IMPROVEMENT OF ERED FEC MECHANISM FOR VIDEO TRANSMISSION OVER WLANs

Thesissubmitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Mansi Maini

(801333011)

Under the supervision of:

Dr. Anil Kumar Verma

Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

May 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Improvement Of ERED FEC Mechanism For Video Transmission Over WLANs", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Anil Kumar Verma* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature:

(Mansi Maini)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Anil Kumar Verma)

Associate Professor, CSED

Countersigned by

(Dr. Deepak Garg)

Head

Computer Science and Engineering Department

Thapar University

Patiala

(Dr. S. S. Bhatia)

Dean (Academic Affairs)

Thapar University

Patiala

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guide, **Dr. Anil Kumar Verma,** Associate Professor, Computer Science and Engineering Department, Thapar University, who has been very concerned and has supervised the work presented in this thesis report. He has helped me to explore this vast field in an organised manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to **Dr. Deepak Garg**, Head of Department, CSED and **Ms. Jhilik Bhattacharya**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my parents, friends and the almighty for showing me the right direction, to help me to stay calm in the oddest of the times and keep moving even at times when there was no hope.

Mansi Maini

801333011

ABSTRACT

Devices like laptops, PDAs, desktops, smartphones and other types of workstations are progressively shifting towards WLAN technology due to the ample advantages it offers like mobility, increased scalability of network, cost effectiveness, availability of internet even in public places and high network speeds without cumbersome wiring. With the advent of wireless technology, a lot research focus has been shifted towards improving the performance of WLANs for transmission of text, audio and video files. In particular, the sharing and transmission of multimedia files over WLANs is becoming commonplace as more and more communication is occurring via technologies like videoconferencing, television broadcasting, video playback and voice over internet. Video transmission in particular presents a challenge in juggling the quality of service parameters with the timeliness of delivery of the video.

WLAN typically suffers from low QoS parameters as compared to wired networks. WLANs are noisier, have more delay, higher packet loss rate and are more prone to interference due to overlapping frequencies and physical obstructions. One of main drawbacks of using WLAN is that it suffers from high packet loss rates. This error rate is decreased by using error detection and correction codes. One of the most common schemes used to correct the error is Forward Error Correction (FEC). Schemes like Constant Error FEC, Adaptive FEC and Random Early Detection FEC are commonly used in WLAN but they all fall victim to burst errors. Burst errors are errors which corrupt or lose packets in a continuous sequence. In this scenario bulk of packets are lost in a sequence making it very difficult or even impossible for the packets to be reconstructed at the receiver's end even with the help of FEC. Thus to overcome the effect of burst errors in transmission, this proposed technique tries to incorporate the concept of interleaving by randomising the position of source packets and the redundant packets produced by the FEC scheme.

Keywords: FEC, ERED FEC, Video Transmission, WLAN

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Multimedia is redefining the way we communicate with each and share our thoughts and ideas. gone are the days when it was imperative to be physically present to attend a conference or a lecture, when we had to watch our favourite show at a particular time, when talking to someone on the phone entailed only hearing their voice. The evolution of networks and reduction in hardware cost has enabled the data transmission to include multimedia files in addition to text files. While it is a known fact that transmission of such files is faster and more efficient in wired networks rather that in wireless networks; yet the use of WLANs is becoming more prevalent. This can be attributed to its tremendous advantage of mobility. It is getting increasingly difficult to tie a group of people to one location and get them connected through a wired network. WLANs are more accessible and have remote connectivity, therefore theyare able to connect people sitting at opposite ends of the world.

1.1 MOTIVATION

Video streaming has become one of the most useful and important applications to be used over the Internet. With applications varying in fields such as voice over internet, teleconferencing, broadcast television etc, video streaming is rapidly gaining importance in the field of information and data communication. Applications that require video transmission over the wireless network demand that the video be delivered at high speed, in a timely fashion and with high reliability. Now, the wireless local area networks (WLANs) are well equipped to transmit videos at a high bit rate but the quality of service (QoS) of WLANs is still a challenge. The wireless channel by nature is an unreliable one and is prone to falling victim to various distortions like scattering, attenuation, external noise, multipath interference etc. [1]. These distortions cause the wireless network to become an unreliable and error prone network.

For video streaming to become completely error free, the videos need to be streamed via a reliable transport protocol like TCP. But streaming a video via TCP is not always a viable option because TCP does not give preference to delivering a video on time. Rather TCP trades timeliness for an error free delivery. But streaming real time video gives

paramount importance to timely arrival of video packets and it can cope with slight errors in the video packets and overcome them by using error detection, correction and concealment codes. One of the most efficient and commonly used methods for error detection and correction is Forward Error Correction (FEC). FEC is a technique used to detect and correct the errors occurring in data transmission over unreliable and noisy channel. FEC works by adding redundant packets to the source packets, such that loss of a few packets in the whole block will not adversely affect the video quality and the receiver will be able to reconstruct the entire block with the help of available source and redundant packets.

While FEC is a very productive mechanism and can help lowering the packet error rate dramatically yet can be rendered inefficient due to burst errors. Burst errors are errors which occur in a continuous manner and afflict the packets in a contiguous sequence. WLAN is particularly vulnerable to burst errors because when the channel conditions for wireless channels deteriorate, they deteriorate for a long distance or a long period of time. Due to this the packets being delivered in that period of time are affected and are hence lost, incorrectly sequenced or corrupted. To overcome this, a lot of research work has been focused on designing efficient FEC schemes and implementing them for various applications like real time streaming, multicasting and VoIP. But all the FEC schemes are liable to burst errors.

This is where the importance of this study stems from. The eradication of burst of errors will dramatically improve the video quality of the video streamed over wireless networks. Even if complete eradication of burst error is not possible, still the effects of these errors can be minimised by taking appropriate steps so that the packets lost during burst errors can be recovered [2]. The motivation of my research came from coming across a variety of FEC mechanism, which catered to a variety of aspects of video streaming, but fell short on dealing with burst errors. Their performance, throughput and efficiency suffered because their mechanism did not employ a technique to combat the effect of burst error. High frequency of burst errors also increases the packet error rate and decreases the quality of the video being streamed. A low quality of video is virtually as useless as a video delivered late. Even though real time applications favour timeliness over QoS, yet completely ignoring the QoS can lead to disastrous results at the receiver's end. To deal with the problem of burst errors, this thesis has suggested the idea of using interleaving techniques to randomize the distribution of redundant packets and distribute them evenly over the frame so that even if burst errors occur, their effect can be mitigated by the surviving redundant and source packets.

1.2 CHALLENGES

The area of streaming videos over the wireless network in real-time is fraught with challenges. Managing the requirements of real time video streaming along with the capabilities of WLAN is a challenging task. While WLANS have undeniable advantages of mobility, ease of access, connectivity of multiple devices without additional cost and scalability, it falls short on the QoS front. It is a known fact that wireless networks experience less speed, more delay, more packet loss and overall lower standard of QoS parameters. But the advantages of WLANs far outweigh its disadvantages, thereby making it the preferred network for communication. Some of the challenges faced while dealing with wireless networks are [3]:

- High interference is experienced in the WLAN networks causing inflation in the packet error rate. This interference occurs from various devices that use and share the same or neighbouring spectrum.
- Large packet loss occurs due to signal fading. The signals of a WLAN travel in open and are hence more susceptible to fading. The long distances between the APs and the obstructions caused by buildings and other objects cause the signals to be rerouted and they fade in this process.
- Transmission of multimedia requires compression of audio and video data. Therefore it is critical that the compression and decompression rates of the data should be high, thereby assuring high video and audio quality at the receiver.
- WLANs are more liable to have burst errors as compared to wired networks. This necessitates the use of error detection, correction and concealment algorithms. While these algorithms are efficient in removing errors and producing better data quality, they produce a lot of overhead and processing latency.

The main challenge of wireless communications is to lower the error rate to ensure high quality video transmission. High error rates are generated when the packets are delayed, rerouted to incorrect destinations or corrupted. The error rate is controlled and lowered by using error correcting and concealment codes. Forward error correction (FEC) is one of the most widely used mechanisms for error correction. In the scenarios when timely delivery of a video is paramount, the FEC schemes help in providing reliability and high video quality by sending extra packets called the redundant packets which will help in

ensuring that if some packets are lost then the whole frame can be reconstructed with the help of redundant packets.

Though FEC is has many advantages like being media independent, having easy computation and implementation, being fast and optimum for real time applications and have high efficiency in packet recovery, yet it suffers from many drawbacks [4]:

- The overhead cost in implementing FEC can make the whole transmission scheme a lot more expensive than it was originally.
- Special protocols need to be designed for computation, generation and implementation of FEC redundant packets.
- The transmission of FEC packets can add to the already congested network and can cause severe network delays and packet losses. Due to this, it is important to find an optimal FEC rate which can manage heavy traffic congestion and still transmit enough redundant packets to ensure packet recovery.
- The mechanisms used to finding a reasonable FEC rate concentrate on only one aspect of fixing the redundancy rate, whereas it is direly required that a culmination of factors should be considered before deciding the redundancy rate.
- Several of the FEC mechanisms are adversely affected by burst errors and are able to do very little when the error guard encompasses the redundant packets.

All these existing challenges have prompted the researchers over the years to find solutions and techniques that will overcome these disadvantages and form a solution such that it overcomes all the above problems all the while keeping the overhead to a bare minimum. The focus of my study will be centred on trying to minimize the effect of burst errors in video streaming over WLANs.

1.3 IMPORTANCE OF THE STUDY

The proliferation of wireless devices has prompted a revolution in the way we connect and communicate with each other. Communication is no longer bound to just calling each other or sending a quick text. The realm of communication has expanded to having live videos streamed directly to our wireless devices in the form of broadcast television, teleconferencing, virtual presence, voice over internet and many other such applications. Advent of wireless technology has ensured that the future holds a special place for IP based applications such as video streaming, ecommerce, medical procedure training, distance

education and real-time surveillance. All these applications require real-time video transmission over WLAN. Advantages of streaming videos over wireless channels are [5]:

- It has brought around the trend of bring your own devices (BYOD) which has resulted in increased productivity of employees and reduced the cost of providing hardware borne by companies.
- Increased mobility of networks has made communication and transmission of audio/video files more convenient.
- Applications like VoIP, teleconferencing and virtual presence have made face-to-face communication really easy and convenient such that two people sitting on the opposite ends of the world can communicate with each other and that too at a very nominal rate.
- Live streamed videos enable various applications like distance education, real-time surveillance, procedure control and live television broadcast.

The significance of my study stems from the fact that despite a rapid rise in the use of video steaming in the wireless media, the video quality suffers a great deal due to packet loss. This packet loss is due to a number of reasons, with the most prominent reason being burst errors corrupting the packets in bulk and rendering the FEC mechanism useless. The FEC mechanism is a great way to control the errors occurring in the packets but this technique is inefficient when burst errors occur in large quantities and the redundant packets are also lost along with the source packets. This is why it is essential to find a technique which can combat the effects of burst errors without causing too much overhead.

1.4 THESIS OUTLINE

The thesis is divided into chapters giving the overview, presenting the research conducted to conduct this study, stating the problem encountered with the existing system and describing the simulation and results. Chapter 2 gives the overview of what the wireless networks are, their architecture and components, the standards established and followed for their implementation, explanation of video streaming, the evolution of compression standards used for audio and video files and the protocols followed to achieve video streaming.Chapter 3 presents the literature survey conducted while carrying out the study for the thesis. This chapter discusses the challenges faced while transmitting video over WLAN, explains the concept of error detection and correction, the methods in which error control can be achieved

and the basic concept and protocols of automatic repeat request (ARQ). It then explains the concept of forward error correction (FEC) and discusses the variations in the basic scheme that have been proposed so far. Chapter 4 evaluates the problems faced by the FEC mechanisms so far and tries to outline a solution for one of the major challenges faced by the FEC, that is, errors that occur in a burst. This chapter also outlines a few objectives that are hoped to be achieved through the proposed scheme. Chapter 5 presents the simulators used to carry out the study, the environment created for the study, the approach proposed and the components of the simulations. Chapter 6 shows the results of the simulated environment and the results achieved by mathematically solving the proposed scheme. These results are then compared to some of the popular FEC mechanisms and analysis is conducted for parameters like the traffic, FEC rate and video quality. Chapter 7 concludes the study by providing the summary of the study carried out and the findings. Future scope of the study and some proposed research areas are suggested and discussed as well.

CHAPTER 2

OVERVIEW

Wireless networks are networks that do not require cables for connecting the devices to the internet. Wireless networks can be wireless cellular networks, wireless local area networks, space networks etc. WLANs are networks that connect multiple devices using the radio frequency spectrum for communication. The wireless networks began as high-costing and difficult to implement networks that would only be employed if the wired LAN was not an option. But in the recent year the cost of hardware and infrastructure have lowered so much that use of wireless networks is now standard.

2.1 ARCHITECTURE OF WLAN

Architecture of WLAN refers to the components that are employed in the deployment of the network, the way those components are set up and the way the components interact with each other to provide seamless communication in the network. The basic architecture of WLAN consists of the following components [6]:

- Medium
- Stations
- Base Service Set
- Extended Service Set
- Distribution System

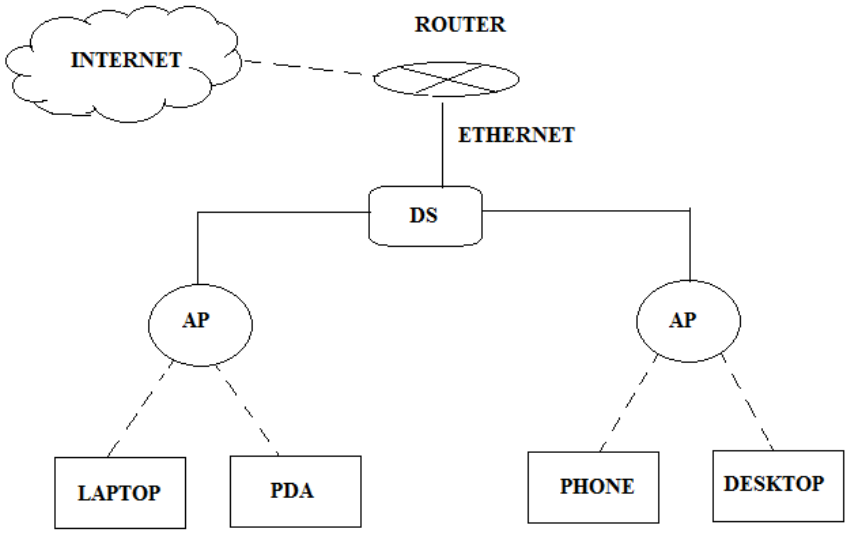

Figure 2.1: Basic Architecture of WLAN

Medium

Medium refers to the channel chosen for carrying the data for communication. In the field of data comm8unication, medium can either be guided or guided. The guided medium has a definitive path laid out by cables connecting various devices, whereas the unguided medium does not have a definitive path and depend upon microwave or radio wave frequencies to carry its signal. In the case of wireless networks, the medium is an unguided one and for WLANs the unguided media chosen is the radio frequencies.

Stations

Stations are all the devices that have the capability of being able to connect to a wireless medium. Such devices are often connected with each other to form the building blocks of the wireless network. All stations have an in built wireless NIC. A wireless NIC is a network interface card that connects a computer network that communicates via radio waves rather than via Ethernet. Generally stations are categorised as either wireless Access Points (AP) or as wireless clients. AP is a device which enables wireless connection between devices that can connect to a wireless network and the devices that cannot connect to a wireless network. It generally gets connected to a router through a wired network or it can even be an inbuilt component of the router itself, thereby enabling the router to be used as a device that can connect directly to a WLAN. These routers with inbuilt APs are called wireless routers and they behave like base stations for the wireless networks and are responsible for transmitting

and receiving the signals sent by wireless devices so that communication can occur. The wireless clients are the personal devices like laptops, desktops, smartphones and other workstations which are equipped with a wireless NIC and can hence communicate with the AP. The wireless clients are generally mobile devices that can be carried around and their positon can vary all across the globe but this is not a requisite for being a wireless client. Wireless clients can be stationary devices as well, just as long as they have a wireless NIC. Most of the devices these days come with an inbuilt wireless NIC.

Basic Service Set

Basic Service Set (BSS) is a small cluster consisting of the set of all stations that can communicate with each other. BSS operates in two modes; infrastructure BSS and independent BSS. The infrastructure BSS entails that in one BSS there should be once AP and all the clients that are connected to that AP. Two infrastructure BSS can communicate with each other through their APs and the clients of one BSS can send data to the client of another BSS. The APs in the BSS act as routers, transmitting signals to the APs of other BSS. The independent BSS works in the ad-hoc network and it entails that the BSS does not contain any AP. The independent BSS contains only client devices in an ad hoc mode and these clients do not need an AP to connect with each other. Every BSS is identified by a unique number called Basic Service Set Identification (BSSID). The BSSID acts as the MAC address for the AP of that particular BSS.

Extended Service Set

Extended Service Set (ESS) is a culmination of two more BSS which are connected to each other for communicating. In every ESS, the APs of the member BSS are linked to each other through a distribution system. All the member BSS of a single ESS have the same value various outgoing properties like the security certificates, the connection information to an Ethernet and all the other information that is required by the logical link layer. Each ESS is identified by a unique identification number called the service set identification (SSID) [7]. The SSID is a 32 byte number which is given to each ESS such that a network can be distinctly be referred by that number.

Distribution System

A distribution system (DS) is a system which allows all the APs present in an ESS to be get connected to each other. DS are used to increase the area that can be covered by a particular

WLAN between mobile clients [8]. The advantage using a DS is that the APs don not need to connect to backbone Ethernet individually to get connected to a wired network. This also means that the Ethernet is less crowded with devices that need to be connected to it. DS also make it easier for various ESS to get connected to each and to form a bigger network. One of the prime advantages of ds is that the MAC address of the client stations are preserved even when they are travelling from one BSS to another. Infact as long at the data sent from one client to another remains within an ESS, the MAC address of the source remains preserved.

2.2 Types of WLAN

WLANs follow the set of protocols defined by the IEEE 802.11 standards. According to these standards, the WLAN can be deployed in one of the following two ways:

- Infrastructure mode
- Ad hoc mode

Infrastructure mode

Majority of WLANs are deployed in the infrastructure mode. In this mode, a single base station connects all the wireless clients in a particular area and acts as a hub for those clients. This base station is connected to Ethernet through guided media and acts as the intermediator between the wireless devices and the wired network [9]. This base station behaves like a fixed wireless access point and is generally in a particular area and has defined range. The base station is then responsible for providing service to all the clients that are located within that range. In bigger networks spanning across a large area, the number of base stations may increase and the clients that have access to two or more access points can then choose between the available points depending upon which access point is able to give the best quality of service. The infrastructure mode follows a client-server type of setup where the access point is providing service to the other wireless devices.

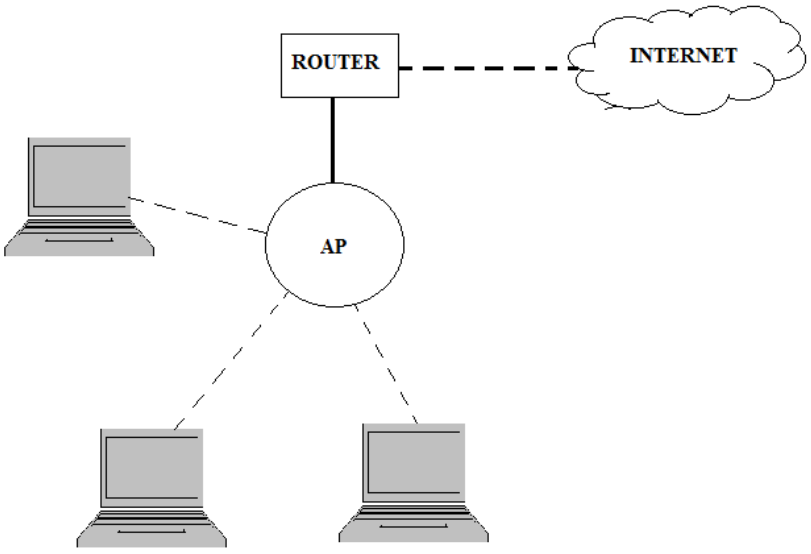

Figure 2.2: Infrastructure based WLAN

Ad hoc mode

The ad hoc network works in a peer-to-peer environment where all the clients communicate directly with each other. The ad hoc mode does not support the use of access points and the link between all the stations in an area is direct. In this type of communication, all the clients are treated like nodes and the delivery of message is conducted by sending the data from one node to another [10]. These nodes do not interfere with the message, rather they are employed just for relaying the message from source to destination. Bluetooth, MANETS, VANETS and FANETS are prime examples of ad hoc wireless networks. The ad hoc networks have a decidedly less smooth routing and connectivity as compared to the infrastructure wireless networks because of the constant mobility of the clients and the absence of a proper infrastructure. The ad hoc networks are particularly useful in the areas where the stations are constantly moving and changing their locations drastically.

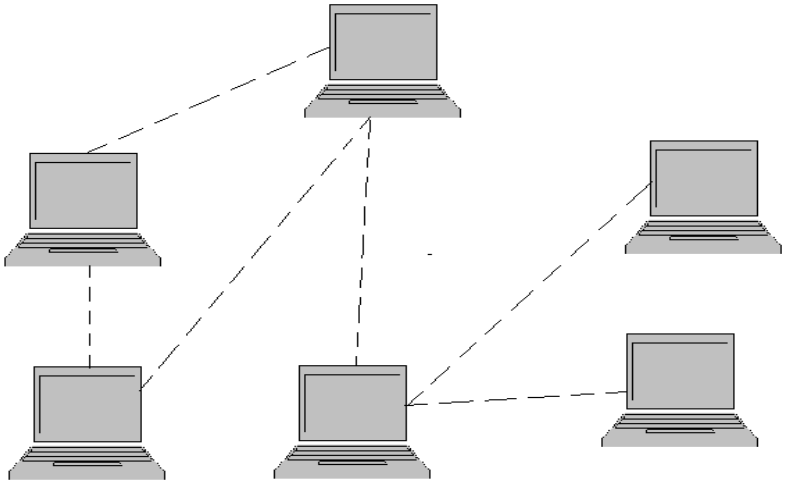

Figure 2.3: Ad hoc WLAN

2.3IEEE STANDARDS FOR WLAN

IEEE 802.11 is the standard allotted for the protocols and standards proposed and followed for the functioning of WLANs. It was first proposed in 1997 and since then amendments to the basic proposition have been made to update and keep up with the emerging technology [11]. These standards are defined, revised and maintained by the LAN/MAN wing of the IEEE society. These standards are applied to the Media Access Control (MAC) Layer and the physical layer components, thereby defining the complete functionality of these layers in the case of WLANs. The frequency bands employed for WLANs are 2.4, 3.6, 5 and 60 GHZ. The main standards for the WLAN are 802.11 a/b/g /n and ac.

802.11 a

The first amendment to the original 802.11 was suggested in 1999 and was called 802.11 a. The changes in this standard were made at the physical layer, where the medium was fixed to be OFDM waveform at the frequency of 5.8 GHz. The data rate of transmission changed from 1.5 to 54 Mbps as compared to the original standard. This standard operated at a high frequency as compared to the other standards and therefore had shorter wavelength. But shorter wavelength isn't an issue for networks confined within a small area. This lead to extensive use of this standard in the corporate and institutional set up where short wavelength can be ignored in the favour of higher transmission rates. The band of 5 GHz is not very crowded thereby decreasing the contention rate of this standard, but the overall range is less

than other standards. It has also been noted that since it has lower wavelength, the waves of 802.11 a are easily absorbed by walls therefore the area of coverage of this standard is not as wide as the other standards.

802.11 b

IEEE 802.11 b was the next updation to the original standard. It kept the MAC layer protocols the same as the original but it made a difference to the way the modulation technique was applied. It made use of the complimentary code keying modulation technique in the 2.4 GHz frequency band. The data rate defined for the transmission and reception in this standard is 11Mbps. This is a substantial boost in throughput as compared to the rate achieved in the original standard. This boosted the popularity of this standard and it started being used as the standard technology for WLANs. A perceptible drawback of using this standard is that it experiences a lot of interference from other devices which are being operated at 2.4 GHz frequency band.

802.11 g

This standard was proposed in 2003 and was a combination of 802.11 a and b. It works on the 2.4 GHz frequency band but uses the modulation technique of OFDM for transmission. It gives the maximum bit rate that can be provided by the physical layer, that is 54 Mbps but this rate does not include the forward error correction codes. The average rate generated by this standard is around 22 Mbps after accounting for the FEC codes. While this standard gave better data rates than 802.11 b,its throughput was less than 802.11 a. This was because the devices that were operable for 802.11 g were designed in such a way that they should be backward compatible with 802.11 b. This caused a lot of legacy code issues and the performance of the throughput was further degraded.

802.11 n

This standard was proposed in 2009 and was designed in such a way that it could operate on 2.4 and 5 GHz frequency bands. The purpose of this amendment was to improve on the previous standards by increasing the throughput and the transmission rates to 600 Mbps. Although the theoretical data rate has been suggested at 600 Mbps, the actual maximum throughput varies greatly from 78 Mbps to 288 Mbps depending upon the number of antennas used and the bandwidth it is utilizing. The proposal also aimed at standardizing the use of multitudinous antennas and frame aggregation. The use of multiple incoming and outgoing

antennas ensured that unique data can be carried simultaneously in separate data streams in the same channel. This increases the bandwidth capacity and the overall throughput. This phenomenon is achieved by employing spatial division multiplexing, which encodes and multiplexes various streams of independent data in a spatial manner such that they can propagate within a single bandwidth without interfering with each other. Frame aggregation refers to binding the service data units and protocol data units with the data being sent at the physical layer. This is required because even though the maximum throughput at the physical layer is quite high, it is not that high at the user's side because of the overhead caused by the headers, acknowledgment frames, contention settlement and frame spacing. Frame aggregation helps in minimizing the overhead time and increases the throughput at the user level.

802.11 ac

The new standard proposed came out in 2013 and was primarily built upon the previous 802.11 n standard. This standard proposed that the number of data streams should be increased from 4 to 8 and the width of each data stream should also be increased from 40 MHz to 80 MHz in the 5 GHz band. This proposal aimed to increase the number of data streams in the band and to increase the data rate of the transmissions. The increased number of data streams is handled by using a higher order of modulation in the spatial division modulation. The proposed standard supports greater number of data streams for the user and the sender supports higher density of modulations and extended channel binding. Significant changes were made to the MAC layer protocols and specifications to support the all the changes.

2.4VIDEO STREAMING

Multimedia refers to the amalgamation of different content types in a single message to be transmitted. Content types include text, audio, video, images, animation and user interactive media. The dawn of wireless technology with higher data rates and wider bandwidths available for media transmission has enabled easy and fast exchange of multimedia over the WLANs. The streaming of media means transmission of multimedia in a way that the receiver is constantly receiving the sent content while the streaming server is sending the multimedia. Streaming of videos in particular means that the receiver is receiving the video at the same time as the sender is sending it. This type of delivery method is known as

streaming. The whole video file is divided into small blocks and each block contains a number of packets that are segmented into frames. Generally the transmission of videos entail that the video is deconstructed at the sender side while being transmitted and all the packets are delivered to the receiver via routing protocols, then they are reassembled at the receiver end before being presented to the user. Video streaming allows the client to begin viewing the video file even before the whole file has been received by the receiver.

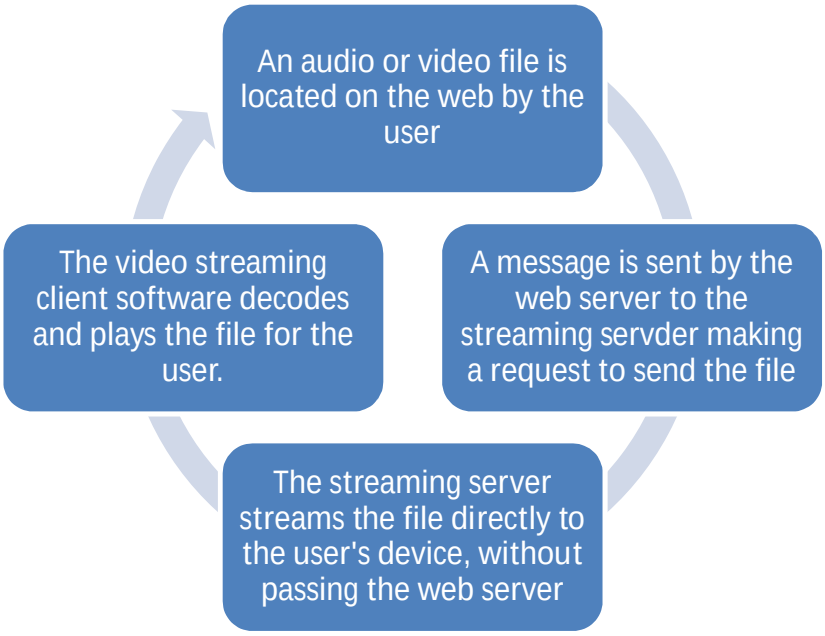

Figure 2.4: Methodology of video streaming

Live streaming of media has been around since the early 1990s when a few researchers at a university experimented with streaming a band. But video streaming has made very slow progress over the years because of the limitations of available bandwidth and limitations in the CPU power [12]. Once the constraints of the weak CPU power and underequipped operating systems were removed, the limitations in the network power became apparent. The bandwidth of the network and the data rates provided by them proved to be another obstacle in the transmission of the multimedia. The transmission of multimedia requires high data rate, otherwise the file can take many hours to get downloaded or streamed. As the improvements in the protocols for wired and wireless networks came into existence, the higher data rates also improved and sending and receiving multimedia became an everyday routine rather than a novel idea. For a very long time the only providers of video and audio content were television and radio broadcasters and we viewed their content via our televisions and radios. But in the recent years the

concept of multimedia viewing has evolved from traditional television and radio to viewing all the content on your personal computing device like laptops, desktops, smartphones and other various workstations. In fact, the control of the media to be distributed no longer lies solely with the television broadcasters. The advent of video streaming has enabled everyone with a recording camera and an internet connection to share their own multimedia content over the internet. This technology is more peer-to-peer (P2P) oriented and has allowed all the devices to behave like streaming servers to distribute their media.

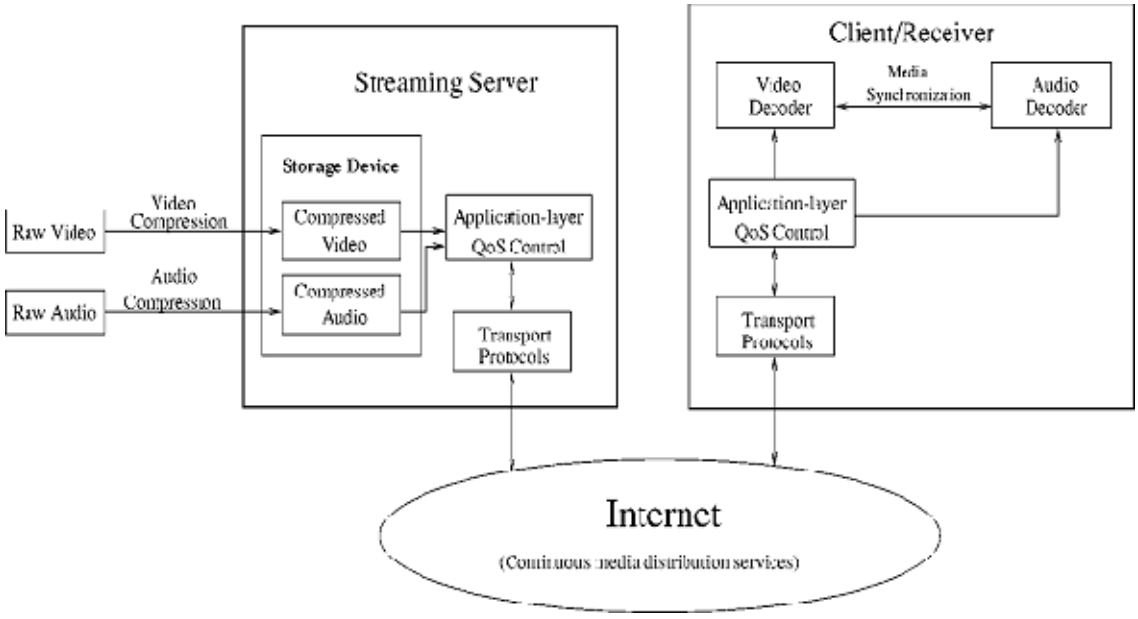

Figure 2.5: Architecture of Video Streaming

2.5 VIDEO COMPRESSION STANDARDS

Data compression refers to the process of taking the data to be delivered and encoding it in such a manner that that the encoded data had lesser bits than the original data. Data compression is also referred to as source coding because when the data is being transmitted, the sender is responsible for encoding the data and reducing the length of the data, hence the compression occurs at the source. Data compression is one of the most effective methods to save storage space and transmission and reception time of the data. There are many advantages of using data compression [13]:

- It consumes less disk space, creating space for more data to be stored in the same amount of space.

- The data transfer rate gets incremented, thereby decreasing the load on the network to transmit heavy files.
- It is a good solution towards reducing congestion on the network.
- If the file size has decreased, then the cache memory of the buffer can store more data in it, thus the hit rate increases, thereby decreasing the time required to display data.
- It can be used for distributing software on portable memory devices, for compressing data in hard disk and other memories and for faster and cheaper data transmission.

Data compression can either be lossless or lossy. Lossless compression is based upon conducting statistical analysis on the data and then eliminating redundancy. In this method, the compression does not actually eliminate any information; rather it bunches together the information that is being repeated and encodes it in a less redundant fashion. The main advantage of using lossless compression is that it doesn't lose any information and the whole information is completely reconstructed at the receiver's side. Lossy compression is based on the exact opposite technique than lossless compression. In the lossy technique, the algorithm makes assumptions about the data and removes the data that seems non-essential to the algorithm. This technique works on the principle that human eyes perceives information in a certain way and the human brain can ignore a lot of missing data and still form the perfect picture. This enables the lossy algorithm to filter such information and keep only that data which is necessary and are particularly successful in compressing and transmitting images, videos and music files.

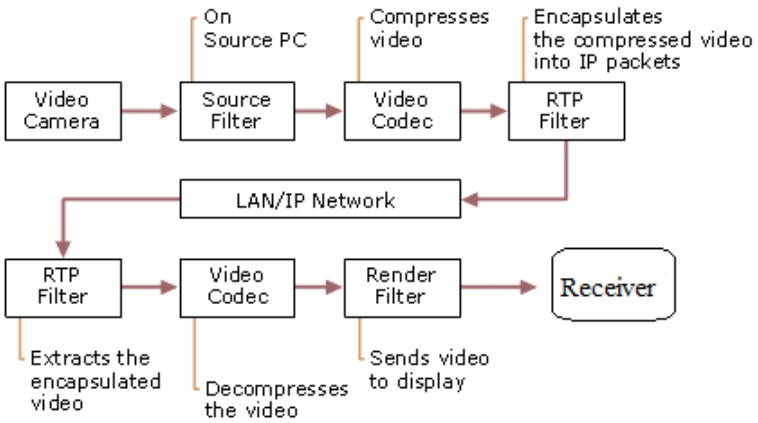

Figure 2.6: Video Compression Methodology

Video compression is one of the key aspects of data compression. Video compression follows a particular format while compressing a video file. This format specifies how the content of the video should be represented for storage and transmission, how it should be deconstructed and reconstructed and at what rate should the compression occur. A software that is capable of converting a video file from format to another and is capable of compressing and decompressing a video file is called a video codec. Video codecs are generally used in combination with compression algorithms to compress the images and frames in a video. Video compression algorithms use a combination of spatial and temporal compression such that when the images of the frames are compressed the rate of the frames and the motion carried out by the images is compensated for [14]. In addition, the audio of the video file is also compressed in parallel with video compression. Though the two processes are different and occur simultaneously but in separate data streams, they are combined at the time of transmission and reconstruction such that the whole video file appears with all the frames and the audio intact. Majority of the video compression algorithms are lossy compression because although lossless compression provides better data rate than uncompressed video file, yet it is far slower than a lossy compression. A typical lossless compression can provide compression factor of around 3 but a lossy compression can provide compression factor anywhere between 20 and 200, depending upon the format being used. The ubiquitous trade off between the quality of the video and the cost of compression and decompression make the selection of a compression format all the more important. A very highly compressed video may consume less space and be transmitted very fast but visible distortions in the video may be present. Various video compression standards have been proposed and widely accepted over the years [15]. Some of the most common standards are presented in Table 1.

Table 2.1: Video compression standards

Year	Standard	Salient Features	Applications
1988	H.261	• Designed for transmission over ISDN lines • Operational bit rate lies between 40 kbps and 2 Mbps • Frame sizes supported are: CIF and QCIF	Video-conferencing

		• Sampling scheme used is 4:2:0	
1993	MPEG-1	• An enhancement of H.261 • Data rate is reduced dramatically by removing the sections of video that are not clearly perceptible by the human eye • The sampling scheme used is 4:2:0 • The frame size supported is: SIF • It made judicious use of I-frames which enabled faster rates of coding and de-coding of the video file	Video CD
1995	MPEG-2	• An improvement of MPEG-1 • Not optimal for bit rates lower than 1 Mbps • Better performance than MPEG-1 at 3 Mbps and higher • Provided compression for HDTV cameras and DVD quality of movies • It supports both interlaced videos as well as progressive videos • Compresses frames into I-frames, P-frames and B-frames. • Supports sampling scheme of 4:2:0, 4:2:2 and 4:4:4	DVD Video, Blu-ray Video, HDTV, XDCAM, Broadcast TV, Satellite TV and Digital Cable TV
1996	H.263	• Low bit rate compression • Originally designed for low quality but fast delivering video conferencing and video telephony • Used mainly with circuit switched networks • Mostly it is same as MPEG-2 but it can support high bit rates as well as	Low quality but quick delivering video conferencing and video telephony.

		low bit rates • Supports 5 different frame sizes	
1999	MPEG-4	• Maximum data rate varies from 180 Mbps to 3600 mbps • Supports sampling schemes of 4:2:0, 4:2:2 and 4:4:4 • It has 21 different profiles which support a number of video applications ranging from low quality and low resolution to high definition TV broadcasting. • Each profile has a different bit rate, sampling scheme, encoding scheme, frame support and resolution • Used with popular codecs like DivX, Xvid, Nero digital and QuickTime.	Videos uploaded and downloaded from the internet, Videoconferencing, Broadcast TV
2003	H.264 AVC	• AVC refers to Advanced Video Coding • It is a motion-compensation and block-oriented compression format • It is one of the most used compression standard and is specifically used for encoding of all Blu-ray discs • It provides high quality of video even at lower rates • It provides flexibility to be applicable for a wide variety of video applications such as high and low bit rates, different resolutions, network packets, live TV, HD broadcast, hard disk storage and more. • It is, in essence, the amalgamation of a lot of popular standards that came	Blu-ray disc, HDTV, Digital Video Broadcasting, IPod TV, Apple TV

		before it	
2009	Dirac	• Open and freely available compression format developed by BBC researchers • Aims to give high quality video compression of the category UltraHD • It operates at the resolution for HDTV and gives higher quality and lower bit rates than the previous standards • The previous standards used discrete cosine transforms for video compression but Dirac uses wavelet compression • Wavelet compression allows it to support variable bit rate as well as constant bit rate • It is backward compatible with all the previous standards and also supports its contemporary standards	HDTV, UHDTV, Digital Broadcasts, Video On Internet, Live HD video streaming
2013	H.265	• It is also called High Efficiency Video Coding (HVEC) compression format • It is an enhancement of the H.264 AVC format • It doubles the compression ratio of AV and provides same video quality • It can support the highest resolution of the Ultra HDTV, which is 8K UHDTV at 4320p and resolution of 7680x4320 pixels • It supports features like different ranges of formats, different sampling schemes and scalable coding extension	UHDTV, 3-D Video, HD Videoconferencing, Animation, Live Streaming HDTV

2.6PROTOCOLS FOR VIDEO STREAMING

Video streaming requires certain protocols which can synchronize the sender-receiver relationship and dictate the rules of media transfer between them. Video streaming is often adaptive in nature, that is, the rate of transfer gets adjusted according to the transfer conditions. Video streaming is basically of two types; real-time and on-demand. On-demand streaming means that a person requests the viewing of a particular video and that video is played for him. In this type of streaming the videos are recorded and kept in a repository which is accessible to everyone but it is individually played for every device. An example of on-demand streaming is youtube, which lets the client view videos on demand, which are already kept in its database. In real time streaming, there is a fixed time for a video to appear on the internet and the client can connect to the network to receive the video [16].

The on demand streaming and the real-time streaming use different transport layer protocols to make deliveries. The Transmission Control Protocol (TCP) is a reliable transmission protocol. This means that if the packet fails to be delivered or has some error in it, then TCP will retransmit the packet till it is received properly. Its counterpart is the User Datagram Protocol (UDP) which makes a best effort delivery of the packets. In UDP if some packets are lost or corrupted, it does retransmits the packets. Each protocol has its advantages and disadvantages. TCP provides a generally error free transmission of the data, but this reliability makes a trade off with timely delivery of the video. To check for errors, wait for acknowledgements and retransmit the corrupted packets, TCP requires time, hence it is slower than UDP. Now, buffering and delayed delivery of the videos is accepted in the on-demand scenario but completely unacceptable in the real-time scenario. The real time streaming can accept slight skips in the video frames but it cannot accept late delivery and jitters. A delay in the delivery of real time video is expected and acceptable but that delay must be constant so that the client does not feel any perceptible difference in the viewing. Jitters are delays which are not constant and jitters cause uneven viewing of the video. This is why real time videos are streamed using the UDP protocol. The protocols which maintain video streaming are discussed below:

- **Real Time Transport Protocol (RTP)**

RTP is a family of protocols with the first ever draft submitted in 1996, which has been specifically for real time users. Although it can be coupled with either TCP or UDP, it is

generally used in combination with UDP to deliver a video in a timely manner. RTP is a transport layer protocol which works above UDP protocol and contains many streams of data that need to be delivered and reconstructed at the receiver's side. RTP has some companion protocols which may or may not be used while employing the RTP protocol [17]. Real Time Control Protocol (RTCP) is a session layer protocol which is specifically used with RTP to provide feedback information to it about the quality of video being delivered. Real Time Streaming Protocol is a presentation layer protocol used for the purpose of defining when and how to play the video. It works in a manner similar to HTTP but it is a stateful protocol and defines states like play, pause and record for the video. Another protocol called Resource Reservation Protocol (RSVP) is a transport layer protocol which is used to setup and maintain a session. The combination of these protocols is known as the RTP protocol stack. The RTP protocol stack may or may not be supported by an operating system. If it is not supported by the OS then standalone third party players like RealPlayer or plugins like Flash may be used for RTP/UDP video streaming.

- **Real Time Messaging Protocol (RTMP)**

RTMP is a protocol that was specifically designed to stream audio and video between a flash player and a browser. Initially a propriety protocol for Flash players, this protocol has gained usability in some other third party software as well, but the basic premise of the protocol remains that it should be used with Flash players [18]. It is used on top of TCP protocol and maintains a smooth, strong and low delay communication. It operates by splitting the audio and video stream into smaller fragments and then interleaving and multiplexing those streams to the user so that the fragments arrive without being lost and without too much delay. The basic RTMP protocol has numerous varitions such as combining the RTMP with the TLS/SSL connection to provide a secure transmission, encrypting the RTMP with Adobe's propriety encryption scheme and encapsulating the RTMP data in an HTTP request to bypass firewalls.

- **HTTP Live Streaming (HLS)**

It is a propriety protocol developed by Apple to be used specifically with iOS. Developed in 2014, it provides the feature of streaming at an adaptive bit rate such that the streaming rate can get altered in between depending upon the network conditions and the quality of the video. This protocol works by dividing the whole video file into small HTTP-based segments and then encoding each segment at a different bit rate [19]. Once the streaming starts, the

client can alternate between streams of different bit rates depending on the quality of the video that he is receiving. But one of the prerequisites of using this protocol is that it needs to download the extended M3U playlist, which contains all the functions, control information and other meta data required by the streams in the transmission. Since HLS is based purely on HTTP format, therefore it is able to bypass the firewalls which allow HTTP traffic. This is in stark contrast with RTMP because RTMP would get filtered and rejected by these firewalls. HLS works in an architecture made up of a server, a distributor and a client. The server is responsible for coding and encapsulating the video file in proper format and then chopping it up into smaller segments which will be delivered to the distributor. The distributor is a normal web server which takes a client's request to view a file, retrieve that file in the correct format from the streaming server and then deliver it to the client. The job of the client is to request a file, receive that file from the distributor and reassemble all the segments of the file to form a continuous and well flowing video which can be viewed by the user.

- **Adobe HTTP Dynamic Streaming (HDS)**

This protocol was a combination of HLS and RTMP in the sense that it is a HTTP based protocol but it is compatible with flash player. The HLS has all the makings of a good streaming protocol but it was compatible with only iOS and .m3u extension files [20]. To design a protocol that had the qualities of being encapsulated with HTTP and having adaptive streaming rate, Adobe designed a new protocol stack which would enable high video quality deliverance over HTTP traffic so that it is able to surpass the checks put in place by the firewalls. Bypassing the firewalls is especially beneficial because of the existence of Content Delivery Networks (CDNs) which is a large network of servers that is spread across various data centres connecting the internet. The CDN is a special network which was designed and built to provide a large repository of content which can be delivered to clients at a high quality and is readily available. The acceptability of the HTTP protocol enables the HDS to access and retrieve content from a CDN and deliver it to the clients without being detained. The HDS protocol requires Flash player for playback, which means it is more suitable for desktops than for smartphones.

- **Other Protocols**

Many more propriety streaming protocols have emerged in the recent years, some with a wide selection of feature and some with the basic features. The basic fundamental behind the

use of so many propriety protocols rather than a couple of standard protocols is that each and every software aims to provide a particular set of services. These services may have different and widely varying requirements such that each service may require a different encoding scheme, a different resolution, compression, sampling scheme, delivery scheme etc. For this purpose, they modify the existing protocols or design their own protocol stack to match their particular needs. For example, the Microsoft Smooth Streaming is a protocol stack which is fragmented into very small chunks and distributed over HTTP traffic and this protocol is compatible only with Silverlight and IIS applications. Examples of other propriety protocols include MPEG-DASH, Shoutcast and BitTorrent Live Streaming.

CHAPTER 3

Literature Review

In communication over computer networks, it is not always necessary that the data will reach the destination in the exact condition that it was transmitted. Chances are that some of the bits in the data might be corrupted or erased. In fact, chances are that a number of data packets might be lost over the network. The loss or corruption of bits is known as an error in data transmission. Errors are caused by a number of factors like attenuation, noisy channel, interference, congestion over the network, low QoS parameters and poor channel conditions. Errors are handled by the data link layer through error detection and correction mechanisms.

3.1 CHALLENGES OF VIDEO STREAMING OVER WLAN

Video streaming is infiltrating every part of our digital life. From entertainment to communication, every sphere has an application for video streaming. Communicating through videoconferencing, seeking entertainment through live broadcast television, reviewing video through playback streaming, real time surveillance feeds for security and many more applications are proliferating all over the world. But streaming video over WLAN is not a facile task; there are plenty of challenges faced. Some of the paramount concerns are[21]:

- **Limited Bandwidth**

  Limited bandwidth is one of the most crippling disadvantages possessed by WLAN in the face of wired networks. The wired networks are undeniably faster than the wireless networks. Now the lower bandwidth of the WLAN is not apparent when the file to be transferred is of a smaller size, but the transmission rate difference is glaring with large file sizes. Streaming of live video like a TV broadcast typically requires all the bandwidth it can get, and WLAN's lower bandwidth can become a reason for low quality of the video

- **End- to-end delay**

  End to end delay refers to the time taken by a packet to travel from the source to destination. End to end delay is a culmination of all the delays that are encountered in the time that the packet leaves the source and is received by the destination. This

delay considers the transmission delay, the propagation delay, the processing delay and the queueing delay.

- **Large number of users over WLAN**

  As the usability of the WLANs increases, the number of users that get connected to the same wireless network also increases. This leads to over congestion of the medium because all the users are trying to send or receive packets. Over congestion of the medium causes collision of the packets and the packets get lost of corrupted. Contention or collision avoidance mechanisms lead to under-utilization of the link which can increase the time taken for a packet to be delivered.

- **Packet loss**

  Packet loss occur for a variety of reasons ranging from noisy medium of air, interference from other frequencies, interference from other devices operating at dame frequency, scattering of the waves, refraction and rerouting caused by physical obstacles, multipath interference and attenuation. All these factors cause high packet loss rate which deteriorates the quality of the video being delivered.

3.2 ERROR CONTROL

Error detection and correction is an important aspect of computer networks as it is used to ensure reliable delivery of data over potentially unreliable network. It is one of the tasks performed by the data link layer of the OSI model. Error detection and correction are two separate phenomena. Error detection involves detecting whether or not the received data has any errors, corrupt symbols or lost packets. Its job is not to tell the positon of errors or the sequence of the packets that are lost, rather it just tells whether the data sent is different from the data received or not. Error correction entails that if the error has been detected then determining the position of the error, sequence number of the lost packet and then reconstructing the data to resemble the original data [22].

The data detection and correction is carried out by adding redundancy bits to the original data. The functionality of redundancy bits is to make a special relationship between the original data and the redundancy bits so that authenticity of the sent data can be verified by checking the relationship. Redundancy bits also help in pinpointing the location of the errors and the sequence number of the lost packets and help in recovering from the errors. Just employing error detection is not enough to secure a reliable delivery of the data. It must be combined with error correction schemes to improve the quality of the video streaming and

to make sure that the packet loss rates do not spike uncontrollably [23]. Error correction schemes are a combination of error detection and error correction mechanisms and are used to find if the error has occurred, the location of the error and finally correcting the error so that the final data reassembled by the receiver is error free. Error correction schemes are basically of types: automatic repeat request (ARQ) and forward error correction (FEC).

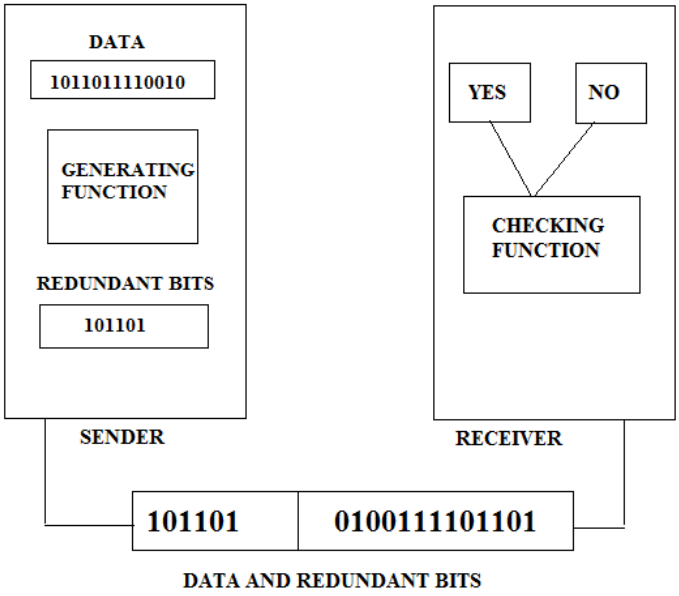

Figure 3.1: Redundancy check for error control

3.3 AUTOMATIC REPEAT REQUEST (ARQ)

ARQ was one of the basic mechanisms used by the data link layer to control the error over the channel. ARQ uses the concept of acknowledgements (ACK), which are the messages sent by the receiver to the sender indicating that it has correctly received a packet. ACK packets are sent in the same format as the data packets but without any data and the field of packet type set as ACK. ACK packets are used throughout the communication, while establishment, data transmission and connection termination. The sequence number of the ACK packets correspond to the packets for which the acknowledgment is being given and these sequence numbers help the sender find out whether the packet has reached receiver or not [24]. The basic fundamental working of the ARQ is that for every packet or every group of packets that is received by the receiver, it sends an ACK packet to the sender. The ACK packets and the data packets are in a particular sequence such that the receiver keeps a track of all the packets it is receiving and keeps arranging it in a particular sequence. Depending

upon the protocol being followed, the receiver either sends ACK after every packet it gets of sends a combined ACK for a group of packets it has received.

If any one of the packet in the sequence is missing then no ACK is sent for any of the packets received after the missing sequence number. The sender keeps sending the packets in the sequence as long as it keeps getting the ACKs. As soon as it doesn't get an ACK it stops the transmission and wait for the ACK to arrive. If the ACK does not arrive till the timeout period, the sender re sends the packet number from where it stopped getting the ACK. Now if the lost packet arrives at the destination and the packets fall back in sequence then the ACK is sent and normal transmission is resumed. But if the packet is consistently being lost then the sender will retransmit the packet only a number of times before discarding the packet. There are three major protocols that have been standardized for the ARQ mechanism and they are discussed below:

- **Stop and Wait ARQ**

  This was the first and the simplest implementation of the ARQ mechanism. In this method the sender sent only one frame before it waited to get the ACK from the receiver. The fact that it waits for ACK after every packet means that in this protocol, the packet is never lost or arriving out of order. While this method is very effective at making sure that all the packets are intact, it is very slow and the time taken to deliver the whole video is much more than the other protocols.

- **Go-Back N ARQ**

  In this protocol, the sender decides the number of packets it is allowed to transmit before it has to wait for the ACK to arrive. This number is commonly referred to as the window size. In this case the receiver keeps tracking all the packets that it has received and puts those packets in the correct sequence. If any of the packets is missing in the sequence then ACK is sent for the packet just before the missing packet. Upon receiving the ACK, the sender repeats the transmission of all the packets after the ACK, not just the missing packet. While the transmission time of the packets is decreased, the redundancy of the packets increases. The receiver and the channel is overwhelmed with the packets which did not require retransmission.

- **Selective Repeat ARQ**

  In this method the sender decides upon a window size and is allowed to transmit all the packets as allowed by the window size without waiting for their ACK packets.

The receiver keeps sending the ACK for each packet it receives and keeps a track of the packets it has received and the ones that are lost. Once all the packets in the window size have been transmitted, the sender checks which ACK it has received and which are missing. Only those packets are retransmitted for which no ACK was received. This method removes the redundancy of sending packets which had been received correctly by the destination.

Advantages of ARQ:

- **Reliable transmission**: This protocol is particularly used with the TCP protocol to ensure reliable delivery of the video by making sure all the packets have arrived and are in order.
- **Lower error rate:** Synchronizing the packets with the ACK packets makes sure that the sender is intimated as soon as some packet is left out of the sequence so that it can be retransmitted. This leads to the lowering of error rate in the video streaming.
- **High video quality:** If the packets are not lost, corrupted or out of order then the quality of video being received is very high.
- **QoS oriented:** This protocol is very quality oriented and aware of the QoS parameters and makes sure that the throughput, efficiency and the quality of the video remain in good shape.

Disadvantages of ARQ:

- **Time consuming**: The time spent waiting for ACKs and the time spent on retransmissions increases the total time taken for delivering the video.
- **Congestion:** Generally the packets are dropped or lost because of bad channel conditions or heavy traffic. Constant sending of ACK packets contribute to the traffic on the network. And if the network is already over congested then constantly sending ACKs or retransmitting all the packets will only increase the congestion on the network.
- **Uses up a lot of bandwidth:** It is already quite clear that the wireless networks do not enjoy the high bandwidth enjoyed by the wired network. The constant sending of ACKs, after every small group of data packets, only decreases the bandwidth available for the actual data.

- **Not ideal for real time:** waiting for ACK and retransmitting a packet till it has been received consumes a lot of time and interrupts normal transmission of the packets and takes up a lot of time. This setup is not suitable for real time applications where the reception of video is time bound and too much delay can cause the application to fail.

3.4 FORWARD ERROR CORRECTION (FEC)

ARQ has a crippling disadvantage of taking too much time to deliver packets and to cause unnecessary delays and congestion over the network by multiple retransmissions. This makes ARQ inefficient for real time applications, where timeliness of the video is of paramount importance. This is where FEC has proved to be more efficient in dealing with errors.FEC, also known as channel coding, is a technique of controlling error over noisy channels by appending extra bits, known as redundant bits, to the original source packets [25]. The redundancy bits attached enable the receivers to detect the errors that may have occurred anywhere in the packet.

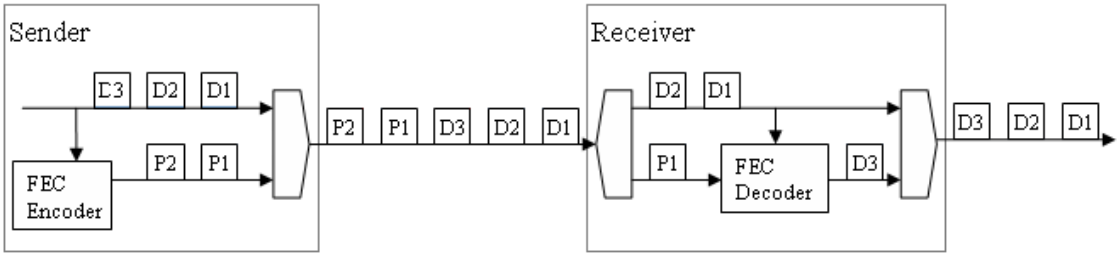

Figure 3.2: Basic FEC Mechanism

The basic principle behind FEC is that the source packets in a block of video are injected with some number of redundant packets. The number of redundant packets to be transmitted is chosen in such a way that the whole block of video can be reconstructed at the receiver's end even if some of the packets in the block are missing. The FEC packets are constructed certain deterministic algorithm. When a video stream is transmitted, it is divided into *i* blocks. Each block contains a sum total of *n* packets. In a block of *n* packets, there are *k* source packets and *h* redundant packets such that *h= (n-k).*

So according to the FEC principle, if the number of packets lost in a transmission does not exceed *h,* then the whole block of packets can be reconstructed at the receiver using the source packets and the redundant packets received [26]. Consequently, if it is noticed that

the packet error rate is being increased and the number of packets being lost has incremented, then the number of redundant packets being sent with the source packets is also increased. The number of redundant packets to be injected are determined using various methods of coding theory such as Reed-Solomon codes, Golay codes, Hamming codes and so on. The RS code theory has been used quite widely because no other scheme is known to provide recovery of lost data from a lesser number of received data symbols [27]. Moreover, the number of redundant packets may or may not change depending upon the type of implementation of FEC.

3.5 TYPES OF FEC

FEC mechanisms can be implemented in various ways depending upon the type of network being used and the parameters which are being given precedence. The classification of the FEC mechanisms can be done in the following manner:

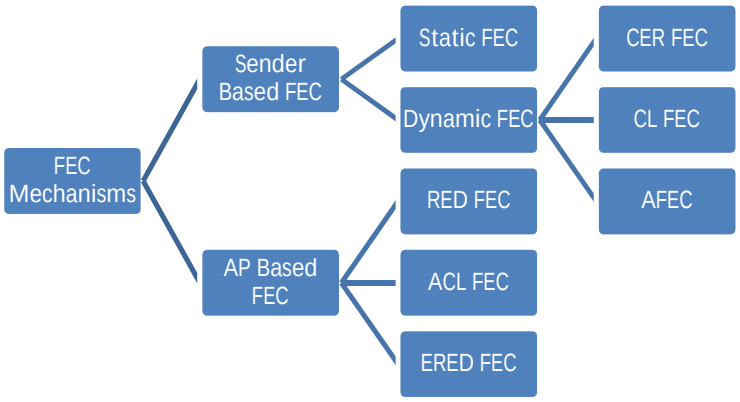

Figure 3.3: Categorization of FEC mechanisms

3.5.1 Sender based FEC

Conventionally, FEC are sender based. This means that the sender generated and codes the redundant packets to be sent. The sender based FEC schemes can generally be classified to be either static FEC schemes (SFEC) or dynamic FEC schemes (DFEC). The SFEC scheme [28] keeps the total number of redundant packets constant. This implies that despite the changes in the network conditions, the number of packets that will be injected in a block with remain constant throughout the transmission. This makes SFEC a bit unreliable for packet recovery because it does not consider the real time conditions of a network. So, if the network was too heavily congested, it would need more redundant packets to be transmitted

so that the block can correctly be reconstructed. But SFEC fails to recognise this need and will keep providing low number of redundant packets.

This flaw in SFEC led to the development of dynamic FEC (DFEC) [29]. DFEC schemes let the FEC rate be altered and tuned according to the current network conditions. The FEC rate may change according to the network load or the channel conditions or the signal to noise ratio of the channel. In many DFEC schemes the FEC rate is altered in accordance with the information given by receiver. This information may be any parameter being considered by the sender and receiver and the FEC rate may be tuned in accordance with that parameter.

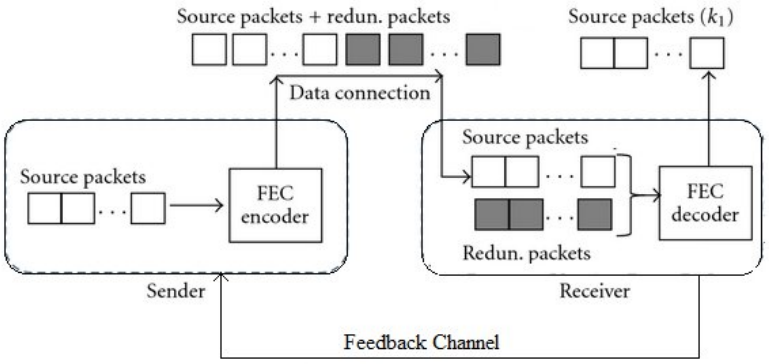

Figure 3.4: Sender Based FEC Mechanism

- **Constant Error Rate FEC (CER FEC)**

Takahata et al.[30] proposed a method in which the packet error rate (PER) is calculated periodically and the feedback is sent to the sender so that the FEC rate can be adjusted to maintain a constant PER. In this method, a constant check is being maintained at the receiver's end to monitor the number of packets being lost in each transmission. This information is then fed back to the sender so that the number of redundant packets can be increased or decreased to maintain the constant PER. The main advantage of keeping the PER as the checking parameter is that a constant PER can ensure a constant delay and minimal jitters. If the receiver is aware of how much delay it can expect in the video streaming, then it can adjust the application requirements and the buffering rate in such a manner that the user does not experience broken or interrupted video

- **Cross Layer FEC (CL FEC)**

Bajic et al [31] proposed a scheme useful for the multicast transmission of videos over the wireless LAN (WLAN). Multicasting is an efficient way to conserve resources in the event where the same video needs to be transmitted to a number of users. In this method, each of the receivers is required to send feedback to the sender enumerating the number of packets lost during the transmission. The sender calculates the maximum number of packets which were decoded by each of the receivers and adjusts the FEC rate according to that information. In this method, the FEC is adjusted according to the maximum number of packets decoded by the user which gave the highest error rate. This enables the technique to judge the channel conditions and make sure that all the users are able to get the full video stream without any losses. While this is a useful method to ensure quality of video to all users, it also generates a lot of redundant traffic over the network which may cause congestion and consequently cause even more packet loss. Moreover, even if majority of the users are experiencing low error rate, yet the FEC rate needs to be increased to suit the needs of user experiencing the highest loss rate. This introduces undue latencies in the network.

- **Adaptive FEC (A FEC)**

Park et al [32] proposed a scheme specifically to be used for real time transmissions over WLAN. In real time transmissions, the QoS parameters cannot be given paramount attention and have to be compromised in favour of timeliness. For real time applications it is imperative that the video packets should be delivered and reconstructed in time but slight errors and little number of lost packets can easily be ignored. AFEC is a scheme which calculates the FEC rate depending upon the network delay. As the network delay decreases the number of redundant packets increases and vice versa. Network delay is calculated by the round trip time (RTT) taken by the packet to start from the source, reach the destination and be back to the source. The RTT indicate the delays present in the network, the processing and queuing time taken and the obstacles present in the channel.

3.5.2 AP BASED FEC

The FEC redundancy rate in sender based schemes is calculated according to the acknowledgement messages sent by the receiver stating the packet error rate or the network load or the channel conditions. But a significant amount of time is spent calculating the required FEC rate. Thus the FEC rate may not be completely accurate in its depiction of the current network status. This flaw can attributed to the fact that the acknowledgement messages have to be sent to the sender because the FEC rate is traditionally calculated at the

application layer of the sender. A rectification of this problem was proposed by Lin et al [33], where they proposed that the FEC mechanism should be implemented at the Access Point (AP) of the Wireless Network. The scheme suggested that the FEC rate should be calculated at the AP without taking feedback. This scheme was titled Enhanced Adaptive FEC (EAFEC). The FEC in this scheme is calculated dynamically while considering two parameters: network load and channel conditions. The channel conditions are judged by the number of retransmissions occurring for a particular block. The network load is calculated by queue length present at the AP. The bigger the queue length, the more heavily congested is the traffic.

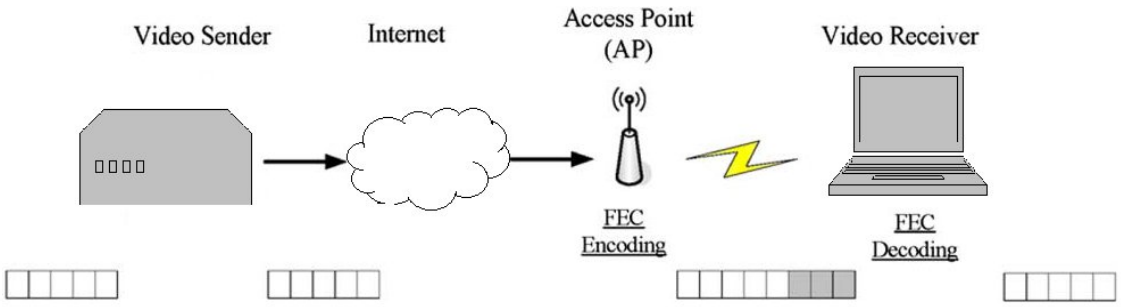

Figure 3.5: AP Based FEC

- **Random Early Detection FEC (RED FEC)**

A common problem observed in the above schemes is that when the packets are being lost due to network congestion and delay, the redundancy packets are increased to make up for the lost packets. The additional packets cause the network to become more congested and the PER increases. The rectification of this problem was provided by Lin et al [34] when they proposed a scheme in which the redundant packets are generated at the AP in accordance with the network conditions. This scheme observes the AP queue. If the queue is short then the redundancy packets are increased but if the AP queue is long then the redundancy packets are kept at a minimum. This method is adopted so that the network traffic load can be considered.

- **Adaptive Cross Layer FEC (ACL FEC)**

Han et al [35] proposed at scheme which considered the network loss rate during the transmission. They titled this scheme as Adaptive Cross Layer FEC (ACLFEC). In this scheme, the information about the network loss is gathered at the MAC layer using the ARQ

function. The FEC rate is calculated at the application layer with the help of UDP protocol. This scheme takes advantage of various functionalities available different layers. It also keeps a check on the redundancy rate by constantly observing the failure rate of packets as reported by the MAC layer. In ACL FEC, the FEC rate is changed dynamically according to the network conditions. But it does not consider the traffic on the network. Consequently, when the network is congested there is a higher chance of packet loss.

- **Enhanced Random Early Detection FEC (ERED FEC)**

Lin et al [36] proposed an Enhanced Random Early Detection FEC (EREDFEC) scheme in which the packets are generated in accordance with both the network traffic conditions as well as the condition of the wireless channel. This method worked at easing up the network traffic load without compromising the quality of the video over the WLAN. The network load is calculated by observing the AP queue and the network conditions are observed by calculating the number of packet retransmissions. This method has proven to be more efficient than the other two AP based schemes.

3.6 COMPARISON OF THE FEC SCHEMES

All the techniques discussed in this paper for implementing FEC have certain unique characteristics which make them ideal for some particular situations. In this section, a comparison of those techniques has been presented followed by an analysis of their usability, trade offs and applications.

Every scheme has certain parameters which have been ignored or given low priority, in favour of giving higher priority to some of the other parameters. These trade offs have been discussed in Table 1, where the schemes have been compared to each other with respect to major parameters. These parameters are: the Quality of Service (Qos) parameters like delay, attenuation and jitter, observing the network traffic, considering channel conditions and adhering to time constraints.

Table 3.1: Comparison of schemes based on network parameters

Scheme	QoS Parameters	Network Traffic	Channel Conditions	Time Constraints
CER FEC	High	Low	High	Medium
CL FEC	Medium	Medium	High	Medium
A FEC	Low	High	Low	High
RED FEC	High	High	Medium	Medium
ACL FEC	High	Low	High	Medium
ERED FEC	High	High	High	Low

Table 3.1 shows that CER FEC places the QoS parameter provisioning at a very high priority hence it is not an appropriate scheme for transmitting a video within a very tight time constraint. It also places a high priority on the channel conditions and keeps a constant check on the conditions so that adjustments in the FEC rate can be made as soon as the channel starts to deteriorate. Conversely, A FEC places very high priority on time constraints, therefore it is ideal to use this scheme in case of hard real systems. CL FEC is a scheme developed to handle multicast transmissions, therefore, it constantly needs to monitor the channel conditions so that the feedbacks from various receivers calculated fast. RED, ACL and ERED FEC mechanisms are such that they need to provide high QoS provisioning therefore they need to keep a constant monitor on the network traffic as well as the channel conditions.

Table 3.2 presents various advantages and disadvantages of each scheme implementing the FEC. The pros and cons of each of the schemes include various aspects like whether it is able to provide optimal QoS support or which applications it can be used for and which applications can it not be used for. Moreover the complexity of certain algorithms can prove to be a disadvantage even though the algorithm aims to improve the other aspects. The tradeoff between complexity and functionality is very evident in the case of ERED FEC as it has overcome the deficiencies in RED and ACl FEC but the resulting algorithm can take more time and increase complexity. Certain schemes like AFEC are innately better at certain

specific applications like real time systems while CL FEC is made particularly to suit the multicast environment.

Table 3.2: Pros and Cons of FEC schemes

Scheme	Pros	Cons
CER FEC	Gives QoS control in real time transmissions over either wired or wireless media or a mixture of both.	Altering FEC based on just PER can lead to congestion of network when PER increases.
CL FEC	Comprehensive scheme for multicast video transmission, adjusting FEC according to the packet loss rate of all the receivers involved.	PER in multicasts can be misleading if PER of one receiver is significantly higher than the other receivers and this can cause degraded performance of the scheme.
A FEC	Scheme to provide FEC for real time video transmission without succumbing to latencies provided by QoS providing retransmission based schemes.	The real time constraints for hard real systems can cause the FEC to perform inefficiently causing large data loss which cannot be recovered in the given time constraint.
RED FEC	Produces redundant packets in advance when the traffic is light so that the network does not clog.	Too many early packets can stop the channel from reaching its optimal efficiency.
ACL FEC	Distributes the tasks over the application and MAC layer to take advantage of the already available functions and protocols to optimize the FEC rate.	Tends to congest an already congested network causing a higher PER.
ERED FEC	Observes both network conditions as well as network traffic load to provide optimal FEC rate.	The algorithm has a higher complexity than others because of its various considerations.

CHAPTER 4

PROBLEM STATEMENT AND OBJECTIVE

4.1 Problem Statement

As discussed in the previous chapters, each of the existing FEC methods have certain drawbacks which inhibit the performance of the FEC scheme. The traditional static FEC scheme has the obvious drawback of keeping the FEC rate constant regardless of the network conditions. The common FEC schemes used for wireless networks consist of the AP-based schemes of ACL-FEC, RED-FEC and ERED FEC. Out of these, ACL-FEC adjusts the FEC according to the channel conditions but does not pay any heed to traffic congestion. On the other hand RED FEC adjusts its FEC rate in accordance with the traffic congestion but does not consider the channel conditions. A solution to this was combining both the schemes and developing a scheme that could adjust its FEC rate in accordance with both the traffic load and the conditions of the wireless channel. Hence ERED FEC was developed, but even this scheme is susceptible to inefficient performance and degraded quality of video transmission during burst errors. WLANs, in particular are afflicted with burst errors, as the wireless channel is susceptible to noise, attenuation, multiple spectrums and many other distortions which can lead to loss of packets in continuous groups. If the network experiences too many burst errors or burst errors that are too long then the performance of FEC is severely degraded because in MPEG format the frames are intra coded. This means many of the frames depend upon each other to be decodable. This gives rise to the need of including a provision in the schemes that can deal with burst of errors. Interleaving the FEC redundant packets with the source packets and placing these redundant packets randomly within the whole packet is one way to ensure that when burst of errors occur, the FEC is robust enough to be able to reproduce all the frames at the receiver's side.

4.2 Objectives

The objectives of this thesis are:

1. To suggest a scheme that is able to overcome the drawback of low video quality transmission because of burst of errors.
2. Validate the suggested scheme through simulations.

3. Compare the suggested scheme with the existing schemes and analyse the advantages and disadvantages of the proposed scheme.

CHAPTER 5

SIMULATION AND IMPLEMENTATION

Simulation of the study entails creating an environment which replicates the real life environment and contains all the components present in a real life scenario. The components in the simulation are expected to behave in a way that is similar to the way actual components would behave when subjected to certain conditions. The simulation of the FEC mechanisms include setting up a topology consisting of wired and wireless components, sending server, receiver, medium to carry data, access point and external noise. The simulator creates an environment in which it is possible for the users to see how the data is being transmitted from sender to receiver and mimic all the problems that are observed in the real life networks.

Simulators used in computer network simulations are of two types: discrete event simulation (DES) and continuous dynamic simulation (CDS) [36]. The DES performs the simulations in relation to time. All the events that are supposed to occur are queued and carried forth in a particular order. The simulator reads the events from the queue and executes them, producing some effect which is recorded for later observation.CDS is used to simulate numerical solutions of an equation and is used to provide results of complex equations which require a part of the equation to be solved first and its answer to be used in the other parts. Most of the network simulators are DES because they are used to detect flaws and gaps in logic and design of a topology.

There are a number of DES based simulators available for research and testing. Some examples of these include Network Simulator (ns) [37], Optimized Network Engineering Tools (OPNET) and NetSim. Ns is an open source simulator whereas OPNET and NetSim are propriety simulators. For the purpose of my thesis I chose to work on the ns-2 simulator because it is an open source simulator and the aim of my thesis was to implement the FEC mechanism and its improvement in an ad-hoc based environment. Ns-2 performs well for ad hoc networks and gives realistic simulation results for any implementation done in the ad hoc networks.

5.1 OVERVIEW OF NS-2 SIMULATOR

The network simulator was designed in 1997 by a group of researchers at the Lawrence Berkley National Laboratory [37]. The core of the simulator is coded in C++ but the simulation environment is scripted in Tcl. Tool Command Language (TCL) is a scripting language that allows the users to define their own languages, which can be embedded into the application, generate scenarios and user interfaces. The ns-2 simulator uses the Object TCL (OTCL) [38] as its scripting language, which enables it to link the C++ objects to the OTCL objects. The OTCL acts as a front end to the simulator by graphically displaying the network scenarios. The ns-2 can support both wired and wireless networks, hence it is ideal to create an environment which can simulate the combination of wired and wireless network and can be used to relay a video file from one end of the network to another with the added packet losses, noise and other such distortions.

5.2 ARCHITECTURE OF NS-2

The basic architecture of ns-2 consists of an OTCL script simulation program, an OTCL interpreter, an ns simulator library, a simulation result analyser and a NAM network animator. The OTCL script simulation program is a program which allows the user to manipulate the OTCL file so that the user can initiate the creation of the scenario that he wants. The OTCL interpreter is used to execute the script that is being run by the simulation program. An ns simulation library contains components like the event scheduler, network component objects and network setup help manuals. The event scheduler is a concept used by the ns simulator to stack the events of the simulation and specify when to start and end which event. The network components specify the components that are to be used in the topology. This includes description of their functionalities and their behaviour.

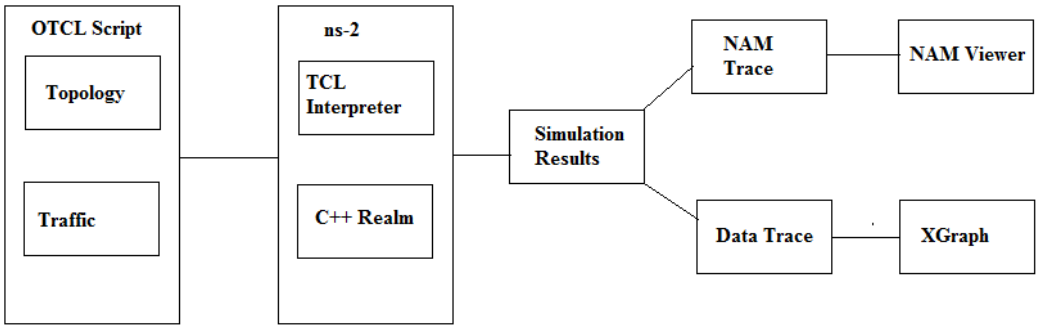

Figure 5.1: Architecture of ns-2

The components used in ns2 simulator are:

OTCL scripting language

OCTL is the TCL language with the object oriented extensions. TCL is a fully dynamic, event driven scripting language which can directly execute commands. Everything in this language can be over-ridden and redefined in a dynamic manner. It is also able to execute user based and time based events.

Trace File

Trace files are the files created for describing and specifying the values of various variables that are changed, affected or displayed when a TCL script is run. Figure 1 shows the format of a trace file.

The fields of the trace file are:

- Event Type Identifier: describes whether the event is a packet enqueue (+), packet dequeue (-), packet drop (d), packet reception (r) or packet collision at MAC level (c).
- Time: states the time at which the string of packet trace was created.
- Source Node: ID of the node where the trace begins.
- Destination Node: ID of the node where the trace ends.
- Packet Name: the type of packet being traced.
- Packet Size: the size of packet in bytes.
- Flags: a 7 digit string used to specify various congestion controls.
- Flow ID: ID used by user to specify each flow at the input OTCL script.
- Source Address: IP address and port number of source node.
- Destination Address: IP address and port number of the destination node.
- Sequence Number: the sequence number of the packet generated at the network layer.
- Packet Unique ID: it is the unique ID possessed by each packet.

NAM

Network Animator (NAM) is a graphic tool which is used to visually exhibit the simulation topology and the simulated and real-world packet traces. It can display the whole topology layout and possesses tools that can be used to inspect and analyse each and every component

of the topology. Moreover, it supports packet level animation and can demonstrate the actual relay method of the packet from source to destination.

AWK Language

AWK is an interpreted language that is typically used for processing text and extracting and reporting data. It is a data driven programming language that is used in ns2 to particularly process data obtained in the trace file.

XGraph

It is an inbuilt graph plotter of the ns2 simulator. It is used to input values from a program and to show the results graphically. The graphical representation of data and the obtained results help in analysing the results in an easy manner.

5.3 ARCHITECTURE OF THE PROPOSED SCHEME

The architecture followed in the proposed scheme is that of an AP-based FEC. The sending video server is connected to the routers, which are connected to the internet and the internet delivers the videos to the wireless APs. The APs deliver the videos to the receivers wirelessly after adding the redundant packets. For the purpose of our thesis, we have assumed that the wired part of the network is loss free. Since the scheme proposed is an AP-based FEC scheme, therefore the FEC rate for the packets is decided by the AP. For this reason the mechanism is divided into consists of six parts:

a) Packet classifier
b) Queue length monitor
c) Packet error rate monitor
d) FEC generator
e) Interleaving
f) Video quality monitor

Figure 5.2: Process of the proposed scheme

Packet Classifier

When a video server transmits a video, it encapsulates the video in the Real-Time Transport Protocol (RTP) and the video is transmitted wirelessly to the receiver. When the packet arrives at the AP, the header information of UDP is checked to extract the RTP header. RTP is a protocol that has been designed to transmit multimedia over the IP networks. RTP is a useful protocol for delivering real-time media because it provides inbuilt facilities of making up for jitter and delay, detecting packets that have arrived out of sequence and multicasting and broadcasting over networks. RTP is usually used with UDP because it is a real time protocol, therefore it prefers timeliness over totally error free delivery [39]. Minor errors and packet losses can be compensated with the use of FEC schemes. The AP extracts the RTP header and gathers information like which type of media is being transmitted, which multimedia format is being extracted, the timestamp of the header, the sequence number of the packet etc.

Queue Length Monitor

The queue length monitor is used to monitor the length of the queue at specified intervals of time to judge the network conditions. Since the FEC rate of the scheme is fixed by considering both the channel conditions and the network conditions, therefore it is imperative for the scheme to keep a constant check on the queue length of the AP. The length of the AP queue shows whether the network is lightly loaded, heavily loaded or has medium load. If the network traffic is too much and there is congestion on the network, then the length of the queue will be quite long because the packets will be taking more time than usual to get transmitted. In this case the FEC rate is kept to a bare minimum because the network is already suffering from congestion and sending extra FEC packets will only add to the existing congestion. If there is almost no traffic on the network, then the network is very lightly loaded and the queue is almost empty. In this case it can be considered good sense to increase the number of FEC packets especially if the channel conditions are not good.

Packet Error Monitor

Packet errors indicate either corrupt packets or lost packets. The corrupt packets are those in which a portion of the symbols are lost, incorrect or in the wrong format, such that the whole packet becomes unreadable and hence the packet needs to be discarded. The lost packets are those packets which fail to reach their destination over the network. Both types of losses are

categorised under packet errors. Packet errors are known to occur in the network when the channel conditions are not suitable for packet delivery. The channel conditions include the effects of attenuation, multipath scattering, spectrum interference, signal to noise ratio, scattering, fading etc. it is too expensive to analyse each and every aspect of channel conditions and calculate how it affects the transmission, therefore we use an easy indicator of Packet Error Rate (PER) to judge the channel conditions. If the PER is low, that means the channel conditions are suitable for packet delivery, whereas if the PER it too high then the channel conditions are not useful for packet delivery. When the PER is low, the FEC can be high or low depending upon the queue length, but if PER is high, it is highly recommended that FEC rate should also be high to compensate for the packets being lost.

FEC Generator

The FEC generator is used to finding and optimizing the FEC rate associated with the network conditions. The FEC generator finds the PER by analysing the number of retransmissions for a particular block. It then generates an FEC rate suitable for the PER such that the PER can be decreased to ensure good video quality. Then the queue length of the AP queue is taken into account to moderate the FEC rate. Two threshold values of lower threshold (TH_L) and upper threshold (TH_H) are decided for the queue length according to heuristics. If the queue length is lower than TH_L then the FEC is fixed to the maximum FEC rate regardless of the PER. Conversely, if the queue length is greater than TH_H then the FEC rate is fixed at 0 to clear up the congestion. But if the queue length lies between the two thresholds then the FEC rate is fixed by scaling the maximum FEC rate according to the traffic and the PER, which needs to be lowered.

Interleaving

Interleaving in the proposed scheme is done at the AP by creating an array at the outgoing face of the AP. Once the FEC rate has been fixed, an interleaving factor id decided by considering the number of FEC packets and the source packets present in the block. This factor makes sure that the FEC packets are appropriately and evenly distributed in the outgoing sequence so that the transmission does not fall victim to the burst errors that plague the WLAN networks. The AP maintains an array in which the sequence numbers of the packets are input as they are processed by the AP. These packets are a combination of source packets and redundant packets. Now, traditionally these packets are transmitted in such a manner that in the frame, the source packets appear before the redundant packets. But when

interleaving is applied then this structure of frames is modified by peppering the redundant packets in between source packets. After interleaving, the distance between each redundant packet will be equal to the interleaving factor.

Video Quality Monitor

MPEG-4 is an audio-video compression format introduced in 1998. This format is used to compress the audio and video data so that it can be optimally used for transmission over the internet, telephone and broadcast television services. A standard MPEG-4 structure contains three types of frames; I frame, P frame and B frame [40].The I frame are called Intra-coded frames and they are coded and decoded on their own. These frames do not have any dependency on any other frame. The P frames are called Predictive-coded frames and they are coded and decoded depending upon the I frame or the P frame that came before it. The B frame is called the Bi-directionally coded frame and its coding and decoding are dependent upon both the I or P frames preceding it and succeeding it. The video sequence is often broken down into small, manageable units called Group of Pictures (GOP). Generally, the GOP pattern consists of two parameters called I-to-I distance, represented by N and I-to-P distance, represented by M. the whole GOP can then be defined as G(N,M). The video stream is divided into video frames and the video frames are segmented into video packets in accordance with the maximum size of packets allowed by the network. The video frame is considered to be decodable if certain number of packets, in the whole frame, are decodable. The number of packets that need to be decodable for the whole frame to be decodable is called the Decodable Threshold (TH_D). TH_D is defined as a value between 0 and 1 and it expresses the fraction of packets that need to be decodable in order for the whole frame to be decodable. The packet may be directly undecodable or indirectly undecodable. Directly undecodable means that insufficient number of packets were received for the frame to be decodable. Indirectly undecodable means that the frame depends upon a frame which is directly undecodable.

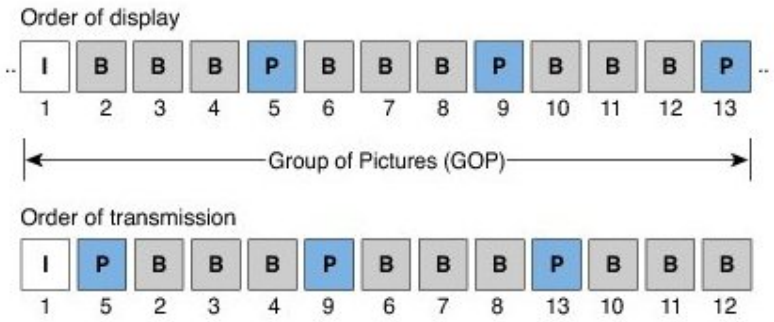

Figure 5.3: Relationship between I, P and B frames

5.4 SIMULATION ENVIRONMENT

The proposed scheme was simulated by creating a testbed on the NS-2 simulator which consisted of a video server in the Internet. The internet is simulated by wired network and an Access Point which is simulating the IEEE 802.11 standard. This access point connects the receiver to the Internet. The NS-2 simulator created an environment in which the video server was able to send a video over the internet, via the AP and to the receiver. The testbed was configured in such a way that the routing information from video server to the router to the internet was fixed in advance and the wired network was kept error free. Meanwhile the wireless network was configured to have a variety of packet error rates to test the scheme at various different packet error rates. Even the receiver is configured to have variable loss rates. There are plenty of standard MPEG-4 trace files like “Highway”, “Akiyo”, “Foreman” etc which are available for such simulations. In our simulation, we have used the “sample” video which contains 3000 frames. It is encoded using the QCIF format which is a standard MPEG-4 format. The GOP structure of the video is IBBPBBPBB (N=9, M=3). The video is made from 1024 video packets and these packets are streamed at the rate of 30 frames per second.

5.5PROPOSED SCHEME

The proposed scheme is divided into six parts:

I. Finding the maximum size of the AP queue
II. Finding the current size of the AP queue
III. Estimating the packet error rate
IV. Deciding the FEC redundancy rate
V. Interleaving the FEC packets

VI. Calculating the DFR

All the parts of the scheme are combined together in this sequence to give an optimum FEC redundancy rate for each block of packets in the video stream.

I. Finding the maximum size of the AP queue

The length of the AP queue indicates the network traffic. If there is a lot of traffic on the network then the queue will be almost full and if there is light traffic then the queue will be almost empty. To determine when the queue is full we need to find out the maximum capacity of the queue. In this method, the maximum capacity of the queue is determined by initially bombarding the AP queue with packets so that the queue reaches its saturation limit, whereby it can no longer accept any more packets and starts to drop them. For a lightly crowded queue, the packet error rate (PER) is very low because there is ample space in the queue. So through simulations it has been observed that as the queue starts filling up, the PER starts increasing and once the PER becomes greater than 0.2, the queue is full and will drop all packets arriving. So in our algorithm, we have kept the PER threshold at 0.2. We will stop bombarding the queue with packets when the PER becomes greater than 0.2. Initially the rate of sending the packets (R_{si}) is fixed at 50 packets/sec and packets are sent to the AP at that rate for 30 seconds. A counter i is initialised at 1 to count the number of packets entering the queue and is incremented at every packet sent. It is assumed that the processing of the queue is stopped for the purpose of determining the threshold. Another counter c is initialised at 0 to count the number of the packets when the R_{si} gets fixed. The PER is calculated and compared to the threshold value. If PER is greater than 0.2, then we increment the counter c to 1 and fix the $R_{si}$to the current rate. We then send two more packets at the same rate and compare the PER. If PER remains greater than two, then the queue has reached its maximum limit. At this point we count the number of packets in the queue by checking the counter i. if the PER value is calculated to be less than 0.2 in any of the above calculations then we reinitialize the counter c to 0 and increment the $R_{si}$by 50 and keep repeating this after every 30 seconds till the PER starts to become greater than 0.2 again.

The notations used in the pseudo codes are shown in Table 5.1

Table 5.1 Notations used in the pseudo code

Terms	**Definition**
R_{ri}	Rate of receiving the packets
R_{si}	Rate of sending the packets
PER	Packet Error Rate
Q_{max}	Maximum packets the AP queue can hold
RTT_{max}	Maximum Round Trip Time
RTT_{min}	Minimum Round Trip Time
Q_w	Queueing weight
Q_b	Length of queue in terms of how many bytes are in the queue
Q_l	Length of queue in terms of how many packets it is holding
P_s	Probability of a packet's success
P_f	Probability of packet's failure
P_{pkt}	Probability of packet's failure when it is transmitted just once
R_{max}	Maximum number of transmissions allowed for a packet before it is discarded.
$P_{e,i}$	Estimated Packet Error Rate
RT_w	Weighting factor of the retransmissions
FEC_MODEL	Maximum value of FEC that can be reached according to the requirements of QoS parameters
MAX-FEC	Maximum value of FEC according to the reference model chosen
$Q_{av,i}$	Weighted average queue length
Q_w	Queueing weight
$Q_{l,i}$	Length of the queue at the i^{th}packet
TH_L	Lower threshold of the queue
TH_H	Higher threshold of the queue
FEC_{final}	Final FEC Redundancy Rate
$P_{e,i}$	Estimated Packet Error Rate for the i^{th}packet
n	Total number of packets in the video stream
s	Size of the block
i	No of packets in one block
k	Number of redundant packets

h	Number of source packet
FEC_{final}	Final FEC redundancy rate
F_{int}	Factor of interleaving
DFR	Decodable Frame Rate
DEC_I	Number of I frames that are decodable
DEC_B	Number of B frames that are decodable
DEC_P	Number of P frames that are decodable
$Total_I$	Total number of I frames sent
$Total_B$	Total number of B frames sent
$Total_P$	Total number of P frames sent

The pseudo code for determining the maximum threshold of the queue is given as:

$R_{ri} \leftarrow 0$, $i \leftarrow 0$, $PER \leftarrow 0$, $R_{si} \leftarrow 0$, $c \leftarrow 0$

repeat

$i \leftarrow i + 1$

$R_{si} \leftarrow R_{si} + 50$

send packets at R_{si} for 30 seconds

$R_{ri} \leftarrow$ no of packets in the queue/no of packets sent

$PER = 1 - (R_{ri}/R_{si})$

if $PER > 0.2$ then $c \leftarrow c + 1$

until $(PER > 0.2)$ & $(c=3)$

$Q_{max} = i$

II. Finding the current size of the AP queue

Once the maximum capacity of the queue has been calculated, the AP queue is emptied of the packets and the real transmission of the packets begins. In the proposed algorithm, the FEC redundancy rate is decided by the considering both the current queue length and the estimated packet loss rate. To calculate the current queue length, we need to find the queueing weight, which can be calculated by subtracting the highest delay and the lowest delay experienced.

The highest delay occurs when the queue is full and is measured by calculating the round trip time (RTT) when the queue is full. Similarly the lowest delay is calculated by measuring the RTT when the queue is empty. The queueing factor when multiplied with the throughput, gives the size of the queue in bytes. The throughput of the queue is measured by dividing the number of packets received by the number of packets sent. The queue length obtained is the length in bytes. To find out the number of packets in the queue, we divide the queue length by the size of each packet. Since the maximum transmission unit (MTU) for IEEE 802.11 is 7981 bytes, therefore we will make sure that the size of the packet remains with the MTU limit.

The pseudo code for determining the length of the queue is given as:

n← total number of packets to be sent, i← 0

repeat

$Q_w \leftarrow RTT_{max} - RTT_{min}$

t← packets received/ packets sent

$Q_b \leftarrow Q_w * t$

if $P_s < 7981$

$Q_l = Q_b / P_s$

else

discard packet

i←i + 1

until (i>= n)

III. Estimating the packet error rate

After calculating the queue length the packet loss rate is estimated. The packet loss rate varies in throughout the video stream and is different for each block of packets, but changing the packet loss rate a large number of times, depending upon the wireless channel conditions, can cause a lot of overhead and can cause delay in calculating the FEC redundancy rate. Therefore we estimate the packet loss rate depending upon the weighting factor, probability

of losing a packet in the transmission and the estimated packet loss rate of the previous block. To calculate the probability of failure of one packet, we need to find out the probability of a packet being lost or failed to be receive when it is transmitted just once. In addition we also need to know the number of times a packet will be retransmitted before it is discarded. But since the probability of a packet being received successfully increases with the number of times it is retransmitted. Therefore, the probability of packet loss that is calculated with the combination of failure probability of a packet being transmitted once and the number of times it can be transmitted should be referred to as the effective probability of packet failure.

The pseudo code for estimating the packet error rate is given as:

seti← 1

repeat

$P_s = (1 - P_{pkt}) * (P_{pkt})^{i-1}$

i←i + 1

until ($i>R_{max}$)

$P_f = 1 - P_s$

n= no of blocks in the video stream, i← 0

repeat

i←i + 1

$P_{e,i} = (RT_w * P_s) + (1 - RT_w) * P_{e,i-1}$

until (i>= n)

IV. Deciding the FEC Redundancy Rate

The FEC rate for the algorithm is determined by taking into account both the queue length and the estimated packet error rate. The queue length of the current block is not considered directly, rather the a value of queue length is considered which is calculated by considering the queueing weight with the length of the queue in the present block and the length of the queue in the previous block. This value may be referred to as the weighted average queue length ($Q_{av,i}$). This value is then compared to the lower threshold (TH_L) and the higher

threshold (TH_H) values of the queue length. Through simulations it has been found that to get optimum estimation of when the queue is lightly loaded and when it is heavily loaded, the TH_L is kept at 30% of the maximum of queue length and the TH_H is kept at 80% of the maximum queue length. Now if the $Q_{av,i}$ value is more than TH_H then the queue is heavily loaded and the number of FEC packets is set to 0 to avoid overcrowding the queue. If the $Q_{av,i}$ value is less than TH_L then the queue is very lightly loaded and the number of FEC packets is set to MAX-FEC. The value of MAX-FEC is determined according to the requirements of the QoS parameters. If the $Q_{av,i}$ value is lies between TH_L and TH_H then the number of FEC packets are determined by equating the MAX-FEC value, the queue length of the current block, the estimated packet error rate and the threshold values.

Pseudo code for deciding the FEC Redundancy Rate is given as:

set MAX-FEC = FEC_MODEL (according to QoS parameters)

k = no. of blocks in a video stream, i$\leftarrow$ 0

repeat

i$\leftarrow$i + 1

$Q_{av,i} = (Q_w * Q_{l,i}) + \{(1 – Q_w) * Q_{l,i-1}\}$

$TH_L \leftarrow 0.3*Q_{max}$, $TH_H \leftarrow 0.8* Q_{max}$

if ($Q_{av,i} < TH_L$) then

FEC_{final} = MAX-FEC

else if ($Q_{av,i} > TH_H$)

$FEC_{final} = 0$

else

$FEC_{final} = (MAX\text{-}FEC) * \{(TH_H-Q_l)/(TH_H-TH_L)\} * P_{e,i}$

V. Interleaving the FEC packets

Once the FEC rate has been decided the redundant packets are concatenated with the source packets. But this method has a slight drawback. It is well known that errors generally occur in the form of burst errors and not randomly in single bits. Since the MPEG-4 has frames which are intra coded and hence to some extent, depend upon their predecessors to be decoded. If the length of the burst error is too long then too many of such frames may be lost such that the whole block is rendered non-decodable. To avoid this we use interleaving of the FEC packets. The interleaving is done by setting up an array at the outgoing of the AP such that the packets can be randomised when they are being sent from AP to the receiver. The interleaving factor decides the distance between two redundant packets and the source and redundant packets are picked from the array and queued at the outgoing queue.

The pseudo code for interleaving the FEC packets is given as:

n← no. of packets in the video, s ← size of the block

i← n/s

k←FEC_{final}

h= i - k, where h are source packets and k are redundant packets

F_{int} = ceilvalue[i/k]

VI. Calculating the DFR

Decodable Frame Rate (DFR) is a metric used to analyse the quality of an MPEG video transmitted over a network. The value of DFR oscillates between 0 and 1. The closer the value is to 1, the better is the quality of the transmitted video. DFR is measured at the receiver end and it is one of the paramount parameters to validate the efficiency of the proposed scheme. The DFR is calculated by taking the sum of the decodable I frame, P frames and B frames and diving it by the total number of frames sent. A frame if considered decodable if it contains at least a fixed portion of frames which are decodable and not corrupted. This value of fixed portion of frames is called the decodable threshold and it defines the minimum number of frames which are required to decode the whole frame. The DFR is calculated using the formula:

$$??? = \frac{??? + ??? + ???}{???? + ???? + ????}$$

5.6 MATHEMATICAL RESULTS OF THE PROPOSED METHOD

The proposed method is validated by comparing the results obtained by mathematically carrying out the pseudo code and by simulating the proposal in the virtual environment created. The values obtained mathematically are given in Table 5.2

Table 5.2: Mathematical results of the proposed scheme

Parameter	**Improved ERED**
Q_{max}	53 packets
RTT_{max}	11.3 µs
RTT_{min}	2.7 µs
Q_w	8.6
$P_{e,i}$ in light load	0.14
$P_{e,i}$ in medium load	0.25
$P_{e,i}$ in heavy load	0.38
TH_L	15
TH_H	43
Average FEC rate	5

CHAPTER 6

RESULT ANALYSIS

The proposed scheme is tested in the ns-2 simulator with the created testing environment, as described in the previous chapter. The mathematical results obtained from the pseudo code were presented in the preceding chapter and in this chapter we present the simulation results of the proposed algorithm with the existing ERED algorithm. The results for various parameters as obtained from the simulation of both algorithms are shown in Table 1.

Table 6.1: Comparison of values obtained from simulations

Parameter	**Static FEC**	**AFEC**	**ERED**	**Improved ERED**
Q_{max}	50 packets	52 packets	52 packets	53 packets
RTT_{max}	13.4 µs	12.2 µs	12 µs	11 µs
RTT_{min}	3.3 µs	2.8 µs	3 µs	2.5 µs
Q_w	9.4	9.1	9	8.5
$P_{e,i}$ in light load	0.13	0.1	0.16	0.12
$P_{e,i}$ in medium load	0.3	0.21	0.2	0.23
$P_{e,i}$ in heavy load	0.42	0.39	0.4	0.37
TH_L	10	18	15	16
TH_H	47	41	40	43
Average FEC rate	3	6	6.5	5

Table 6.1 shows that the values obtained by the proposed scheme are in agreement with the values obtained through simulation, thereby validating the model proposed.

Now we compare the proposed scheme with the existing schemes of traditional static FEC, Adaptive FEC and ERED FEC along the performance parameters like Packet Error Rate, DFR and queue length.

6.1 PACKET LOSS RATE

The Packet Loss Rate is one of the most important metrics to analyse the performance of an FEC scheme. If the FEC is robust then the rate of packets being lost will be low because the

redundant packets will reconstruct the lost packets at the receiver's end. Here we are comparing the packet loss rate of each video packet, as obtained by simulating the static FEC algorithm, adaptive FEC algorithm, ERED FEC and ERED FEC with the proposed improvement. The simulation of each algorithm is done on the "Sample" video, whose description has been given in the previous chapter.

Figure 6.1: Average Packet Error Rate per Video Block

As can be seen in the graph, the proposed improvement helps in lowering the packet loss rate in the video blocks of the video stream. Lower packet loss rate indicate an improvement in the traffic load and congestion because lower loss rate means less retransmissions which will help the network remain congestion free for new packets. The total number of packets have been grouped into sections of 30 packets and the average PER for each group of 30 packets was calculated and plotted to obtain the xgraph.

6.2 FEC RATE AT DIFFERENT TRAFFIC LOAD

Different amount of traffic, ranging from very lightly loaded to very heavily loaded, was generated through a period of 300 seconds. The performance of each of the algorithms is observed for the varying traffic in terms of the number of FEC packets generated. According

to various mechanisms, the static FEC algorithm does not alter its stream of FEC packets, the A FEC scheme keeps the number of redundant packets on the higher side, but lowers it slightly when the traffic load is too heavy. The ERED algorithm is particularly sensitive to both the traffic load and the channel conditions, therefore it increases the FEC rate in light traffic and decreases it heavy traffic. The proposed scheme behaves similar to ERED algorithm and adjusts the FEC rate in accordance with the traffic.

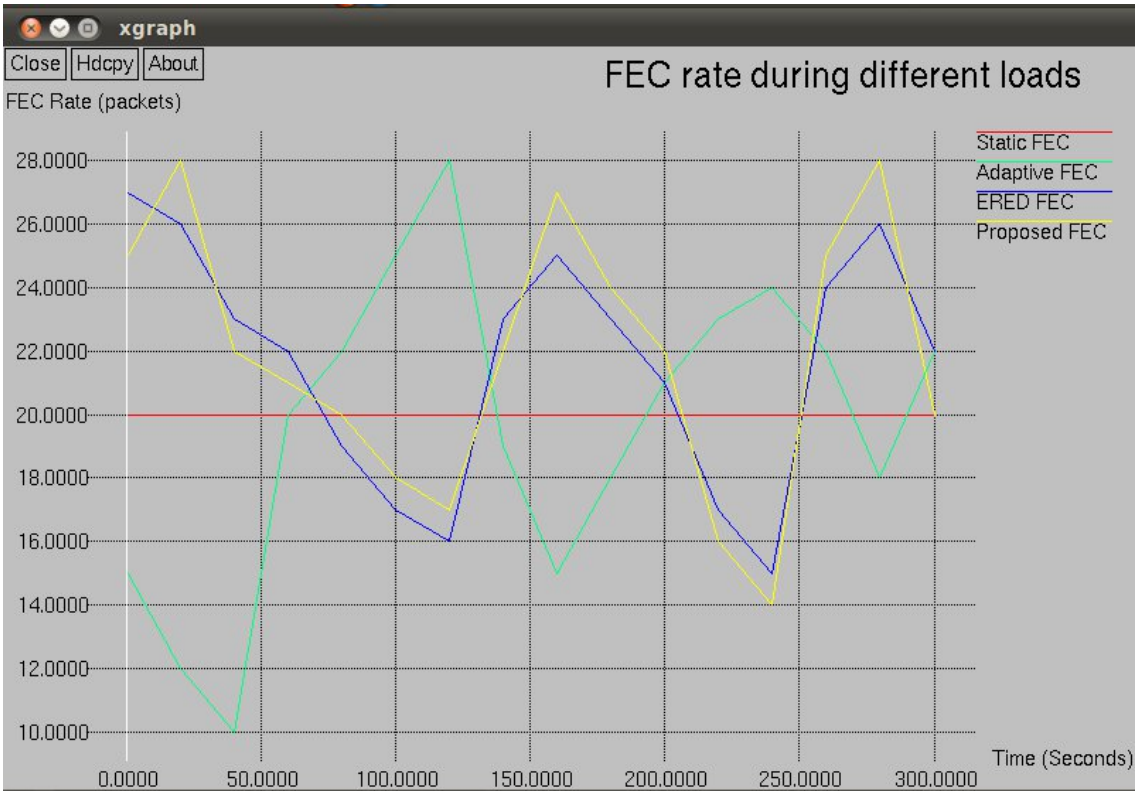

Figure 6.2: FEC Rate During Different Loads

6.3 EFFECT OF BURST ERRORS ON NUMBER OF PACKETS RECEIVED SUCCESSFULLY

The main objective of the proposed improvement was to increase the success rate of received packets despite the presence of burst errors. All the existing FEC schemes are susceptible to burst errors, some more than others. The video was delivered using different algorithms and introducing burst errors at random times and of random lengths to observe the number of packets that can successfully reconstructed at the receiver's end.

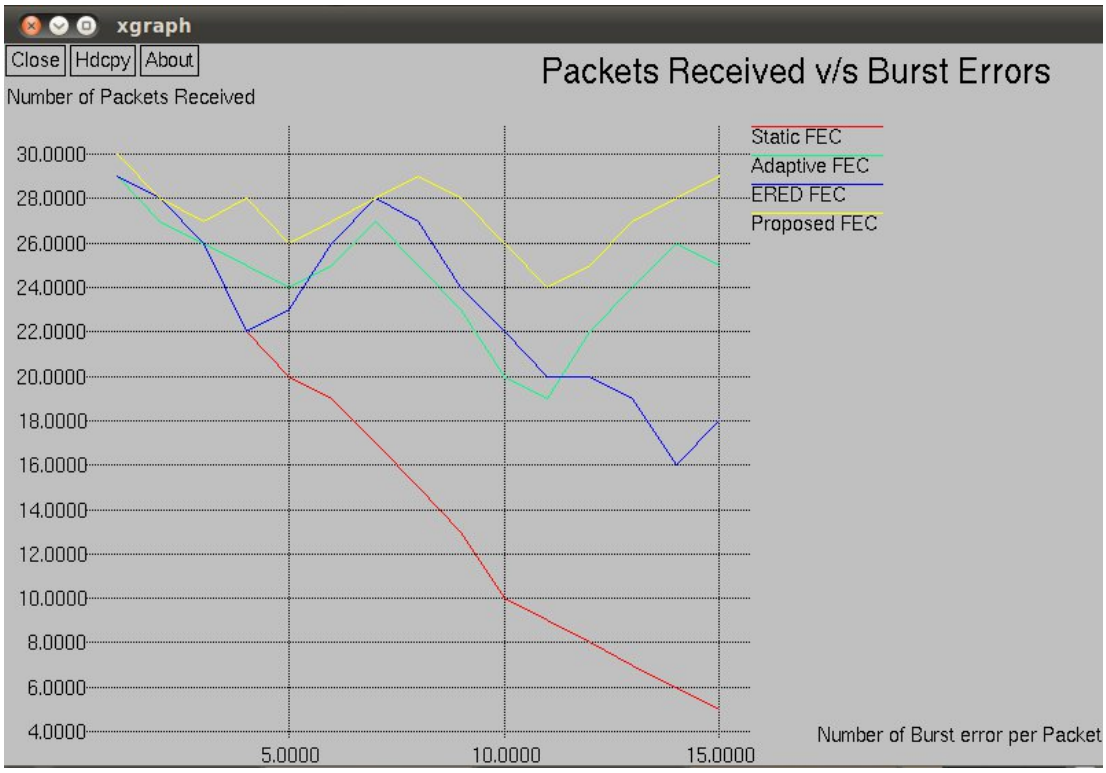

Figure 6.3: Packets Received v/s Burst Errors

It is clear from figure 6.3 that as the length and frequency of burst errors increased, the number of packets that could be reconstructed successfully in each scheme got affected. The performance of static FEC kept degrading and AFEC and ERED tried to fluctuate their FEC rate and increase their performance but ultimately failed to do so at large number of burst errors. The proposed scheme, however, had better results at reconstructing the packets because its performance during burst errors allowed the survival of enough packets that the whole block could be reconstructed.

6.4DFR FOR DIFFERENT FEC RATES

DFR is one of the prime parameters to analyse the quality of the received video and packet error rate is a parameter to explore the channel conditions. The correlation between DFR and Packet Error Rate is explored while fixing the FEC redundancy rate equal to 1, 2, 4 and 6.

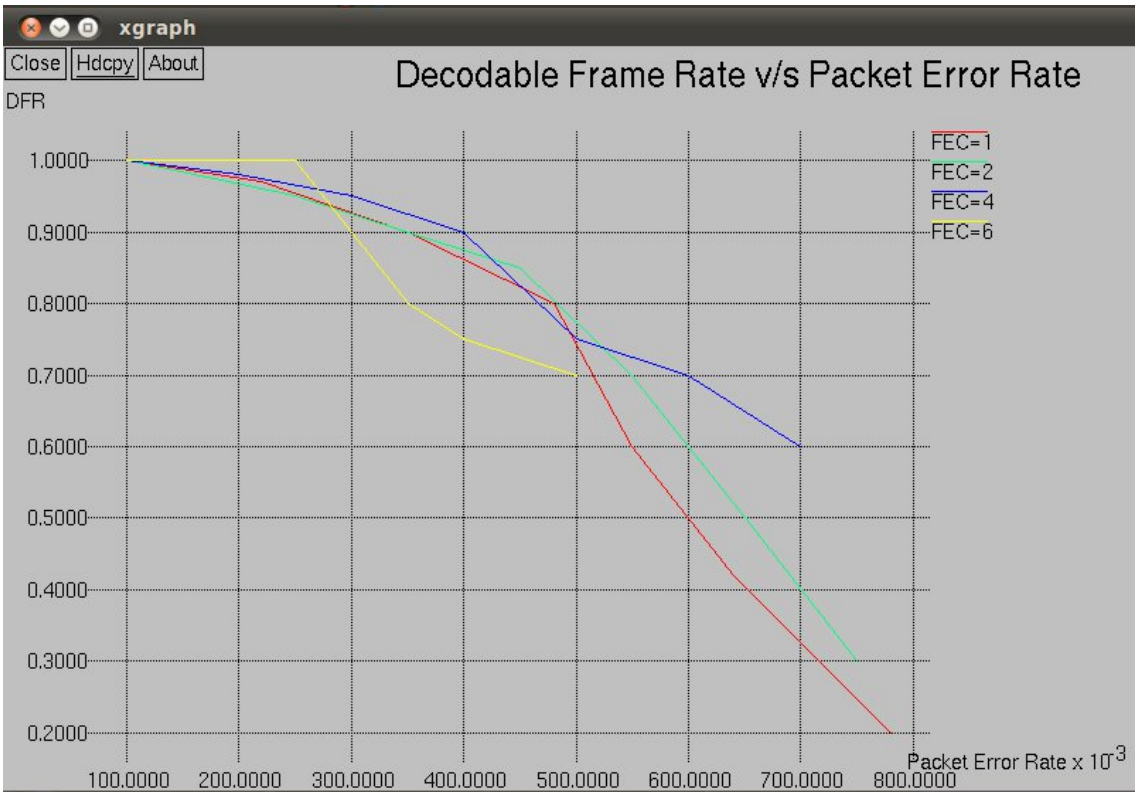

Figure 6.4: DFR v/s Packet Error Rate

Figure 6.4 shows that as the FEC rate increases, the packet error rate is decreased. This implies that a sufficient number of packets reach the destination without any errors and the whole packet is successfully reassembled. The more the number of successfully received packets, the better is the quality of the video. DFR is increased as the packet loss rate is decreased.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

The ERED FEC mechanism is a popular mechanism which employs techniques to evaluate both the network traffic and the channel conditions. But in the scheme that was proposed, the technique of interleaving was also introduced so that the effect of burst errors can be minimised. Through simulations we observed that by applying interleaving, the packet error rate per video block decreased. This consequently affected the traffic load as well because the lowering of packet rate will result in less number of retransmissions, hence the network will remain congestion free. The FEC rates of each scheme are fixed according to the algorithm followed by it. It is observed that the FEC rate of the static FEC does not alter at all, while the FEC rate of AFEC alters depending upon the traffic on the network. The FEC rate in the case of ERED FEC and the proposed scheme remain closer in value to each other. This is because the interleaving affects the number of recovered packets, packet error rate and the video quality but it has little effect at the fixing of the FEC rate. The proposed scheme also performed well in coping with the burst errors, while other schemes had deteriorated performance. The number of packets successfully reconstructed at the receiver's end during the burst errors is a validation that interleaving helped improve the performance of the FEC scheme.

Though there are visible performance improvements in coping with burst errors yet there are a few areas in which the proposed method falls short. The interleaving process at the AP causes some delay in the overall processing and transmitting of the packets. Perhaps, in the future AP devices with high computational power can be employed to overcome this shortcoming. The queue processing of the AP combined with the interleaving array and the time taken to transfer the bits over the medium cause a delay which might hinder the performance of real time video transmission, so perhaps a separate and faster processer can be deployed at the AP to deal with the process of interleaving and to make it faster.

References:

[1] A Mammadov, and B Abbasov. "A review of protocols related to enhancement of UDP performance in wireless and WLAN networks."*Application of Information and Communication Technologies (AICT), 2014 IEEE 8th International Conference on*.IEEE, 2014.

[2] C.H Lin, C.K Shieh, and W.S Hwang. "An access point-based FEC mechanism for video transmission over wireless LANs."*Multimedia, IEEE Transactions on* 15.1, 2013

[3] W Wang, S.C Liew, and V.O Li. "Solutions to performance problems in VoIP over a 802.11 wireless LAN." *Vehicular Technology, IEEE Transactions on* 54.1, 2005

[4] D Wu, Y.T Hou, and Y.Q Zhang. "Transporting real-time video over the Internet: Challenges and approaches." *Proceedings of the IEEE*88.12, 2008

[5] S.H Chang et al. "A priority selected cache algorithm for video relay in streaming applications." *Broadcasting, IEEE Transactions on* 53.1, 2007

[6] K Ahmavaara, H Haverinen, and R Pichna. "Interworking architecture between 3GPP and WLAN systems." *Communications Magazine, IEEE* 41.11, 2009

[7] D Zhu et al. "Analysis of Protocol Based on Extended Service Set for IEEE 802.11 Infrastructure WLAN." *2014 International Conference on Identification, Information and Knowledge in the Internet of Things, Beijing, China*. 2012.

[8] E.S Arrais and C.C Monteiro."Analysis of infrastructured WLAN with Distribution System." *Advanced Communication Technology (ICACT), 2013 15th International Conference on*.IEEE, 2013.

[9] A Ganz, Z Ganv and K Wongthavarawat, “Multimedia Wireless Networks - Technologies, Standards and QoS”, Prentice Hall PTR, Upper Saddle River, NJ, 2004.

[10] Y Singh et al. "Performance Evaluation of On-Demand Multicasting Routing Protocols in Adhoc Networks." *Recent Trends in Information, Telecommunication and Computing (ITC), 2010 International Conference on*.IEEE, 2010.

[11] “Standard for Information technology-- Telecommunications and information exchange between systems—Local and metropolitan area networks-- Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz”IEEE 802.11ac, 2013

[12] Li, Bo, and Hao Yin. "Peer-to-peer live video streaming on the internet: issues, existing approaches, and challenges [Peer-to-Peer Multimedia Streaming]."*Communications Magazine, IEEE* 45.6,2007

[13]J.J Ahmad, H.A Khan, and S.A Khayam."Energy efficient video compression for wireless networks." *Information Sciences and Systems, 2009.CISS 2009.43rd Annual Conference on*.IEEE, 2009.

[14] R Puri and K Ramchandran. "PRISM: A new robust video coding architecture based on distributed compression principles." *Proceedings of the annual allerton conference on communication control and computing*.Vol. 40.No. 1. The University, 2006

[15] “Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification,” ITU-T Rec. H.264 and ISO/IEC 14496-10 AVC, 2014.

[16] G Cheung, A Ortega, and N.M Cheung. "Interactive streaming of stored multiview video using redundant frame structures." *IEEE Transactions on Image Processing* 20.3, 2011

[17] J Kim et al. "Implementation of quality of service control and security based on real-time transport protocol." *Broadband Network & Multimedia Technology (IC-BNMT), 2013 5th IEEE International Conference on*.IEEE, 2013.

[18] G Pan and H Xue. "Real time analysis of current transport protocols in high loss networks." *Computer Science and Network Technology (ICCSNT), 2011 International Conference on*.Vol. 4.IEEE, 2011.

[19] “HTTP Live Streaming Overview”; https://developer.apple.com/library/mac/documentation/NetworkingInternet/Conceptual/StreamingMediaGuide/Introduction/Introduction.html; Accessed on 13 March 2015

[20] “HTTP Dynamic Streaming”; http://www.adobe.com/in/products/hds-dynamic-streaming.html; Accessed on 13 March 2013

[21] T Paul and T Ogunfunmi. "Wireless LAN comes of age: Understanding the IEEE 802.11 n amendment." *Circuits and Systems Magazine, IEEE* 8.1, 2008

[22] Z Zhang. "Some recent progresses in network error correction coding theory." *Network Coding, Theory and Applications, 2008. NetCod 2008.Fourth Workshop on*.IEEE, 2008.

[23] D.A Eckhardt and P Steenkiste."Improving wireless LAN performance via adaptive local error control." *Network Protocols, 2003.Proceedings.Sixth International Conference on*.IEEE, 2003.

[24] L Badia et al. "Analysis of an automatic repeat request scheme addressing long delay channels." *Advanced Information Networking and Applications Workshops, 2009.WAINA'09.International Conference on*.IEEE, 2009.

[25] A Badr et al. "Streaming codes with partial recovery over channels with burst and isolated erasures.", IEEE Transactions, 2014

[26] E. Maani and A. Katsaggelos, “Unequal error protection for robust streaming of scalable video over packet lossy networks,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, pp. 407–416, 2010.

[27] X. J. Dong and P. Varaiya, “Saturation throughput analysis of IEEE 802.11 wireless LANs for a lossy channel,” *IEEE Commun.Lett.*, vol. 9, no. 2, pp. 100–102, 2005.

[28] J. Dan, F. Pascal, and J. Aleksandar, “Forward error correction for multipath media streaming,” *IEEE Trans. Circuits Syst. Video Technol.*,vol. 19, pp. 1315–1326, 2009.

[29] M. Tun, K. K. Loo, and J. Cosmas, “Error-resilient performance of Dirac video codec over packet-erasure channel,” *IEEE Trans. Broadcast.*, vol. 53, pp. 649-659, Sep. 2007

[30] K. Takahata, N. Uchida, and Y. Shibata, “Packet error and frame rate controls for real time video stream over wireless LANs,” in *Proc. Int. Conf. Distributed Computing Systems Workshops, ICDCSW2003*, pp. 594–599, 2003

[31] I. V. Bajic, “Efficient cross-layer error control for wireless video multicast,” *IEEE Trans. Broadcast.*, vol. 53, pp. 276–285, 2007.

[32] K. Park and W. Wang, “AFEC: An adaptive forward error correction protocol for end-to-end transport of real-time traffic,” in *Proc. Int. Conf. Computer Communications and Networks, ICCCN1998*, pp. 196–205, 2004

[33] C. H. Lin, C. H. Ke, C. K. Shieh, and N. Chilamkurti, “An enhanced adaptive FEC mechanism for video delivery over wireless networks,”in*Proc. Int. Conf. Networking and Services, ICNS2006*, 2006.

[34] C. H. Lin, C. K. Shieh, N. Chilamkurti, C. H. Ke, and W. S. Hwang, “A RED-FEC mechanism for video transmission overWLANs,” *IEEE Trans. Broadcast.*, vol. 54, no. 3, pp. 517–524, 2008.

[35] L. Han, S. Park, S. Kang, and H. P. In, “An adaptive cross-layer FEC mechanism for video transmission over 802.11 WLANs,” in *Proc. Int. Conf. Internet, ICI 2009*, pp. 209–215, , 2009

[36] C. H. Lin, C. K. Shieh, W.S. Hwang, “An Access Point-Based FEC Mechanism

for Video Transmission Over Wireless LANs”, IEEE Transactions on Multimedia, vol. 15, no. 1, 2013

[37] “The ns-2 documentation” http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf, Accessed on: 24 March 2015

[38] “OTcl: The User Language”, http://nile.wpi.edu/NS/otcl.html, Accessed on: 30 March 2015

[39] A.M Yeasir, M.M Alam and F Ahmed."SIP-Based QoS in IP Telephony." *Journal of Networks* 9.12, pp: 3415-3426, 2014

[40] D Goyal, N Hemrajani and R Gurjar. "Comparative Analysis of Performance of WMV & MPEG formats Video Streaming in a Cloud.", IEEE Tans. Broadcast, vol. 57, no. 4, 2011

[41] “Basic concepts of video streaming and the evolution of video compression standards”, http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/videodg/vidguide/basics.html, Accessed on 2 April 2014

List of Publications

PAPER PUBLICATION

- M. Maini and A.K. Verma, "Evolution of FEC Mechanisms for Video Transmission over WLAN", *The 5th International Conference on IT Convergence and Security 2015 (ICITCS2015)*, Kuala Lumpur, Malaysia, August 2015. [Accepted]
- M. Maini and A.K. Verma, "Improvement of ERED FEC Mechanisms for Video Transmission on WLAN",*Twelfth International Conference on Wireless and Optical Communications Networks (WOCN2015)*, M.S. Ramaiah Institute of Technology and Bangalore University, Bangalore , Karnataka India, September 2015. [Accepted]

VIDEO PUBLICATION

A video about the journey of this research has been published on www.youtube.com and the link for the video is given as:

https://www.youtube.com/watch?v=dmBZK1n88U8