DESIGN AND IMPLEMENTATION OF HIGH QUALITY H.264 VIDEO STREAMING OVER WIRELESS MESH NETWORKS

by

FIRAT BİRLİK

Submitted to the Graduate School of Engineering and Natural Sciences

in partial fulfillment of

the requirements for the degree of

Master of Science

Sabancı University

Fall 2008

DESIGN AND IMPLEMENTATION OF HIGH QUALITY H.264 VIDEO STREAMING OVER WIRELESS MESH NETWORKS

APPROVED BY:

Asst. Prof. Dr. Özgür Gürbüz (Thesis Supervisor)	…….
Asst. Prof. Dr. Özgür Erçetin (Thesis Supervisor)	…….
Assoc. Prof. Dr. Albert Levi	…….
Prof. Dr. Bülent Sankur	…….
Assoc. Prof. Dr. Erkay Savaş	…….

DATE OF APPROVAL: …….

To my family

&

To my fiancée Müge

ACKNOWLEDGEMENTS

I would like to express my gratitude to my thesis advisors Özgür Gürbüz and Özgür Erçetin for their invaluable guidance and encouragement throughout this thesis. I also would like to thank Albert Levi, Bülent Sankur and Erkay Savaş for reading and commenting on this thesis.

I am grateful to AirTies Wireless Networks for funding my thesis research and I want to thank Metin İsmail Taşkın for his priceless support in course of my research.

I am indebted to my family for their support, encouragement and love during my studies. Last but not the least; I am grateful to my sweetest, Müge, for keeping my spirit up all the times with her love and friendship.

ABSTRACT

DESIGN AND IMPLEMENTATION OF HIGH QUALITY H.264 VIDEO STREAMING OVER WIRELESS MESH NETWORKS

Fırat Birlik

Master of Science, 2008

Asst. Prof. Dr. Özgür Gürbüz

Asst. Prof. Dr. Özgür Erçetin

Keywords: wireless mesh networks, h.264, wireless video streaming

Wireless multimedia home servers are the next generation of home entertainment systems. From a single broadband connection entering a residence, the multimedia stream is transmitted to television headsets and other peripherals by using only wireless links. The provision of high quality time-critical multimedia services in indoor environment is very challenging due to high attenuation and multi-path fading caused by the walls and contention in the shared channel.

In this thesis, we demonstrate that the newly proposed wireless standard on wireless mesh networks can help improve the coverage while supporting Quality of Service requirements of both multimedia and data users, when the video packets are given EDCA priorities based on their importance according to the new high definition video streaming standard H.264.

We support our hypothesis by presenting test results gathered from both simulations and from a real implementation test bed, where we observe very low delay and very few packet losses in video stream and almost no loss in perceived video quality even in the presence of high contending neighboring data traffic.

ÖZET

KABLOSUZ ÖRGÜ AĞLARINDA DURAKSIZ YÜKSEK KALİTE H.264 GÖRÜNTÜ İLETİMİ TASARIMI VE UYGULAMASI

Fırat Birlik

Yüksek Lisans, 2008

Yrd. Doç. Dr. Özgür Gürbüz

Yrd. Doç. Dr. Özgür Erçetin

Anahtar Sözcükler: kablosuz örgü ağları, h.264, kablosuz duraksız görüntü iletimi

Kablosuz çoklu ortam ev sunucuları gelecek neslin ev eğlence sistemleridir. Tek bir geniş bant internet bağlantısından eve ulaşan veri ve görüntü bilgileri, kablosuz cihazlar aracılığıyla televizyon alıcıları ve diğer görüntü işleme cihazlarına kablosuz olarak aktarılır.

Yüksek kaliteli ve zaman kısıtlı çoklu ortam servislerinin iç mekânlarda kablosuz iletimi, beton duvarlardan ve ortak kanallardaki mücadeleden kaynaklanan yüksek orandaki sinyal zayıflaması ve çoklu sinyal saçılması sebebiyle oldukça zorlayıcıdır.

H.264 görüntü standardı göz önüne alınarak, farklı EDCA öncelikleriyle iletilen kesintisiz görüntü akışı paketleri ve yeni önerilen kablosuz örgü ağ standardı ile kısıtlı kapsama alanı sorununu, hem görüntü iletiminin hem de veri kullanıcılarının servis kalitesi gereksinimlerini karşılayarak çözüyoruz.

Sunduğumuz yöntem ile çok yüksek çevresel trafik varlığında dahi düşük gecikme ve çok düşük paket kaybı oranları elde edebiliyor ve algılanan görüntü kalitesinin üst düzeyde korunmasını sağlıyoruz. Önerdiğimiz tekniğin performansını, hem çok sayıdaki benzetimlerden hem de gerçek uygulamalı test platformundan elde edilen sonuçlarla gösteriyoruz.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS

ACK	Acknowledgement
AIFS	Arbitration Inter-Frame Space
AODV	Ad-hoc On demand Distance Vector
AP	Access Point
ARP	Address Resolution Protocol
BE	Best Effort
CDF	Cumulative Distribution Function
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CODEC	Coder Decoder
CW	Contention Window
CZD	Czenakowski Distance
DCF	Distributed Coordination Function
DIFS	DCF Inter-Frame Space
EDCA	Enhanced Distributed Channel Access
IDR	Instantaneous Decoding Refresh
IEEE	Institute of Electronics and Electrical Engineering
IP	Internet Protocol
IPTV	Internet Protocol Television
LAN	Local Area Network

MAC	Medium Access Control
MCD	Mesh Control Daemon
MCL	Mesh Control Layer
MP	Mesh Point
NAL	Network Abstraction Layer
NIC	Network Interface Card
PHY	Physical Layer
PSNR	Peak Signal to Noise Ratio
QoS	Quality of Service
RREP	Route Reply
RREQ	Route Request
TCP	Transmission Control Protocol
TV	Television
VCL	Video Coding Layer
VI	Video
VLAN	Virtual Local Area Network
VO	Voice
WMN	Wireless Mesh Network

1 Introduction

High quality television broadcasts are being deployed to residences using satellite, cable television (TV) or Internet Protocol Television (IPTV) services. Among these services, IPTV is relatively new and emerging alternative that makes use of existing high capacity networks for broadband internet access. In IPTV service, operators install a network switch at the customer's broadband connection and layout Ethernet cables from the switch to television head sets. Wireless Access Points (APs) seem to be a convenient drop-in replacement for the switch and all the cabling, but regular Institute of Electronics and Electrical Engineering (IEEE) 802.11 APs do not meet transmission quality requirements of a multimedia service. Wireless video transmission via 802.11 APs is fragile against background data traffic such as internet access, and may not cover a house completely at the same transmission rate. The coverage may be extended using repeaters, but this requires additional planning by the customer or the operator. Also, multi-hop 802.11-based wireless networks usually implement Distributed Coordination Function (DCF), where each wireless node competes for the channel access. An end-to-end route may contain many relay nodes for a packet to traverse, and this competition creates increase in end-to-end delay and packet loss probability to which video streaming is very sensitive. These major problems precluded 802.11 equipment replacing indoor cabling until now.

Our proposed approach is to improve the high quality home multimedia experience using wireless mesh technology and adapting the packet prioritization strategies similar to those proposed in [1] in order to be able to stream DVD or better quality media to any position in the house. In this work, we overcome both coverage and contention problems by combining Wireless Mesh Networks (WMNs) with a smart Enhanced Distributed Channel Access (EDCA) based prioritization algorithm.

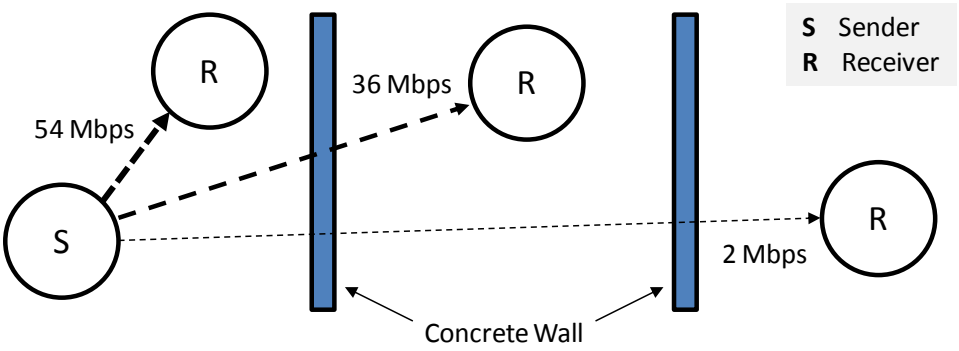

Figure 1.1 Concrete walls cause high attenuation on wireless signal

Often, APs are not in the line-of-sight with each other, but there are walls in between attenuating the signal strength like in Figure 1.1. A very high capacity wireless link can drop to very low values if there are several concrete walls in between. In such cases, WMNs help with their self-organization capability to establish and maintain high quality links between APs, and provide alternate better routes without user intervention. Although WMNs help improve coverage of the network, they also increase contention in the network. It is well known that video streaming is sensitive to packet loss and delay jitter, both of which are unavoidable by regular 802.11 equipment. EDCA is a medium access method proposed in [2], introducing different priority traffic classes with different contention window sizes, and Arbitration Inter-Frame Space (AIFS) values. The probability of channel access of a packet can be controlled based on its priority class. In order to provide better service to video traffic, video packets can be assigned to higher EDCA classes. Thus, over a multi-hop path, video traffic competes only with other traffic with the same or higher priority at every relay node reducing the delay and loss probability of those packets.

As demonstrated later in the thesis, using EDCA over WMN is not sufficient to solve contention problem in the network. In particular, there can be several video streams competing for the channel. For this reason, we use certain characteristics of H.264 video encoding/decoding (codec) standard. H.264 is a very recent codec designed to support higher quality video by decreased bandwidth requirements [3]. It is being recently employed by high definition movie players [4], and HDTV broadcasts. IPTV operators also plan to use H.264 codec widely due to its lower resource requirement compared to currently employed standards. H.264 packetizes the video

stream into several frame types. Some of the frame types are more important than other in constructing the image. In our implementation, more important video packets are mapped to higher priority EDCA classes than those video packets with less important content. By such a mapping, the delay and loss probability of important packets would be better than those for less important video packets. This prioritization scheme helps improve the contention in the network, and provide higher throughput to the background data traffic.

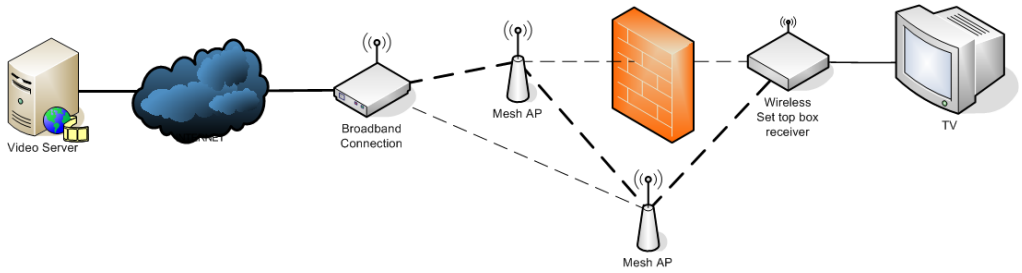

Figure 1.2 Sample scenario for Indoor Wireless Video Distribution using Wireless Mesh Technology

In Figure 1.2, a sample scenario for Wireless Video Streaming in a regular home is shown. The television service enters the residence with a broadband connection. In this scenario broadband router is part of the Wireless Mesh Network as well as two other Access Points. Finally, the Wireless Set Top Box near the television is connected to the Wireless Mesh Network. Wireless Mesh Network selects the most appropriate path for the video transmission between the Broadband Router and the Set Top Box. The best path avoids the high attenuation caused by the walls with alternate relaying paths.

In prior work, WMNs are investigated for extending wireless transmission ranges and for providing higher end-to-end throughput [5]. Recently, several companies have started producing APs with wireless mesh support. There are also efforts to improve the quality of streaming H.264 media over single-hop 802.11 wireless networks [1]. Prior work also aims to improve the video quality over wireless transmission [6] [7] [8] [9] by designing either layer-3 solutions or modifications in the encoder. Our proposed approach differs from prior work, since we keep both the network packets and the encoding process the same.

2 Background

2.1 IEEE 802.11: Medium Access

In IEEE 802.11 [10], the wireless channel is a shared medium like the wire is shared in Ethernet. Unlike the Ethernet, in wireless communication a transmitting peer does not have the possibility to listen to what is actually transmitted at the same time. So instead of collision detection algorithms, in IEEE 802.11 networks collision avoidance techniques are employed.

In Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is the technique used by 802.11 standard [10], a node with a packet to transmit should listen to the channel. If the channel is idle, it can start transmission immediately. If the channel is busy, it waits until the channel is idle again. As every node with a packet to transmit will do the same thing, to avoid collision every node picks a random number and backs off according to this selected random number before transmitting. As nodes will probably pick different numbers, one of them will start transmission while others are waiting. In this case, other nodes should wait again till the channel becomes idle. If two or more nodes transmit at the same time, packets of both will be lost. In this case, they will not get their acknowledgement messages to indicate the packet loss and they will try again later with different random numbers and with different back-off durations.

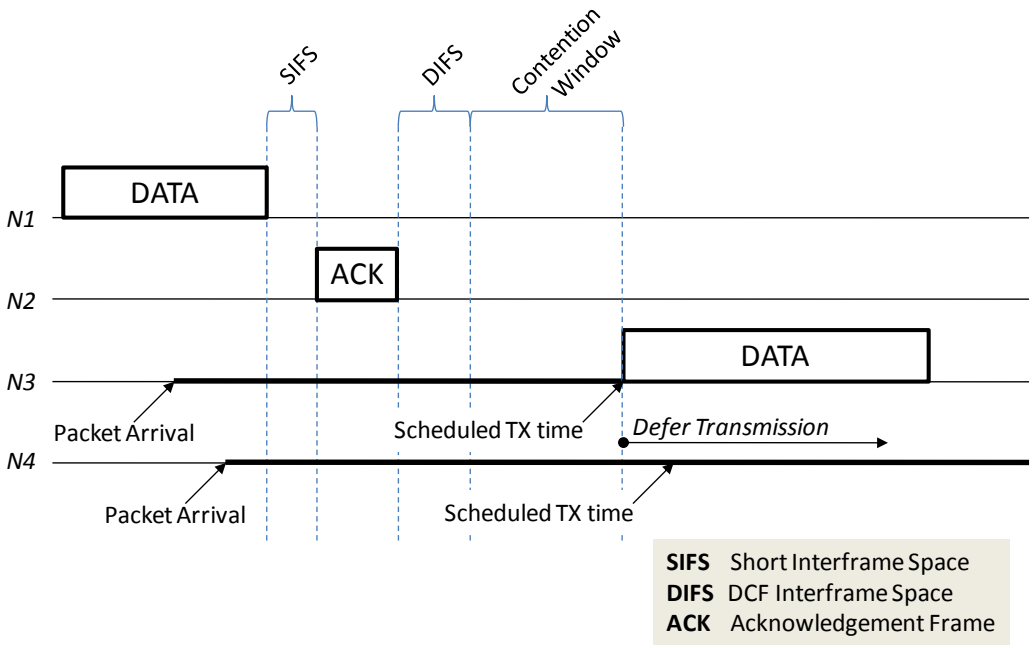

Figure 2.1 Sample DCF medium access scenerio, where channel is busy and two peers (*N3, N4*) are ready for transmission

A sample DCF [10] channel access scenario is shown in Figure 2.1. At the beginning, N1 is transmitting and channel is busy. N2 is the recipient of the data transmission. After N1 finishes transmission, N2 immediately sends an Acknowledgement (ACK) packet. Because of the possible distance between two nodes, N1 may receive ACK packet at most after Short Inter-Frame Space (SIFS) duration. While the transmission of N1 is going on, N3 and N4 gets packets ready to be transmitted. As the channel is busy, they listen to the channel and wait until it is idle at least for DCF Inter-Frame Space (DIFS). After this period is over, they schedule their transmissions according to a random number they pick. This random number is selected from two numbers called CW_{min} and CW_{max}. The time window, where each node that is ready for transmission is scheduling its transmission according to a random back-off window is called Contention Window. The node with the lowest selected back-off duration starts transmitting, because the channel is still idle. As soon as other nodes detect the transmission of the winner of the contention, they start waiting until the channel is idle again.

In CSMA/CA every node has similar probability for transmission. If several nodes are waiting to transmit, one node's probability for a successful transmission is diminished and expected transmission duration increases. Because of the equal channel

access probabilities, nodes with bigger packets will get higher transmission durations, while nodes with smaller packet get lower transmission durations. Nodes with smaller packets should contend for the channel more often. So the available throughput is partitioned between clients relatively to their transmission durations.

2.2 IEEE 802.11e: Wireless Multimedia Extensions

In regular 802.11 DCF [10], there is no quality of service support. To compensate the lack of Quality of Service (QoS), in IEEE 802.11e [2], a prioritization scheme with different channel access probabilities is defined. This scheme can be referred to an improved version of DCF access method, which is called Enhanced Distributed Channel Access (EDCA).

As stated before, every node has equal channel access probability in 802.11 DCF [10], because they pick their random numbers for back-off from the same pool. In EDCA [2], every access category has different upper and lower back-off limits, which ensures that their channel access probabilities are different. These limits are called "Contention Window Min" (CW_{min}) and "Contention Window Max" (CW_{max}) values.

	AIFS	cwMin	cwMax
Voice	2	3	7
Video	2	7	15
Best Effort	3	15	1023
Background	7	15	1023

Figure 2.2 Suggested default EDCA parameters by IEEE 802.11e amendment [2]

In EDCA [2], four access categories are defined, "Best Effort" (BE), "Background" (BG), "Video" (VI) and "Voice" (VO). Best effort is identical to regular IEEE 802.11 [10] traffic priority. Background category is lowest priority while video and voice are higher priority access categories. Packets that will be transmitted in higher priority access categories will have lower CW_{min} and CW_{max} values. This means, their back-off duration will probable lower than regular priority packets. This ensures that higher priority packets will have a better chance to be transmitted on the channel

before lower priority packets. Typical default values for different EDCA access categories are given in Figure 2.2.

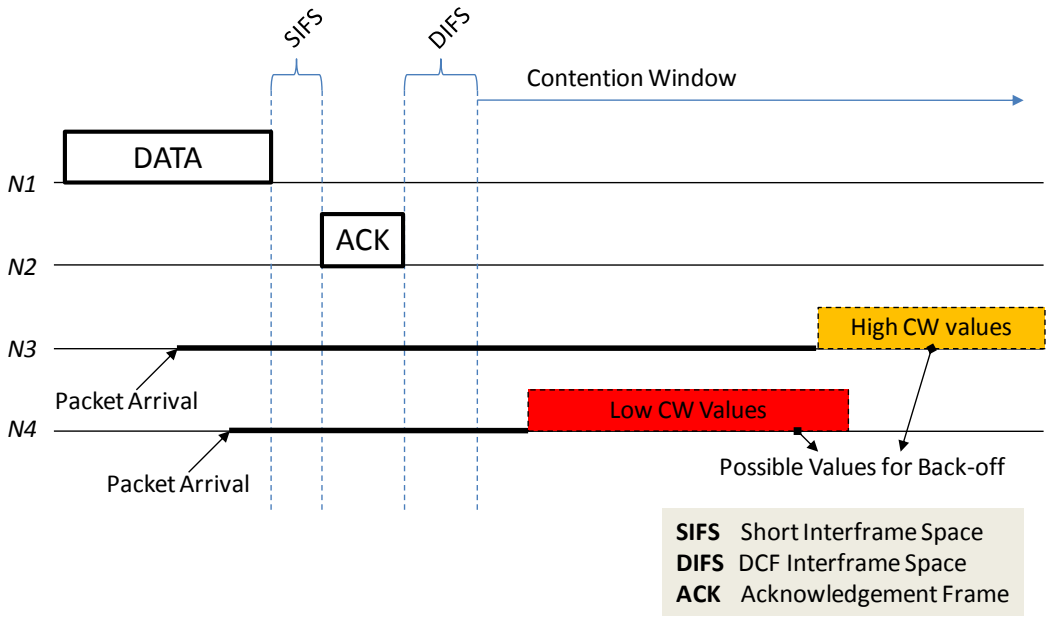

Figure 2.3 Effect of different CW values on channel access with EDCA

Considering the scenario in Figure 2.1, Figure 2.3 shows the effect of a higher priority traffic class on the transmission probability. In Figure 2.3, both parties N3 and N4 are enqueued data packets while a transmission of N1 is in place. In regular DCF, N3 and N4 had similar probabilities of channel access. In Figure 2.3, N4 is assigned to a higher priority class. Both rectangles on N3 and N4 contention window time frame show the possible back-off values that the node can pick from. As N4 has lower possible back-off values compared to the possible back-off values of N3, N4 has a higher chance to start transmitting compared to N3. So as N4 has a higher priority, in Figure 2.3, N4 gets the channel access and transmits enqueued data packet unlike in Figure 2.1, where both parties had the same channel access probability.

This mechanism does not support any QoS guarantees, but it only partitions available channel resources according to some priority scheme. For example, in a high contention environment, every access category will suffer from the low resources, but available resources will be shared among active transmitters proportional to their priorities.

2.3 IEEE 802.11s: Wireless Mesh Networking

In 2003, Institute of Electronics and Electrical Engineering (IEEE) 802.11 Working Group formed the Task Group "S". 802.11s Task Groups purpose is forming the Wireless Mesh Network (WMN) amendment [5]. After a series of ballots to eliminate submitted proposals, there were only two finalists See-Mesh and Wi-Mesh proposals left. These two proposals were finally merged and formed the current IEEE 802.11s Draft [5].

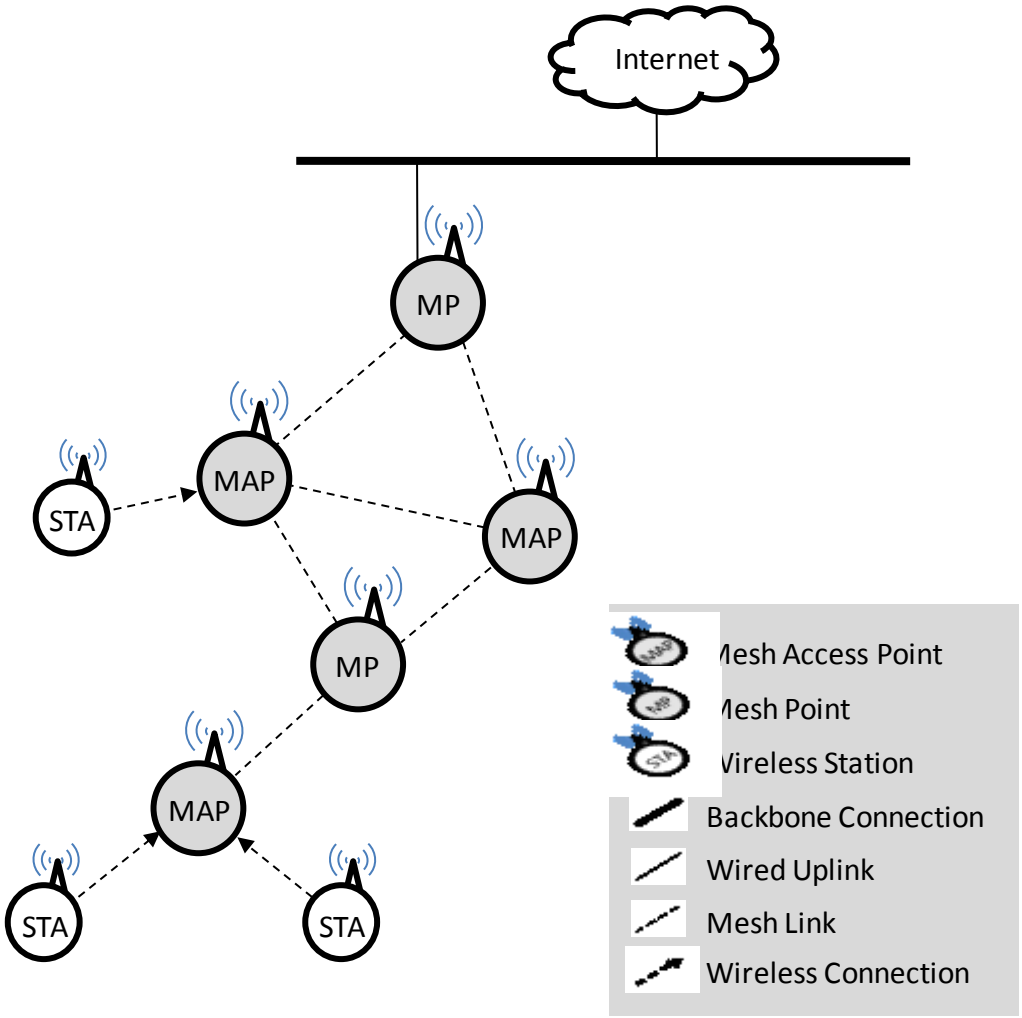

Figure 2.4 A typical Wireless Mesh Network Scenario providing internet service to wireless clients

Currently IEEE 802.11a/g systems support physical rates up to 54 Mbps [10] and with the new enhancement IEEE 802.11n [11] these rates are risen up to 600 Mbps.

Although transmission rates have increased, service coverage is still limited because of strict power regulations, so each access point providing connectivity to a single network should be connected to the backbone. The purpose of Wireless Mesh Networks is to eliminate this requirement by relaying the traffic between mesh nodes wirelessly [5]. A typical mesh networking scenario is shown in Figure 2.4.

As shown in Figure 2.4, IEEE 802.11s [5] defines mesh capable devices as Mesh Points (MP). An Access Point can be also a Mesh Point at the same time, thus giving service to regular 802.11 clients connecting the Wireless Mesh Network. In Figure 1.2, our wireless mesh network application is depicted, where wireless broadband router, access points, and also wireless set top boxes are mesh points. In this typical usage scenario, wireless broadband router and mesh access points extend the service to regular wireless clients that do not incorporate wireless mesh networking standard like a wireless notebook computer. On the other hand, wireless set top box is only a participant in the wireless mesh network and it only relays mesh traffic, but does not extend service to non-mesh clients. So the wireless set top box is only a mesh point in this case.

Mesh Points detect other Mesh Points in the region and they try to establish links with as many Mesh Points as they are able to connect. A wireless link between two Mesh Points to form or enhance a Wireless Mesh Network is called a Mesh Link. A set of Mesh Links that form a path between two Mesh Points is called a Mesh Path. Mesh Path's should not contain loops. Mesh Path's are discovered on the fly throughout the Mesh Network with routing algorithms that are previously agreed by every Mesh Point in the network.

IEEE 802.11s [5] defines Hybrid Wireless Mesh Protocol (HWMP) as the mandatory routing algorithm for Wireless Mesh Networks. It is basically a combination of Ad-hoc On demand Distance Vector (AODV) [12] and tree-based routing. IEEE 802.11s also supports any other routing algorithms as optional enhancements with the only requirement that each Mesh Point within the same Wireless Mesh Network should support and use the same routing algorithm.

Capabilities of Mesh Points should be detected at the handshake phase by establishing the Mesh Link. So if the capabilities of new Mesh Points that are trying to

join the network and the capabilities of the nodes currently within the Wireless Mesh Network are incompatible, they will fall back to mandatory defaults.

IEEE 802.11s [5] introduces several additions and enhancements to the current 802.11 Medium Access Control (MAC) protocol for congestion control, power save and to IEEE 802.11e Quality of Service [2] support. It also introduces channel selection strategies for the whole Wireless Mesh Network. IEEE 802.11s also proposes several enhancements to support the end-to-end security requirements of Wireless Mesh Networks via IEEE 802.11i, which is the security amendment for 802.11 wireless networks. IEEE 802.11i considers only the security between an Access Point and a station. In WMNs, the traffic not only flows between the stations and the access point, but it is also relayed and transmitted wirelessly between access points.

The Wireless Mesh Network implementation presented in the following chapters of this thesis is similar to IEEE 802.11s draft and they are compatible to some extent, but IEEE 802.11s is a highly changing draft, which was far from complete as the implementation was taking place, as well as this thesis is written.

2.3.1 AODV Routing Algorithm

In Ad-hoc On demand Distance Vector (AODV) algorithm [12], a data packet with unknown destination route triggers the route discovery. Originating node should send ROUTE_REQUEST packets to every neighbor. If a neighbor doesn't know a route to the destination, it forwards ROUTE_REQUEST packet to its immediate neighbors by incrementing hop count by 1 specified in the packet. Every node that receives a ROUTE_REQUEST packet learns that it can reach the originator by the next hop from which it received the ROUTE_REQUEST packet with the specified hop count. So in a discovery, every node within the network learns how to reach the originator. It is necessary; because it is unknown which nodes will take part in the bidirectional route. So every node learns how to reach the originator.

If the destination node is hit by a ROUTE_REQUEST packet, it generates a ROUTE_REPLY packet and transmits this packet to immediate neighbor to reach the originator. This ROUTE_REPLY packet is forwarded to next hops learned from the

ROUTE_REQUEST packets by intermediate nodes, and they learn how to reach the destination, which is necessary for bidirectional communication. Finally, every node within the network learns how to reach the originator, but only nodes participating within the active route learns how to reach the destination.

In AODV algorithm [12], unused or idle routes are dropped from routing tables. In this way memory requirement for routing tables are kept to the minimum. For example, in a discovery every node learns how to reach the originator, so every node adds a routing entry, which may never be used by the nodes that are not part of the route. In this case, after a specific duration these unused entries will expire and dropped. In an active transmission, only the nodes that are part of the active route know how to reach both end points.

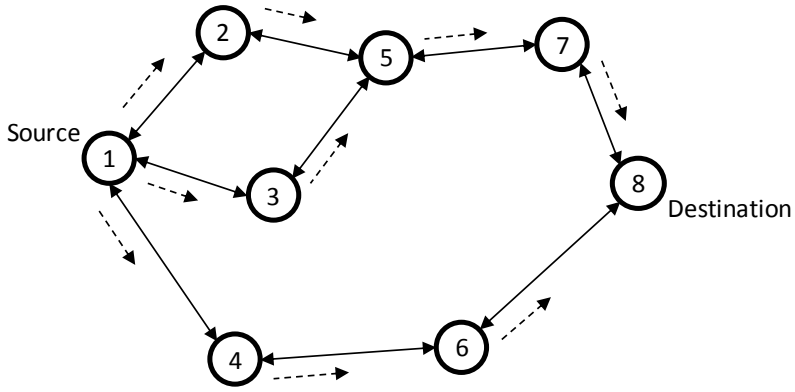

Figure 2.5 Propagation of a Route Request (RREQ) Packet

A route discovery is initiated by the Source node trying to find a path to a Destination node. Source sends RREQ packets to its immediate neighbors. Each node that is not the destination node forwards received RREQ packet to its immediate neighbors after updating the cost to use the path that RREQ packet has already traveled. In Figure 2.5, source node '1' initiates the discovery and each sent RREQ packet is shown with dashed arrows. Finally a RREQ packet reaches the destination node '8'. At each node receiving RREQ packets, a temporary route entry is created to reach source node '1'. So after RREQ packet has traversed whole topology, each node will have a valid route to reach the originator.

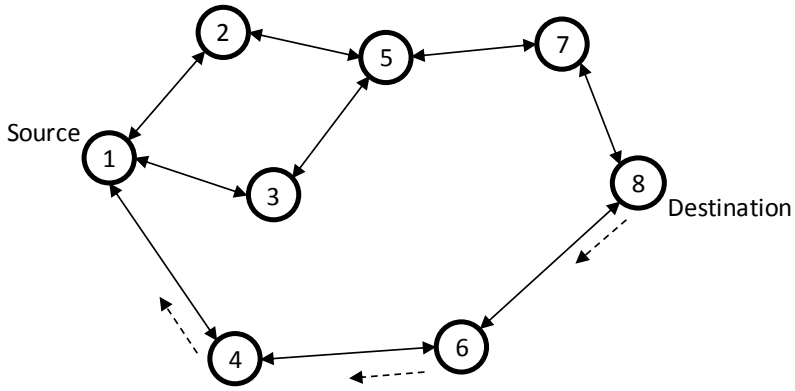

Figure 2.6 Traversal of Route Reply (RREP) Packet

After a RREQ packet has reached destination node ‘8’, it immediately generates a RREP packet and sends it to the neighbor from which RREQ packet has been received. As each node has a valid route entry to the originator node, RREP packet will be relayed by intermediate nodes to the source node like in Figure 2.6.

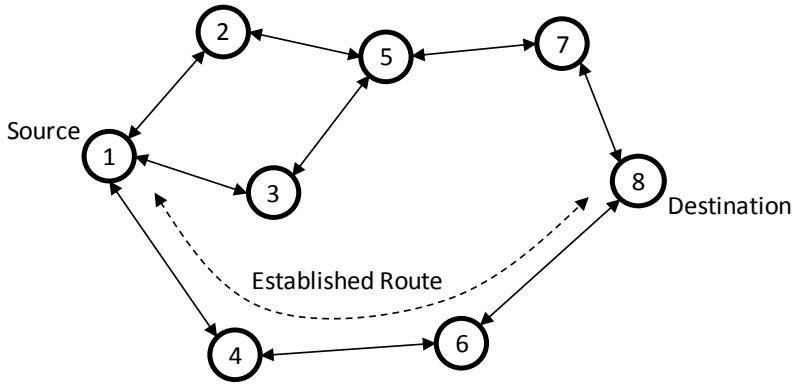

Figure 2.7 Established Bidirectional Route after discovery

After RREQ packets have traversed the topology, destination node and any intermediate node will know how to reach the originator. After RREP packets have been relayed up to source node, source node will have a valid route to reach the destination. As seen in Figure 2.7, a bidirectional route will be established between source and destination nodes. Any route entry in each node will expire if it is not used for a specific duration, which is set to 60 seconds in our implementation.

2.4 H.264 Video Encoding Standard

H.264 encoder [3] consists of two independent layers. First layer is Video Coding Layer (VCL), which is responsible for compression of raw video feed. VCL is independent from the employed transport mechanism. Output of VCL is video slices. Second layer is Network Abstraction Layer (NAL). NAL is responsible for generating transferrable packets.

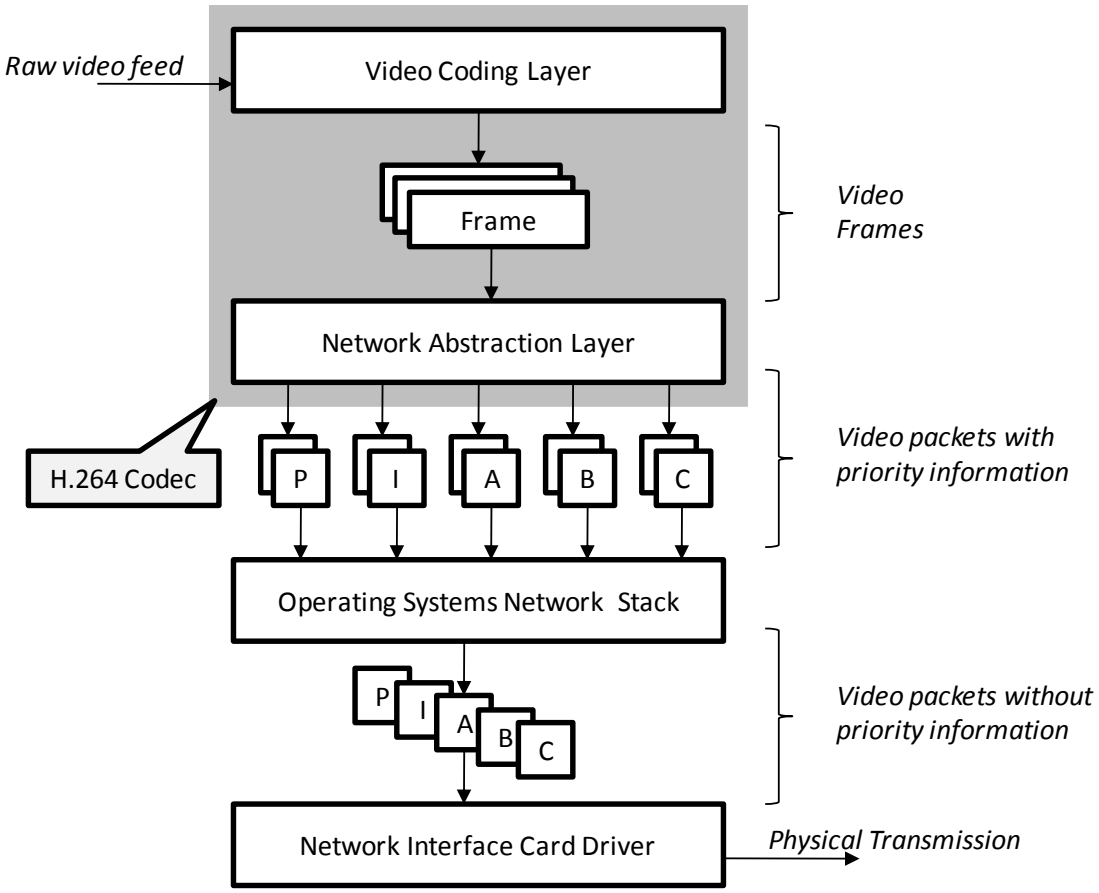

Figure 2.8 H.264 codec encodes raw video feed into H.264 video frames that are then packetized in Network Abstraction Layer (NAL). These packets are transferred by the operating system with the same priority.

In Figure 2.8, a general overview of the H.264 [3] codec is shown. Raw video is fed into H.264 codec's Video Coding Layer (VCL). VCL, then transforms raw video feed into video frames that are passed on to Network Abstraction Layer (NAL). At NAL, video frames are split into network transferrable packets. These packets are passed to the operating systems network stack with the standard socket interface, and packets leave the encoding layer. At encoding layer, types and priorities of packets are

known, but at network stack this information is lost. So from the operating system's perspective, each video packet has the same priority. Network stack hands over these packets to Network Interface Card (NIC) driver, which transfers these video packets physically through the Network Interface Card (NIC). A Network Interface Card can be any type of wired or wireless interface, such as an Ethernet card or IEEE 802.11 wireless interface.

Partitioning is an extension for network abstraction layer, which generates network packets with different priorities [3]. Parameter set concept (PSC) packets contain picture size, display window, optional coding modes employed, macro block allocation map and so on. Instantaneous Decoding Refresh (IDR) frames contain a coded picture that can be decoded without needing any other frame. Partition A packets contain inter-frame motion vectors and depend on both previous and next packets. Partition B and C packets contain texture related information which also depends on many previous and next packets.

Every packet type generated by NAL depends on PSC packets. As the information within the PSC packet does not change very frequently, PSC packets can be transmitted in a reliable way, or they can be transmitted multiple times to ensure reception. PSC can be also mapped to lookup tables and included information of the PSC packet can be piggybacked within other frame types.

IDR packets are very important, because multiple consecutive partitions A, B and C packets depend on IDR frames. Loss of a single IDR frame may lead to consecutive failures. Decoder may not be able to decode many consecutive frames afterwards. Partition A packet are also very important. Without proper reception of motion vectors, decoded video will contain multiple erroneous frames.

Partition B and C type packets are of lesser importance. Loss of these types of packets will lead to quality decrease, but it will not prevent decoding frames, so no frame loss will occur.

3 Problem Statement

3.1 Video Streaming Requirements

In a video streaming system, raw video is encoded, packetized and transmitted over a packet network. Clients receive these video packets and they try to decode the original video out of these packets. Video decoding is a time critical process, where each frame has to be decoded and displayed before a strict deadline. While transmitting video packets may get lost, arrive late or even arrive out of order. A late packet that is required for decoding an already decoded frame cannot be used anymore, so it is dropped.

Delay jitter is defined as the variation of the delay. Although there are several codecs that are more tolerant to delay jitter and packet loss, they should be minimized for a high quality video streaming over wireless mesh networks.

3.2 Video Streaming over Wireless Mesh Networks

In a video streaming system, recipients perform a real-time operation, which requires decoding and displaying frames at a specific frame rate. The original video is assembled out of the received packets considering dependencies and packet deadlines. In a wireless network, packets may be lost or delayed significantly, and this may degrade the quality of displayed video because of the missing information. Before discussing the challenges of video streaming over a multi hop WMN, we review the problems of video streaming over a single hop 802.11 wireless link.

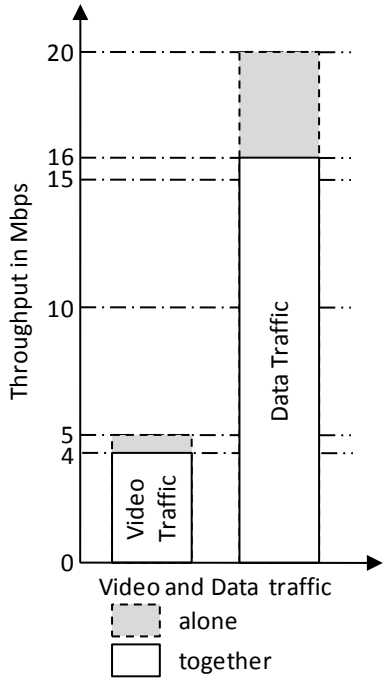

Figure 3.1 Both Data and Video traffic try to obtain different amounts of channel. If both are transmitted, both traffics are suppressed relative to their requirements.

In IEEE 802.11 [10] based systems, higher layer protocols for data transmission employ greedy algorithms like Transmission Control Protocol (TCP) that try to maximize active channel usage. However, video traffic requires a specific amount of throughput and if contending data traffic tries to allocate all available bandwidth, both flows are suppressed. As an example, consider a hypothetical channel with maximum available throughput of 20 Mbps. There are two users transmitting a 5 Mbps video and 20 Mbps UDP data respectively that is shown also in Figure 3.1. When channel is shared fairly, both flows suffer a 20% packet loss. However, for video, 20% packet loss may have devastating consequence of completely halting the video decoding.

Another problem of IEEE 802.11 links is high delay jitter, which is defined as the variance in delay. In order to decode the video properly, video packets have to received within their specific deadlines; otherwise frame is decoded without those packets. Any packets later than a limit are eventually dropped at the receiver. The aforementioned problems are exacerbated in WMNs due to increased contention associated with increased relays. Another issue is the processing/queueing delays imposed by each intermediate mesh relay node. In a WMN nodes at the center of mesh network may relay more packets than the mesh nodes at the periphery. Therefore, the transmission

buffer of the nodes at the center would contain more packets than peripheral nodes, increasing the delays in the network. For this reason, intelligent resource allocation among existing flows should be investigated.

4 Proposed Solutions

4.1 Packet Prioritization

In order to accomplish high quality multi-hop wireless video transmission over WMNs, the required end-to-end throughput should be sustained and the cumulative delay jitter has to be minimized. Assigning video packets a higher priority than the rest of the packets, results in shorter back-off durations, hence lower jitter. In order to ensure that required end-to-end throughput is made available to video packets, video traffic should be resilient to suppression by data traffic. This is not an easy task as there is no bandwidth allocation mechanism within 802.11 standards. Nevertheless, as demonstrated in this thesis, by using intelligent prioritization of packets, loss, delay and jitter of video packets can be decreased, which in turn minimizes the quality degradation of the decoded video. This comes at the expense of decreased throughput of background data traffic, but as shown in our results unless the available resource is extremely scarce, this decrease is tolerable.

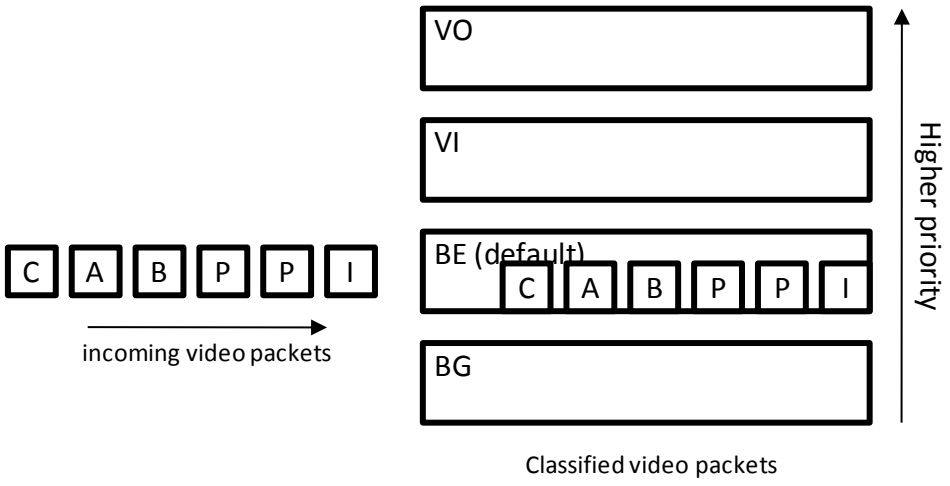

Figure 4.1 All video packets are transmitted using default access category of EDCA (Regular DCF)

4.1.1 Basic Prioritization

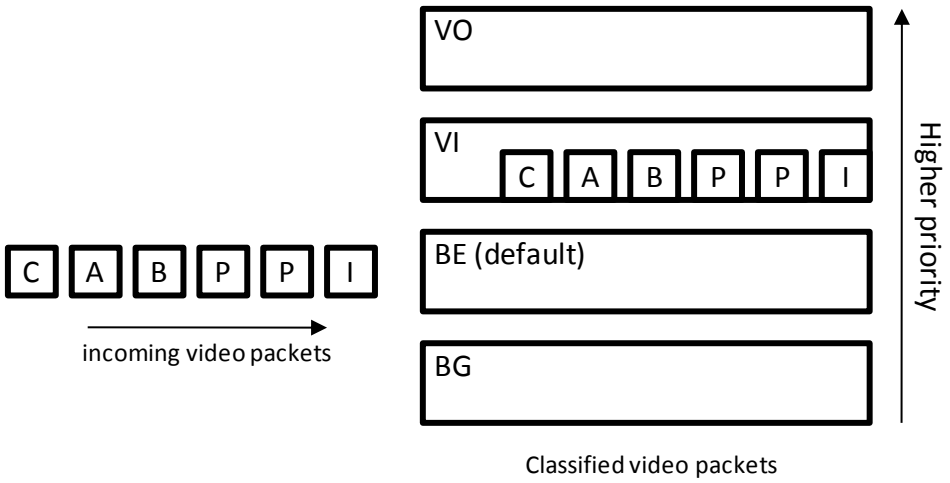

Figure 4.2 Using "*Basic Prioritization*", all video packets are transmitted using the same high priority EDCA class, either Video (VI) class or Voice (VO) class. In figure, each video packet is transmitted using the Video (VI) class.

In order to minimize delay, jitter and loss of video packets, we use IEEE 802.11e EDCA to assign higher priority to video traffic. As indicated earlier, EDCA defines four access categories with varying priorities. Without any prioritization each video packet is transmitted using Best Effort (BE) access category that is shown in Figure 4.1. In basic prioritization scheme, each video packet is assigned to a higher priority EDCA class, which is either Video (VI) or Voice (VO), and data traffic is assigned to a lower priority class, which is shown in Figure 4.2. In WMNs, video packets have to be transmitted with high priority in each intermediate transmission. In order to accomplish this task, intermediate nodes should be able to classify video packets, and relay them with the predefined EDCA class.

4.1.2 Smart Prioritization

Basic prioritization algorithm treats all video packets with the same priority. However, H.264 codec has a network abstraction layer (NAL), which is responsible of creating network transferable packets with varying importance. In a high contention environment, video packets may also get dropped according to basic prioritization. However, since the basic prioritization scheme assigns all video packets the same

priority, the dropped packets may be from important *P* or *I* frames. This would significantly reduce the video quality at the receiver.

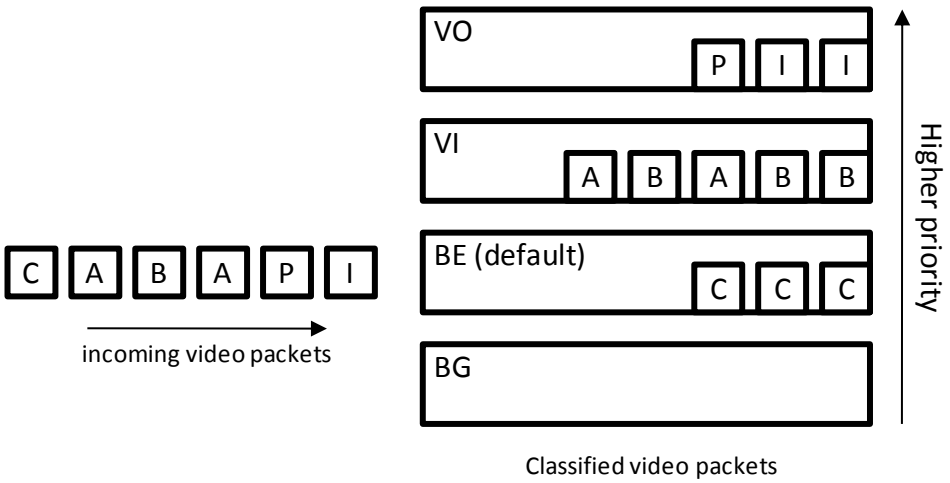

Figure 4.3 In "*Smart Prioritization*", each video packet is inspected and transferred using different priority EDCA classes according to their priorities in decoding process

In order to minimize the quality degradation, we differentiate video packets according to their importance by assigning them to different higher priority EDCA classes. Thus, in high contention environments, more important video packets are protected more than the low importance video packets. In our implementation, *I* frames are assigned to VO class, *P* and *A* frames are assigned to VI class and *B* and *C* frames are assigned to BE class, which is also shown in Figure 4.3. By this approach, in case video packets are dropped, lower priority video packets get dropped first; thus minimizing the quality degradation at the video output.

Another problem imposed by basic prioritization is the accumulated video packet contention. In single hop transmissions, video packets contend only with data traffic by maintaining a high chance of success. In WMNs, video packets also contend with each other. If a video packet has to be transmitted over 3-hops where all nodes are in the same contention domain, and video traffic is 3 Mbps, the effective contending video traffic will be 9Mbps. When there is contention among high priority traffic, consecutive collisions may occur which in turn increases packet loss, delay and jitter. However, smart prioritization scheme regulates the contention in the network by reducing the number of packets contending at each priority class.

5 Implementation

5.1 General Architecture Overview

Our mesh implementation has three major functions, mesh node discovery, mesh link establishment and routing. General structure can be viewed in Figure 5.1. Parts that are shaded gray are our mesh layer implementation extensions.

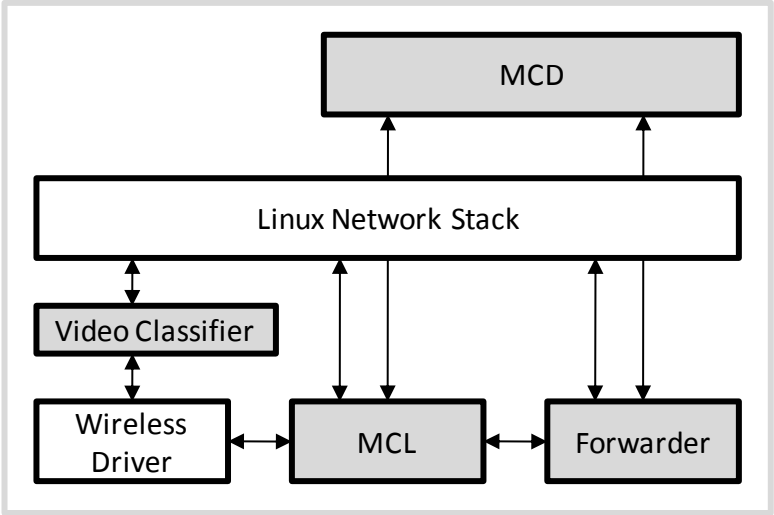

Figure 5.1 General Architecture Overview of Wireless Mesh Networking and Video Prioritization implementation

For mesh control packet exchange, Mesh Control Layer (MCL) is introduced. MCL is responsible for communication of mesh control packets that are required for mesh node recognition, mesh link establishment and maintenance.

On top of MCL, Mesh Control Daemon (MCD) is implemented. While the purpose of MCL is supplying an out-of-band control communication channel using the underlying WIFI driver, MCD is responsible for decision making. Mesh node discovery and mesh link establishment handshake are done by MCD over MCL.

Monitoring link qualities, neighbor failures and making appropriate routing decisions is also other main jobs of MCD.

Routing has also two parts, route discovery and actual layer-2 packet forwarding. Employed routing algorithm is a modified version of Ad-Hoc on demand routing protocol (AODV), which will be described in more detail later. Route discovery is also done by MCD over MCL. Packet forwarding is done by another layer called '*Forwarder*'. Forwarder has the responsibility of forwarding packets to appropriate links decided by the routing algorithm. These links may be uplink Ethernet connections or other established mesh links.

Auto-healing of the mesh network in case of node or link failures is handled also by MCD. After detecting node and link failures, appropriate route error messages are sent to neighboring links for notification. If any route is broken, another route will be discovered and used instead.

5.2 Control Message Communication

Our 802.11 wireless mesh network implementation consists of several parts like auto-configuration, auto-healing and routing. All these distinct layers require a proper control message communication with neighboring nodes.

In regular 802.11 protocols MANAGEMENT, CONTROL and DATA frames are three packet types. Management frames are protocol related packets, which are used to join, re-join, leave or probe clients and access points. Control frames are much smaller packets than management packets and they are used to control packet transmission, specifically to track the transmission status of data frames. Data frames are used to transmit the payload.

In all three packet types only data packets are tracked for successful transmissions. After every data packet transmission and acknowledgement control packet (ACK) should be received. Otherwise, the transmission is assumed failed and frame is retransmitted an ACK packet is received from the remote peer or a specific

number of retransmissions is reached. ACK mechanism is not used for control and management frames.

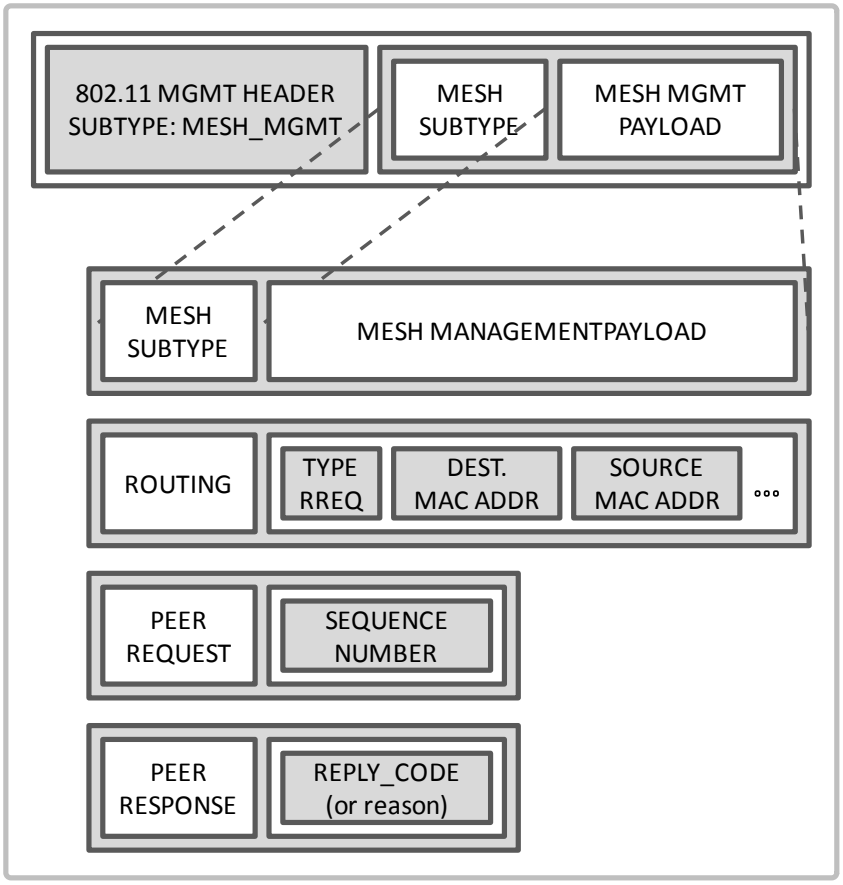

Figure 5.2 Mesh Management Frames have different subtypes indicated by the "*Mesh Subtype*" field in the management packet payload. Different subtypes have different payload interpretations like in the figure.

For wireless mesh network implementation, mesh nodes require a means of communication with each other for previously stated layers. We defined for this type of communication a subtype of management frames which we call MESH_MANAGEMENT packet type.

Mesh management is a subtype of 802.11 management packets, but mesh management packets also contain several subtypes within its payload. PEER_REQUEST, PEER_RESPONSE subtypes are used by auto-configuration layer for peer handshake algorithm. Mesh management payload is interpreted according to subtype. For example, in PEER_REQUEST packets, there is 2 bytes length payload containing a sequence number. In PEER_RESPONSE packets, there is also a 2 bytes

length payload, which is interpreted as a REPLY_CODE. More samples of mesh management frames can be seen in Figure 5.2.

5.3 Neighbor Discovery

Mesh nodes appear as regular 802.11 access points to clients. Only difference is in the content of periodic beacons, which is actually a special type of 802.11 management frames used by access points. Each mesh capable access point includes a special information element only recognizable by other mesh capable access points. Clients and other 802.11 equipment safely ignore this element.

Existence of mesh information element means that the device sending this beacon is actually a mesh capable access point. Mesh information element also includes a "MESH-ID" field to differentiate mesh networks within the same area. If the MESH-ID field within the mesh information element matches mesh identifier of the receiving node, then they are in the same mesh network.

If both parties belong to the same mesh network and they are in the transmission range of each other, they should create a mesh link between them for data transmission and relaying. So, the peer that detected other side first, sends a PEER_REQUEST packet to the remote party. Remote party either accepts the connection request or denies for some reason. In both cases, remote party sends a PEER_RESPONSE packet with the PEER_OK, PEER_DENY or PEER_ERROR code. If PEER_OK code is received, mesh link is created between two parties and routing layer immediately starts using this link in the routing decisions. If in any case, a PEER packet is not answered, it is decided that the packet is lost and retransmitted in periodic intervals until a predefined timeout occurs. As default, periodic retries are sent once a second until 3 seconds of default timeout occurs. If in the defined interval no response is received, remote party is marked as erroneous. If peer handshake falls to error state, it will be retried not before some predefined amount of time has passed, which is 60 seconds as default. So deadlocks are avoided.

If both parties send PEER_REQUEST packets and wait for PEER_RESPONSE packets, both parties will wait indefinitely for the other party to respond, thus causing a

deadlock situation. To avoid such deadlock cases, a 32-bit random number is included within the PEER_REQUEST packets. If a party receives a PEER_REQUEST packet while waiting for PEER_RESPONSE, it compares the number included within the original PEER_REQUEST that has been sent and the number included within the received packet. The lower numbered request is considered as never existed, so either the node responds with a PEER_RESPONSE packet or continues to wait for the remote party to send the PEER_RESPONSE. If random numbers are equal, the handshake starts over at both sides. So it is ensured that in any case, the handshake will be completed.

Mesh nodes may also possess different mesh capabilities. Information elements contained in the beacons and other mesh management frames manifest these capabilities to neighboring nodes. Routing algorithms, routing metrics and other implementation or version specific features are examples of the information contained in the capability elements. With the help of these elements, incompatible mesh nodes will not try to establish mesh links.

Implementation of Neighbor Discovery in our Wireless Mesh Network implementation is based on the IEEE 802.11s [5] amendment draft at time of implementation. Since then IEEE 802.11s has enhanced the Neighbor Discovery procedure and our implementation is renamed as “Passive Scanning”, while a new discovery scheme using Probe Request and Probe Response frames is introduced as “Active Scanning”. [13]

5.4 Link Maintenance and Monitoring

Maintaining mesh links is based on basically monitoring status of remote peer. If remote peer is not responsive to active routing protocol packets or stops broadcasting its periodic beacons, a mesh node should destroy the mesh link and notify routing layer of the change in the topology. If remote peer is detected again, thus returning back to life, the link has to be created again with a new peer handshake sequence.

Link quality monitoring is another issue for routing to decide which link has lower cost if used and it is different than link maintenance. In routing section, link quality monitoring is explained in detail.

5.5 Routing

5.5.1 Requirements for Routing Layer

In wireless mesh networks, there is no fixed topology, it is created and maintained actively without planning by mesh nodes. Rapidly changing topology issue causes many problems to be solved which do not exist in planned infrastructure networks.

Unlike a wired network, a wireless mesh networks underlying topology may change rapidly. New mesh nodes may join the network, old mesh nodes may leave or they may change geographical locations. A new obstruction between two nodes may be presented which may prevent data communication between previously communicating wireless mesh peers. Auto-configuration adapts the topology according to these changes and notifies routing algorithm of the change. From that point, it is routing layers responsibility to maintain best end to end paths between communicating clients over the mesh network.

In a wireless mesh network, link qualities and their respective residual capacities change rapidly. Because of the fading channel and the contention, determining rapidly changing residual capacity is very hard. Throughput and the jitter caused by each link over the entire network should be known to determine the best end to end path.

Both jitter and throughput are changing over time and they also depend on the active traffic over the link, traffic of neighbors and total channel capacity which is also rapidly changing over time. Even in such a changing environment, routing algorithm should adapt itself and provide best possible paths available.

As neighboring traffic may affect current capacity, high density of control messages have also negative effect on residual capacity. In this highly changing environment, control message traffic should be kept to the minimum.

Mesh capable access points are commonly low end devices with limited computational power and memory. A regular access point is an embedded computer with around 4-8 megabytes of memory and very limited CPU which can barely handle soft switching of client packets with other clients. Because of the limited resources, routing algorithm should require a very small memory footprint and complex computations should be avoided.

Another prerequisite for the routing layer is that bidirectional routes have to be established in a very short duration. In the duration of discovery, data traffic packets cannot be forwarded without a proper path definition. So mesh nodes can either drop data packets for the ongoing discovery or they can buffer packets until a proper path is established. Both in buffering and drop cases, discovery has to be completed in a very short time to minimize the effect on clients.

Broadcasting packet may seem more comfortable for unknown destinations while discovery is in progress, but it should be avoided in wireless mesh networks. Wireless channel is a shared medium and for proper broadcasting, every mesh link has to be traversed by the data packet, which might be a very high number in dense networks. Even in sparse networks, wireless channel will be overly loaded, which might affect other ongoing packet transmissions where only a very small subset of mesh links should be traversed.

In our wireless mesh implementation, we used a modified version of Ad-Hoc On-Demand Distance Vector Routing protocol (*AODV*) to overcome previously stated problems.

5.5.2 Modified AODV Algorithm

Original AODV algorithm [12] is a robust and fully distributed routing algorithm with very low resource requirements. Reactive nature and idle route expiration

minimizes the resource requirements of the routing layer if AODV is used. On the other hand, original AODV algorithm is designed to be a layer-3 routing algorithm which lacks layer-2 Address Resolution Protocol (ARP) addressing. So it can only support IP networks. Other unsuitable feature for wireless mesh networks is that it uses hop count as if using each link has the same cost, which is not appropriate for wireless mesh networking. So we modified and adapted original AODV algorithm to Wireless Mesh Networks.

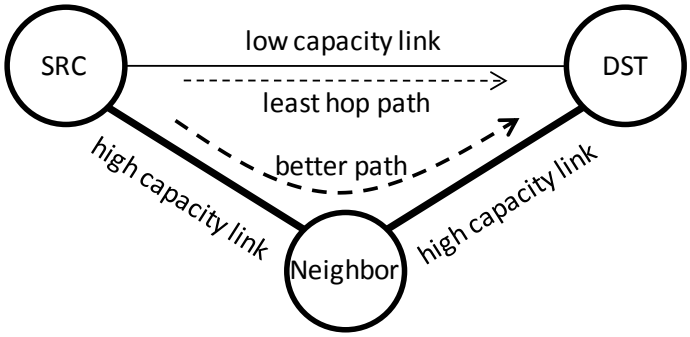

Figure 5.3 A two hop route containing to high capacity links can have higher capacity compared to single hop travel. Using a capacity aware metric, AODV will find the "*better*" path instead lowest hop count path.

Our main difference from the original AODV protocol [12] is that our wireless mesh network is designed to be identical to a layer-2 switch from the perspective of clients. This feature assures that any Ethernet encapsulated protocol can be used over the Wireless Mesh Network without the requirement of any change. So Wireless Mesh Network can be deployed as a replacement to a bridged Ethernet infrastructure. [5]

Being identical to a layer-2 switch means that a packet should be transmitted entirely identical from the source to the destination in each layer. In layer-3 routing like in the original AODV, MAC header of the packet is altered to reflect 1-hop communicating peers MAC addresses. Packets are routed according to their layer-3 IP addresses. To be identical to a layer-2 switch, our modified AODV algorithm had to work in layer-2. Discoveries and route maintenance is done according to layer-2 MAC addresses. In this approach, mesh points do not alter packets, but they just forward to next hop neighbors. This approach can also be called packet switching, because the original packet is transmitted as it is.

Another major difference of our modified algorithm from the original AODV [12] is the control messages. In original AODV, control packets including routing packets are transmitted as regular data frames. In our modified version, control messages for the routing layer are transmitted as mesh management frames. For this purpose, a subtype of mesh management frames is defined and used by the routing layer. ROUTE_REQUEST, ROUTE_REPLY and ROUTE_ERROR packets are encapsulated within this packet type.

Original AODV algorithm [12] is basically a distributed shortest path algorithm. It finds shortest path between two nodes, where link costs are 1. This way discovered paths will be paths with least hop count. This is another problem for wireless mesh networks, because link capacities will drop with increasing distance. As in Figure 5.3, least hop path will use links with highest distance possible, which will eventually result in a low capacity path. On the other hand, a better route may exist with higher hop count, where links within the route may have higher capacity. As wireless channel is a shared medium, capacities of two links in the same collision domain will diminish, because only one of them can transmit at a time. For example, if we have a throughput of 20 Mbps in each high capacity links, the path of two such links may have only 10 Mbps throughput at maximum. To discover such "better" links, least hop metric had to be updated to reflect link capacities.

5.6 Video Classifier

In order to transmit video packets with appropriate access categories, we designed and implemented a packet inspection and classification engine to work between the network driver and the network stack of the Linux kernel. If a packet is released from the network stack for transmission, it is captured by the Video Classifier, and it is inspected by comparing it with known codecs and packetization techniques. If the packet is identified as an H.264 NAL unit packet, it is processed further to detect the packet type, and it is handed to the driver with a priority tag determined according to Basic or Smart prioritization scheme.

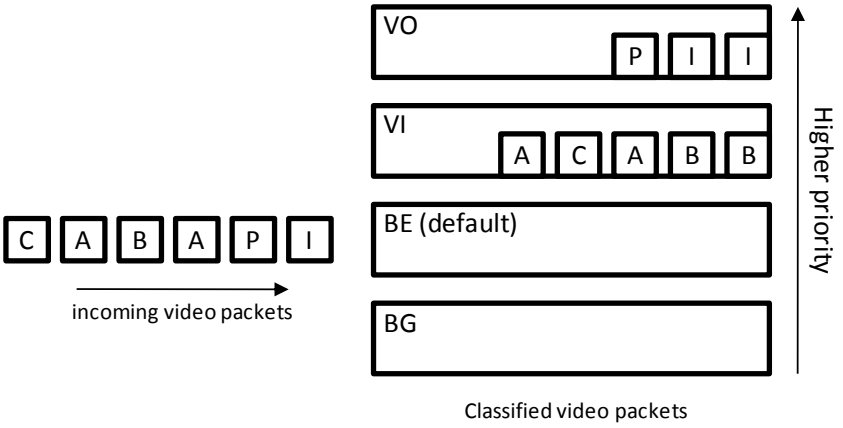

Figure 5.4 In our Smart Prioritization Algorithm implementation, video packets are transmitted using Voice (VO) and Video (VI) queues according to their importance in the decoding process. To avoid packet loss and to make video traffic more resistant to neighboring data traffic, no video packets are transmitted using Best Effort (BE) queue.

In the simulations the real smart prioritization algorithm with full data partitioning support is investigated, where *C* packets are enqueued to BE queue. Although our first intention was to exploit the data partitioning support of H.264 encoder [3] to give the ambient traffic a fairer share of the channel, we concluded that even the small loss in video quality is not acceptable for entertainment services. So for the real implementation we had to change our algorithm slightly to a more basic and more aggressive algorithm, where every video packet is of higher priority compared to the ambient traffic. So we moved *C* packets to VI class. In Figure 5.4 the implementation of our Smart prioritization algorithm is depicted. For basic prioritization, all video packets are enqueued in the same priority queue (VI or VO). In simulations, every video packet is enqueued to VI class.

6 Performance Evaluation

6.1 Simulation Environment

In order to show the positive impact of our proposed prioritization algorithm compared to regular DCF [10] transmission and also compared to the basic prioritization scheme, first we modeled a multi-hop wireless mesh network using OPNet Modeler v11 [14] over which we can stream RTP-hinted H.264 video streams. In our simulation setting, we used an H.264 [3] stream with a mean bit rate of 3072kbps, which is transcoded from an MPEG-2 DVD video with highly varying scenes. Network transferable H.264 packets are equal to 1450 bytes.

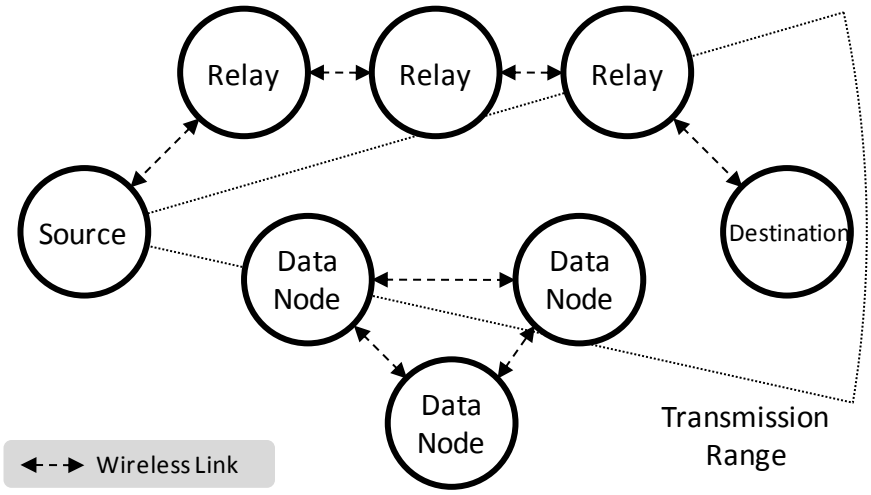

Figure 6.1 In our simulation setup, video packets are transmitted over 4 hops and there are 3 data nodes generating background data traffic.

There are also a number of interferers transmitting packets with size of the MTU and their transmit buffers are always full, which models a worst case high background traffic. Source, destination, all three intermediate relay nodes and data nodes generating background traffic are in the transmission range of each other. In simulation setting,

each node has about 2Mb of buffers, which corresponds to at least 2000 packets. Simulation setting can be seen in Figure 6.1.

6.2 Simulation Results

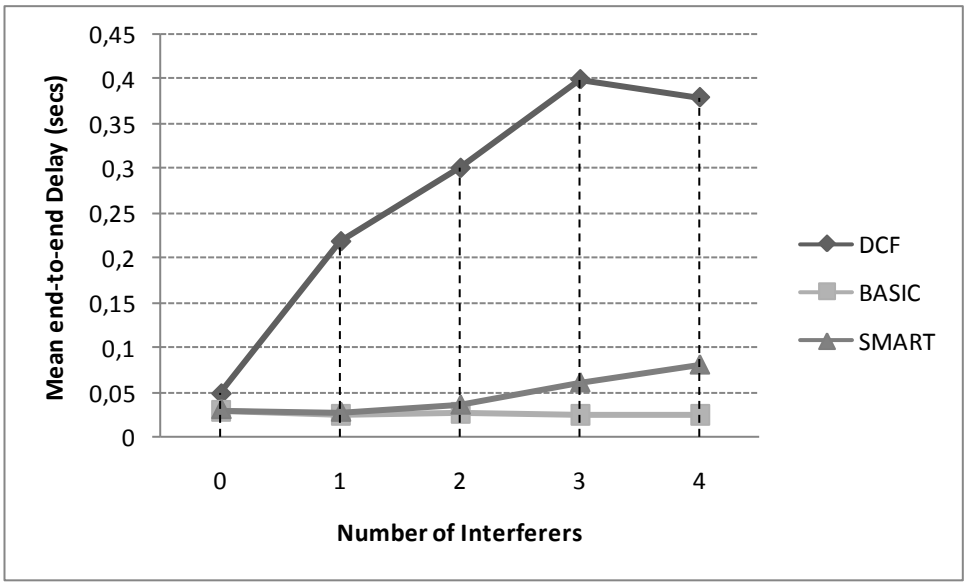

Figure 6.2 Mean end-to-end delay against number of interferers

As it can be observed from the mean end-to-end delay in Figure 6.2, DCF is very sensitive to the interfering traffic. From 50 ms of end-to-end delay in no interferer case, it increases rapidly over 400 ms in 4 interferer case. Simple EDCA mapping of H.264 packets to one higher access category easily overcomes the fragile nature of DCF. In no interferer and even in 4 interferer cases, the mean end-to end delay stays below 50 ms, which can be achieved by DCF only if there is no other traffic on the channel. By simple EDCA mapping, video stream clearly suppresses the interfering transmissions, whereas by our proposed prioritization algorithm we achieve a fairer share of the channel by allowing slight increase in the mean end-to-end delay. In smart prioritization, video packets may wait longer than basic prioritization, while the number of interferers is increased. This is because of the higher contention of data packets, which cause several collisions on low priority video packets that did not happen in basic prioritization.

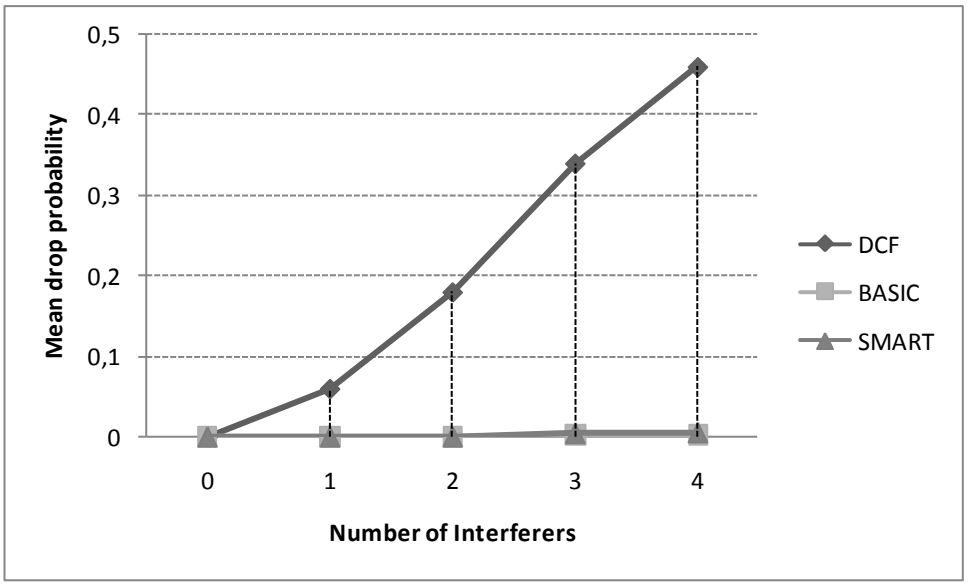

Figure 6.3 Mean end-to-end packet drop probability

The mean packet drop rates are given in Figure 6.3, which clearly states that in DCF, packet drops are due to buffer overflows. The maximum retransmission counts increase rapidly by the increasing number of interferers, which eventually results in almost 50% of all video packets in the 4 interferer case. The simple EDCA mapping and our proposed prioritization algorithm are not affected as much as regular DCF.

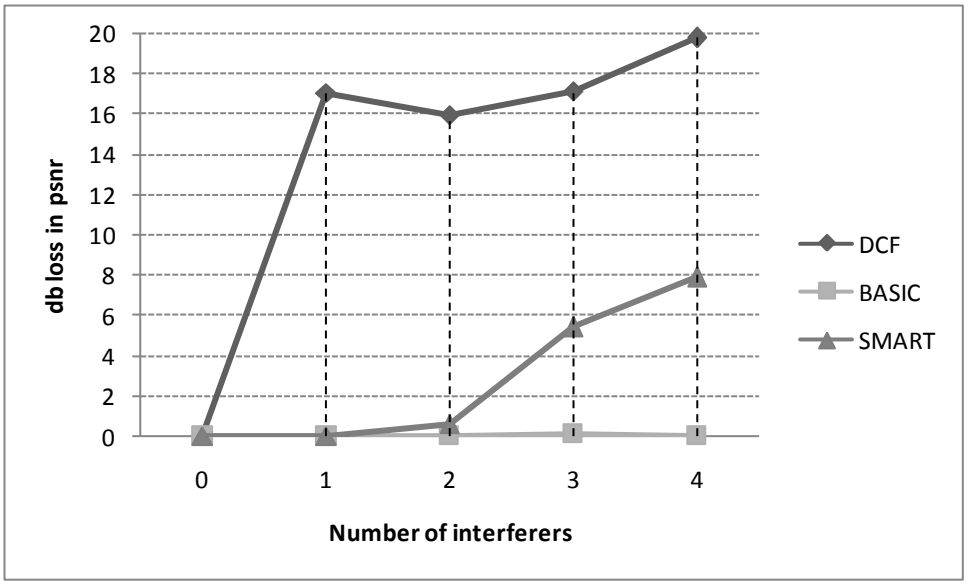

Figure 6.4 Peak Signal to Noise Ratio (PSNR) Loss in db
against number of interferers

In video quality comparison in Figure 6.4, DCF looses 17 dB in single interferer case and a maximum of 20 dB with all 4 interferers activated. As simple EDCA

suppresses all the data nodes, it provides the best picture quality, with below 1 dB loss in 4 interferer case. Our proposed algorithm, on the other hand, adapts to traffic condition by slightly decreasing video quality again to fairly coexist with the interferers. Although the suppression of data traffic, in 4 interferer case the 8 dB loss in PSNR value corresponds to an extremely poor quality video for most of the practical applications and especially when there are action scenes or rapid scene changes. That is the reason we changed our algorithm, so that every video packet is transmitted with a higher priority to save the video quality as much as possible.

There are also various other metrics for video quality comparisons like Universal Quality Index (UQI), Video Quality Metric (VQM), Perceptual Evaluation of Video Quality (PEVQ), Structural SIMilarity (SSIM) and Czenakowski Distance (CZD), but we selected PSNR, because it is currently widely used for objective video quality comparisons.

6.3 Implementation Setup

We have implemented the mesh networking functions together with both basic and smart prioritization algorithms on 802.11g APs. In our implementation, we used APs with 8 MB memory and 180 MHz system-on-chip MIPS CPU. An Atheros based wireless chipset, which fully supports EDCA in hardware level and six distinct hardware queues are used. One of the queues is assigned for beacon transmission while other four queues are assigned to four EDCA classes. As the wireless driver, we used a highly modified version of proprietary Atheros LSDK 5.0.28 driver. The operating system is based on Linux 2.4.x kernel with an updated and recent network stack. In full functional idle state with no traffic flowing, the system has about 200 Kb of free memory. Because of some implementation limitation of Linux kernel, a memory page of size 4 kb has to be allocated for each network packet, so the capacity of all queues together is less than 50 packets. Although our APs have very limited processing power and memory, they were able to function properly under heavy traffic.

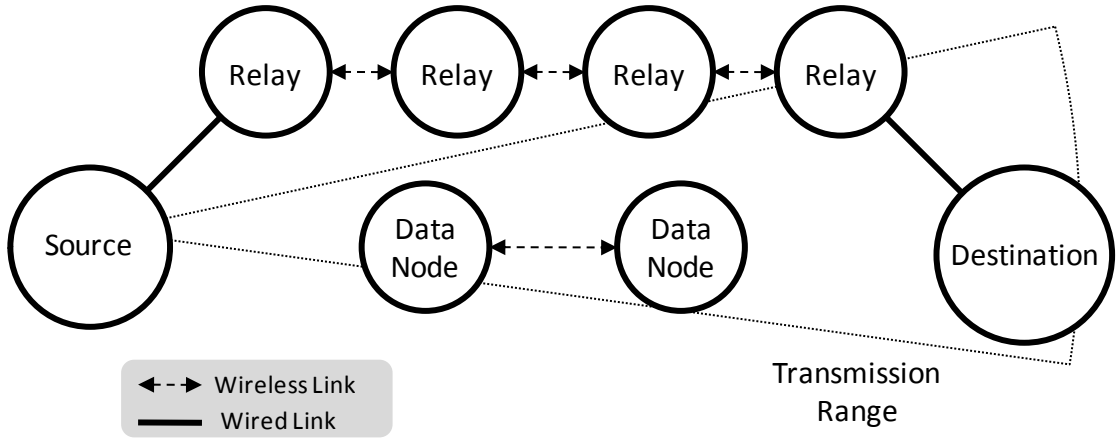

Figure 6.5 In our real test bed scenario, video traffic is transmitted over 3 wireless hops and there are two neighboring data nodes generating background traffic.

During our test runs, routing layer is disabled by adding static multi-hop routes to APs. This ensures that any delay or packet drop due to routing layer is prevented while the effects of multi-hop and background data traffic are investigated. As depicted in Figure 6.5, there are four APs, and three hops between the ingress and egress APs in our test bed. The source and destination clients are connected to the APs with wired links. All test results are average of five different test runs and it is ensured that the ambient noise/interference level remains the same during the runs.

6.4 Test Results

In our tests, we analyzed the performance of video streams under various traffic conditions. In our tests, we investigate the performance of DCF, basic and smart prioritization schemes. We also consider two variations of basic prioritization scheme, where all video packets are either classified as Voice (VO) or Video (VI) EDCA classes. Data traffic is always sent at the Best Effort (BE) class, which has the default priority of a regular DCF transmission. We tested video streaming performance against varying amounts of background UDP data traffic. The video is streamed at approximately 3 Mbps bitrate and the total channel capacity is about 14 Mbps. If no packet is lost, video consumes 9 Mbps alone over three hops. The upper limit of the theoretical residual capacity is about 5 Mbps. In the following figures, end-to-end delay of transport layer is measured and depicted.

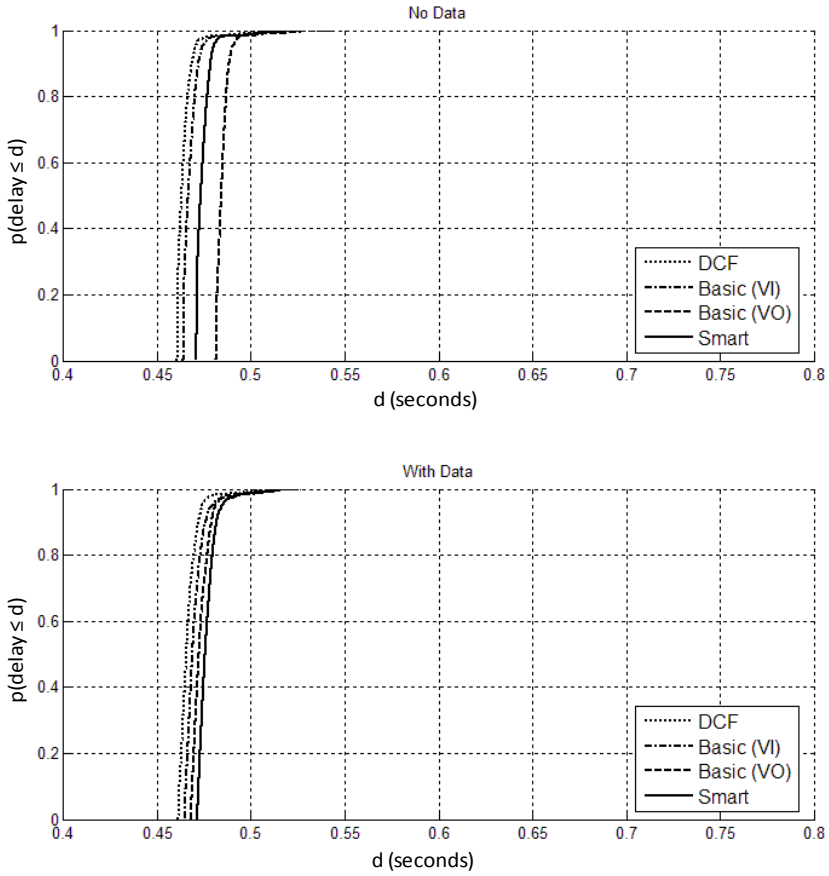

Figure 6.6 Cumulative end-to-end delay probability distribution at 3 Mbps of neighboring data traffic

Let X be a continuous real-valued random variable, its Cumulative Distribution Function (CDF) is given by the following equation:

$$F_X(x) = P(X \leq x)$$

Cumulative delay distribution of DCF, two basic classifications and smart classification at 3 Mbps of UDP data traffic is shown in Figure 6.6. With no data traffic and with data traffic below the residual capacity, delay distribution curves are very similar. The only differing factor is contention window sizes, which determines how long nodes should wait before transmitting. So, if the channel capacity is not reached, each transmission scheme accomplishes a lossless and low delay transmission resulting high quality video output.

Steepness of CDF curves means that variance of delay experienced by each video packet is very low. So if the channel capacity is not reached, any transmission technique can provide a low delayed end-to-end transmission medium.

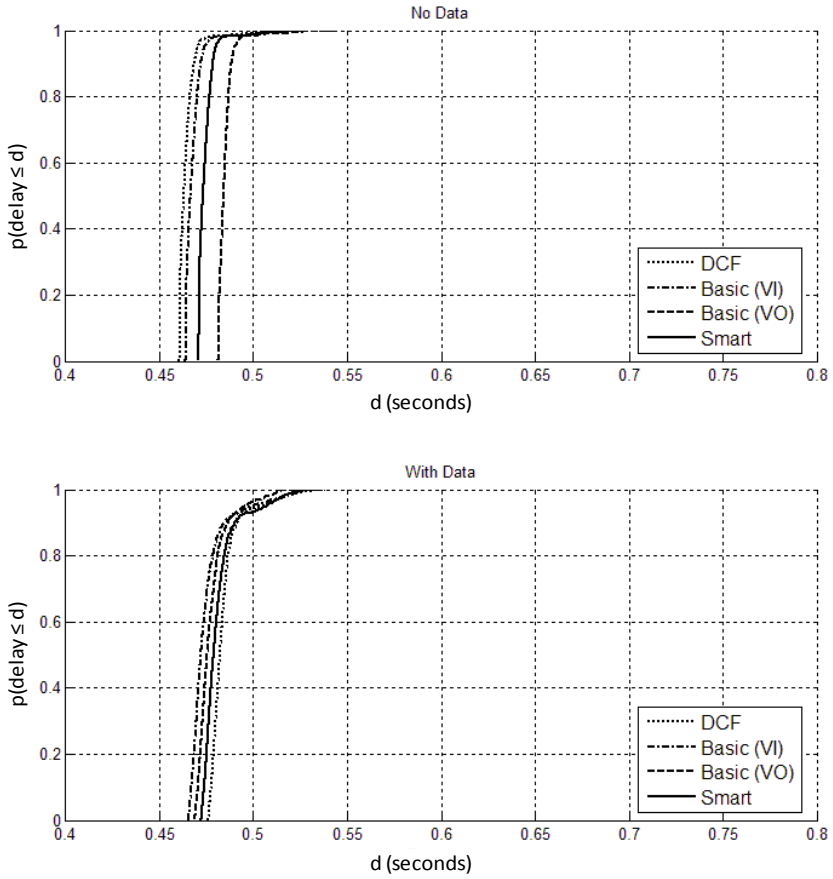

Figure 6.7 Cumulative end-to-end delay probability distribution at 6 Mbps of neighboring data traffic

In Figure 6.7, ambient data traffic reaches the residual capacity of the channel. In all prioritization modes, delay starts increasing. This is observed from the cut on the curves at higher delay values, but the behavior of DCF curves does not change. This is because of the buffers at intermediate nodes get full very rapidly, so video packets are discarded immediately. The number of video packets that can be transmitted end-to-end is decreasing, and the ones that are being successfully transmitted are the ones winning the contention. So their end-to-end delay does not increase.

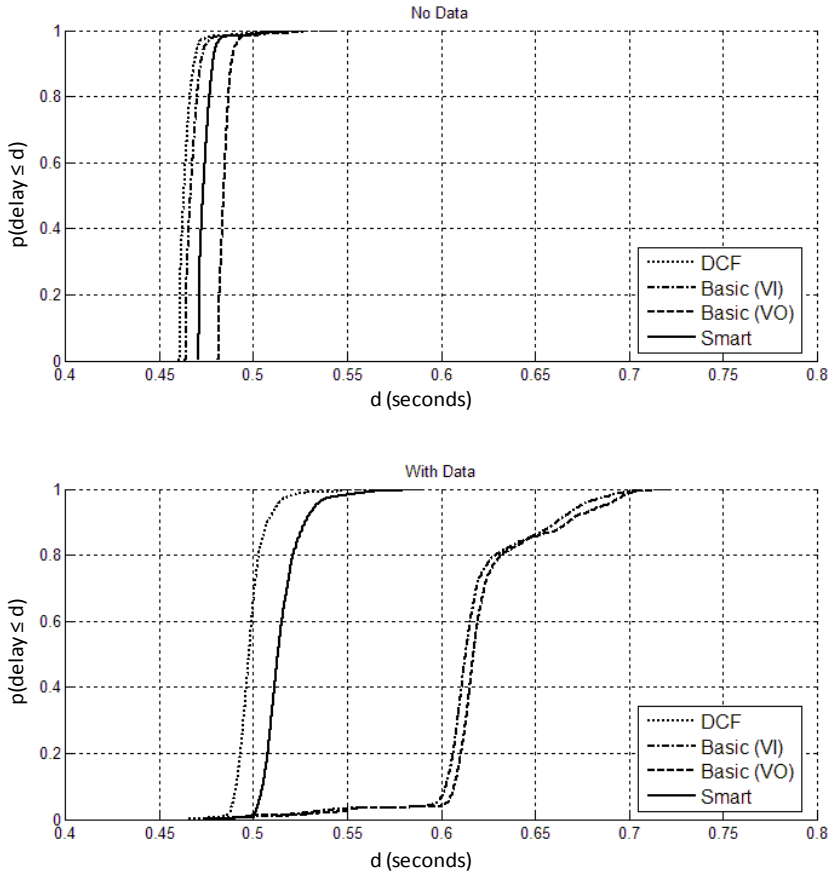

Figure 6.8 Cumulative end-to-end delay probability distribution at 13 Mbps of neighboring data traffic

In Figure 6.8, ambient data traffic is increased to 13 Mbps. At this setting, we observe that video packets transmitted with both Basic prioritization schemes experience a very high end-to-end delay compared to DCF and Smart prioritization schemes. DCF curves behave similarly to the delay curves at lower data rates, because this scheme drops video packets very rapidly.

In smart prioritization, video packets are enqueued to two different priority queues. So contention in each class stays low, so that enqueue rate is always lower than dequeue rate. Because smart prioritization stays stable, there are no dramatic increases in delay or drop rates.

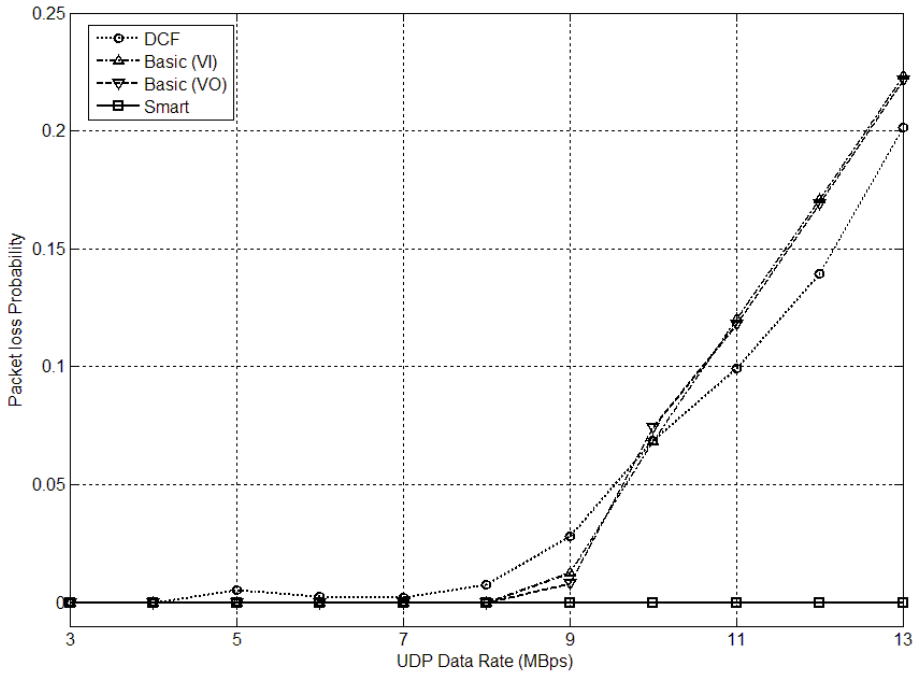

Figure 6.9 End-to-end video packet loss probability against varying amounts of UDP data traffic

In Figure 6.9, the video packet loss probability is plotted with respect to the contending data traffic load. If contending data traffic reaches the virtual upper limit of 5Mbps, DCF medium access scheme starts losing video packets. However, in basic and smart prioritization schemes, data traffic is suppressed, and there is no video packet loss until data traffic reaches 8Mbps. Hence, entire video is transferred without losing any information. When data traffic exceeds 8Mbps, the basic prioritization scheme starts losing video packets, whereas the smart prioritization scheme prevents any video packet loss until data traffic reaches 13Mbps.

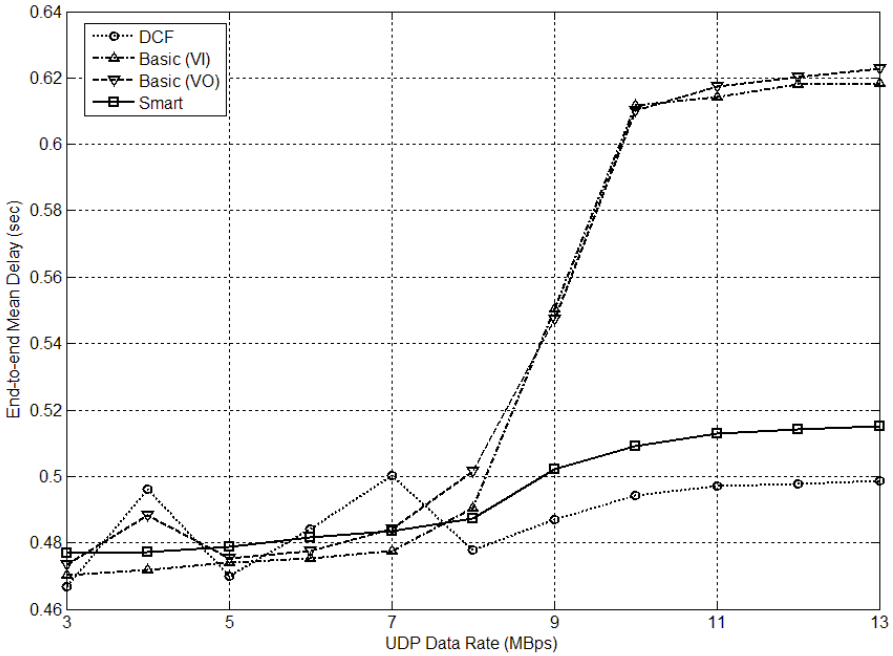

Figure 6.10 End-to-end mean delay against varying amounts of UDP data traffic

As observed in Figure 6.10, all transmission schemes including DCF have similar end-to-end mean delay until background data traffic becomes 8Mbps. Our test results indicate that DCF experiences high delay jitter, while other schemes experience slowly increasing delays. When background data traffic exceeds 8 Mbps, both of the basic prioritization schemes enter a rapidly increasing delay pattern until 10 Mbps of data traffic. In the meantime, both DCF and smart prioritization do not experience any rapidly increasing delay. However, unlike smart prioritization scheme, the main reason the packet delay of DCF is not increasing is due to the large loss of video packets, while successfully transmitting only a few.

In basic prioritization, fluctuations on CDF curves are observed. These fluctuations could be due to limited number of experiments. In basic prioritization, all video packets contend with each other over all three hops with the same high priority. After the amount of ambient data traffic passes a certain threshold, the contention becomes so high, that low CW values in high priority classes are unable to eliminate contentions of video packets resulting in increasing number of collisions. Basic prioritization becomes unable to transmit at a rate higher than the incoming video, thus

becoming unstable. So video packets get dropped or they experience a very high end-to-end delay.

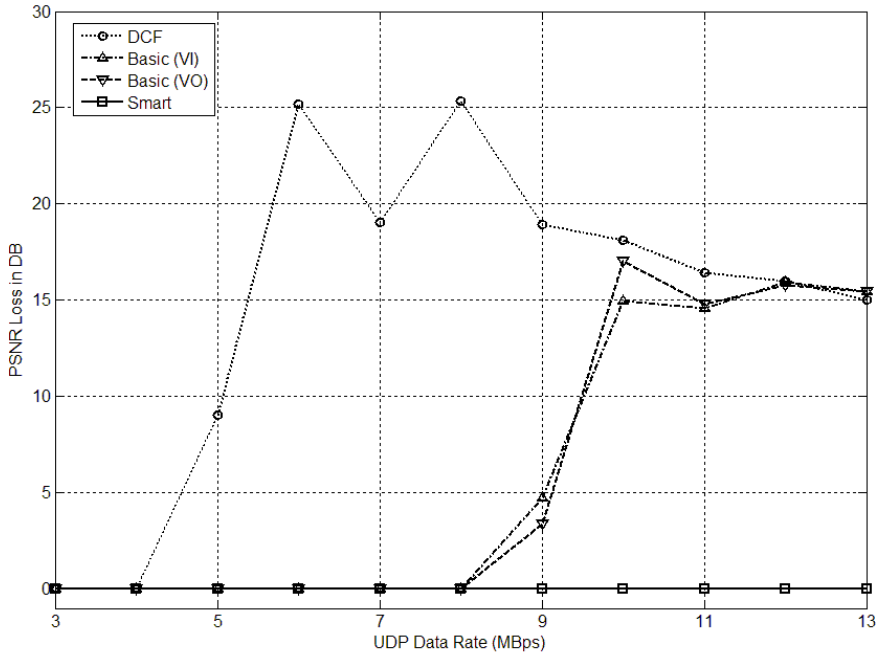

Figure 6.11 PSNR Loss against varying amounts of UDP data traffic

Next, in order to understand the video quality we considered PSNR loss of the decoded video. PSNR loss is defined as the difference between the PSNR value of the original and decoded video. In Figure 6.11, the PSNR loss for different schemes is given with respect to varying background data traffic. Consistent with packet loss probability given in Figure 6.10, with DCF, the video quality immediately drops approximately 9 db when the channel capacity is reached, and it further drops 20-25 dB when total traffic is increased beyond the channel capacity. Both of the basic prioritization schemes do not suffer from significant quality degradation until data traffic is 8Mbps, while smart prioritization maintains no quality degradation until the 13 Mbps background UDP traffic.

An interesting and also somewhat counter-intuitive result is that basic prioritization schemes suffer extensively by rapidly increasing delay and packet loss. This is actually because the transmission buffers of the intermediate nodes get full, and packets are delayed or dropped in the buffers. The APs used in the test have only 200 KB of free memory, which accommodates up to 50 packets. Sharing this small buffer

between different queues makes the actual available buffer size even smaller. In basic prioritization schemes, all video packets contend with each other with the same priority. Thus, with high background data traffic, the number of packets waiting in these queues increase faster than the effective service rate, which in turn causes video packets to miss their deadlines and get dropped. In smart prioritization, video packets are distributed to two different queues. Since every queue has a different priority, the packets in each queue contend only with each other. Therefore, buffers on each high priority class remain stable where enqueue rate is smaller than the dequeue rate.

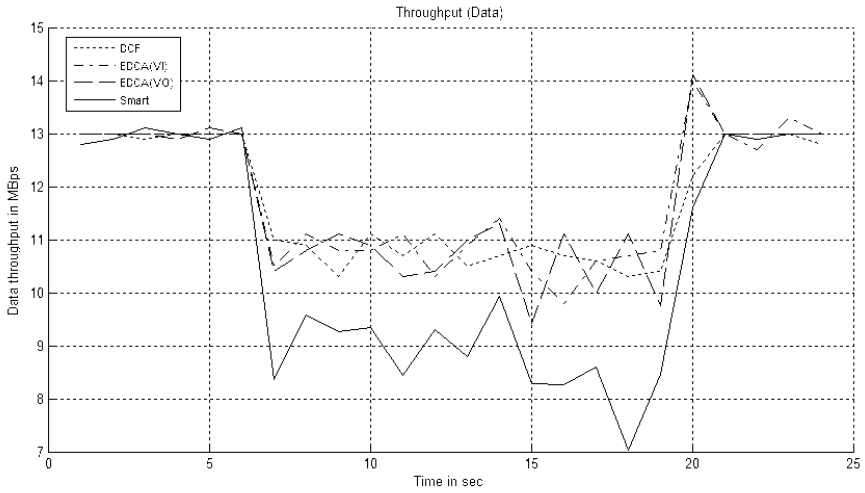

Figure 6.12 TCP data throughput with 3 hop 3 Mbps video streaming

Because of the lack of a proper testing tool, we could not be able to measure throughput of UDP data traffic, therefore we measured the performance of data traffic together with video by observing TCP streams in the same test environment.

In Figure 6.12, it is shown how a typical TCP connection suffers from the video transmission. Unlike other tests, we could not In this scenario, video is being transferred between 6^{th} and 20^{th} seconds. 3 Mbps video is transmitter over 3 wireless links. Both DCF and Basic prioritization algorithms maintain a relatively higher throughput than Smart prioritization. In smart prioritization, data traffic suffers from long delays and packet drops due to buffer overruns. Because packet transmissions will fail more often at higher transmission rates, TCP's exponential back-off algorithm will not be able to achieve throughput values like in DCF or basic prioritization.

7 Conclusions and Remaining Issues

7.1 Conclusions

WMNs make the wireless video transmission over 802.11-based networks more complicated. Because of the extra delay and packet drops imposed by multi-hop transmissions, the basic 802.11 DCF transmission scheme is not appropriate to support video transmission. For video transmission over WMN, the basic EDCA prioritization makes sense if large memory buffers are available on mesh nodes. However, if the resources are scarce, basic prioritization may suffer from high delays and packet loss in heavy background data traffic conditions. With our proposed smart prioritization algorithm, we overcome the additional delay and packet drop probabilities, while requiring very small buffer sizes on APs. The background data traffic is suppressed, but the utilization of the shared channel is much higher than the basic prioritization scheme, since there are fewer collisions.

There are still some remaining issues about video transmission using WMN that prevents adoption of this technology by actual IPTV service operators. In real IPTV services, video streams are transmitted using multicast packets, which are transmitted as broadcast packets with a fixed low bitrate in the wireless medium. Another practical problem is the lack of 802.1q Virtual Local Area Network (VLAN) support in WMNs and especially with integrated multicast support. IPTV service operators segment their network using 802.1q VLAN's for billing purposes. Before these problems and further unforeseen problems are solved, wireless video transmission will not be able to be deployed widely in IPTV services.

7.2 Remaining Issues

Video streams are commonly transmitted using multicast streams. Especially in wide area networks used for video streams like in IPTV networks, multicast is a prerequisite to minimize the load on the backbones. In 802.11 wireless networks, multicast streams are transmitted using a lower bitrate without waiting an ACK from the recipients. In pure 802.11g environment, this bitrate may rise up to 24mbps, as it is limited only to 1mbps in mixed mode. In either way, underlying rate selection algorithm and retransmissions are disabled for multicast video streams if the wireless equipment implements multicast support in the first place. A possible solution would be gathering information about which clients are interested in which streams and sending appropriate streams to interested clients as unicast. Solving wireless multicast problem in single access point case would be easy to handle compared to wireless mesh networks. In 802.11 wireless mesh networks, multicast distribution is a more complicated problem to be solved. Unlike the single access point case, in a mesh network, multicast information should be integrated within the routing algorithm. Every node joined to a stream has to receive every individual packet, so multicast information should be either distributed among every node or there should be a central controller.

Another problem to be solved for wireless mesh networks to support IPTV operation is that there is almost always an underlying internet service beforehand and a separate IPTV service added afterwards. Both services are transmitted over the same underlying network and they are separated using different 802.1q Virtual Local Area Networks (VLAN) for different billing plans set by the operators business strategies. In 802.1q VLAN's, IP packets include a VLAN field within the IP header that indicates to which VLAN this packet belongs. Every VLAN has a specific 12bit identifier for distinction. In IPTV case, video service, data service and other possible services are transmitted over different VLAN’s. This helps the operator to charge for video service and data service in a distinct and more appropriate way.

Supporting and managing VLAN's throughout a wireless mesh network is another problem to be solved to support a real IPTV service. To accomplish this efficiently, routing algorithm has to understand and find routes according to vlan settings. In

wireless mesh networks, which are identical to a layer-2 switches from the clients perspective, it is possible to omit the existence of VLAN's and drop inappropriate packets at the end points for unicast traffic, because VLAN's are defined in IP layer (layer-3), which is invisible at MAC layer (layer-2). In this approach, the mesh network will be busy a little more than required, as these packets may be dropped beforehand and not be transferred to the end point at the first place. A more complex derivative of supporting VLAN problem shows up at the multicast traffic. If the multicast transmission is supported within the wireless mesh network, it should be also bounded with VLAN's. One client connected to a vlan should not be able to join a multicast stream within another vlan.

There may be other problems required to be solved before high quality wireless video transmission can be done over 802.11 equipment and recently emerging IPTV operators can make use of wireless instead of cabling in houses.

8 References

[1] Ksentini, A., Naimi, M. and Gueroui, A., "Toward an improvement of H.264 video transmission over IEEE 802.11e through a cross-layer architecture." *Communications Magazine.* January 2006, Vol. 44, Issue 1, pp. 107-114.

[2] IEEE 802.11e., "Wireless LAN Medium Access Control (MAC) Enhancements for Quality of Service (QoS)." IEEE 802.11e draft 8.0, 2004.

[3] ITU-T Rec. H.264/ISO/IEC 14496-10 AVC, JVTG050, (VJT) ISO/IEC MPEG, ITU-T VCEG., "International Standard on Joint Video Specification." 2003.

[4] NVIDIA., Nvidia PureVideo. [Online] March 2007. http://www.nvidia.com/page/purevideo.html.

[5] IEEE 802.11s Working Group., [Online] March 2007. http://grouper.ieee.org/groups/802/11/.

[6] Chakrabarti, S. and Mishra, A., "QoS issues in ad hoc wireless networks." *IEEE Communications Magazine.* February 2001, Vol. 39, Issue 2, pp. 142-148.

[7] Shigang, C. and Nahrstedt, K., "Distributed quality-of-service routing in ad hoc networks." *IEEE Journal on Selected Areas in Communications.* August 1999, Vol. 17, Issue 8, pp. 1488-1505.

[8] Shiwen, M., et al., "Video transport over ad hoc networks: multistream coding with multipath transport." *IEEE Journal on Selected Areas in Communications.* December 2003, Vol. 21, Issue 10, pp. 1721-1737.

[9] Setton, E., et al., "Cross-layer design of ad hoc networks for real-time video streaming." *IEEE Wireless Communications.* August 2005, Vol. 12, Issue 4, pp. 59-65.

[10] 802.11, IEEE Std., "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications." 1999.

[11] 802.11n, IEEE., "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhancements for Higher Throughput Draft 3.0." 2007.

[12] Perkins, C. E., Royer, E. M. and Das, S. R., "Ad Hoc on Demand Distance Vector (AODV)." [Online] July 2000. http://www.ietf.org/internet-drafts/draft-ietfmanet-aodv-06.txt.

[13] Hiertz, G. R., et al., "Principles of IEEE 802.11s." *Computer Communications and Networks.* August 2007.

[14] OPNET Technologies., Making Networks and Applications Perform. [Online] 2008. http://www.opnet.com.