la qualité de service pour ce type de réseaux est difficile. Le standard IEEE 802.11e a été proposé afin d'intégrer de la qualité de service dans les couches MAC et physique. IEEE 802.11e introduit des classes de services avec différentiation à la priorité d'accès. Mais cette solution est plutôt spécifique aux réseaux locaux sans fil et ne fonctionne pas nécessairement pour les réseaux multi-sauts. La deuxième famille de solutions se concentre sur la couche réseau . Une catégorie de ces solutions propose la réservation des ressources, notamment la bande passante le long d'un chemin afin de garantir la bande passante de bout-en-bout. Une autre classe cherche à contrôler l'admission sans réservation préalable de ressources. Enfin, des cadres fonctionnant au niveau de plusieurs couches ont également été proposés afin de fournir de la qualité de service.Ces derniers supposent l'utilisation dans les couches inférieures d'un protocole de routage réactif qui couple la phase de Découverture de Chemin au contrôle d'admission et la réservation de ressource.

A.1.4 Solutions de Routage pour les réseaux multi-saut et pour les réseaux maillés

En ce qui concerne les protocoles de routage, il y a deux grandes familles de protocoles de routages dans les réseaux multi-saut. Les protocoles de routage réactifs agissent sur le principe de demande c.à.d. la construction de routes en cas de besoin. Elles permettent de réduire considérablement la surcharge de paquets de routage dans le réseau. Les protocoles proactifs suivent une approche dans laquelle l'information de routage est régulièrement diffusée à travers le réseau afin que les tables de routage de chaque noeud soient mises à jour. Par conséquent, les routes sont disponibles là tout moment, mais il y a une surcharge causée par l'échange de messages périodiques. La plupart de réseaux maillés utilisent les protocoles réactifs ou une variation de ces protocoles. Par contre, ces protocoles ont été proposés pour les ré-

seaux ad hoc qui ont des différences fondamentales avec les réseaux maillés. Il y a plusieurs aspects à considérer afin de développer des protocoles efficaces pour les réseaux maillés. Premièrement, est-ce qu'il faut choisir un protocole proactif ou réactif. Deuxièmement, est-ce que le protocole sera cross-layer ou simple. Récemment, les travaux montrent que l'aspect cross-layer peut améliorer la performance au prix de casser la structure modulaire de la pile de protocoles.

A.2 Chapitre 2 : sélection de routes dans les réseaux maillés sans fil

A.2.1 Introduction

Depuis plusieurs années, les protocoles de routage pour les réseaux ad hoc ont utilisé la stratégie de trouver le plus court chemin entre une source et une destination . La sélection du plus court chemin entre deux routeurs est un bon choix si tous les liens (sans fil) dans le réseau ont exactement les mêmes caractéristiques. En réalité, ils peuvent y avoir des différences énormes en termes de performances(par exemple, le taux de pertes sur le lien et la capacité du lien) et donc, le nombre de sauts n'est pas une bonne approche, particulièrement pour les applications basées sur Internet qui nécessitent de bonnes performances. Dans un réseau maillé, nous distinguons deux types de trafic : le trafic "peer-to-peer" et le trafic orienté vers les passerelles. Le trafic "peer-to-peer" reste confiné au sein du réseau maillé. Nous proposons une métrique de routage pour ce type de trafic. Le trafic orienté vers les passerelles se réfère au trafic émanant des utilisateurs au sein du réseau maillé, à destination de l'Internet et qui passe par des passerelles. Nous proposons une extension de la métrique de routage afin d'acheminer ce type de trafic.

A.2.2 Considérations de conception pour le routage dans les réseaux maillés

Nous considérons quatre exigences principales afin de définir une métrique de routage efficace. Premièrement, les métriques de routage doivent être stables c'est-à-dire qu'elles ne doivent pas provoquer des changements fréquents de route ou des oscillations qui peuvent affecter la stabilité de l'itinéraire. Deuxièmement, la métrique de routage doit capturer les caractéristiques essentielles des réseaux maillés. Troisièmement, la métrique de routage doit être conçue de manière à ce que les chemins à coût minimum puissent être trouvés par des algorithmes efficaces qui ne soient pas "NP-difficile". Enfin, la métrique de routage doit veiller à éviter la formation de boucles de routage. Toutes ces quatre exigences sont nécessaires pour concevoir métriques de routage efficace.

A.2.3 Examen de métriques de routage pour les réseaux maillés sans fil

L'un des travaux pionniers dans le domaine des métriques de routage est celui qui a défini la métrique "Expected Transmission Count" (ETX). ETX représente le nombre moyen de transmissions (retransmissions incluses) requis à la couche liaison afin de transmettre avec succès un paquet sur un lien sans fil. Dans ETX, les voisins échangent périodiquement des petits paquets ce qui permet àchaque noeud de prendre connaissance du taux de paquets qui sont reçus dans les sens avant et arrière sur le lien. Les noeuds calculent lETX comme le produit des taux de succès dans les deux directions. ETX est une métrique de routage isotonique. ETX fournit une approximation de la qualité du lien en termes de la qualité du canal de propagation, dubruit présent sur le lien et de l'interférence physique sur le lien. .
La métrique de routage "Expected Transmission time" (ETT) a été dernièrement proposée. Elleaméliore la métrique ETX en intégrant le débit physique des liens radios. Comme ETT est basée sur la métrique ETX, elle capture aussi l'interférence physique de la liaison, mais ne saisit pas explicitement l'interférence logique (interférence protocolaire qui se produit à cause du mécanisme CSMA de IEEE 802.11). ETT est une métrique isotonique.

La métrique "Weighted Cumulative Expected Transmission Time" (WCETT) est une extension de la métrique ETT. La motivation principale de WCETT est de réduire l'interférence Intra-flux en minimisant le nombre de noeuds d'un chemin qui opèrent sur le même canal. Par contre, WCETT n'est pas isotonique et ne capture pas l'interférence logique.

La métrique de routage "Interference-Aware Routing Metric" (iAWARE) prend en compte l'interférence intra-flux et l'interférence inter-flux dans le calcul de la métrique de routage. La métrique utilise le rapport entre SINR et SNR afin de capturer les variations des interférences physiques. Mais elle ne saisit pas l'interférence logique . IAWARE est une métrique de routage non-isotonique.

La métrique de routage "Metric for Interference and Channel Diversity" (MIND) avance que la mesure active de la qualité des liens par le biais de paquets de routage peut causer une surcharge significative sur le réseau. Le métrique MIND repose sur des mesures passives. La métrique a deux composantes, une composante qui inclut à la fois l'interférence physique et l'interférence logique et une deuxième héritée du WCETT qui compte le nombre de liens sur un chemin qui opèrent sur le même canal. Comme MIND travaille localement au niveau d'un noeud sans tenir compte des autres, les deux noeuds extrémités d'un lien peuvent avoir une vision incomplète de l'état du canal ce qui va introduire des erreurs dans l'approximation de la qualité du lien.

A.2.4 La métrique de routage proposé : "Expected Link Performance"

Il y a quatre composantes principales qui constituent notre métrique " Expected Link Performance " (ELP) . Elles sont détaillées ci-après : ***1 - La Taux de perte du lien -*** La technique utilisée par ETX et d'autres métriques usuelles afin d'estimer le taux de transmission avec succès (ou de pertes) en utilisant l'échange de petits paquets (dits paquets sonde) n'est pas précise. Le calcul suppose que le taux de pertes dans les deux directions d'un lien est le même ce qui n'est pas vrai. . De plus, l'approximation des taux de perte telle que réalisée par ETX est inexacte car les paquets sondes sont de taille beaucoup plus petite que les paquets de données ce qui cause une sous-estimation du taux de perte de paquets de données. Notre métrique intègre cette asymétrie dans les calculs afin de donner plus d'importance aux taux de pertes de paquets de données.

2 - L'interférence du lien - Nous distinguons deux types d'interférences : l'interférence physique et l'interférence logique. Nous en avons parlé brièvement dans la section précédente. L'interférence physique se réfère à des interférences au niveau du signal et se produit lors de la transmission d'un paquet sur le canal lorsque les signaux en provenance d'autres communications simultanées affectent le signal d'origine ce qui peut provoquer l'échec de la transmission. Nous mesurons l'interférence physique en utilisant le taux de pertes de petits paquets sur le lien comme expliqué dans la section précédente. L'interférence logique est le temps que pendant lequel le protocole ajourne l'accès du noeud au medium parce que les autres noeuds sont en train d'émettre sur le canal partagé ou lorsque le noeud est en procédure de Backoff. Elle traduit le fait qu'un noeud est empêché d'accéder et de transmettre par le protocole (dans notre cas, CSMA / CA) sur le canal due à une activité des noeuds voisins. Nous mesurons l'interférence logique par le rapport du temps pendant lequel le noeud est empêché d'envoyer sur une fenêtre de temps.
3 - La capacité du lien - ELP prend également en considération les capacités du lien (c'est-à-dire le débit physique de transmission sur le lien radio). Ceci est important pour favoriser les liens avec les capacités les plus élevées . En effet, plus le débit est élevé plus courte est la durée de transmission et par voie de conséquence plus courtes sont les interférences causées par cette transmission sur son voisinage.

A.2.5 L'évaluation de performance d'ELP

L'évaluation de performance d'ELP a été faite en comparaison aux métriques de routage usuelles (Hop Count, ETX, ETT et iAWARE) par simulation sur le logiciel de simulation NS-2. ELP a été implémenté dans AODV et DSDV. L'évaluation a été faite pour les protocoles de transport TCP et UDP. La charge du réseau a été variée afin de voir son effet sur les performances. Les résultats pour AODV et DSDV montrent que globalement ELP donne de meilleures performances en termes de délai de bout en bout et de débit.

A.2.6 Extension d'ELP (ELP-GS) pour le trafic orienté vers les passerelles

Dans la section précédente, nous avons proposé la métrique de routage (ELP) pour choisir la route entre deux routeurs internes au réseau maillé sans fil. Dans cette section, nous proposons une extension du ELP (ELP-GS), qui est une métrique de routage pour le trafic orienté vers les passerelles La métrique considère à la fois la charge de passerelle et la qualité de la route (exprimée par ELP) vers la passerelle. Toutefois, avant que les routeurs puissent envoyer le trafic vers les passerelles, ils doivent savoir l'identité des passerelles actives et les routes vers celles-ci. L'annonce de la présence de passerelles est généralement effectuée par la passerelle via des messages d'annonce, nous proposons également un protocole de découverte de passerelle qui intègre la diffusion de la métrique . ELP-GS intègre la charge des passerelles en plus d'ELP dans la métrique de routage. La charge est mesurée comme l'occupation moyenne (sur le long terme) du buffer de l'interface réseau côté réseau maillé . Pour lisser les variations instantanées, l'occupation moyenne est calculée en utilisant la technique de filtrage du premier ordre "Weighted Moving Average".

A.2.7 L'évaluation de performance d'ELP-GS

L'évaluation de performance d'ELP-GS a été faite en comparaison aux métriques de routage les plus utilisées par simulation sours NS-2. Les résultats montrent qu'ELP-GS donne de meilleures performances en termes de délai de bout en bout, de débit et de sur-débit dû aux paquets de routage

A.3 Chapitre 3 : Maintenance de route dans les réseaux maillés sans fil

A.3.1 Introduction

Des travaux montrent que malgré l'absence de mobilité dans les réseaux maillés basés sur IEEE 802.11, les protocoles de routages réactifs (AODV et DSR étonnamment) souffrent d'une instabilité de route en raison de ruptures de route fréquentes ce qui entraîne une dégradation importante des performances. Dans les réseaux IEEE 802.11, suite à huit échecs de transmission , la couche liaison envoie une notification d'échec à la couche réseau et la couche réseau considère le lien comme coupé et par voie de conséquence certaines routes comme coupées. Il est pertinent de distinguer les liens de "bonne" qualité qui ont des problèmes de transmission temporaires des liens de "mauvaise" qualité ayant des problèmes de transmission soutenus afin que les déclarations de coupure de liens (et donc de routes) dues à des pannes de transmission transitoires soient évités. Nous proposons un nouveau mécanisme de la maintenance de route qui tient compte de plusieurs facteurs afin de distinguer les liens avec des problèmes de transmission transitoires qui peuvent s'attendre à une amélioration et

ceux qui ont un problème de transmission soutenu. Sur la base de cette information , le mécanisme proposé prend une décision cohérente quant à la rupture de lien.

A.3.2 L'instabilité de routes : Causes et Conséquences

La norme IEEE 802.11 spécifie que la couche liaison doit rapporter les problèmes de transmission aux couches plus élevées si elle n'arrive pas à transmettre une trame avec succès sur le lien après un certain nombre de tentatives de transmission. Comme discuté précédemment, la limite normale est de 8 tentatives (une transmission et sept tentatives de retransmission ultérieures) ou 4 pour les paquets avec une taille supérieure à un seuil. Dans les réseaux multi-saut sans fil, les paquets de données traversent plusieurs noeuds avant d'arriver à destination et c'est normal que certains paquets rencontrent des problèmes de transmission sur certains liens (à cause d'interférence, bruit etc.). Les protocoles de routage pour les réseaux multi-saut sans fil dépendent des noeuds intermédiaires pour détecter les coupures des liens et les en informer. Si un noeud intermédiaire n'arrive pas à transmettre des données sur le lien suivant, soit il informe la source que le lien est coupé, soit il lance une requête locale de récupération de route si un tel mécanisme est disponible. Chaque rupture de route introduit des paquets de routage dans le réseau, qui créent plus d'interférences ce qui causent davantage de ruptures de route. Chaque coupure implique que la source doit commencer une nouvelle phase de découverte de route et pendant la phase d'établissement de route, les paquets de données doivent attendre. Pour cette raison, il y a des retards dans le réseau. Les protocoles de routage réactifs ont deux phases, comme décrit dans la section précédente : La phase de découverture de la Route et la phase de Maintenance de la Route. La plupart des travaux existants se concentrent sur l'optimisation de la découverte de la route. Notre motivation principale est qu'il y a eu peu de recherches pour définir un mécanisme plus efficace évitant les ruptures fréquentes de liens liées à des problèmes de transmission transitoires.

A.3.3 Etat de l'Art des solutions existantes

Alors qu'il existe un certain nombre de solutions sur la façon de faire face aux ruptures de route, y compris la récupération locale de route et l'utilisation de routes alternatives, peu de travaux se sont penchés sur le fait que de nombreuses ruptures de liens sont temporaires et que la maintenance de route peut être améliorée La première classe de solutions proposent de maintenir des routes de secours de sorte à ce que si la route principale est coupée, une route alternative peut être directement utilisée sans avoir à lancer de nouvelle phase de découverte de route. Il y a au moins deux problèmes avec ce genre de solutions. Premièrement, les routes de secours sont généralement créées au même moment que la route principale. Ainsi, après que les données aient été acheminées via celle-ci pendant un certain temps, les voies de secours peuvent être devenues obsolètes et ne plus nécessairement représenter une route viable. Deuxièmement, l'hypothèse que la notification rapportée par la couche

liaison représente une coupure effective du lien peut ne pas être vraie en raison d'un certain nombre d'autres facteurs, par exemple l'interférence, bruit, etc. La deuxième classe de solution....

A.3.4 Motivation

Nous pensons que les performances du réseau peuvent être nettement améliorées en évitant les ruptures de route inutiles plutôt que d'utiliser des mécanismes de recouvrement de route. Nous visons à développer un mécanisme qui peut améliorer la précision de détection de la rupture lien afin de l'intégrer dans le mécanisme de maintenance de route des protocoles de routage réactif. Notre solution cherche principalement à faire la différence entre es liens peu performants depuis une longue période de temps de ceux qui éprouvent des problèmes temporaires de transmission. Plutôt que de chercher systématiquement à se remettre de ruptures de route douteuses, nous cherchons à introduire une certaine résilience quant à la coupure de route. Nous prolongeons nos travaux préliminaires (Ashraf U. 08) pour améliorer la maintenance des routes dans les réseaux maillés sans fil. Des procédures de maintenance route efficaces sont proposées et ensuite analysées par simulation sur NS-2 Il est important de noter que le mécanisme proposé n'est pas conçu comme un remplacement, mais comme un complément aux approches qui visent à découvrir des routes de rechange ou en utilisant d'autres mécanismes tels que la réparation locale de routes

A.3.5 Mécanisme Efficace de Maintenance de Route

Le but principal de la "Efficient Route Maintenance" (ERM) est de décider du moment où il faudrait déclarer un lien comme coupé. Avec cet objectif à l'esprit, ERM établit une distinction entre deux types de liens : les liens de "bonne" qualité qui peuvent néanmoins avoir des problèmes de transmission transitoires et les liens de "mauvaise" qualité qui ont des problèmes de transmission relativement permanents. Il y a deux composants principaux dansERM : L'Estimation de la Qualité du Lien et La décision sur la coupure du lien. ERM propose deux mécanismes complémentaires pour l'évaluation de la qualité du lien : un mécanisme passif (dit mécanisme Listen)fondé sur l'écoute passive du médium et un mécanisme actif (dit mécanisme Hello) qui nécessite l'échange de petits paquets entre les noeuds afin de calculer la qualité d'un lien plus précisément.

A.3.6 1. L'Estimation du Qualité du Lien

A. Mécanisme "Listen"

Le mécanisme "Listen" estime la qualité du lien en "écoutant" le médium en utilisant les informations disponibles localement au niveau du noeud. Cela signifie qu'il n'y a pas de composant actif ou de paquets supplémentaires générés par le mécanisme.

La qualité physique du lien est prise en compte en utilisant le rapport signal sur interférence et bruit (SINR) qui est considéré comme un bon indicateur de la qualité de lien. Comme "Listen" est un mécanisme passif, il ne peut utiliser que l'information disponible localement. Pour un lien (i, j) on note la SINR mesuré au noeud i pour des données reçues de la part du noeud j comme SINR (i). Il s'agit d'une approximation dans laquelle il est supposé que le lien a la même qualité dans les deux directions. Afin d'avoir une idée de la performance à long terme du lien, le noeud i maintient la moyenne du SINR pour toutes les trames reçues pendant une fenêtre de temps glissante . La qualité logique d'un lien est prise en compte en utilisant la métrique que nus avons proposé au chapitre 2 comme moyen de mesurer les interférences logiques.

B. L'Estimation du Qualité du Lien : Le "Hello" Mécanisme

Ce mécanisme " Hello " dispose d'un composant actif par lequel des informations sont échangées entre les noeuds en utilisant des paquets de contrôle. Comparable au mécanisme " Listen " d'évaluation de la qualité du lien, le mécanisme " Hello " effectue des estimations de la qualité physique et logique du lien. Pour estimer la qualité physique de la liaison nous utilisons de nouveau le SINR,à la différence que l'on considère le lien SINR . Le mécanisme Listen suppose que la qualité du lien est la même dans les deux sens ce qui n'est pas nécessairement toujours vrai. Grâce aux informations échgangées entre les noeuds i et j d'unlien (i, j), le SINR(i,j)est fixé au SINR mesuré au noeud j pour les transmission en povenance du noeud i. Considérons l'exemple de la figure 3.7. Pour un lien unidirectionnel (i, j), le récepteur j maintient la SINR des trames reçues du noeud i sur une fenêtre glissante de temps. Périodiquement, le noeud j transmet des petits paquets au noeud i contenant le SINR moyen des trames reçues. Ce mécanisme est plus précis plus précis que le m écanisme " Listen ".Avec le mécanisme " Hello " , la qualité logique d'un lien est égale au maximum des taux moyens d'interférence calculés individuellement au niveau de chaque extrémité du lien.

A.3.7 2. La Décision de la coupure du Lien :

Ce composant entre en action suite à une notification de la liaison de (après 8 tentatives de transmission échouées) . La décision de déclarer le lien comme coupé dépend de la qualité du lien (la qualité physique ou qualité logique dépasse un seuil). Les qualités de liens sont mesurées sur une durée de dix secondes afin de prendre une décision cohérente avec la qualité du lien en général. Pour la qualité physique, la décision est simple parce que nous nous reposons sur des valeurs de seuil pré-définies (par exemple 10 dB pour 11 Mbps). Si la valeur du SINR au long-terme est inférieure à ce seuil, le lien est déclaré comme coupé. Pour la qualité logique qui est représentée par le rapport du temps que le noeud est empêché d'envoyer par rapport au temps total, on fait une étude de sensibilité pour plusieurs seuils (0.6 - 0.9).

A.3.8 L'évaluation de Performance

Nous mettons en oeuvre notre mécanisme de la maintenance de la route dans AODV. La solution est comparée à l'AODV classique, l'AODV avec réparation locale du lien (une coupure du lien est réparée localement par un noeud intermédiaire en diffusant un message " Route-Request " à la place de la source). Les évaluations sont faites pour le cas mono radio mono canal ainsi que deux radio par noeud et deux canaux par noeud. Les résultats montrent une amélioration de performance jusqu'à 100% en termes de débit moyen, de délai, de taux de coupure des routes. L'ERM offre également de bonnes performances dans le cas multi-radio multicanaux.

A.4 Chapitre 4 : Cadre pour la garantie de la Qualité de Service dans les réseaux maillés sans fil

A.4.1 Introduction

Une majorité des solutions existantes pour fournir de la Qualité de Service dans les réseaux maillés sans fil sont proposée pour les réseaux dont les noeuds sont équipés d'une seule interface radio opérant toutes sur un seul canal. En raison de la réduction du coût du matériel, les réseaux multi-radios et multi-canaux sont devenus bon marché et il est donc intéressant de proposer une solution de qualité de service pour les réseaux multi-radios multi-canaux. La motivation principale de cette contribution est le fait qu'il y a peu de solutions qui exploitent la diversité de liens (la disponibilité de plusieurs liens entre voisins, opérant sur des canaux différents). Notre solution exploite explicitement la diversité de liens de deux manières :

1. Parfois un lien unique ne peut supporter la bande passante requise. Notre solution considère tous les liens disponibles entre deux noeuds (ou un saut sans fil) comme une seule liaison logique dont la bande passante est égale à la somme des bandes passantes des différents liens. Ceci contribue à améliorer le taux d'admission de flux avec des exigences sur le débit.

2. Deuxièmement, la solution ne distribue pas aléatoirement la charge du flux arrivant sur tous les liens disponibles entre deux noeuds. La distribution de charge est fonction de l'interférence présente sur le lien. La solution proposée prévoit un mécanisme élégant pour capturer explicitement les interférences (inter-flux) dues aux flux existants dans le réseau ainsi que les interférences (intra-flux) subies par les flux admis dans le réseau.

A.4.2 Le cadre pour la garantie de qualité de service

Il y a quatre phases de notre cadre de QdS :

A.4.2.1 Phase 1 : La découverte de voisinage

Dans la phase de découverte du voisin, les noeuds doivent découvrir leurs voisins sur l'ensemble de leurs interfaces radio disponibles pour créer une table de voisinage.

A.4.2.2 Phase 2 : La découverte de route avec garantie de débit

Un noeud qui souhaite trouver une route avec une garantie de débit déclenche une phase de découverte de route où un paquet " Route Request " est diffusé sur le réseau. Un noeud recevant le "Route Request "exécute les procédures suivantes :

A. Estimation de la bande passante - Dans cette phase, d'une part, le noeud estime la bande passante disponible au niveau de chacun de ses liens en utilisant le concept de graphe de conflit construit en prenant en compte les interférences provenant des flux existants ainsi que les interférences intra-flux causées par ce nouveau flux s'il venait à être admis . Des graphes de conflit sont déduits la bande passante disponible au niveau de chaque lien et par la même le bande passante totale disponible au niveau de chaque saut.

B. Décision d'admission- Dans cette phase, le noeud vérifie s'il est capable d'offrir la bande passante requise par le nouveau flux. Si oui, alors la bande passante requise peut être supportée par ce noeud. Sinon,il est tout simplement abandonné.

C. Partage de Charge - est également effectuée dans la solution proposée Dans cette phase, la charge est distribuée sur les différents liens d'un saut sans fil. La répartition de trafic pour le flux entrant est faite en proportions inverses aux interférences présentes sur chacun des liens.

D. Réservation de ressources - Dans cette phase, la réservation des ressources est finalisée lorsque les noeuds recoivent le message de " Route Response " en provenance de la destination.

A.4.2.3 Phase 3 : La détection du non-respect de la QdS et de récupération

Une fois le contrôle d'admission et les phases de réservation de ressources sont finis, la source peut commencer à envoyer du trafic vers la destination. Mais, afin de se protéger contre une violation éventuelle de la QdS, toute violation de la garantie de bande passante est détectée et rapportée à la source. La recouvrement implique généralement une autre phase dedécouverte de route.

A.5 Conclusion

L'objectif de cette thèse est de contribuer à l'amélioration de la QoS et du routage dans les réseaux maillés sans fil. Nous y proposons une métrique de routage permettant de sélectionner des chemins performants aussi bien entre les routeurs internes du réseau maillé sans fil qu'entre ces mêmes routeurs et les passerelles vers l'Intrenet. Nous proposons également une amélioration du mécanisme de maintenance de routes des protocoles de routage réactifs. Notre proposition améliore la stabilité des routes et par cconséquent les performanes du réseau. Enfin, nous proposons un cadre conceptuel permettant d'offrir des garanties de Qualité de service dans des réseaux mmulti-intefaces multi-canaux. Ce cadre exploite la diversité des liens afin d'améliorer l'admissibilité des flux.

References

[802 02] *IEEE WG, Draft "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications : Medium Access Control (MAC) Enhancements for Quality of Service (QoS)", 802.1 le Draft 3.1*. May 2002. (Cité page 16.)

[802 04] *IEEE standard for Local and Metropolitan Area Networks - Part 16 : Air Interface for Fixed Broadband Wireless Access Systems*. 2004. (Cité page 11.)

[802 08] *IEEE unapproved draft IEEE P802.11s/D1.09, "Draft Standard for Information Technology - Telecommunications and Information Exchange between Systems - LAN/MAN Specific Requirements - Part 11 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications : Amendment : Mesh Networking*. 2008. (Cité pages 24 et 73.)

[A. A. Pirzada 06] M. Portmann A. A. Pirzada & J. Indulska. *Evaluation of MultiRadio Extensions to AODV for Wireless Mesh Networks*. in Proceedings of the ACM MobiWac, 2006. (Cité pages 25, 73 et 88.)

[A. P. Subramanian 06] M. M. Buddhikot A. P. Subramanian & S. C. Miller. *Interference Aware Routing in Multi-Radio Wireless Mesh Networks*. IEEE Wksp. Wireless Mesh Networks, 2006. (Cité pages 9 et 21.)

[AA Pirzada 07a] M Portmann AA Pirzada R Wishart. *Multi-Linked AODV Routing Protocol for Wireless Mesh Networks*. Globecom, 2007. (Cité page 21.)

[AA Pirzada 07b] M Portmann AA Pirzada R Wishart. *Multi-Linked AODV Routing Protocol for Wireless Mesh Networks*. Globecom, 2007. (Cité page 88.)

[Alicherry 05] Bhatia R. Alicherry M. & L. Li. *Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks*. ACM Mobicom, 2005. (Cité pages 9, 109 et 113.)

[Ashraf 07] Usman Ashraf, Guy Juanole & Slim Abdellatif. *Evaluating Routing Protocols for the Wireless Mesh Backbone*. Wireless and Mobile Computing, Networking and Communication, IEEE International Conference on, 2007. (Cité page 3.)

[Ashraf 08a] Usman Ashraf, Guy Juanole & Slim Abdellatif. *An Interference and Link-Quality Aware Routing Metric for Wireless Mesh Networks*. Proceedings of the 68th IEEE Vehicular Technology Conference, VTC Fall 2008, 2008. (Cité pages 3 et 62.)

[Ashraf 08b] Usman Ashraf, Abdellatif Slim & Guy Juanole. *Efficient Route Maitenance in Wireless Mesh Networks*. Wireless Pervasive Computing, 2008. ISWPC 2008. 3rd International Symposium on, 2008. (Cité page 3.)

[Ashraf 08c] Usman Ashraf, Abdellatif Slim & Guy Juanole. *Route Stability in Wireless Mesh Access Networks*. Embedded and Ubiquitous Computing, IEEE/IFIP International Conference on, 2008. (Cité page 3.)

[Ashraf 09] Usman Ashraf, Abdellatif Slim & Guy Juanole. *Gateway Selection in Backbone Wireless Mesh Networks*. Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE conference on, 2009. (Cité page 3.)

[B. Sadeghi 02] A. Sabharwal B. Sadeghi V. Kanodia & E. Knightly. *Opportunistic media access for multirate ad hoc networks*. ACM MobiCom, 2002. (Cité page 85.)

[B. Wang 08a] M. Mutka B. Wang. *QoS-aware fair rate allocation in wireless mesh networks*. Elsevier Journal on Computer Communications, Volume 31, Issue 9C, 2008. (Cité pages 20, 105 et 109.)

[B. Wang 08b] M. Mutka B. Wang. *QoS-aware fair rate allocation in wireless mesh networks*. Elsevier Journal on Computer Communications, Volume 31, Issue 9, 2008. (Cité page 108.)

[Borges 09] Vinicius C.M. Borges, Daniel Pereira, Marilia Curado & Edmundo Monteiro. *Routing Metric for Interference and Channel Diversity in Multi-Radio Wireless Mesh Networks*. Proceedings of the 8th International Conference

on Ad-Hoc, Mobile and Wireless Networks, 2009. (Cité pages 43, 44, 45 et 47.)

[Brar 06] Gurashish Brar, Douglas Blough & Paolo Santi. *Computationally Efficient Scheduling with the Physical Interference Model for Throughput Improvement in Wireless Mesh Networks*. ACM Mobicom, 2006. (Cité page 109.)

[C-F Huang 04] H-W Lee C-F Huang & Y-C Tseng. *A Two-Tier Heterogeneous Mobile Ad Hoc Network Architecture and Its Load-Balancing Routing Problem*. ACM/Kluwer Journal of Mobile Networks and Applications, vol.9, no.4, pp.379-391, 2004. (Cité page 65.)

[C. Perkins 03] E. M. Royer C. Perkins & S. Das. *Ad hoc On-Demand Distance Vector (AODV) Routing*. IETF RFC 3561, 2003. (Cité pages 21, 24 et 83.)

[Chen 05] L. Chen & W. Heinzelman. *QoS-aware Routing Based on Bandwidth Estimation in Mobile Ad Hoc Networks*. IEEE Journal on Selected Areas in Communications, 2005. (Cité pages 18, 48 et 106.)

[Chu 08] X Chu. *Provisioning of Parametrized Quality of Service in 802.11e Based Wireless Mesh Networks*. Mobile Networks and Applications, Vol 13, April 2008. (Cité page 17.)

[C.M. Chung 01] Y.H. Wang C.M. Chung & C.C. Chuang. *Ad hoc on-demand backup node setup routing protocol*. IEEE International Conference on Information Networking, 2001. (Cité pages 73 et 79.)

[Couto 02] Douglas S. J. De Couto, Daniel Aguayo, Benjamin A. Chambers & Robert Morris. *Performance of Multihop Wireless Networks : Shortest Path is Not Enough*. Proceedings of the First Workshop on Hot Topics in Networks, October 2002. (Cité pages 31 et 65.)

[D. Aguayo 04] S. Biswas-G. Judd D. Aguayo J. Bicket & R. Morris. *Linklevel measurements from an 802.11b mesh network*. SIGCOMM Comput. Commun. Rev. 34 (2004) (4), pp. 121_132., 2004. (Cité pages 26 et 47.)

[D. Aguayo 05] J. Bicket D. Aguayo & R. Morris. *SrcRR A high throughput routing protocol for 802.11 mesh networks*. MIT, Tech. Rep., 2005. (Cité pages 21, 25, 26, 33, 49 et 73.)

[D. B. Johnson 03] D. A. Maltz D. B. Johnson & Y. Hu. *The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)*. IETF MANET, Internet Draft, 2003. (Cité pages 21 et 23.)

[D. Nandiraju 06] N. Nandiraju-D.P. Agrawal D. Nandiraju L. Santhanam. *Achieving Load Balancing in Wireless Mesh Networks Through Multiple Gateways*. International Workshop on Wireless Mesh-Networks and Applications, 2006. (Cité page 65.)

[De Couto 03] Douglas S. J. De Couto, Daniel Aguayo, John Bicket & Robert Morris. *A High-Throughput Path Metric for Multi-Hop Wireless Routing*. Proceedings of the 9th ACM International Conference on Mobile Computing and Networking, MobiCom, September 2003. (Cité pages 26, 36, 38, 48, 58, 59 et 84.)

[Devu Manikantan Shila 08] Tricha Anjali Devu Manikantan Shila. *Load-aware Traffic Engineering for Wireless Mesh Networks*. Elsevier Computer Communication journal, special issue in wireless mesh networks, vol. 31, no. 7, pp. 1460-1469, 2008. (Cité pages 34 et 47.)

[Fiore] Marco Fiore. http ://www.telematica.polito.it/fiore/. (Cité page 51.)

[F.P. Setiawan 08] I. Sasase F.P. Setiawan S.H. Bouk. *An Optimum Multiple Metrics Gateway Selection Mechanism in MANET and Infrastructured Networks Integration*. IEEE WCNC, 2008. (Cité page 65.)

[Fre 09] *Freifunk [Online]*. Available : http ://start.freifunk.net/, 2009. (Cité page 13.)

[G. Holland 01] N. Vaidya G. Holland & P.Bahl. *A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks*. MobiCom, 2001. (Cité page 85.)

[G.-S. Ahn 02] A. Veres G.-S. Ahn A. Campbell & L.-H. Sun. *SWAN : Service Differentiation in Stateless Wireless Ad Hoc Networks*. Proceedings Infocom, 2002. (Cité page 18.)

[Garey 79] M. R. Garey & D. S. Johnson. *Computers and Intractability : A Guide to the Theory of NP-Completeness*. 1979. (Cité page 112.)

[Genetzakis 08] M. Genetzakis & V. A. Siris. *A contention-aware routing metric for multi-rate multi-radio mesh networks*. IEEE SECON, 2008. (Cité page 34.)

[Gupta 00] P. Gupta & P. Kumar. *Capacity of Wireless Networks*. In IEEE Transactions on Information Theory, volume 46, pages 388-404, 2000. (Cité pages 9 et 109.)

[Gupta 04] R. Gupta & J. Walrand. *Approximating Maximal Cliques in Ad-Hoc Networks*. PIMRC, 2004. (Cité page 112.)

[Haas 98] Z.J. Haas & M.R. Pearlman. *The zone routing protocol (ZRP) for ad hoc networks (Internet-draft)*. Network (MANET) Working Group, IETF, 1998. (Cité pages 21, 79 et 80.)

[Iannone 05a] L. Iannone & S. Fdida. *Meshdv A distance vector mobility-tolerant routing protocol for wireless mesh networks*. IEEE ICPS Workshop on Multi-hop Ad hoc Networks from theory to reality (REALMAN), 2005. (Cité page 21.)

[Iannone 05b] L. Iannone & S. Fdida. *Meshdv : A distance vector mobility-tolerant routing protocol for wireless mesh networks*. IEEE ICPS, Workshop REALMAN, 2005. (Cité page 24.)

[Iannone 05c] L. Iannone & S. Fdida. *MRS : A Simple Cross-Layer Heuristic to Improve Throughput Capacity in Wireless Mesh Networks*. CoNEXT, 2005. (Cité page 25.)

[Iannone 05d] L. Iannone & S. Fdida. *MRS : A simple cross-layer heuristic to improve throughput capacity in wireless mesh networks*. CoNext, 2005. (Cité page 27.)

[IEE 99] *IEEE Std. 802.11-1999, Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 1999. (Cité pages 1 et 73.)

[Int 00] *HFA3861B ; Direct Sequence Spread Spectrum Baseband Processor, Intersil*. Jan. 2000. (Cité page 51.)

[Int 04] *Understanding Wi-Fi and WiMax as Metro-Access Solutions*. Intel White Paper, 2004. (Cité page 10.)

[J. Jun 03] M.L. Sichitiu J. Jun. *The nominal capacity of wireless mesh networks*. IEEE Wireless Communications, 2003. (Cité page 64.)

[J. P. Sheu 04] S.K. Wu J. P. Sheu C.H. Liu & Y.C. Tseng. *A priority MAC protocol to supprt real time traffic in ad hoc networks*. Wireless Networks, vol 10, no. 1, pp. 61,69, 2004. (Cité page 16.)

[J. Shin 05] J. Na A. Park J. Shin H. Lee & S. Kim. *Load balancing among internet gateways in ad hoc networks*. IEEE 62nd Vehicular Technology Conference, VTC, 2005. (Cité page 65.)

[J. Tang 05] W. Zhang J. Tang G. Xue. *Interference-Aware Topology Control and QoS Routing in Multi-Channel Wireless Mesh Networks*. ACM Mobihoc, 2005. (Cité pages 112 et 116.)

[Jitu Padhye 05] Venkat Padmanabhan Lili Qiu-Ananth Rao Jitu Padhye Sharad Agarwal & Brian Zill. *Estimation of Link Interference in Static Multi-hop Wireless Networks*. Internet Measurements Conference, October, 2005. (Cité page 47.)

[Josh Broch 99] David A. Maltz Josh Broch & David B. Johnson. *Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks*. ISPAN, 1999. (Cité page 66.)

[K. Chen 02] S. H. Shah K. Chen & K. Nahrstedt. *Cross layer deisgn for data accessibility in mobile ad hoc networks*. Journal of Wireless Communications, 2002. (Cité page 19.)

[K. Jain 03] V. Padmanabhan L. Qiu K. Jain J. Padhye. *Impact of interference on multi-hop wireless network performance*. MOBICOM, 2003. (Cité pages 47, 107 et 111.)

[K. N. Ramachandran 06] Kevin C. Almeroth K. N. Ramachandran Elizabeth M. Belding-Royer & Milind M. Buddhikot. *Interference-aware channel assignment in multi-radio wireless mesh networks*. IEEE Infocom, 2006. (Cité pages 9, 47, 112 et 113.)

[K. Ramachandran 05a] G. Chandranmenon-S. Miller E. Belding-Royer K. Ramachandran M. Buddhikot & K. Almeroth. *On the Design and Implementation of Infrastructure Mesh Networks*. IEEE WiMesh2005, 2005. (Cité pages 21, 25 et 73.)

[K. Ramachandran 05b] G. Chandranmenon-S. Miller E. Belding-Royer K. Ramachandran M. Buddhikot & K. Almeroth. *On the Design and Implementation of Infrastructure Mesh Networks*. IEEE WiMesh2005, 2005. (Cité page 27.)

[K. Ramachandran 07a] E. Belding-K. Almeroth K. Ramachandran I. Sheriff. *Routing stability in static wireless mesh networks*. Passive and Active Measurement Conference, 2007. (Cité pages 33 et 49.)

[K. Ramachandran 07b] E. Belding-K. Almeroth K. Ramachandran I. Sheriff. *Routing stability in static wireless mesh networks*. Passive and Active Measurement Conference, 2007. (Cité page 80.)

[K. Yonggyu 07] S. Myunghwan K. Yonggyu J. Yeonkwon & M. Joongsoo. *Loadbalanced Mesh Portal Selection in Wireless Mesh Network*. IEEE Military Communications Conference, 2007. (Cité page 65.)

[Karol Kowalik 07] Brian Keegan Karol Kowalik & Mark Davis. *RARE - Resource Aware Routing for mEsh*. ICC, 2007. (Cité pages 21 et 47.)

[Kim 06] K.-H. Kim & K. Shin. *On Accurate Measurement of Link Quality in Multi-hop Wireless Mesh Networks*. In Proc. of the ACM MobiCom Conf., 2006. (Cité page 48.)

[L. Bononi] et al. L. Bononi. *A differentiated distributed coordination function MAC protocol for cluster-based wireless ad hoc networks*. Proceedings of the 1st ACM international workshop on performance evaluation of wireless ad hoc, sensor, and ubiquitous networks. (Cité page 16.)

[L. Luo 08] H. Liu-M. Wu L. Luo D. Raychaudhri & D. Li. *Improving End-to-End Performance of Wireless Mesh Networks through Smart Association*. IEEE Wireless Communications and Networking Conference, 2008. (Cité page 65.)

[Lee 00] S.-J. Lee & M. Gerla. *AODV-BR : Backup Routing in Ad hoc Networks*. IEEE WCNC 2000, 2000. (Cité pages 73 et 79.)

[Leung 01] Liu J. Poon E.-Chan A.-L.C. Li-B. Leung R. *MP-DSR : A QoS-aware Multipath Dynamic Source Routing Protocol for Wireless Ad-hoc Networks*. 26th IEEE Annual Conference on Local Computer Networks, 2001. (Cité page 18.)

[Lin 97] C.R. Lin & M. Gerla. *Asynchronous multimedia multihop wireless networks*. IEEE INFOCOM, 1997. (Cité page 17.)

[Lin 08] Yuxia Lin & Vincent W.S. Wong. *An Admission Control Algorithm for Multi-hop 802.11e-based WLANs*. Elsevier Computer Communications Journal, vol. 31, no. 14, pp. 3510-3520, September 2008. (Cité page 17.)

[M. R. Pearlman 00] Z. J. Haas M. R. Pearlman & S. I. Mir. *Using Routing Zones to Support Route Maintenance in Ad Hoc Networks*. Proc. IEEE Wireless Commuications. Network Conference, 2000. (Cité pages 79 et 80.)

[M.A. Ergin 08a] L. Liu-D. Raychaudhri M.A. Ergin M Gruteser & H. Liu. *Available bandwidth estimation and admission control for QoS routing in wireless mesh networks*. Elsevier Journal on Computer Communications, Volume 31, Issue 9, 2008. (Cité pages 17, 105 et 108.)

[M.A. Ergin 08b] L. Liu-D. Raychaudhri M.A. Ergin M Gruteser & H. Liu. *Available bandwidth estimation and admission control for QoS routing in wireless mesh networks*. Elsevier Journal on Computer Communications Volume 31, Issue 9, 2008. (Cité page 20.)

[Misra 00] Sudip Misra, Subhas Chandra Misra & Isaac Woungang. *Guide to Wireless Mesh Networks*. pp 121-122, 2000. (Cité page 34.)

[OLS 03] *Optimized Link State Routing Protocol (OLSR)*. Rfc3636, 2003. (Cité pages 21 et 22.)

[P. Kyasanur 05] N. H. Vaidya P. Kyasanur. *Routing and Link-layer Protocols for Multi-Channel Multi-Interface Ad Hoc Wireless Networks*. Technical Report, University of Illinois at Urbana-Champaign, 2005. (Cité page 41.)

[P. Sinha 99] R. Sivakumar P. Sinha & V. Bharghavan. *CEDAR : A core-extraction distributed ad hoc routing algorithm*. IEEE INFOCOM, 1999. (Cité page 18.)

[P. Subramanian 06] M. M. Buddhikot P. Subramanian & S. Miller. *Interference aware routing in multi-radio wireless mesh networks*. In IEEE Workshop on Wireless Mesh Networks (WiMesh), 2006. (Cité pages 42 et 47.)

[Park 97] Vincent D. Park & M. Scott Corson. *A highly adaptive distributed routing algorithm for mobile wireless networks*. INFOCOM, 1997. (Cité page 21.)

[Paul 08] S. Paul A.B. Nandi. *Modified Optimized Link State Routing (M-OLSR) for Wireless Mesh Networks*. International Conference on Information Technology ICIT, 2008. (Cité page 21.)

[P.C. Ng 04] S.C. Liew P.C. Ng. *Re-routing Instability in IEEE 802.11 Multi-hop Ad-hoc Networks*. IEEE WLNW, 2004. (Cité pages 73, 79 et 80.)

[Perkins CE 94] Bhagwat P Perkins CE. *AHighly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers*. Proceedings of the Conference on Communications Architectures, Protocols and Applications, 1994. (Cité pages 21 et 22.)

[P.J.B. King 07] A. Etorban P.J.B. King & I.S. Ibrahim. *A DSDV based multipath routing protocol for mobile ad-hoc networks*. 8th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, pages 93 to 98, 2007. (Cité page 21.)

[Q. Xue 02] Q. Ganz Q. Xue. *Qos routing in mesh-based wireless networks*. Int. Journal of Wireless Information Networks V.9, 2002. (Cité page 8.)

[Qin 02] L. Qin & T. Kunz. *Pro-active route maintenance in dsr*. In ACMSIGMOBILE Mobile Computing and Communications Review, pages 79-89, 2002. (Cité pages 79 et 80.)

[R. Chandra 04] V. Bahl R. Chandra & P. Bahl. *MultiNet : Connecting to multiple IEEE 802.11 networks using a single wireless card*. IEEE Infocom, 2004. (Cité page 9.)

[R. Draves 04a] J. Padhye R. Draves & B. Zill. *The architecture of the Link Quality Source Routing Protocol*. eport MSR-TR-2004-57, Microsoft Research, 2004. (Cité pages 21 et 27.)

[R. Draves 04b] J. Padhye R. Draves & B. Zill. *Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks*. proceedings of the 10th Annual International Conference on Mobile Computing and Networking, 2004. (Cité pages 9, 27, 39 et 65.)

[R. Draves 04c] J. Padhye R. Draves & B. Zill. *Routing in multi-radio, multi-hop wireless mesh networks*. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), 2004. (Cité page 27.)

[R. Gupta 05] J. Musacchio R. Gupta & J. Walrand. *Sufficient Rate Constraints for QoS Flows in Ad-Hoc Networks*. INFOCOM, 2005. (Cité page 111.)

[R. Kumar 07] M. Misra R. Kumar & A. K. Sarje. *An Efficient Gateway Discovery in Ad Hoc Networks for Internet Connectivity*. Int. Conf. on Computational Intelligence and Multimedia Applications, V4, pg : 275-282, 2007. (Cité page 65.)

[Ratish J.Punnoose 00] Pavel V.Nikitin Ratish J.Punnoose & Daniel D.Stancil. *Efficient Simulation of Ricean Fading within a Packet Simulator*. Vehicular Technology Conference, 2000. (Cité pages 51 et 90.)

[Royer 99] E. Royer & C. E. Perkins. *Multicast operation of the ad-hoc on-demand distance vector routing protocol*. Proc. of the 5th ACM IEEE Annual Conf. on Mobile Computing and Networking, 1999. (Cité page 21.)

[S. Das 07] S Banerjee S. Das K. Papagiannaki & Y.C. Tay. *SWARM : selforganization of community wireless mesh networks*. ACM CoNEXT, 2007. (Cité page 65.)

[S. Lee 06a] M. Pal-G. Wilfong S. Lee G. Narlikar & L. Zhang. *Admission Control for Multihop Wireless Backhaul Networks with QoS Support*. WCNC, 2006. (Cité page 20.)

[S. Lee 06b] M. Pal-G. Wilfong S. Lee G. Narlikar & L. Zhang. *Admission Control for Multihop Wireless Backhaul Networks with QoS Support*. WCNC, 2006. (Cité page 108.)

[S. Shenker 94] R. Braden S. Shenker & D. Clark. *Integrated services in the Internet architecture : an overview*. Internet RFC 1633, 1994. (Cité page 17.)

[S. Tajima 06] T. Higashino S. Tajima & N. Funabiki. *An Internet gateway access point selection problem for wireless infrastructure mesh networks*. FMUIT, 2006. (Cité page 65.)

[S. Waharte 06] R. Boutab S. Waharte. *Routing protocols in wireless mesh networks : challenges and design considerations*. Multimedia tools and Applications V.29, Issue 3, 2006. (Cité page 8.)

[S.B. Lee 99] X. Zhang S.B. Lee. *INSIGNIA, Internet Draft, draft-ietf-manet-insignia-01.txt*. October 1999. (Cité page 19.)

[S.L. Wu 01] Y.-C. Tseng S.L. Wu S.-Y. Ni & J.-P. Sheu. *Route Maintenance in a Wireless Mobile Ad Hoc Network*. Journal of Telecommunication Systems, Volume 18, Numbers 1-3, 2001. (Cité pages 79 et 80.)

[So 04] J. So & N. H. Vaidya. *A routing protocol for utilizing multiple channels in multi-hop wireless networks with a single transceiver*. Technical report, University of Illinois at Urbana-Champaign, 2004. (Cité page 21.)

[Sobrinho 01] J. L. Sobrinho. *Algebra and algorithms for QoS path computation and hop-by-hop routing in the Inernet*. in IEEE INFOCOM, 2001. (Cité page 36.)

[Song Guo 05] Oliver Yang Song Guo & Yantai Shu. *Improving Source Routing Reliability in Mobile Ad Hoc Networks*. IEEE TRANSACTIONS VOL. 16, NO. 4, 2005. (Cité page 21.)

[Tanenbaum 03] A. S. Tanenbaum. *Computer Networks*. 4th ed. Upper Saddle River, NJ, United States : Pearson Education International, 2003. (Cité page 15.)

[Tobagi 75] F. A. Tobagi & L. Kleinrock. *Packet switching in radio channels : Part II - the hidden terminal problem in carrier sense multiple-access modes and the busy-tone solution*. IEEE Transactions on Wireless Communications, vol.COM 23, no. 12, pp. 1417-1433, 1975. (Cité page 15.)

[U. Ashraf 08] S. Abdellatif U. Ashraf & G. Juanole. *Efficient Route Maintenance in Wireless Mesh Networks*. in 3rd International Symposium on Wireless Pervasive Computing (IEEE ISWPC 2008) Santorini, Greece, 2008. (Cité page 82.)

[V. Kone 08] Ben Y. Zhao V. Kone Sudipto Das & Haitao Zheng. *QUORUM - Quality of service in wireless mesh Networks*. ACM Mobile Networking and Applications, 2008. (Cité pages 20, 105, 107 et 109.)

[W.H. Liao 01] S.L.Wang W.H. Liao Y.C. Tseng & J.P. Sheu. *A Multi-Path QoS Routing Protocol in a Wireless Mobile Ad Hoc Network*. IEEE Internatoinal Conference on Networking ICN, 2001. (Cité page 18.)

[X. Cheng 08] P. Sung-Ju Lee Banerjee-S. X. Cheng Mohapatra. *MARIA : Interference-Aware Admission Control and QoS Routing in Wireless Mesh Networks*. IEEE ICC, 2008. (Cité pages 17, 20, 105, 106, 107, 109, 112, 115, 116 et 118.)

[Xue Q 02] Ganz A Xue Q. *QoS routing in mesh-based wireless networks*. International Journal of Wireless Information Networks 9 v3 :179-190, 2002. (Cité pages 17, 18, 19, 105, 106, 107 et 109.)

[Xue Q 03] Ganz A Xue Q. *Ad hoc QoS on-demand routing AQOR in mobile ad hoc networks*. Journal of Parallel and Distributed Computing, 2003. (Cité pages 18, 19 et 107.)

[Y. Yang 05a] J. Wang Y. Yang & R. Kravets. *Designing Routing Metrics for Mesh Networks*. WiMesh, 2005. (Cité pages 32, 36 et 41.)

[Y. Yang 05b] J. Wang Y. Yang & R. Kravets. *Interference-aware Load Balancing for Multihop Wireless Networks*. echnical Rep. UIUCDCS-R-2005-2526, Department of Computer Science, University of Illinois at Urbana Champaign, 2005. (Cité page 40.)

[Yang 03] Y. Yang & R. Kravets. *Contention-aware admission control for ad hoc networks*. Univ. Illinois at Urbana-Champaign, Urbana-Champaign, IL, Tech. Rep. 2003-2337, 2003. (Cité pages 18 et 48.)

[Yi Hu 07] Hai-Ming Chen-Xiao-Hua Jia Yi Hu Xiang-Yang Li. *Distributed Call Admission Protocol for Multi Channel Multi-Radio Wireless Networks*. Globecom, 2007. (Cité pages 20 et 108.)

[Yu 07] Wu-T.-K. Cheng-R.H. Yu C.W. *A low overhead dynamic route repairing mechanism for mobile ad hoc networks*. Computer Communications 30, 1152-1163, 2007. (Cité pages 73, 79 et 80.)