Wireless LANs

Protocols, Security and Deployment

Anand R. Prasad

Cover designed by the author with the support of: J. Hamard, D. Heering, E. Karipidis, D. Maligin, N. Matoba, P. Mendes, A. Mihovska, M. Monti, L. Muñoz, C. Noda, S. Park S. Thakolsri, A. Villavicencio, T. Walter, H. Wang and the authors' family.

Wireless LANs

Protocols, Security and Deployment

Wireless LANs

Protocols, Security and Deployment

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof.dr.ir. J.T. Fokkema,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen

op maandag 15 december 2003 te 10:30 uur

door

Anand Raghawa PRASAD

elektrotechnisch ingenieur
geboren te Ranchi, Bihar, India

Dit proefschrift is goedgekeurd door de promotor(en):
Prof.dr.ir. I.G.M.M. Niemegeers

Samenstelling promotiecommissie:

Rector Magnificus	voorzitter
Prof.dr.ir. I.G.M.M. Niemegeers	Technische Universiteit Delft, promotor
Prof.dr.ir. P. Demeester	Universiteit Gent
Dr. J. Farserotu	CSEM, Switzerland
Dr. S.H. de Groot	Universiteit Twente
Prof.dr.ir. L.P. Ligthart	Technische Universiteit Delft
Prof.ir. E.F. Michiels	Universiteit Twente
Prof.dr.ir. L.J.M. Nieuwenhuis	Universiteit Twente

Published and distributed by: DUP Science

DUP Science is an imprint of
Delft University Press
P.O. Box 98
2600 MG Delft
The Netherlands
Telephone: +31 15 27 85 678
Telefax: + 31 15 27 85 706
E-mail: info@library.tudelft.nl

ISBN 90-407-2436-9

Keywords: 3

Printed in The Netherlands

To my parents Ramjee and Jyoti Prasad
who sparked the fire of knowledge within me and taught me to control and guide it
To my sister, Neeli, and my brother, Rajeev
together we experimented with the fire of knowledge and learned to enjoy it
To Junko my wife
with whom I will keep the fire alive through our journey of life
To Ruchika my daughter
who will take this fire of knowledge and use it for the best of humankind

Abstract

This thesis presents a broad range of work done in the field of Wireless Local Area Networks (WLANs). It proposes several novel schemes of which performance are analyzed.

The thesis first proposes an Automatic Repeat reQuest (ARQ) scheme named as Selective Repeat / Multi-Copy (SR/MC). The purpose of the proposed SR/MC ARQ scheme is to transmit Internet Protocol (IP) packets efficiently in WLANs. At first the proposed scheme fragments an IP packet and transmits the fragments in Selective Repeat (SR) mode until the last fragment is transmitted after that, if erroneous fragments are still left, it goes in Multi Copy (MC) mode. In MC mode multiple copies of erroneous fragments are transmitted cyclically. A numerical performance analysis of the proposed SR/MC ARQ scheme is done and all its parameters are optimized. Using the simulation results of the Physical layer the optimized values are then used to study the performance of the scheme in terms of throughput both in an Additive White Gaussian Noise (AWGN) channel and a flat Rayleigh fading channel. The numerical results show that the proposed SR/MC ARQ scheme gives an improvement of 8 dB when compared to the Selective Repeat + Stutter Scheme 2 (SR+ST 2) scheme, under flat Rayleigh fading channel using BCH(63,51,2) for the throughput of 0.9. The measurement results also show similar performance. The proposed SR/MC ARQ scheme was implemented and applied for patent by the author; it was used for Wireless Network Interface Card (WNIC), a proprietary WLAN, of Uniden Corporation, Tokyo, Japan.

Next a novel Medium Access Control (MAC) protocol, named as Channel Sharing Protocol (CSP), is proposed. The proposed CSP uses tokens in the wireless medium to give fair access of the medium to a large number of users. The scheme uses a p-persistence algorithm to avoid collision. Simulations were performed to optimize the different parameters of the proposed CSP and to study its performance. A numerical study was also done for performance evaluation. There is a difference between the numerical and the simulation results due to the assumptions made during the numerical performance evaluation. Both the numerical and the simulation results show that the proposed CSP outperforms the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) MAC protocol of the IEEE 802.11 WLANs. A detailed design of the proposed CSP for implementation in WNIC was done and it was applied for patent by the author.

Today the WLANs focus mainly on the non real time data communication while the market is looking towards real time traffic. Bearing this in mind the IEEE 802.11, a WLAN standard, is working on MAC enhancements focusing on Quality of Service (QoS). Several QoS solutions for the IEEE 802.11 existed when the work presented in this thesis was started. These solutions are Blackburst, priority queuing, the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF). The work presented in this thesis was started at the preliminary stages of the IEEE 802.11e standardization. The purpose of the work was to give a first idea of an acceptable solution. In this thesis the four solutions are presented and a qualitative analysis is done. IEEE 802.11e has accepted priority queuing, chosen as the best solution in the thesis, as one of the solutions for QoS.

Security in a wireless medium, a medium accessible to all, is a major issue. The WLAN currently in use, IEEE 802.11, has been found to have several security flaws. Even before the security flaws were publicly known the IEEE 802.11 standardization committee had started working on security enhancements. The work presented in this thesis was done during the

preliminary stage of the IEEE 802.11i, security enhancements of IEEE 802.11 MAC, standardization (then IEEE 802.11e). Some of the ideas were presented to the IEEE 802.11 standardization committee. The work started with proposing requirements for various environments where the WLANs were envisioned to be used. The environments studied in this thesis are enterprise, academic and public. The security requirements for these environments are proposed in this thesis. Security solutions for each environment are also proposed herein. A qualitative analysis of the proposed solutions is also given in this thesis. A common problem in all the solutions was access control; so as to solve this problem an access control protocol is proposed. Finally the security issues for the future wireless communications systems are examined. The standard reflects some of the ideas presented in the thesis. The access control protocol proposed in the thesis, applied for patent by the author, is very similar to the now standardized IEEE 802.11f, Inter Access Point Protocol (IAPP).

System design and planning of the network for the IEEE 802.11 WLANs in different environments is a major issue. The IEEE 802.11 standard gives several options for optimum system design while the standard makes use of the unlicensed band. The unlicensed band can be used by any wireless system fulfilling the regulatory requirements; these systems will cause interference with the IEEE 802.11 WLANs at the same time IEEE 802.11 has limited the number of non-overlapping channels. A study on systems design and deployment of the WLAN network is required. In this thesis the issues related to the IEEE 802.11 system design and results of several deployment related critical issues like coverage, cell/frequency planning, interference, and data rate are examined. This work was used for system design and deployment of the ORiNOCO WLANs of Lucent Technologies. An automatic rate control scheme used by the ORiNOCO product was applied for patent by the author.

Samenvatting (Summary in Dutch)

Dit proefschrift presenteert een breed scala aan werk dat is uitgevoerd op het gebied van *Wireless Local Area Networks* (WLANs). Diverse nieuwe protocollen worden voorgesteld, waarvan de prestaties zijn geanalyseerd.

Als eerste wordt een *Automatic Repeat reQuest* (ARQ) protocol voorgesteld, dat *Selective Repeat / Multi-Copy* (SR/MC) is genoemd. Het doel van dit SR/MC ARQ procotol is het efficiënt versturen van *Internet Protocol* (IP) pakketten over WLANs. Het voorgestelde protocol begint met het fragmenteren van een IP pakket en verzendt de fragmenten in *Selective Repeat* (SR) modus totdat het laatste fragment is verzonden. Als er daarna nog foutieve fragmenten resteren, schakelt het protocol over naar *Multi Copy* (MC) modus. In MC modus worden meerdere kopieën van de foutieve fragmenten cyclisch verzonden. Numerieke prestatie analyse van het voorgestelde SR/MC ARQ protocol is uitgevoerd en de parameters zijn geoptimaliseerd. De optimale waarden, middels simulatie van de *physical layer* verkregen, zijn vervolgens gebruikt om de prestaties van het protocol in termen van doorvoersnelheid te bestuderen voor zowel een *Additive White Gaussian Noise* (AWGN) kanaal als een *flat Rayleigh fading* kanaal. De numerieke resultaten laten zien dat het voorgestelde SR/MC ARQ protocol een verbetering van 8 dB geeft ten opzichte van het *Selective Repeat + Stutter* 2 (SR+ST 2) protocol, gebruik makend van een *flat Rayleigh fading* kanaal met BCH(63,51,2) voor een *throughput* van 0.9. De resultaten van meetproeven vertonen overeenkomstige resultaten. De auteur heeft octrooi aangevraagd voor het voorgestelde SR/MC ARQ protocol en heeft het geïmplementeerd; het is gebruikt voor *Wireless Network Interface Card* (WNIC), een fabrikantseigen WLAN van Uniden Corporation, Tokyo, Japan

Vervolgens wordt een nieuw *Medium Access Control* (MAC) protocol voorgesteld, genaamd *Channel Sharing Protocol* (CSP). Het CSP maakt gebruik van *tokens* om toegang tot het draadloze medium eerlijk te verdelen over een groot aantal gebruikers. Het protocol maakt gebruik van een *p-persistence* algoritme om *collisions* te voorkomen. Voor het optimaliseren van de verschillende parameters en om de prestaties te bestuderen, zijn simulaties uitgevoerd. Tevens is voor de prestatie analyse een numerieke studie uitgevoerd. Er is een verschil tussen de numerieke studie en de simulatie door de aannames die zijn gemaakt tijdens de numerieke prestatie analyse. Zowel de numerieke studie als de simulatie tonen aan dat het voorgestelde CSP beter presteert dan het *Carrier Sense Multiple Access/Collision Avoidance* (CSMA/CA) MAC van de IEEE 802.11 WLANs. De auteur heft octrooi aangevraagd voor het voorgestelde CSP en heeft een gedetailleerd ontwerp voor implementatie in WNIC uitgevoerd.

De huidige WLANs concentreren zich voornamelijk op niet *real-time* data communicatie, terwijl de markt voornamelijk op zoek is naar *real-time traffic.* Met dit gegeven in het achterhoofd, is men bezig de IEEE 802.11 WLAN standaard te voorzien van MAC verbeteringen, gericht op *Quality of Service* (QoS). Op het moment dat werk voor dit proefschrift begon, bestonden er al verschillende QoS oplossingen voor IEEE 802.11. Deze oplossingen zijn *Blackburst, priority queuing,* de *Distributed Coordination Function* (DCF) en de *Point Coordination Function* (PCF). Het in dit proefschrift gepresenteerde werk is begonnen in de voorbereidende fase van de IEEE 802.11e standaard. Het doel van het werk was het geven van een eerste indruk van een acceptabele oplossing. Vier oplossingen, en de kwalitatieve analyse daarvan, worden in dit proefschrift gepresenteerd. IEEE 802.11e heeft gekozen voor *priority queuing*, in dit proefschrift aangewezen als de beste oplossing, als één van de oplossingen voor QoS.

Beveiliging van een draadloos medium, dat toegankelijk is voor iedereen, is een essentieel aandachtspunt. Van het huidig in gebruik zijnde WLAN, IEEE 802.11, is gebleken dat het een aantal beveiligingslekken bevat. Al voordat de beveiligingslekken publiekelijk bekend waren, is het IEEE 802.11 standaardisatiecomité begonnen met het werken aan verbeteringen van de beveiliging. Het in dit proefschrift gepresenteerde werk is uitgevoerd gedurende de voorbereidende fase van verbetering van beveiliging van IEEE 802.11 MAC, de IEEE 802.11i standaardisatie (toen bekend als IEEE 802.11e). Een aantal van de ideeën zijn gepresenteerd aan het IEEE 802.11 standaardisatiecomité. Begonnen is met het voorstellen van vereisten voor de verschillende omgevingen waarbinnen gebruik van WLANs voorzien wordt. De omgevingen die in dit proefschrift zijn bestudeerd, zijn: onderneming, academisch en openbaar. De beveiligingsvereisten voor deze omgevingen worden voorgesteld in dit proefschrift. Beveilingsoplossingen voor elke omgeving worden hier tevens voorgesteld. Een kwalitatieve analyse van de voorgestelde oplossingen wordt tevens gegeven in dit proefschrift. Een algemeen probleem in al de oplossingen was *access control*; om dit probleem op te lossen wordt een protocol voor *access control* voorgesteld. Tenslotte worden de beveiligingsvraagstukken voor toekomstige draadloze communicatiesystemen bestudeerd. De standaard weerspiegelt sommige van de in dit proefschrift gepresenteerde ideeën. Het protocol voor *access control* dat in proefschrift wordt voorgesteld en waar de auteur octrooi voor heeft aangevraagd, vertoond grote gelijkenis met het nu tot standaard verheven *Inter Access Point Protocol* (IAPP) IEEE 802.11f.

Systeemontwerp en netwerkplanning van IEEE 802.11 WLANs in verschillende omgevingen is een essentieel aandachtspunt. De IEEE 802.11 standaard voorziet in diverse mogelijkheden voor optimaal systeemontwerp, terwijl de standaard gebruik maakt van de frequentieband waarvoor geen licentie nodig is. Deze vrij te gebruiken frequentieband kan worden gebruikt door elk draadloos systeem dat voldoet aan door regelgeving opgelegde vereisten. Deze systemen veroorzaken echter interferentie met de IEEE 802.11 WLANs, tegelijkertijd limiteert IEEE 802.11 het aantal niet overlappende kanalen. Een studie naar systeemontwerp en uitrol van het WLAN netwerk is noodzakelijk. In dit proefschrift worden aandachtspunten, gerelateerd aan het IEEE 802.11 systeemontwerp en de resultaten van verschillende aan uitrol gerelateerde aandachtspunten als dekking, planning van *cell/frequency*, interferentie en *data rate*, onderzocht. Dit werk is gebruikt voor het systeemontwerp en de uitrol van de ORiNOCO WLANs van Lucent Technologies. Voor een protocol voor automatische *rate control*, gebruikt door het ORiNOCO product, is door de auteur octrooi aangevraagd.

Preface

न वित्तेन तर्पणीयो हि मनुष्यः

(Not by wealth alone is a man satisfied)

-Rig Ved

Even after all the earthly riches are enjoyed there still remains in the heart a longing for knowledge, true knowledge. It is this longing which resulted in the revelation of this Ph.D. work. This thesis is written for the completion of the Philosophiae Doctor (doctor of philosophy) or Ph.D. degree from Delft University of Technology.

The Ph.D. work was started in 1996 together with my first job as a Research Engineer in Uniden Corporation, Tokyo, Japan. Our group at Tokyo Research and Development (TRC) constituted of 21 young researchers at that time, including the Director. Most people in the group were fresh graduates from Universities. The task of the group was to develop a proprietary Wireless Local Area Network (WLAN). My first task was to design an Automatic Repeat reQuest (ARQ) scheme.

The work was completed successfully with the design of a novel and efficient Selective Repeat/Multi Copy ARQ scheme. The performance of the ARQ scheme was studied separately and together with the baseband simulation. The ARQ was then implemented and tested till it was stable.

After finishing the work on the ARQ my next task was to design a novel protocol for efficient channel access so as to increase the capacity of the proprietary WLAN. The first protocol allowed one user per channel. In order to improve the capacity I designed a Channel Sharing Protocol (CSP) and studied its numerical and simulation performance. After studying the performance I prepared the implementation design of the CSP.

In 1998 the Ph.D. work was continued in Wireless Communications and Networking Division (WCND) of Lucent Technologies, Nieuwegein, The Netherlands. Now the work moved from proprietary WLANs to a WLAN standard based on IEEE 802.11. In WCND as a Systems Architect and member of the New Technology Area (NTA), I fulfilled several tasks including designing security schemes, participating in standardization committees and studying network deployment issues to name a few.

As the IEEE 802.11 standard was looking at Medium Access Control (MAC) enhancements I studied Quality of Service (QoS) mechanisms for IEEE 802.11 and made a qualitative comparison of a few schemes. At the same time I studied security schemes for the IEEE 802.11 WLANs.

The first job for the security schemes was to set the requirements for the envisaged environments in which a WLAN was expected to be used. After I had set the requirements for each environment I worked on solutions and did qualitative analysis of the solutions. Based on these studies a security solution was proposed for IEEE 802.11 WLAN standard.

Parallel to my task as Systems Architect and member of NTA, I also worked together with others on issues related to WLAN deployment.

Wireless technology, although more than a century old, is still an infant in terms of what can be achieved with it while WLAN is barely a decade old technique. Lot of technical challenges still

remain and several new standards and ideas are continuously being developed. At the time of writing this thesis, in the market of WLANs, IEEE 802.11 was the only standard of which products were available and even for this standard study was continuing on both MAC and PHY (PHYsical layer) enhancements.

It is assumed that anyone reading this thesis has prior knowledge of wireless communications.

Acknowledgment

I am very grateful to Prof. I.G.M.M. Niemegeers for his supervision, interest, confidence and for reviewing my work. His comments on the thesis and his support have been invaluable. My sincere thanks also to the committee members Dr. J. Farserotu and Prof. E.F. Michiels for their comments on the thesis.

I would also like to express my gratitude towards Dr. S. Kato who gave me the chance to begin my work at Uniden Corporation in Japan. My sincere thanks also to N. Matsuoka my *sempai* at Uniden Corporation and K. Ogata who worked with me on the Channel Sharing Protocol. Also I want to express my gratitude to Dr. K. Seki and H. Kato for their guidance. My special thanks also to I. Mohamed, a friend with very creative mind and endless lust for knowledge who worked with me and discussed ideas with me very often, a novel coding scheme being one of them. Imine also checked and provided comments on the complete thesis. A special thanks also to my friends A. Taguchi, I. Khan, R. Dayon, who always said that I would achieve my goal and supported me, and to D. Matic who also reviewed and helped in improving the thesis. I would also like to express my thanks to my friends and colleagues from Uniden Corporation: Y. Aketa, M. Fujino, T. Hattori, A. Hirano, Kuwazoe, A. Murayama, Y. Omoya, K. Sanada, Y. Shinohara, M. Takamiya, I. Tonegawa, Yamada and H. Yoshioka. Particularly I would like to thank Y. Shinohara who helped me finding information on the Wireless Network Interface Card project even after both of us had left Uniden Corporation.

Further I would like to thank the Wireless Communications and Networking Division, at Lucent Technologies (now Agere Systems) for allowing me to proceed with my dissertation work; especially J. Kruys (now at Cisco Systems), Dr. B. Tuch, L. Monteban, A. Kamerman and A. Eikelenboom. In particular I would like to thank my colleague and mentor Henri Moelard for his support and encouragement.

At DoCoMo Euro-Labs I received support to finish my Ph.D., for this I would like to thank Dr. A. Murase and Mr. P. Schoo. The cover of the thesis, saying ‘efficiency’ and ‘robustness’ in different languages, was prepared with help of several people, my colleagues in DoCoMo Euro-Labs J. Hamard, E. Karipidis, N. Matoba, P. Mendes, C. Noda, S. Thakolsri, T. Walter and H. Wang, from Capcad D. Maligin, from PCOM:I^3 M. Monti, friends D. Heering, A. Mihovska, L. Muñoz, S. Park and A. Villavicencio and my family.

Delft University regulations requires Dutch version of propositions and abstract if the thesis is written in a foreign language. A friend of mine, D. Heering, translated my propositions and abstract from English to Dutch. I am ever grateful to him to this translation in a very short notice.

As per the Indian way we do not thank the people very close to us, usually the family members, still I would at-least like to mention that my work and career has reached so far due to their well wishes. My parents (Jyoti and Ramjee Prasad) awakened the interest of gaining knowledge within me and my brother (Rajeev Ranjan Prasad) and sister (Neeli Rashmi Prasad) with whom I enjoyed learning while becoming a global citizen. Jami (Mahbubul Alam), my brother in-law, with his energy gave me more power to learn and continue my work than he knows. Sneha, my sister’s daughter, who brings joy and love to everyone. Last but not least, Junko, my wife, who is and always will be with me in any endeavour of my life: a true life partner and Ruchika my daughter who is the light in my eyes.

With this I would also like to show my gratitude towards all other friends and colleagues I have not mentioned here. One cannot achieve anything without the well wishes of the people one knows and people around them. I thank everyone I have ever met for their well wishes.

Anand R. Prasad
Munich, Germany
Wednesday, 05 November 2003

Table of Contents

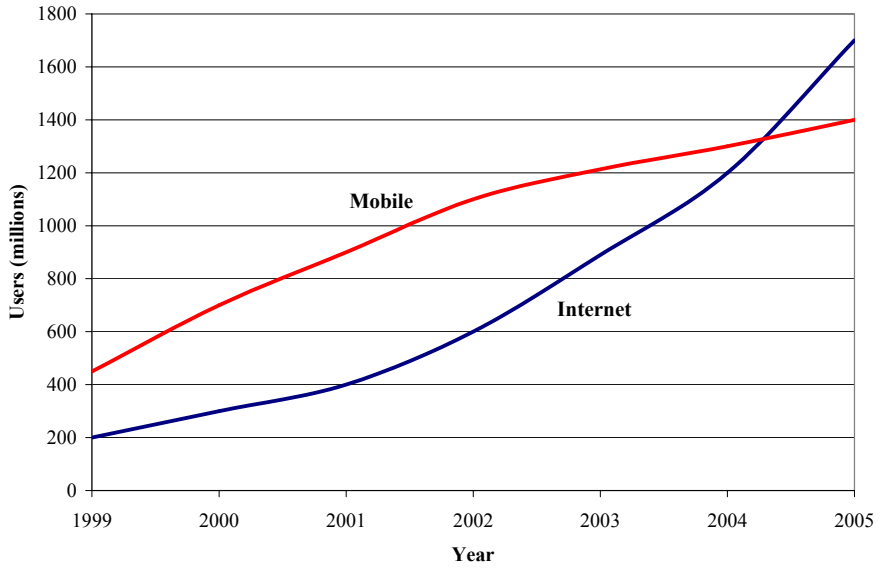
List of Figures

List of Tables

Chapter 1

Introduction

The past decade has shown major changes in the types of communication services provided to the users and the infrastructure used for them. Besides the present-day telephony, Internet access, applications with remote servers, video on demand and interactive multimedia are just a few examples of such services. Internet access is the service that has captured the biggest market and enjoys maximum penetration; this is shown in Figure 1-1 for year and number of users. Wireline communications networks providing these services are mostly known as Wide Area Networks (WAN) and Local Area Networks (LAN).



Source: Emerging Markets in Telecommunications, May 2001, Ericsson http://www.connect.org/

Figure 1-1 Growth in wireless and Internet.

The overall market demand is basically connectivity, mobility and performance. Wireline services can provide connectivity and performance but not mobility together with connectivity; this market demand is depicted in Figure 1-2. Wireless communications is the solution to the requirements of mobility with connectivity. Thus together with the growth of Internet there has been tremendous growth in the field of wireless communications, Figure 1-1. This has also been due to other inherent benefits of wireless, namely decreased wiring complexity, increased flexibility and ease to install. The main reason behind the growth of wireless has been Wireless WANs (WWANs) or mobile technologies based on second generation (2G / 2.5G) standards like Global System for Mobile Communications (GSM) and Personal Digital Cellular (PDC). These technologies mainly provide voice services and some data services at low data rates. 3G systems provide higher data rates with a maximum throughput of 2 Mbits/s, Figure 1-3.

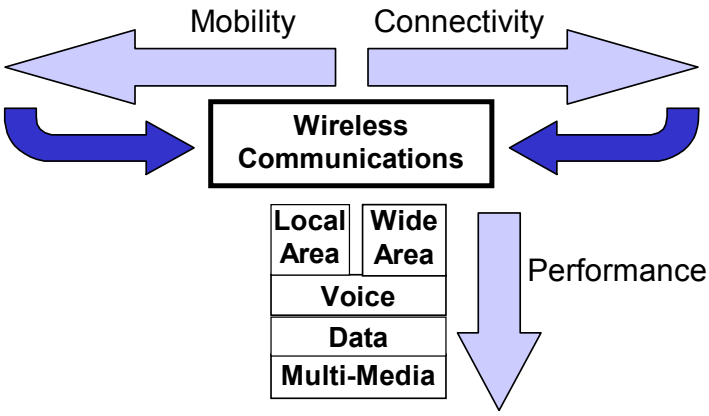


Figure 1-2 Market trend.

Wireless LANs (WLANs) on the other hand provide connectivity, lower mobility and much higher performance in terms of achievable data rate. They are mainly extension of LANs providing high-speed data services with lower mobility. Complementary to WLANs are Wireless Personal Area Network (WPAN) which provide wireless data networking for short range (~10m) at data rates of about 1Mbit/s. A summary of WWANs, WLANs and WPANs standards are given in Figure 1-3 [1-28].

WLANs provide a new forum of access technology in the LAN world. The new access technology fulfils several practical requirements (increased mobility, flexibility, etc.), but still several technical problems remain unsolved. Some of the problems of WLANs are tackled in this thesis.

1.1 WLANs in a Nutshell

WLANs mostly operate using either radio or infrared techniques. Each approach has it own attributes that satisfy different connectivity requirements. The majority of these devices are capable of transmitting information up to several 100 meters in an open environment. In Figure 1-4 an example of WLAN interfacing with a wired network is given. The components of WLANs consist of a wireless network interface card, known as STAtion (STA) and a wireless bridge referred to as Access Point (AP). The AP interfaces the wireless network with the wired network (e.g., Ethernet LAN) [10-16,28].

Figure 1-3 Wide Area, Local Area and Personal Area wireless technologies.

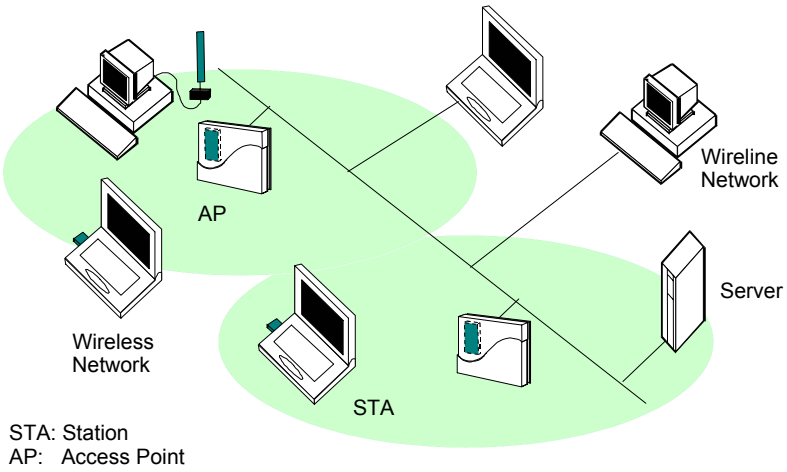


Figure 1-4 A wireless local area network.

The most widely used WLANs use radio waves at the frequency band of 2.4 GHz also known as ISM (Industrial, Scientific and Medical) band. The worldwide availability of the ISM bands, shown in Figure 1-5 and Appendix A: License Exempt Frequency Bands, has made unlicensed spectrum available and promoted significant interest in the design of WLANs. An advantage of radio waves is that they can provide connectivity for non line of sight situations. A disadvantage of radio waves is that the electromagnetic propagation may cause interference with equipment working at the same frequency. Because radio waves propagate through the walls security might also be a problem. Further details of ISM band and other license exempt frequency band standards are given in Appendix B: Comparison WLANs and WPANs Standards.

WLANs based on radio waves usually use spread spectrum technology. Spread spectrum *spreads* the signal power over a wide band of frequencies, which makes the data much less susceptible to electrical noise than conventional radio modulation techniques. Spread spectrum modulators use one of the two methods to spread the signal over a wider spectrum: Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) [29].

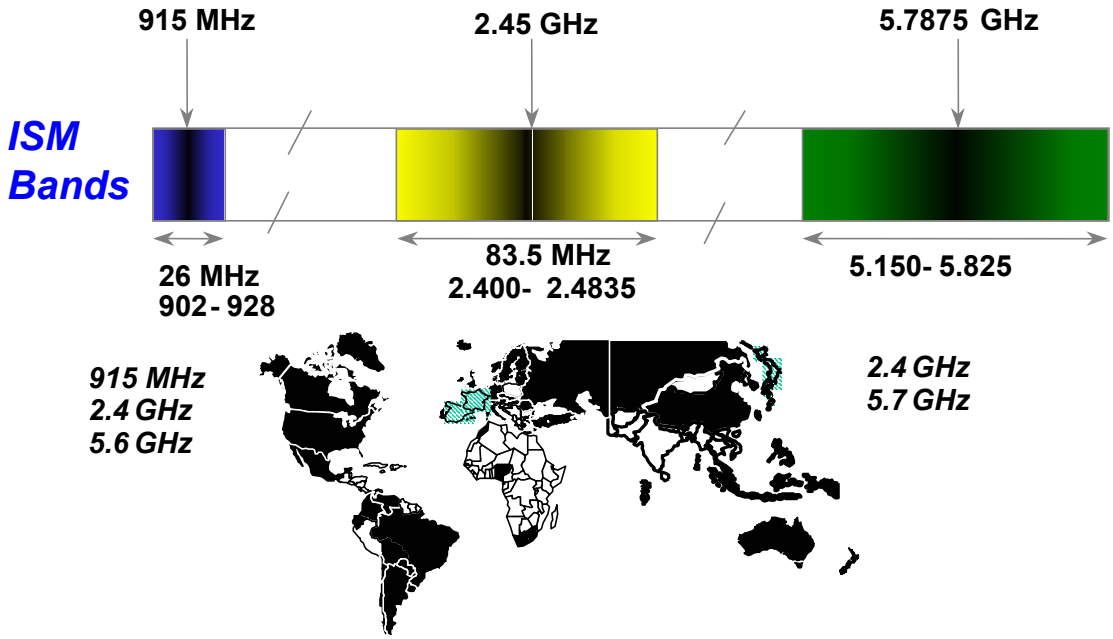


Figure 1-5 Worldwide availability of ISM bands and other license exempt bands.

Figure 1-6 Uniden Corporation WLAN (WNIC).

FHSS works very much as the name implies. It takes the data signal and modulates it with a carrier signal that hops from frequency to frequency as a function of time over a wide band of frequencies. On the other hand DSSS combines a data signal at a sender with a higher data rate bit sequence, thus spreading the signal over the whole frequency band [28,29]. Infrared LANs provide an alternative to radio wave based WLANs. Although infrared has its benefits it is not suitable for many mobile applications due to its line of sight requirement [28].

The first WLAN products appeared in the market around 1990, although the concept of WLANs was known for some years. Figure 1-6 shows Uniden Corporations' WLAN named as Wireless Network Interface Card (WNIC). It was a proprietary system; the first design worked in the 900 MHz ISM band. The main purpose of the system was to provide wireless connection to Network Computers (NC), wireless Internet access and wireless access to e-mail.

WNIC provided 64 kb/s uplink and downlink using Quadrature Phase Shift Keying (QPSK) modulation. A spreading code of 1 Mcps Barker sequence was used. Bose Chaudhuri Hocquenghem or BCH(63,51) was used as error correction scheme. This was because the hardware size of BCH was found to be smaller than other error correction schemes. The specification of WNIC is given in Appendix C: WNIC Specification.

The next generation of WLAN products were implemented on PCMCIA cards (also called PC card) that are used in laptop computers and portable devices. In recent years several WLAN standards have come into being. IEEE 802.11 [10,11,28] based WLAN has been the first and most prominent in the field. IEEE 802.11 has different physical layers working in 2.4 and 5 GHz. Figure 1-7 depicts a Lucent Technologies (now divided between Proxim and Agere Systems) WLAN PC card. It is known as ORiNOCO™, previously it was known as WaveLAN.

Other WLAN standards are HomeRF [13], now considered to be dead, dedicated to home market based on FHSS, besides that High PERformance LAN (HIPERLAN) Type 2 [12,17,21,28] works in the 5 GHz band using OFDM (Orthogonal Frequency Division Multiplexing) technique.

Figure 1-7 Lucent Technologies WLAN PC-Card (ORiNOCO™).

1.2 Research Motivation

The exponential growth of Internet and wireless has brought about tremendous changes in the LAN technology. WLAN technology is becoming more and more important. Although WLAN came into being since the beginning of 1990s the market has just started opening and the technology is still ripening. WLANs are envisaged to be used in several environments like home, office and hot spots to name a few. This is also depicted in Figure 1-8.

The research work reported in this dissertation started towards the end of 1996 when proprietary WLANs were in the market while standardization work was still in progress. The birth of new technology in the wireless arena and the technical challenge thereof was the main motivation for starting this research work. Further details are given in this section.

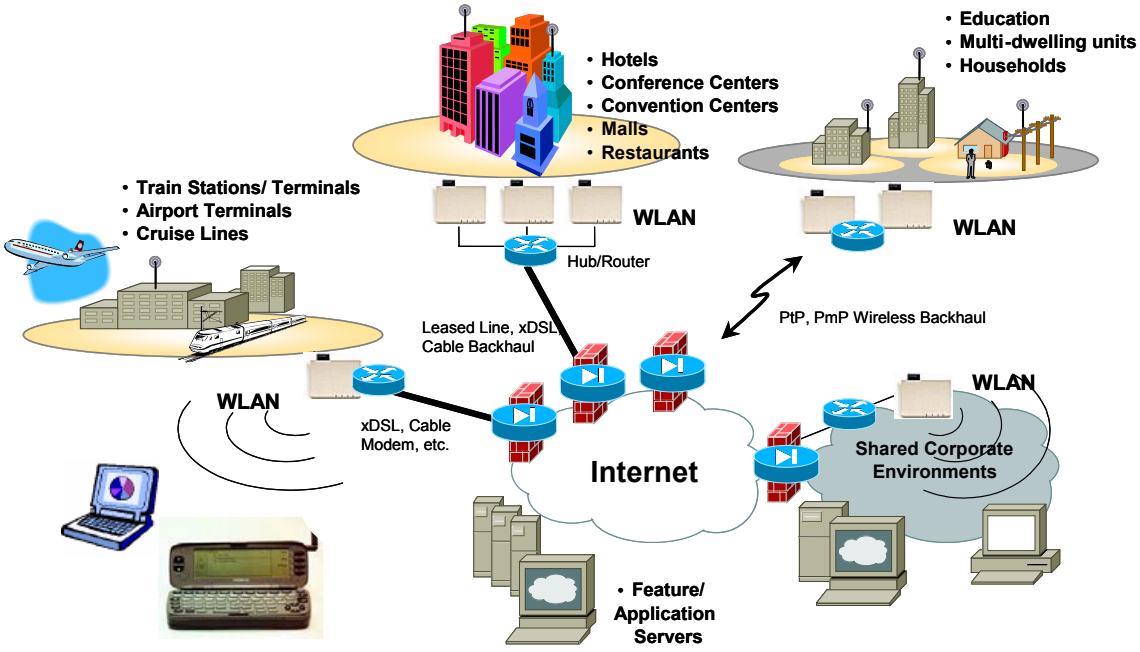


Figure 1-8 WLANs envisaged usage environments.

The primary requirement of wireless Internet is efficient transmission of IP packets in wireless medium. IP packets are designed for wireline communication where error is negligible thus requiring an efficient error correction scheme when used in wireless medium. Basically, error control schemes can be divided in two categories: Automatic Repeat reQuest (ARQ) schemes and Forward Error Correction (FEC) schemes. ARQ schemes are often used for reliable data transmission; this is because FEC requires too many additional bits for perfect data transmission. In the literature several ARQ schemes exist [30,31], but at the time when this work was started none of them were focused on IP packet transmission thus indicating the need for an ARQ for efficient IP packet transmission.

Efficient channel access is also a major issue, as large number of users might want to access the same channel. Here efficiency can be given in terms of throughput and prevention of collision during the channel access. A Medium Access Control (MAC) protocol enables controlled medium access for devices communicating in the same medium. For fulfilling the need of increasing the number of users efficiently communicating in an already crowded and noisy ISM band an efficient MAC protocol is required [29,32].

WLANs are envisioned to be used for real time services which require protocols that can provide the required level of Quality of Service (QoS). As the ISM band is already noisy, achieving true QoS (e.g., voice quality equivalent to toll quality voice on Plain Old Telephone Service or POTS) is difficult. This also brings forward requirements like ease of implementation. Keeping these in mind a study of QoS protocols for WLANs must be done.

A wireless medium is accessible to all, for some this implies the need for higher levels of security than those required for wireline systems. Further WLANs are envisioned to be used in different environments like academia, enterprise, and public spaces. Already current IEEE 802.11 based WLANs are found to have serious security flaws. This brings forward the need for studying security solutions for WLANs such that security requirements for various envisioned usage environments can be fulfilled.

Most of the points mentioned above relate to efficient use of, what many believe is scarce, the wireless spectrum. This motivates the study of WLAN system design and deployment. Deployment itself means studying several things such as co-channel interference, adjacent channel interference and system design to name a few. Study of all these items are, as expected, restricted by the frequency spectrum in use and the number of non-overlapping channels (mostly defined by standards). The challenge is to provide a large number of users with a specified system quality.

1.3 Contributions

The items discussed in Section 1.2 motivated the author to work on various fields related to WLANs. All this work led to contributions to this thesis, they are discussed in this section.

1.3.1 Automatic Repeat reQuest Scheme

There are several known ARQ schemes: Go-Back-N (GBN), Stop and Wait and Selective Repeat (SR) are the most basic ones. In an ARQ scheme correctly received fragments are Acknowledged (ACK) and erroneous fragments are Negatively Acknowledged (NACK). NACKed fragments are then retransmitted. In short, ARQ is an error detection with retransmission scheme [30]. As the purpose of the considered system is wireless IP packet transmission, the efficiency of the system after channel access will depend on the ARQ scheme.

In this thesis, a hybrid ARQ scheme is proposed for IP packet transmission [22,23]. The scheme works in SR mode until all the fragments are transmitted, if a NACK is received, after the last fragment is transmitted, the system goes in Multi-Copy (MC) mode. The proposed hybrid ARQ scheme is named as SR/MC. The proposed hybrid ARQ scheme is optimized in terms of fragment size and number of copies of fragments, M, transmitted in MC mode. First the optimum value for M is calculated for a given IP packet size, fragment size, and throughput. The optimum value of M

is also calculated against the throughput for a given Bit Error Rate (BER), IP packet size, and fragment size. Performance of the proposed ARQ scheme is evaluated in terms of BER, IP packet size and fragmentation size. Additive White Gaussian Noise (AWGN) as well as flat Rayleigh fading channel is used to study the performance of the proposed scheme. Results, in terms of BER and Eb/No, of a DSSS system using QPSK modulation is used to analyze the performance of the ARQ under flat Rayleigh fading channel. All the results are then compared with that of Selective Repeat + Stutter 2 (SR+ST 2) ARQ scheme and conventional GBN [30]. Performance results are obtained with and without BCH(n, k, t) error correction codes.

The optimum result of SR/MC ARQ was found for M=10, and fragment size of 75 bytes. The proposed ARQ outperforms SR+ST 2 and a throughput of 0.9 is achieved for BER of 10^{-3} and IP packet size of 250 bytes [22,23].

SR/MC ARQ was applied for patent and implemented by the author for the proprietary WLAN, WNIC, developed in Tokyo Research and Development Center (TRC) of Uniden Corporation, Tokyo, Japan. The author also implemented simple ARQs like Stop and Wait and Go-Back-N.

Measurement results of the proposed ARQ are similar to the numerical results. The C program of the ARQ implementation was about 1700 lines and the size of the file was 70KB. Processing time required by the ARQ was 1% of the total time required by the WNIC software. With fragment size of 75 bytes and maximum IP packet size of 1500 bytes, which means 20 fragments, memory management was simple and buffer requirement was same as an IP packet size (maximum 1.5KB).

WNIC provided 64 kb/s data rate per user. This data rate was considered enough for Internet browsing and E-mail access through a Network Computer (NC). NC was a concept meant to provide cheap computers to users where all applications were stored in the network. NC did not have any hard-disk. WNIC was also used for Internet browsing and E-mailing through normal computers.

1.3.2 Medium Access Protocol

In the system model considered for this thesis, all STAs communicate via the Access Point AP to each other or the Internet. Especially for wireless systems, scarcity of spectrum must be kept in mind; this scarcity limits the number of STAs accessing the channel simultaneously. At the same time collisions during channel access must be taken care of; increases in collisions decrease the overall efficiency of the system.

This thesis proposes a novel MAC protocol named as Channel Sharing Protocol (CSP) [24]. So as to combat the collision problem faced by multiple access protocols during channel access the proposed scheme makes use of a p-persistence algorithm [24]. To use the channel more efficiently CSP makes use of tokens so that several STAs can join a single channel. The number of STA per channel is fixed.

In this thesis, the performance of the proposed protocol is studied and the throughput results are compared with Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [11]. Performance of CSP is studied using both numerical and simulation methods. The first thing done was optimization of parameters like, p-persistence value, number of channels and number of tokens per channel. CSP was applied for patent by the author and a detailed implementation design was made for second generation WNIC.

The optimum p-persistence value found was 0.5, the number of channels at which the protocol gives the optimum performance is 20 and the number of tokens per channel is 6. Simulation results show that a throughput of 0.85 is achieved for the optimized CSP from the load of 0.1 onwards.

1.3.3 QoS Protocols

The growth of wireless technology will continue with the introduction of new services and applications. Present day WLANs, particularly IEEE 802.11, provide asynchronous/non real time data services. Provision of QoS over WLANs can be very beneficial from the point of view of users, data and voice over same network, and from the point of view of manufacturers, satisfied customers and more sales.

IEEE 802.11 based WLANs provide possibilities for QoS provisioning by using Point Coordination Function (PCF) but it has its limitations [11,27]. The biggest limitation is scalability. Besides that studies have shown that PCF cannot actually provide the required QoS [27].

So as to provide the required QoS four ideas existed when this thesis work was started. A qualitative analysis of the four schemes to achieve QoS over IEEE 802.11 is done in this thesis [20]. The real-time traffic considered is voice as this is the basic need of users, i.e., the provision of voice over data or voice over WLAN. This study was done as a preliminary step for enhancement of the IEEE 802.11 MAC for QoS.

The four possible QoS schemes for IEEE 802.11 were, Distributed Coordination Function (DCF) [11], PCF [11], priority queuing [20] and Blackburst [33]. Qualitative analysis showed that priority queuing was the solution of choice although it did not give as high QoS as Blackburst it fulfilled the requirements of scalability, implementation and was compatible with the standard. Blackburst could be used to get better QoS but it was not compatible with the standard and its implementation was far more difficult. DCF and PCF on the other hand were not considered good enough [20].

IEEE 802.11e, the MAC enhancement for QoS, has selected priority queuing as a possible solution for QoS provision. This shows that the result of the study, priority queuing as the solution of choice, was accurate.

An example is given in this thesis on how QoS can be provided in a WLAN with a protocol stack where each protocol layer understands QoS and with protocols that can provide end-to-end quality.

This thesis also examines issues related to QoS that must be solved in future study. The common tendency is to study end-to-end QoS, i.e., application to application but this cannot be achieved if all the layers in the protocol stack do not have the same understanding of QoS. Another point is that although end-to-end QoS is from application to application, quality is measured based on lower layer parameters like the signal strength or the packet or frame error rates. Quality optimization of an application based on such parameters does not make much sense and study must be done on quality control and measurements based on application layer parameters which are closure to the user perception of quality [34].

1.3.4 Security

Present day WLANs, compliant to IEEE 802.11, combat the security problem using Wired Equivalent Privacy (WEP). WEP has been found to have several security flaws while at the same time WLANs are getting ever popular and are already being used in several different environments including academic, corporate and public environments. The existing level of security is surely not enough for these environments [18,19].

In this thesis requirements of the envisaged environments (corporate, academia and public) are studied. Based on these requirements possible solutions are presented. From the comparison between the solutions the best solution for each environment is chosen. As some flaws remain even in chosen methods, a novel solution to mitigate the flaws is also proposed.

Some ideas studied in this thesis were proposed to the IEEE 802.11 standardization committee. The proposal to use higher layer solutions and IEEE 802.1X are accepted by the standardization committee.

The biggest flaw with the chosen solutions was access control; this flaw can be mitigated by a proposed access control solution which was also applied for patent by the author. The IEEE 802.11f standard uses several ideas proposed in the access control solution.

This thesis also examines security issues which should be studied for a future generation of mobile communications.

1.3.5 System Design and Network Deployment

Spectrum limitation is a major issue in wireless communication. The challenge is to serve the largest number of users with a specified system quality. Therefore good system design and network deployment and study thereof play a very important role [25,26].

In this thesis system design issues of IEEE 802.11 is examined and critical issues which wireless network deployment faces are also studied. The critical issues studied are coverage, cell planning, interference, power management, data rate and security. These issues are dealt with in this thesis focussing mainly on the IEEE 802.11 WLAN based on DSSS in the 2.4 GHz ISM band.

The proposed automatic data rate control scheme, a part of system design, was applied for patent by the author and is implemented and used by ORiNOCO products.

The system design presented in this thesis was used for WLAN product (ORiNOCO) development in Lucent Technologies and the deployment method was also used within the company.

1.4 Thesis Overview

Contributions to this thesis, as presented in Section 1.3, are arranged as given below.

Chapter 2 proposes a new and efficient ARQ scheme for IP packet transmission. In this chapter the scheme is explained and studied in detail. In Chapter 3 an efficient MAC protocol is proposed for WLANs. Both numerical and simulation methods are used to study the performance of the proposed protocol. Study of Quality of Service for WLANs is done in Chapter 4. Security for WLANs is studied in Chapter 5; in this chapter, the requirements of different environments in which the WLAN is envisioned to be used are given together with security solutions for these environments. A novel access control scheme is also proposed. WLAN system design and network deployment issues are given in Chapter 6. This chapter gives practical results for a DS-SS WLAN working in ISM band of 2.4 GHz. Finally in Chapter 7 the conclusions and some recommendations for future work are given.

References

[1] R. Prasad, *Universal Wireless Personal Communications*, Boston, Artech House, 1998.

[2] R.D.J. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Boston, Artech House, 2000.

[3] T. Ojanpera and R. Prasad, *Wideband CDMA for Third Generation Mobile Communications*, Boston, Artech House, 2000.

[4] GSM MoU website, http://www.gsmworld.com

[5] ITU website, http://www.itu.int/imt

[6] The UMTS Forum website, http://www.umts-forum.org

[7] 3GPP website, http://www.3gpp.org

[8] 3GPP2 website, http://www.3gpp2.org

[9] IEEE Personal Communications, vol. 7, no. 2, April 2000.

[10] IEEE 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, November 1997.

[11] IEEE 802.11, “Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless MAC and PHY Specifications: High Speed Physical Layer in the 5 GHz Band”, P802.11a/D6.0, May 1999.

[12] ETSI BRAN, “HIPERLAN Type 2 Functional Specification Part 1 – Physical Layer”, DTS/BRAN030003-1, June 1999.

[13] HomeRF website, http://www.homerf.org

[14] BLUETOOTH SIG website http://www.bluetooth.com

[15] IEEE Personal Communications, vol. 7, no. 1, February 2000.

[16] IEEE 802.15, “Part 15.1: Wireless Personal Area Network Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, May 2000.

[17] A. Kamerman and A.R. Prasad, “IEEE 802.11 and HIPERLAN/2 Performance and Applications”, ECWT 2000, 2-6 October 2000, Paris, France.

[18] A.R. Prasad, H. Moelard and J. Kruys, “Security Architecture for Wireless LANs: Corporate & Public Environment”, pp 283-287, VTC 2000 Spring, 15-18 May 2000, Tokyo, Japan.

[19] A. Prasad and A. Raji, “A Proposal for IEEE 802.11e Security”, IEEE 802.11e, 00/178, July 2000.

[20] A.R. Prasad, “Performance Comparison of Voice over IEEE 802.11 Schemes”, pp 2636-2640,VTC 1999 Fall, 19-22 September 1999, Amsterdam, The Netherlands.

[21] N.R. Prasad et al, “A state-of-the-art of HIPERLAN/2”, pp 2661-2666,VTC 1999 Fall, 19-22 September 1999, Amsterdam, The Netherlands.

[22] A.R. Prasad, ”Optimization of Hybrid ARQ for IP Packet Transmission”, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, March 2001, Volume 16, issue 3, pp. 203-220.

[23] A.R. Prasad, Y. Shinohara and K. Seki, “Performance of Hybrid ARQ for IP Packet Transmission on Fading Channel”, IEEE Transactions Vehicular Technology, May 1999, Vol. 48, Nr. 3, pp. 900-910.

[24] A.R. Prasad and K. Seki, “Capacity Enhancement of Indoor Wireless Communication System with a Novel Channel Sharing Protocol”, ICPWC’97, Mumbai, India, pp. 162-166, 16-19 December 1997.

[25] A.R. Prasad, A. Eikelenboom, H. Moelard, A. Kamerman & N.R. Prasad, “Wireless LANs Deployment in Practice”, chapter of Wireless Network Deployments, edited by R. Ganesh and K. Pahelvan, Kluwer Publications, 2000.

[26] A.R. Prasad, N.R. Prasad, A. Kamerman, H. Moelard, & A. Eikelenboom, “Performance Evaluation, System Design and Network Deployment of IEEE 802.11”, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, October 2001, Vol. 19, Nr. 1, pp. 57-79.

[27] M. A. Visser and M. El Zarki, “Voice and Data Transmission over an 802.11 Network”, pp 648-652, Proc. PIMRC’95, Sept. 1995, Toronto, Canada.

[28] N.R Prasad and A.R. Prasad, editors, *WLAN Systems and Wireless IP for Next Generation Communications*, Artech House, January 2002.

[29] R. Prasad, *CDMA for Wireless Personal Communications*, Artech House, 1996.

[30] M.J. Miller and S. Lin, “The Analysis of some Selective Repeat ARQ Schemes with Finite

Receiver Buffer", IEEE Trans. on Comm., vol. COM-29, no. 9, pp. 1307-1315, September 1981.

[31] J. Walrand, *Communication Networks: A First Course*, Richard D. Irwin, Inc. and Aksen Associates, Inc., Boston, 1991.

[32] H.R. van As, "Media Access Techniques: The Evolution towards terabit/s LANs and MANs", Computer Networks and ISDN Systems, Vol. 26, Issue 6-8, pp. 603-656, 1994.

[33] J. L. Sabrinho and A.S. Krishnakumar, "Real-Time Traffic over the IEEE 802.11 Medium Access Control Layer", pp 172-187, Bell labs Technical Journal, Vol. 1, No. 2, Autumn 1996, N.J., USA.

[34] A. R. Prasad, R. Esmailzadeh, S. Winkler, T. Ihara, B. Rohani, B. Pinguet and M. Capel, "Perceptual Quality Measurement and Control: Definition, Application and Performance", WPMC 2001, 9-12 September 2001, Aalborg, Denmark.

Chapter 2

Hybrid ARQ for IP Packet Transmission

The basic purpose of Wireless Local Area Networks (WLANs) is to extend the wired LANs which are mostly based on Internet Protocol (IP) [1 - 2]. IP was designed to work for a wired medium where errors in packets due to the medium is negligible; normal IP packets cannot survive the error prone wireless channel. To combat the high degree of error caused by wireless transmission of data a robust error control scheme is a necessity. Basically, error control schemes can be divided in two categories: Automatic Repeat reQuest (ARQ) schemes and Forward Error Correction (FEC) schemes. ARQ schemes are often used for reliable data transmission; this is because FEC requires too many redundant bits for perfect data transmission. There are several known ARQ schemes [3 - 18] such as Go-Back-N (GBN), Stop and Wait (SW), and Selective Repeat (SR) which are the most basic ones. In an ARQ scheme correctly received packets are Acknowledged (ACK) and packets received with error are Negatively Acknowledged (NACK). NACKed packets are then retransmitted. In short, ARQ is an error detection with retransmission scheme. As the purpose of the system is wireless IP packet transmission, the efficiency of the system will depend on the efficiency of the ARQ scheme.

This chapter gives a short introduction to basic ARQ schemes like SW, GBN and SR ARQ. After which ARQ schemes in existing WLANs are presented. Next an ARQ scheme for efficient IP packet transmission in WLANs is proposed. The proposed ARQ scheme, SW ARQ and GBN ARQ were implemented by the author. The proposed ARQ scheme was applied for patent and implemented for a proprietary WLAN, known as WNIC, developed at the Tokyo Research and Development Center (TRC) of Uniden Corporation, Tokyo, Japan.

2.1 Automatic Repeat Request Schemes

Error control is basically provided by FEC and ARQ. The benefit of FEC is that it does not require any feedback channel as errors can be corrected at the receiver. On the other hand the issue of FEC is the use of a huge number of redundant bits used to provide error correction. ARQ provides retransmission of erroneous packets by detection of errors. ARQ schemes together with error detection have been widely used for telecommunications. Another approach to error control is through the use of hybrid ARQ schemes which incorporate both FEC and retransmission. Hybrid ARQ schemes offer the potential for better performance.

2.1.1 Basic ARQ Schemes

There are three types of basic ARQ schemes: Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective-Repeat ARQ [15].

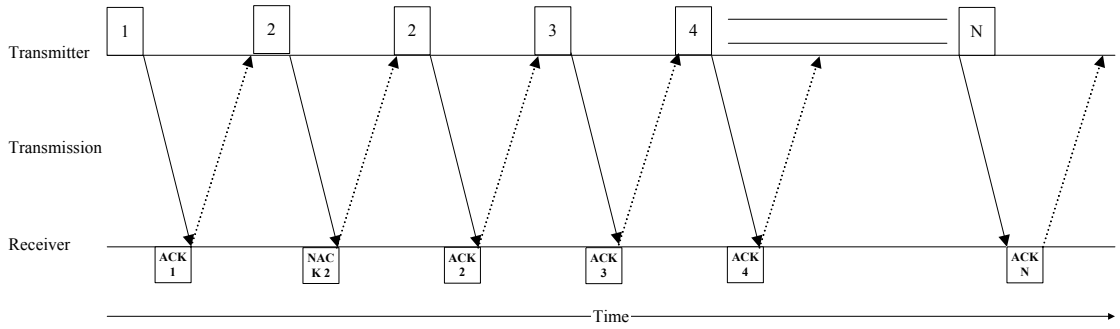


Figure 2-1 Stop-and-wait ARQ.

2.1.1.1 Stop-and-Wait

The Stop-and-Wait scheme represents the simplest ARQ procedure and was implemented in early error-control systems. Transmission Control Protocol (TCP) also makes use of the Stop-and-Wait scheme [19]. In a Stop-and-Wait ARQ error-control system, the transmitter sends a packet to the receiver and waits for an acknowledgment, as shown in Figure 2-1. A positive acknowledgment (ACK) from the receiver indicates that the transmitted packet has been successfully received, and the transmitter sends the next packet in the queue. A negative acknowledgment (NACK) from the receiver indicates that the transmitted packet has been detected in error; the transmitter then resends the packet and again waits for an acknowledgment. Retransmissions continue until the transmitter receives an ACK.

This scheme is simple but inherently inefficient because of the idle time spent waiting for an acknowledgment of each transmitted packet. One possible remedy is to make the packet length extremely long. However, the use of a very long packet does not really provide a solution, since the probability that a packet contains errors increases with the packet length [15]. Hence, using a long packet reduces the idle time but increases the frequency of retransmissions for each packet. Moreover, a long packet may be impractical in many applications because of restrictions imposed by the data format. One way to solve the inefficiency issue is to transfer packets continuously as is done by Go-Back-N ARQ.

2.1.1.2 Go-Back-N

The basic of the Go-Back-N ARQ scheme is illustrated in Figure 2-2. The transmitter continuously transmits packets in order and then stores them pending receipt of an ACK or NACK for each transmitted packet. The acknowledgment for a packet arrives after a round-trip delay, defined as the time interval between the transmission of a packet and the receipt of an acknowledgment for that packet. During this interval, $N - 1$ other packets are also transmitted. Whenever the transmitter receives a NACK indicating that a particular packet, say packet *i,* was

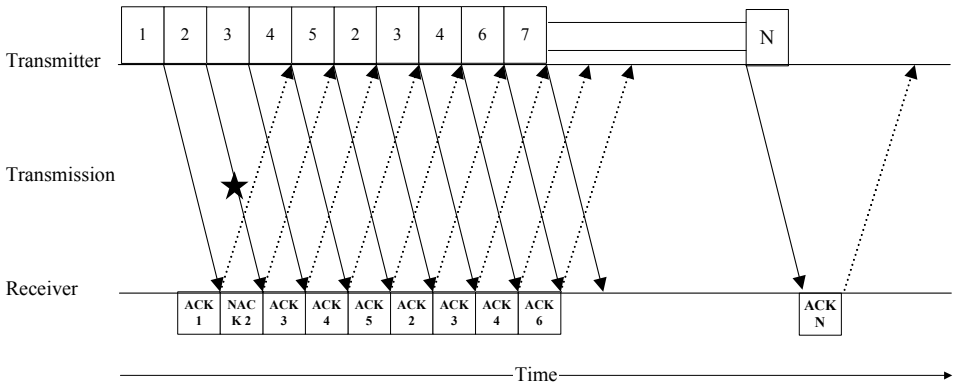


Figure 2-2 Go-Back-N ARQ with N=4.

received in error, it stops transmitting new packets. Then it goes back to packet *i* and proceeds to retransmit that packet and the $N - 1$ succeeding packets which were transmitted during one round-trip delay. At the receiving end, the receiver discards the erroneously received packet *i* and all $N - 1$ subsequently received packets, whether they are error-free or not. Retransmission continues until packet *i* is positively acknowledged. In each retransmission for packet *i,* the transmitter resends the same sequence of packets. As soon as packet *i* is ACKed, the transmitter proceeds to transmit new packets.

The main drawback of Go-Back-N ARQ is that, whenever a received packet is detected in error, the receiver also rejects the next $N - 1$ received packets, even though many of them may be error free. As a result, they must be retransmitted. This represents a waste of transmissions, which can result in severe deterioration of throughput performance if a large round-trip delay is involved. The Go-Back-N ARQ scheme becomes quite ineffective for communications systems with high data rates and large round-trip delays. This ineffectiveness is caused by the retransmission of many error-free packets following a packet detected in error. This can be overcome by using the Selective-Repeat ARQ protocol.

2.1.1.3 Selective-Repeat

In a Selective-Repeat ARQ scheme, packets are also transmitted continuously. However, the transmitter only resends those packets that are NACKed. After resending a NACKed packet, the transmitter continues transmitting new packets (as illustrated in Figure 2-3). With this scheme, a buffer must be provided at the receiver side to store the error-free packets following a received packet detected in error, because, ordinarily, packets must be delivered to the higher layer in correct order. When the first NACKed packet is successfully received, the receiver then releases any error-free packets in consecutive order from the receiver buffer until the next erroneously received packet is encountered. Sufficient receiver buffer storage must be provided in a Selective-Repeat ARQ system; otherwise, buffer overflow may occur and packets may be lost [15].

2.1.1.4 Hybrid ARQ

A combination of any kind of FEC and ARQ can be used to give higher reliability. Combination of these two is known as hybrid ARQ. Hybrid ARQ schemes can be classified in two categories, namely Type-I and Type-II.

Type-I hybrid ARQ schemes have error correction and error detection capabilities. When a packet is detected to have errors the receiver first tries to correct those errors. If the errors cannot be corrected the receiver rejects the received packets and requests a retransmission of the same packet once again. This continues until the packet is either successfully received or successfully decoded.

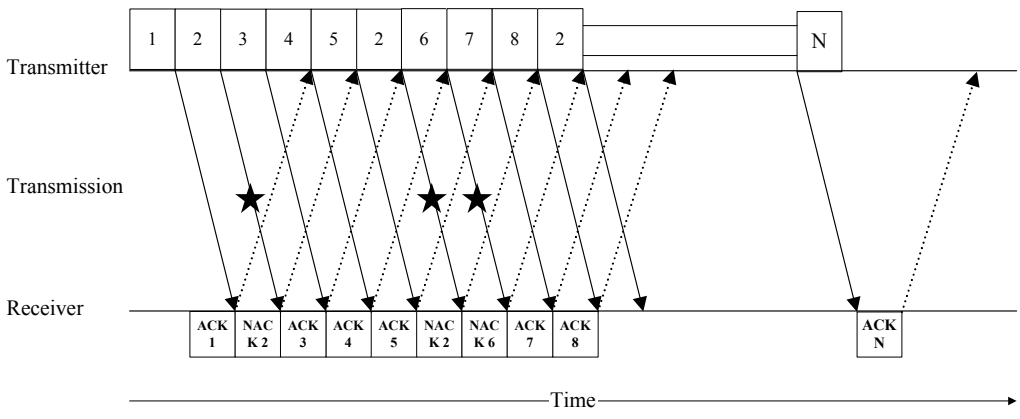


Figure 2-3 Selective-Repeat ARQ.

Type-II hybrid ARQ scheme is an adaptive scheme, a packet in its first transmission is coded with parity-check bits for error detection only. When the receiver detects the presence of errors in a received packet, it saves the erroneous packet in a buffer and at the same time requests a retransmission. The retransmission is not the original packet but a block of parity-check bits which is formed based on the original message and an error-correcting code. When this block of parity-check bits is received, it is used to correct the errors in the erroneous packet stored in the receiver buffer. If error correction is not successful, the receiver requests a second retransmission of the NACKed packet. The second retransmission may be either a repetition of the original packet or another block of parity-check bits. This depends on the retransmission strategy and the type of error-correcting code in use.

2.1.2 ARQ in WLANs

In this section ARQ schemes used in IEEE 802.11 and HIPERLAN Type 2 are presented.

2.1.2.1 IEEE 802.11

ARQ of IEEE 802.11 is an integrated part of the Medium Access Control (MAC) scheme, Carrier Sense Multiple Access with Collision Avoidance and Acknowledgement (CSMA/CA + ACK) [16,17]. IEEE 802.11 uses ARQ in its most basic sense. If a packet is acknowledged by the receiver it is considered not only that the packet was received correctly but that the channel was accessed. If no ACK is received the transmitter goes back to channel sensing mode. One can consider the scheme to be as SR-ARQ until the packets are received correctly but when there is an error the channel sensing comes in action. The standard allows fragmentation but it does not discuss the method to do it optimally.

2.1.2.2 HIPERLAN Type 2

In HIPERLAN/2 the Data Link Control (DLC) layer consists of a Radio Link Control (RLC) sublayer, an Error Control (EC) protocol and a MAC protocol. The Error Control modes of operation are defined to support different types of services [18]:

1. The *acknowledged mode* provides with reliable transmissions by using Selective-Repeat ARQ to improve the link quality.
2. The *repetition mode* provides with a rather reliable transmission by repeating the packets. No feedback channel is available. The transmitter can arbitrarily retransmit packets.
3. The *unacknowledged mode* provides an unreliable, low latency transmission. The transmitter will send the packets in increased sequence number and the receiver will deliver all correctly received ones to the convergence layer. No feedback channel is available. Unicast data can be sent using either acknowledged or unacknowledged mode. Broadcast services can be supported by either repetition mode or unacknowledged mode. Multicast services can be sent in unacknowledged mode or be multiplexed onto already existing user unicast transmissions.

2.1.3 ARQ for Wireless IP

The purpose of Layer-2 in WLANs is to transmit IP packets. This knowledge can be used for designing an optimum Layer-2 ARQ scheme in WLANs. Although this is known, the ARQ in IEEE 802.11 does not consider higher layers; the issue for this standard is the design of the MAC protocol. HIPERLAN/2 uses a much more complex ARQ solution when compared to IEEE 802.11 but once again it is not optimized for IP packets. It is also very much understandable that for systems which only access internet or download e-mails and files, complex solutions will not be necessary.

In this chapter a novel ARQ scheme is proposed for WLANs and performance results are presented. It is considered that the WLAN is used for services like Internet access, E-mailing, file download, etc.. The ARQ scheme presented in this chapter was designed and implemented in a

proprietary WLAN before the IEEE 802.11 and HIPERLAN/2 standards were finalized, still it has benefits which are not recognized by the two standards namely the efficient transmission of IP packet.

2.2 Description of Proposed *ARQ* Scheme

In this section the proposed ARQ scheme is explained. For performance comparison purposes the Selective Repeat + Stutter 2 (SR+ST 2) ARQ scheme [6-12] is also presented in this section. The reason for using SR+ST 2 for performance comparison is that, it is an ARQ scheme that it is relatively close in design to the proposed ARQ scheme.

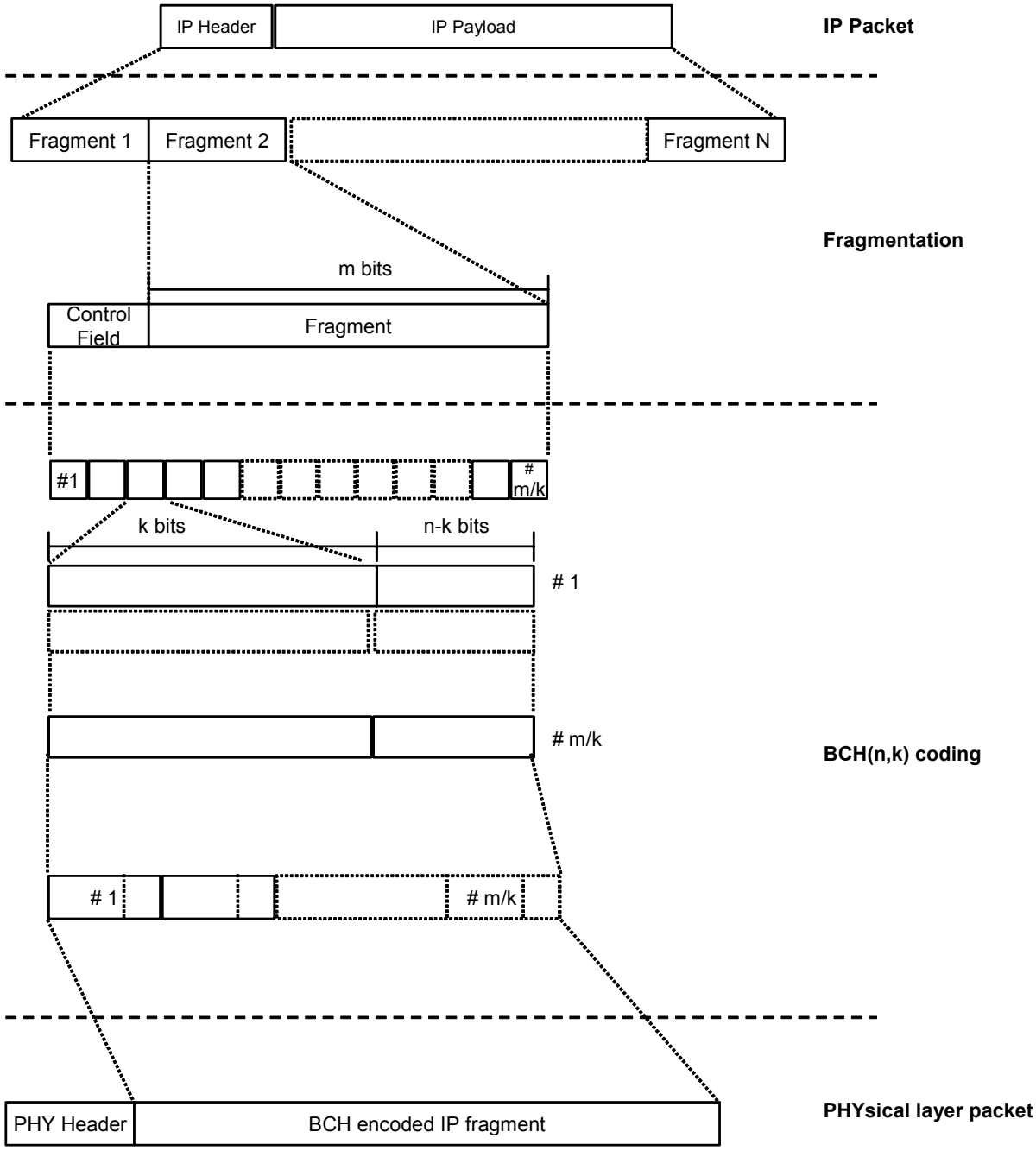


Figure 2-4 IP packet fragmentation and BCH coding.

2.2.1 Proposed ARQ

There are a few things that are known (1) WLANs almost always have an Ethernet as backbone using IP stack, (2) IP packets in Ethernet can vary in size from 40 bytes to maximum 1500 bytes and (3) IP is not meant for error prone environments. The conclusion from these three points is that wireless transmission of large packets, especially those meant for error free environment, can cause lots of error which will lead to a decrease in efficiency therefore IP packets must be fragmented to reduce the effect of error on performance. Although with fragmentation the probability of error will decrease, it will also increase the overhead in terms of fragment numbering for ARQ and increase the memory management requirements. Thus a trade-off exists between fragment size on the one hand and memory management and overhead on the other hand. Therefore, an optimal fragment size must be found which gives high throughput, i.e., uses the channel efficiently, with low overhead and thus low memory management requirement. In Figure 2-4 the fragmentation of an IP packet and associated overhead is shown.

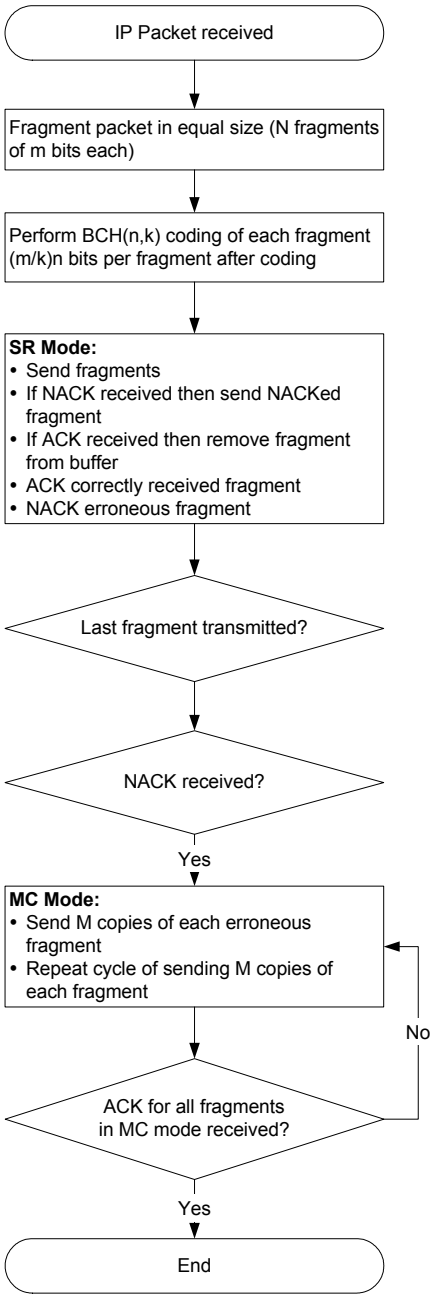


Figure 2-5 Proposed SR/MC ARQ flowchart.

Erratum:
Wireless LANs: Protocols, Security and Deployment
Anand R. Prasad
Page 18, Figure 2-5

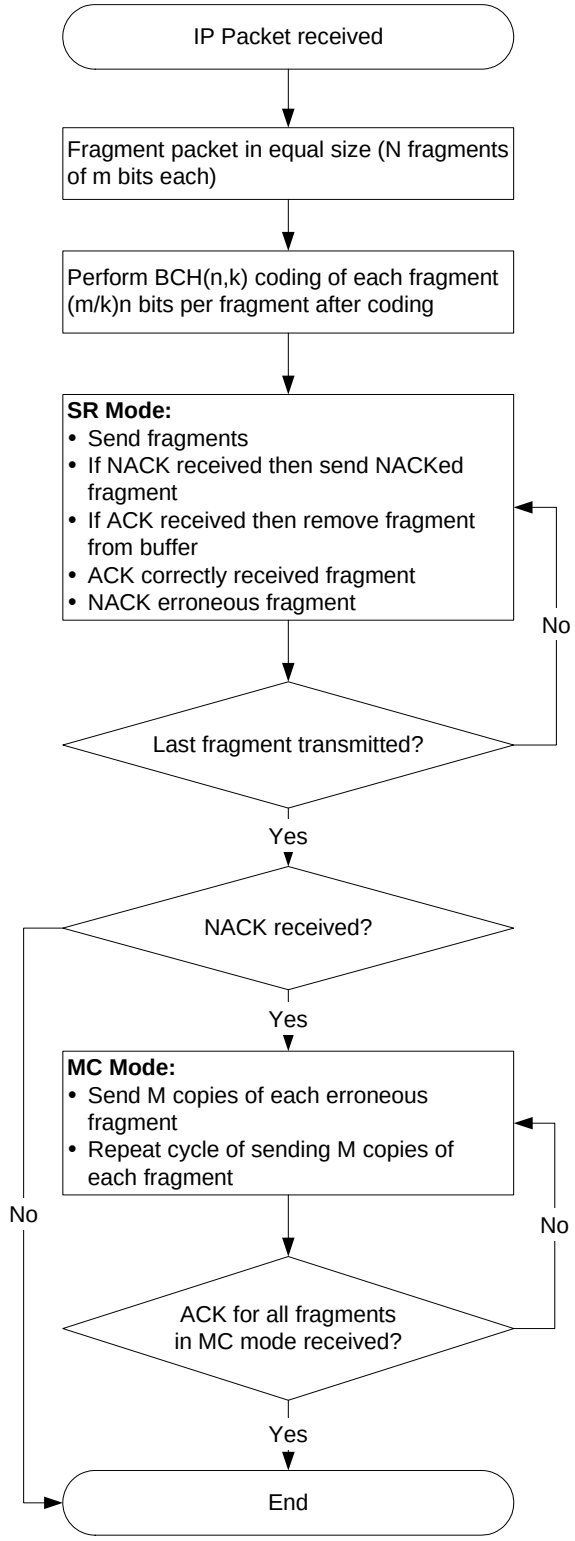


Figure 2-5 Proposed SR/MC ARQ flowchart.

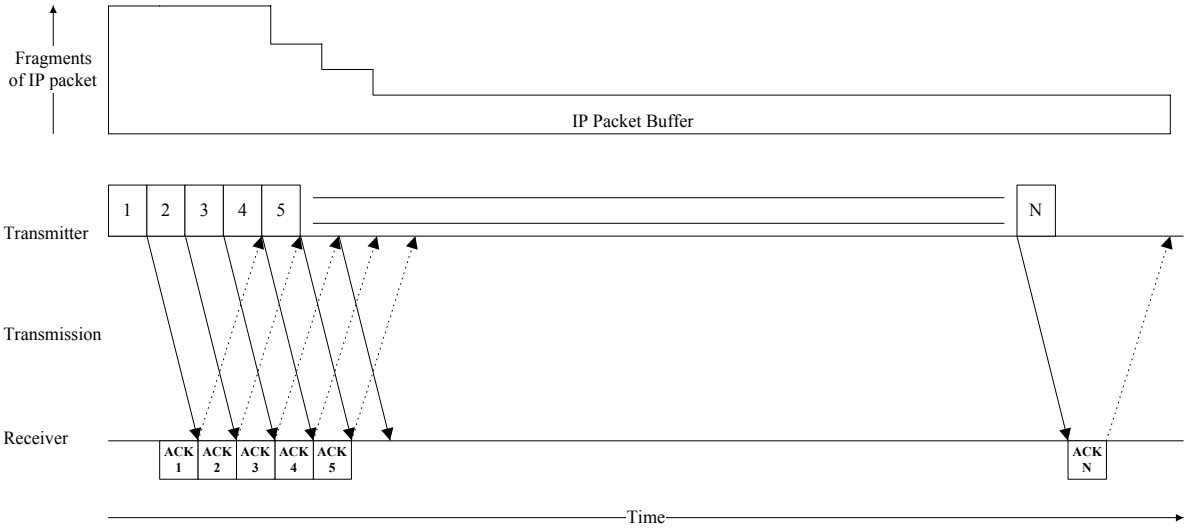


Figure 2-6 IP fragment transmission without error.

The following steps and Figure 2-5 explain the working of the proposed ARQ: (1) an IP packet received by the transmitter is fragmented in N fragments of equal size of m bits, (2) each fragment is given a control field which contains information like sequence number, kind of frame, e.g., data or ACK/NACK or both data and ACK/NACK fields, (3) the fragments and control field are then BCH coded for error correction for this purpose each fragment is divided in m/k equal size blocks of k bits and then BCH coded thus resulting in m/k coded blocks of n bits; the coded fragment of the size (m/k)n is then passed on to the physical (PHY) layer, (4) the system transmits the fragments in SR mode until the last fragment is transmitted, (5) an erroneous or, lost fragment is negatively acknowledged by the receiver, (6) if there are erroneous fragments after the last fragment is transmitted then the system goes in Multi-Copy (MC) mode, where M copies of erroneous or, lost fragments are transmitted cyclically. This cycle of transmitting M copies of erroneous fragments is continued until all the fragments are received without error. The system then goes to the SR mode. This ARQ is named as the SR/MC ARQ.

The proposed SR/MC ARQ is designed to be used for indoor WLAN system and for non-real-time services.

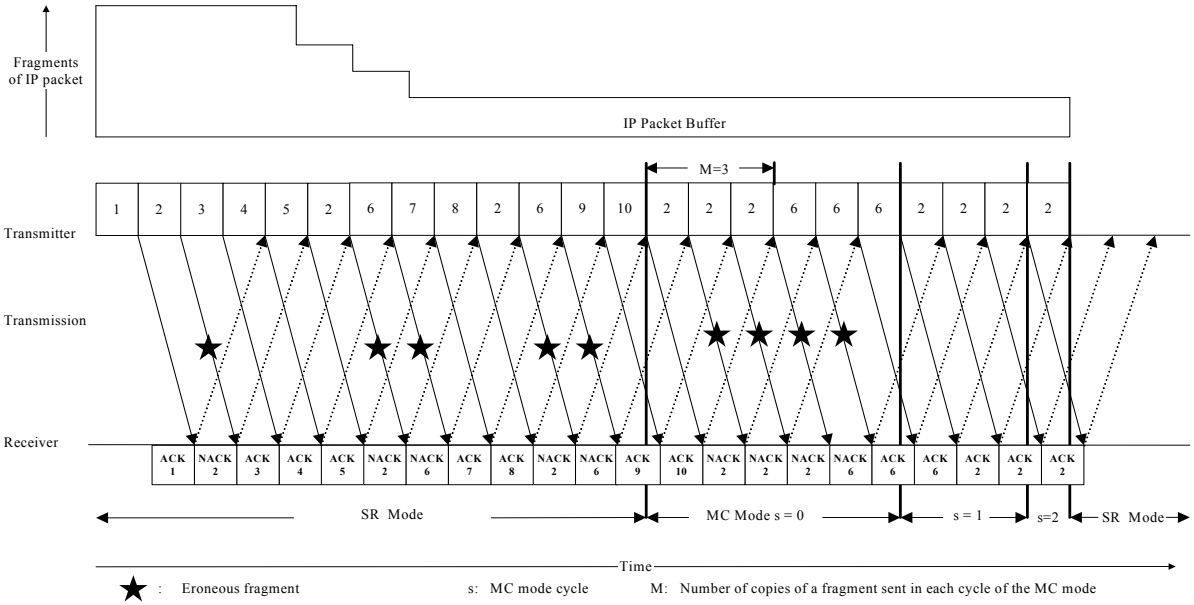


Figure 2-7 Mode change due to error.

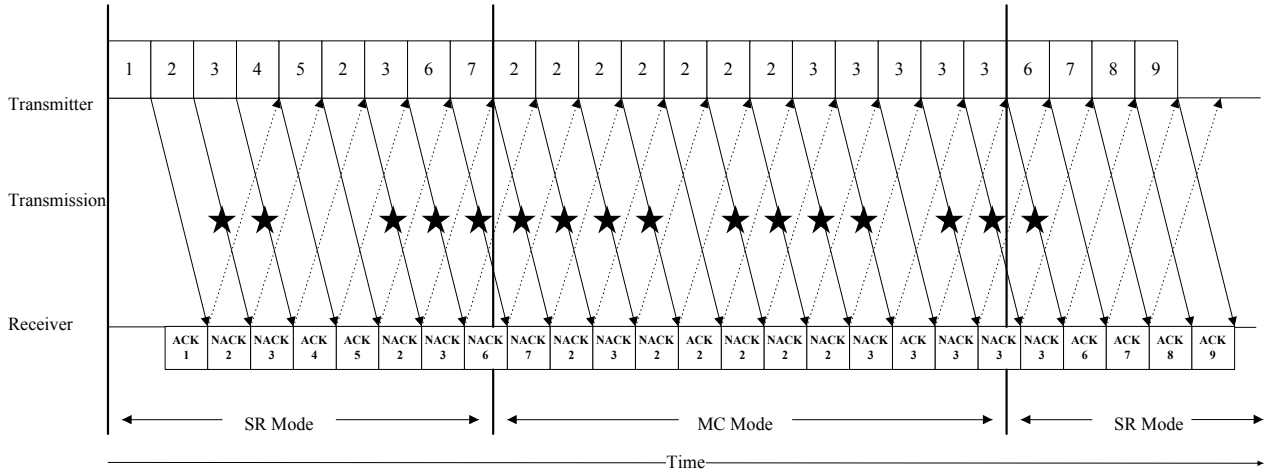


Figure 2-8 Example of *SR+ST 2*.

The transmission of IP fragments without error is shown in Figure 2-6. The transmitter side IP packet buffer decreases as the fragments are transmitted and an ACK is received; each fragment is ACKed by the receiver when received correctly. The receiver, on receiving all the fragments, constructs the IP packet and sends it to the higher layer. Figure 2-7 gives an example of the proposed ARQ transmission with errors and a change in mode. This example is for an IP packet divided in 10 equal fragments. In Figure 2-7 the system remains in SR mode till the last fragment is transmitted. In the SR mode, fragments 2 and 6 are not received correctly so the system goes into MC mode when the NACK for fragment 2 is received after the last fragment is transmitted. In the MC mode M copies, in this example M = 3, of each erroneous fragments (fragments 2 and 6) are transmitted. The cycle of retransmission is continued until ACKs for all the fragments are received. The system then returns back to SR mode.

2.2.2 SR+ST 2

The SR+ST 2 scheme [14] stays in the SR mode for the first retransmission; it goes to the MC mode only if the same fragment is NACKed at least twice (thus the 2). In the MC mode, multiple copies of the NACKed fragment are retransmitted until an ACK is received for the fragment. The system then goes back to the SR mode if no more second NACK is received in the mean time else it remains in the MC mode. An example of this scheme is given in Figure 2-7 with Round Trip Delay (RTD) = 4. Fragments 2 and 3 are received with error they are retransmitted once in the SR mode, the system goes to the MC mode when they are NACKed again. Fragment 2 is first transmitted until an ACK is received for it after which fragment 3 is transmitted. Once an ACK is received for fragment 3 the system goes back to the SR mode.

2.3 Numerical Analysis

This section presents a numerical analysis of the proposed SR/MC ARQ. Equations are derived for throughput analysis, pure data throughput (or goodput) analysis and delay analysis.

2.3.1 Throughput Analysis

A throughput analysis of the proposed SR/MC ARQ scheme is presented in this section [6-12].

For throughput calculations under non-correlated AWGN channel fragment error rate (FER) for the case without BCH is written as [6,8],

$$P = 1 - (1 - p)^m \tag{1}$$

where P is the FER, m is the number of bits in the fragment and p is the BER.

While for BCH(n, k, t) the FER is [6,8],

$$P = 1 - \left(\sum_{x=0}^{t} \binom{n}{x} p^x (1-p)^{n-x} \right)^{\frac{m}{k}} \quad (2)$$

where the knowledge that BCH(n, k, t) divides the fragment in blocks of k bits and adds n – k bits to each block is used. These n – k bits can correct t erroneous bits. x is the number of erroneous bits. Please note that for simplicity the control field size is not considered in calculation. The control field is protocol dependent and the constant field in it will be the packet size information which can be considered negligible when compared to the data in each fragment.

When calculating throughput under Rayleigh fading channel the results from the simulation model are used, Section 2.4. For FER calculation under Rayleigh fading channel Equation (1) is used.

The normalized throughput of any packet transfer scheme is the ratio of number of fragments, N, to be transmitted to the total number of fragments actually transmitted [3]. Thus throughput of the proposed ARQ scheme is [6,8],

$$S = \frac{N}{N_{SR} + N_{MC}} \quad (3)$$

where S denotes the throughput, N is the number of fragments to be transmitted ($N = \left\lceil IP_S / m \right\rceil$, IP_S is the IP packet size in bits and $\lceil \ \rceil$ means round up), N_{SR} is the number of fragments transmitted in the SR mode and N_{MC} is the number of fragments transmitted in the MC mode.

In the SR mode N fragments plus the fragments with an error must be transmitted. Considering i erroneous fragments in the SR mode, the total number of fragments transmitted under this mode is given by [6,8],

$$N_{SR} = \sum_{i=0}^{N} \binom{N}{i} P^i (1-P)^{N-i} ((N-i) + i\frac{1}{1-P}) \quad (4)$$

where $\frac{1}{1-P}$ gives the number of repetitions of an erroneous fragment. Thus, N – i fragments are transmitted without error and i erroneous fragments are repeated $\frac{1}{1-P}$ times, where P is the fragment error probability.

If after the last fragment is transmitted there are fragments with an error then the system goes into the MC mode. Assuming that there are j fragments with error after the last fragment is transmitted. The system enters in the 0^{th} cycle of the MC mode. The probability that there are j erroneous fragments at the 0^{th} cycle is [6,8],

$$P^0(j) = \binom{N}{j} (P^{\frac{1}{1-P}})^j (1 - P^{\frac{1}{1-P}})^{N-j} \quad (5)$$

where, $P^0(j)$ is the probability of j errors in the 0^{th} cycle and $P^{1/(1-P)}$ is the probability that a frame is erroneous after $\frac{1}{1-P}$ transmissions. Now if in the next cycle i out of the j fragments are erroneous then the probability of i erroneous fragments out of j for the cycle s+1 is [6,8,13],

$$P^{s+1}(i) = \sum_{j=i}^{N} q_{ji} P^{s}(j) \tag{6}$$

where, q_{ji} gives the probability that there are i fragments out of previous j fragments with error. While, q_{ji} is represented by [6,8,13],

$$q_{ji} = \begin{cases} (1-P^M)^j & i = 0 \text{ and } 1 \le j \le N \\ \binom{j}{i} (P^M)^i (1-P^M)^{j-i} & 1 \le i \le j \le N \\ 0 & otherwise \end{cases} \tag{7}$$

where M is the number of repetitions of erroneous fragments under MC mode in each cycle. While the number of fragments transmitted during cycle s+1 is iM. The total number of fragments transmitted in MC mode is the sum of number of fragments transmitted from cycle 1 onwards, this can be given as [6,8],

$$N_{MC} = \sum_{s=1}^{\infty} \sum_{i=1}^{N} \left(\sum_{j=i}^{N} P^{s}(j) iM \right) \tag{8}$$

Substituting Equations (8) and (4) in Equation (3) results in [6,8],

$$S = \frac{N}{\sum_{i=0}^{N} \binom{N}{i} P^i (1-P)^{N-i} \left((N-i) + i \frac{1}{1-P} \right) + \sum_{s=1}^{\infty} \sum_{i=1}^{N} \left(\sum_{j=i}^{N} P^{s}(j) iM \right)} \tag{9}$$

which is the expression for throughput of the proposed SR/MC ARQ scheme.

2.3.2 Data Throughput Analysis

As the IP packets used over Ethernet can be as big as 1500 bytes in size, the packet must be fragmented before transmission to get better performance. Although smaller fragment size will lead to better performance it will also require much more overhead thus, optimum fragment size must be calculated. The optimum fragment size can be calculated in terms of actual data throughput, S_D. Where S_D is the ratio of data in each fragment, m bits and the ARQ fragment with overhead, O bits, i.e., O + m bits. Normally O consists of the fragment number, type of frame field, etc., but in this section it is assumed that O consists of the fragment number only. This is a reasonable assumption because O will vary depending on the protocol used but most of the parts besides the fragment number will normally be constant. In case of BCH(n,k) there will be overhead from error correction bits also [8].

S_D for transmission without FEC is given as [8],

$$S_D = \frac{m}{m+O} = \frac{m}{m + \lceil \log_2 N \rceil} \tag{10}$$

where, $\log_2$ of N is the number of bits required for numbering the fragments for a given fragment size and IP packet size.

For transmission with BCH(n,k) S_D is given by,

$$S_D = \frac{m}{m+O} = \frac{m}{m + \left\lceil \frac{m}{k}(n-k) \right\rceil + \lceil \log_2 N \rceil} \tag{11}$$

m/k gives the number of BCH coded parts in a fragment while (m/k)(n-k) gives the number of bits overhead from BCH coding.

2.3.3 Delay Analysis

The time required for transmitting a complete IP packet, or delay, will also give the optimum fragment size. The normalized IP packet transmission delay, d, is the sum of the number of fragments transmitted in the SR and the MC modes given by [8],

$$d = N_{SR} + N_{MC} \tag{12}$$

2.3.4 SR+ST 2 and GBN Equations

SR+ST 2 and GBN are used for performance comparison of the proposed ARQ. The equations used for the throughput calculations of these two ARQs are given in this section.

Throughput of GBN is given by [14],

$$S_{GBN} = \frac{1-P}{1+RTD \cdot P} \tag{13}$$

where RTD is the round trip delay, i.e., the delay in receiving an ACK or a NACK after the fragment is transmitted. For throughput calculation of GBN the RTD was set to 4 because this corresponds with RTD in the WNIC.

The throughput of SR+ST 2 is given by [14],

$$S_{SR+ST2} = \frac{1-P}{1+P^2(1-P)RTD + P_{NN}P(1-P)^2 RTD} \tag{14}$$

where P_{NN} is given by,

$$P_{NN} = \sum_{j=0}^{RTD-1} \sum_{k=2j}^{RTD-2} \frac{(-1)^j RTD!}{(RTD-j-1)!(j+1)!} \cdot \frac{(2RTD-2-2j)!}{(k-2j)!(2RTD-2-k)!} P^{2+k}(1-P)^{2RTD-2-k} \tag{15}$$

As for the GBN, the RTD for SR+ST 2 is 4 when used for WNIC.

2.4 Fading Channel Simulation

The equations derived in Section 2.3 can be used for performance analysis of the proposed SR/MC ARQ in AWGN channel. For the fading channel performance analysis of the SR/MC ARQ, simulation results of the physical layer were used. This simulation was performed by the physical layer development team of WNIC. The simulation model was developed in C programming language and was proprietary software of Uniden Corporation. In this section the channel model and simulation model are given [20].

2.4.1 Channel Model

Choice of an appropriate channel model is necessary for a realistic performance analysis of a communication system [20]. The classical AWGN channel is first considered in this chapter for performance analysis of the proposed SR/MC ARQ (see Section 2.3). In contrast to the AWGN channel with the errors randomly distributed in time, burst errors are experienced in the wireless channels. A typical wireless channel allows relatively reliable communication during certain periods, interrupted by other periods of particularly poor communication. The latter is called

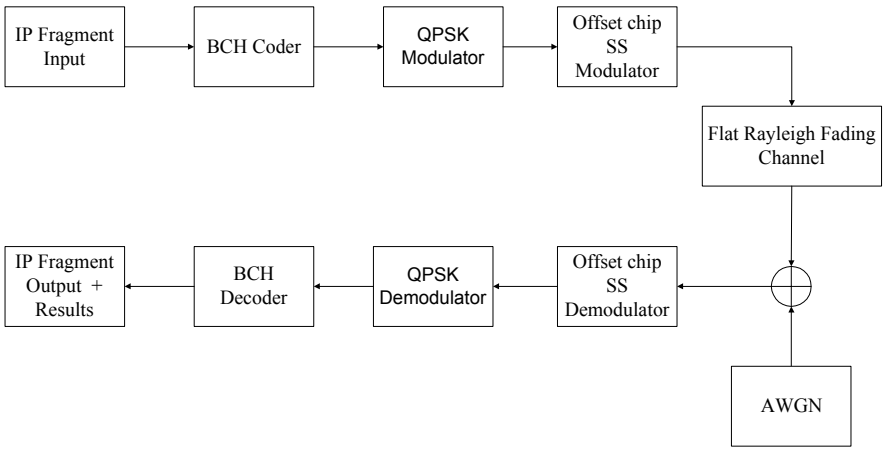


Figure 2-9 Simulation model structure [20].

fading. Wireless communication is being discussed in this chapter, thus the influence of the wireless environment on the efficiency of the ARQ scheme must also be considered.

Fading in wireless networks can be characterized by shadowing and multipath fading. Shadowing occurs due to the presence of obstacles between the transmitter and receiver. Multipath fading occurs because the received signal is a superposition of a large number of reflected signals. Rayleigh fading is a special case of multipath fading in which there is no line of sight component. Rayleigh fading can thus be used for the worst case analysis of the wireless system.

Reflections of surfaces along the path and the movement of the transmitter or the receiver causes deviation in the signal frequency due to a change in the path length between the transmitter and receiver. This is known as the Doppler-frequency-shift. The Doppler frequency shift is given by $f_D=f_C(v/c)$ where v is the rate of change in path length between the transmit and the receive antenna, c is the speed of light, f_C is the carrier frequency of the signal, and f_D is the Doppler frequency shift. The carrier frequency is shifted from f_C to $f_C + f_D$.

As, the system model used in this chapter is concerned with wireless communication allowing slow mobility, a good idea of the performance of the proposed SR/MC ARQ can be achieved by testing the system under flat Rayleigh fading channel with some Doppler shift. Both, AWGN and flat Rayleigh fading channels are used in this chapter together with Doppler shift to study the performance of the proposed SR/MC ARQ.

2.4.2 Structure of the Model

The simulation model structure and simulation parameters that are used in this chapter are given by Figure 2-9 and Table 2-1 respectively [20]. The simulation was done for the WNIC product specifications as given in Appendix C: WNIC Specification. A Doppler frequency of 10 Hz means the user is moving at 12 km/h. BCH was chosen as error correction scheme because its hardware size is smaller than other error correction schemes.

Table 2-1 Simulation Parameters.

FEC	BCH(63,51,2)
Modulation	QPSK
Chip rate	1 Mcps
Bit rate	181.81 kbps
Symbol rate	90.9 ksps
f_D	10 Hz

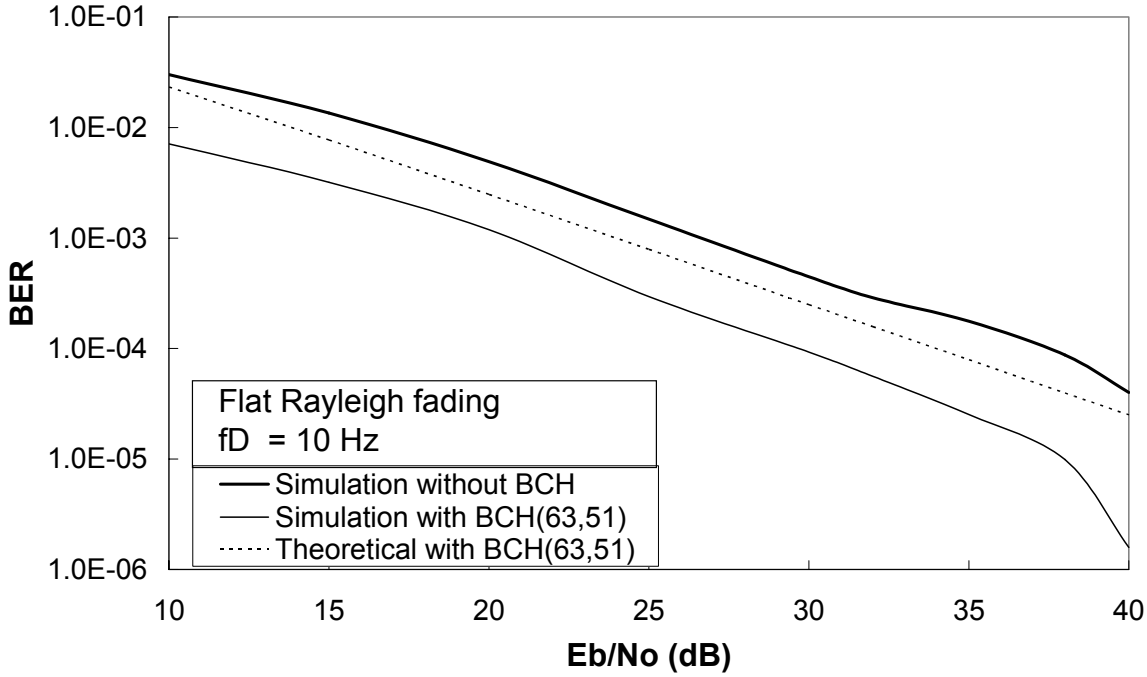


Figure 2-10 BER performance of the assumed radio channel using QPSK modulation. With and without BCH(63,51,2).

IP packet fragments were first BCH coded and then QPSK modulated. The QPSK modulated signal was then Spread Spectrum (SS) modulated before being passed through the flat Rayleigh fading and AWGN channel. The signal thus received was then demodulated and decoded; the result in terms of BER for given Signal to Noise ratio, E_b/N_0, was acquired as output. The results generated from the simulation model, in terms of BER and E_b/N_0, were used to generate numerical results for the proposed ARQ scheme. In Figure 2-10 the output of the simulation model is plotted with and without BCH(63,51,2), a comparison with theoretical result without BCH is also given.

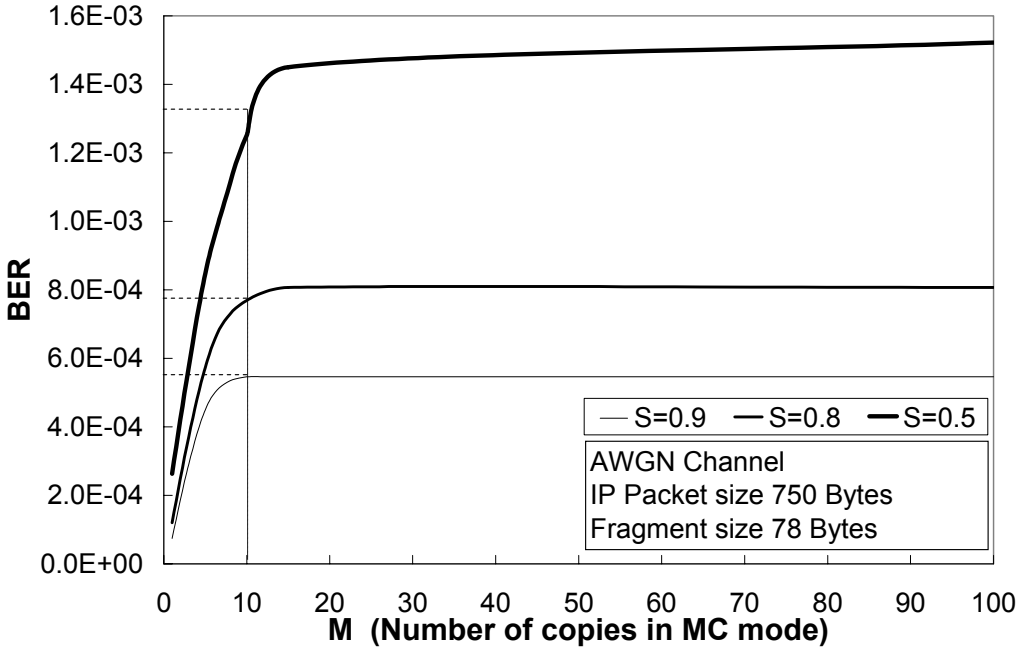


Figure 2-11. M against BER for S = 0.9, 0.8 and 0.5, IP packet size 750 bytes and fragment size 78 bytes.

Table 2-2 M and BER for varying value of S.

M	BER for S=0.9	BER for S=0.8	BER for S=0.5
1	7.4E-05	1.2E-04	2.6E-04
3	2.9E-04	3.7E-04	5.7E-04
5	4.5E-04	5.7E-04	8.5E-04
7	5.2E-04	7.0E-04	1.0E-03
10	5.5E-04	7.7E-04	1.3E-03
15	5.5E-04	8.1E-04	1.5E-03
100	5.5E-04	8.1E-04	1.5E-03

2.5 Numerical Results

Numerical results of the proposed SR/MC ARQ scheme are given in this section. The throughput is calculated using Equation (9). First, the results for an AWGN channel, without BCH based FEC, are examined and then the results for fading channel are examined, with and without BCH. In all the results, throughput refers to normalized throughput.

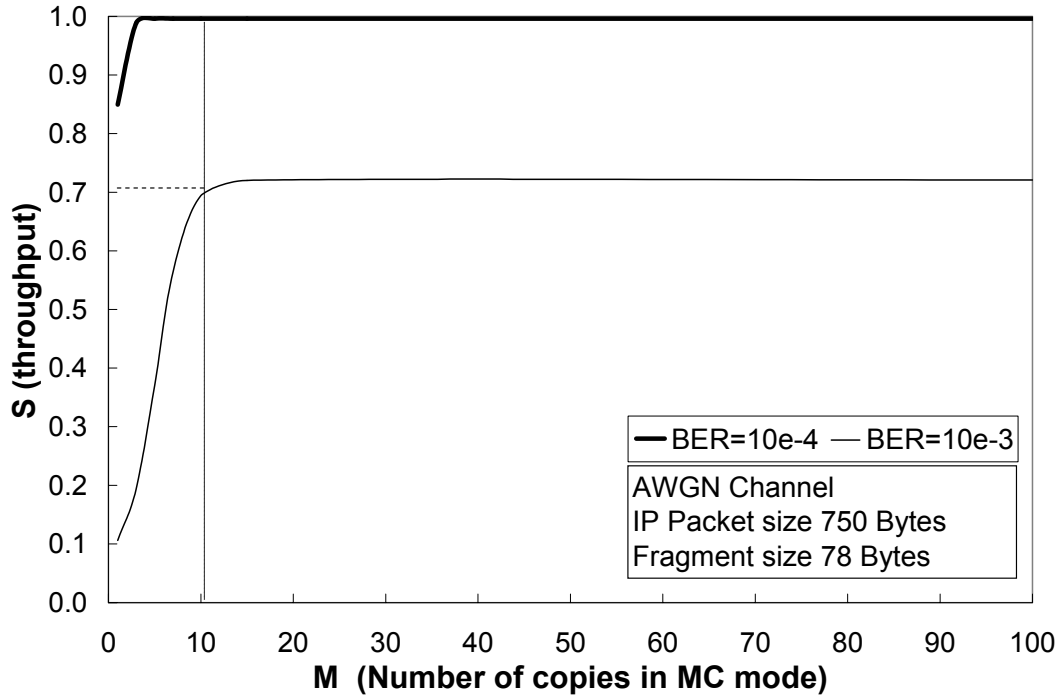


Figure 2-12. M against S for BER = 10^{-4} and 10^{-3}, IP packet size 750 bytes and fragment size 78 bytes.

Table 2-3 M against S for varying value of BER.

M	S for BER=10e-4	S for BER=10e-3
1	0.849	0.106
3	0.988	0.193
5	0.996	0.371
7	0.996	0.564
10	0.996	0.694
15	0.996	0.720
100	0.996	0.721

2.5.1 AWGN Channel

This section presents and examines the results for the proposed SR/MC ARQ scheme under AWGN channel. The ARQ packet must be optimized first which means finding the optimum value for M and IP fragment size.

Using Equation (9) the optimum value of M can be calculated for a given throughput, S, or for a given BER. These results are given in Figure 2-11, which corresponds to the Table 2-2, and Figure 2-12, which corresponds to the Table 2-3, respectively for IP packet size of 750 bytes and fragment size of 78 bytes [6,8]. Both the figures and tables confirm that M = 10 is the optimum value. Similar results were obtained for varying IP packet size and fragment size, i.e., the result is not affected by the IP packet size or the fragment size; this is made clear from Figure 2-14, Figure 2-17 and Figure 2-18. It is obvious from these figures that the throughput of the proposed ARQ decreases for bigger IP packet size and fragment size while the performance for a given IP packet size and fragment size increases as M increases to 10.

Knowing the optimum value for M the next step is to find the optimum fragment size for the proposed ARQ [8]. The optimum fragment size will be the one that gives the maximum throughput and the minimum delay. As small fragment size means large overhead it is also necessary to calculate the ratio of actual data and overhead against the packet size.

Result for fragment size and normalized delay is given in Figure 2-13 for varying IP packet size and BER = 10^{-3} [8]. It is clear from the result that a fragment size of 75 bytes gives the minimum delay. Similarly the result for the throughput against the fragment size is given in Figure 2-14 for varying IP packet size and BER = 10^{-3}. The throughput for varying IP packets is the same until the fragment size of 75 bytes. Similar results as in Figure 2-13 and Figure 2-14 were obtained for other values of BER; this can be explained based on Figure 2-17. The throughput of the proposed ARQ is dependent on the IP packet size, the performance of the ARQ is better for a smaller IP packet size for a given fragment size. Thus even if the normalized delay and the throughput are calculated for varying fragment size the trend of the curves will be similar and the optimum value will not change.

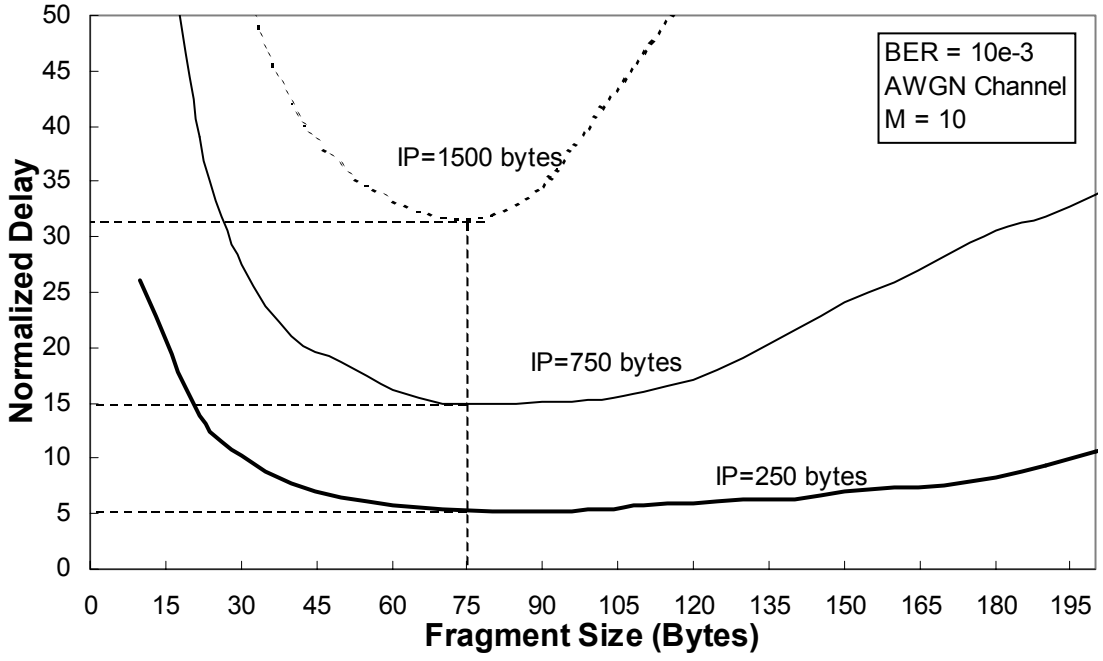


Figure 2-13 Normalized delay against fragment size for varying IP packet size and BER of 10^{-3}.

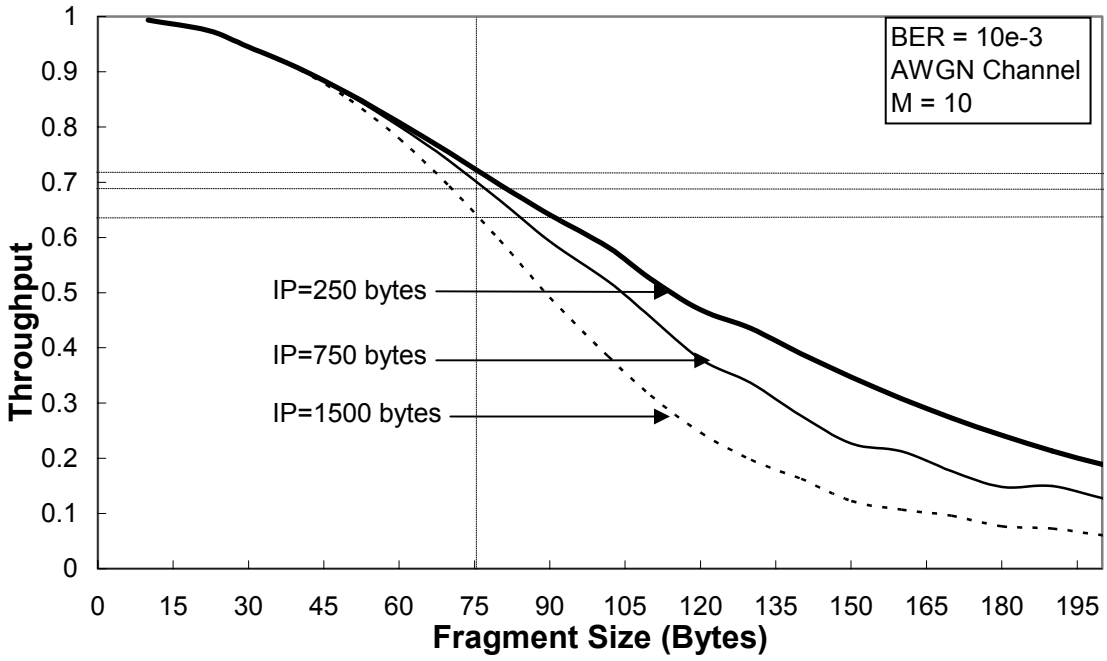


Figure 2-14 Throughput against fragment size for varying IP packet size and BER of 10^{-3}.

An optimum fragment size was also found using Equations (10) and (11), in Section 2.3.2, in terms of actual data throughput and fragment size transmitted without FEC and with BCH(63, 51) for varying IP packet size [8]. In Figure 2-15 and Figure 2-16 results are shown for an IP packet size of 1500 bytes and 250 bytes respectively. In both figures a pseudo constant data throughput is achieved for an IP packet size of 75 bytes for both without FEC and with BCH(63,51,2).

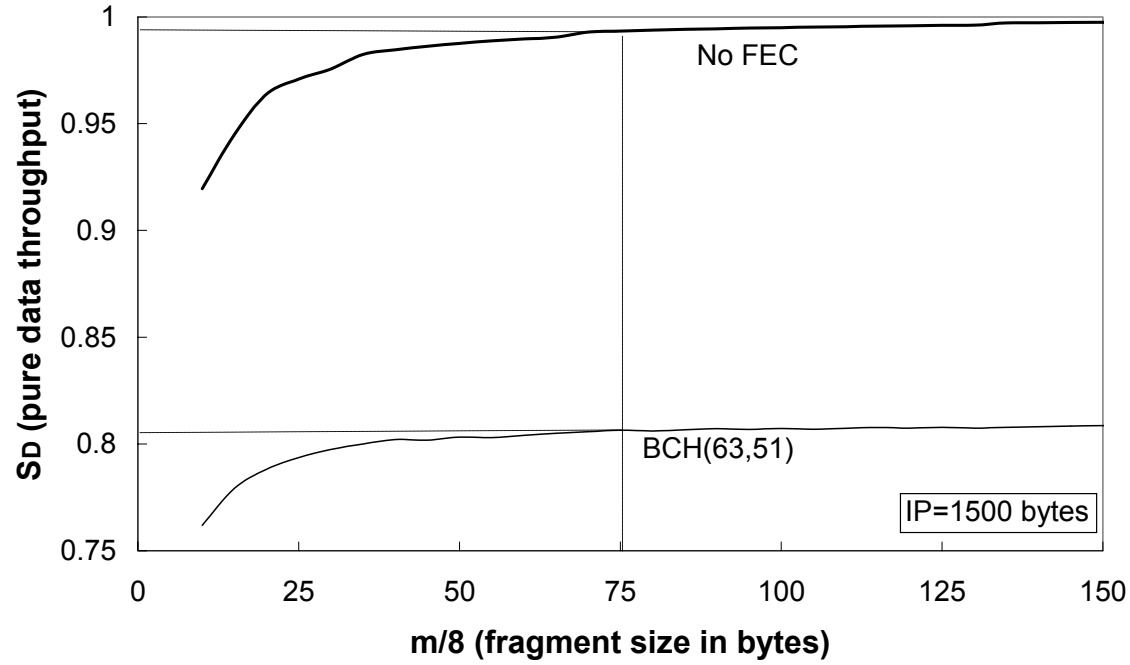


Figure 2-15 Data throughput against fragment size for IP packet size of 1500 bytes with BCH(63,51) and without FEC.

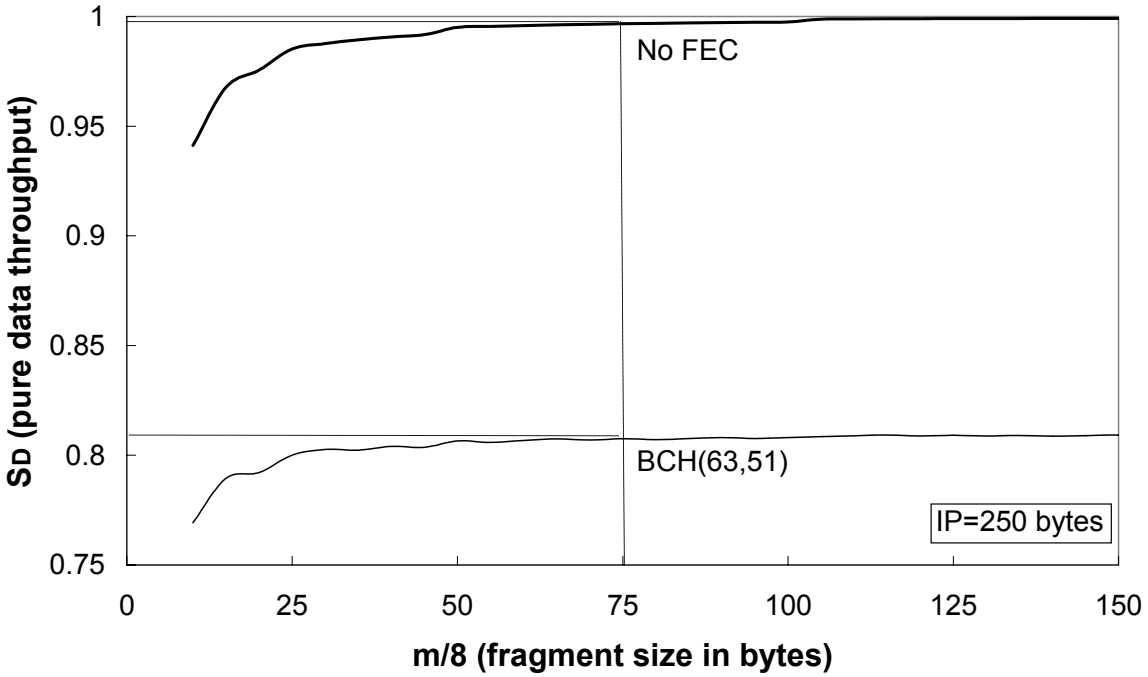


Figure 2-16 Data throughput against fragment size for IP packet size of 250 bytes with BCH(63,51) and without FEC.

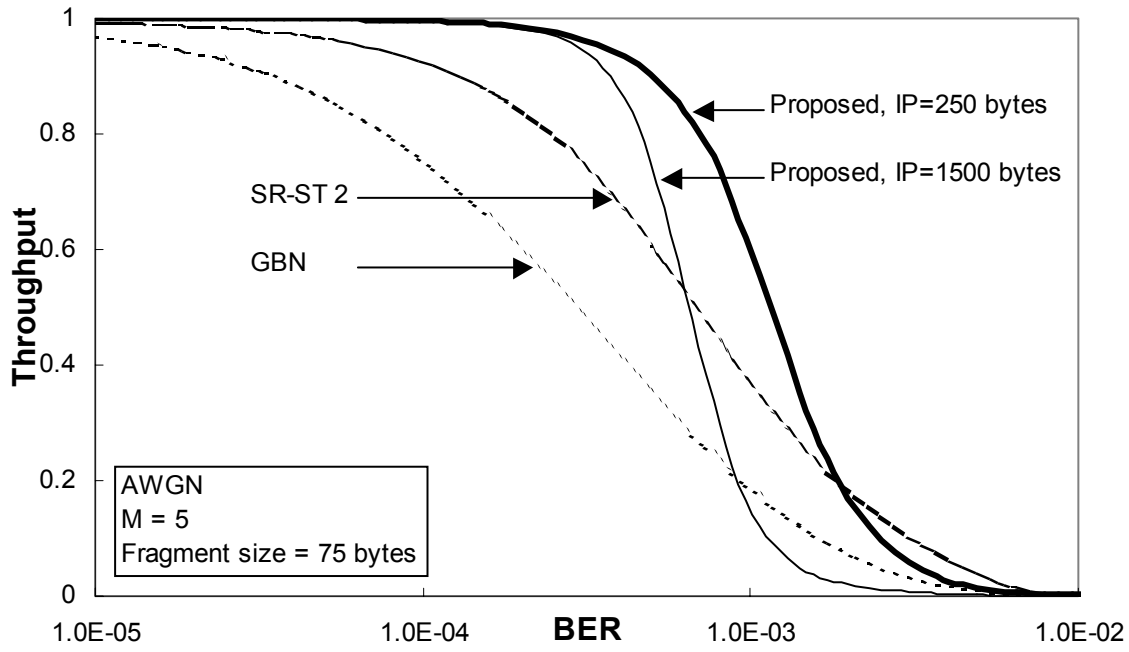


Figure 2-17 Throughput against BER under AWGN channel for SR/MC (proposed) scheme with M=5, GBN and SR-ST 2 with fragment size of 75 bytes and IP packet size of 250 and 1500 bytes.

Now that the optimum value for M, the number of copies of a fragment sent in MC mode, and m, the fragment size, are known the throughput, S, can be calculated using Equation 9. Results of the proposed scheme are compared with GBN and SR+ST 2 [6,8]. In Figure 2-17 the result is given for the proposed scheme for M = 5, fragment size of 75 bytes and IP packet sizes of 250 and 1500 bytes. Performance of the proposed ARQ is better for 250 bytes IP packet compared to 1500 bytes IP packet because the number of fragments transmitted is less thus the probability of erroneous fragments is less. Another point that can be observed here is the abrupt decrease in

throughput of the proposed ARQ for higher BER; the reason for this is the MC mode. The ARQ gives high throughput as long as it is in the SR mode; in the MC mode multiple copies of a fragment is transmitted which causes a decrease in the throughput. As the MC mode occurs only at the end of IP packet transmission the effect is seen even more for higher BER where more fragments are transmitted in MC mode. Figure 2-17 also shows results of SR+ST 2 and GBN, the proposed ARQ outperforms them. Both the SR+ST 2 and GBN are not based on higher layers thus their performance is dependent on fragment size and is independent of the IP packet size. Although SR+ST 2 uses the MC mode its performance decreases gradually because the MC mode does not appear at the end of the transmission but occurs continuously if two NACKs are received for a fragment. Even for M = 5 the proposed scheme, SR/MC, outperforms the GBN and SR+ST 2 for high BER.

In Figure 2-18 the proposed scheme is once again compared with GBN and SR+ST 2 for fragment size of 75 bytes [6,8], IP packet size of 1500 bytes and M = 5 and 10. Once again the proposed scheme outperforms GBN and SR+ST 2 but, the performance for M = 10 is better than for M = 5.

Table 2-4 gives the BER value after which the throughput becomes less than 0.9 for SR+ST 2 and the proposed scheme for varying fragment size and IP packet size [6,8]. It is clear that the proposed scheme performs better than SR+ST 2; a throughput of 0.9 is achieved at even higher BER by the proposed scheme for any IP packet size.

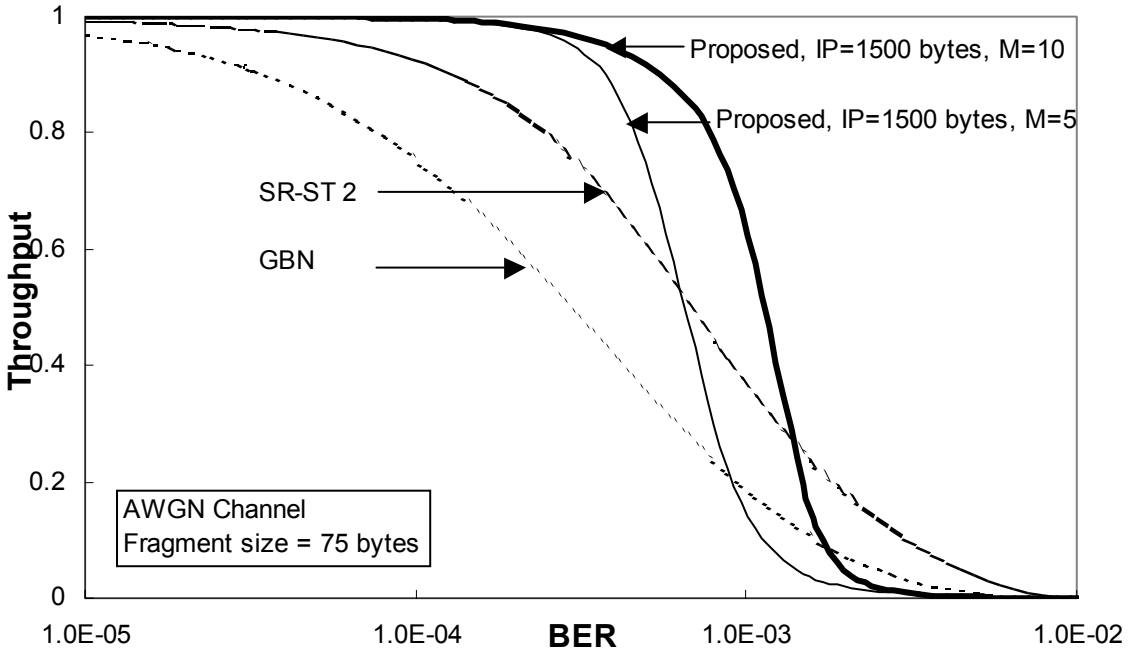


Figure 2-18 Throughput against BER under AWGN channel for SR/MC (proposed) scheme with M=5 and 10, GBN and SR-ST 2 with fragment size of 75 bytes and IP packet size of 1500 bytes.

Table 2-4 BER for SR+ST 2 and proposed scheme for varying IP packet size and fragment size, while S = 0.9.

Fragment Size	SR+ST 2	Proposed scheme; IP packet size 1500 Bytes	Proposed scheme; IP packet size 250 Bytes
39 Bytes	$2.5 * 10^{-4}$	$6.0 * 10^{-4}$	$9.0 * 10^{-4}$
79 Bytes	$1.5 * 10^{-4}$	$4.0 * 10^{-4}$	$5.0 * 10^{-4}$
162 Bytes	$7.0 * 10^{-5}$	$2.0 * 10^{-4}$	$2.5 * 10^{-4}$

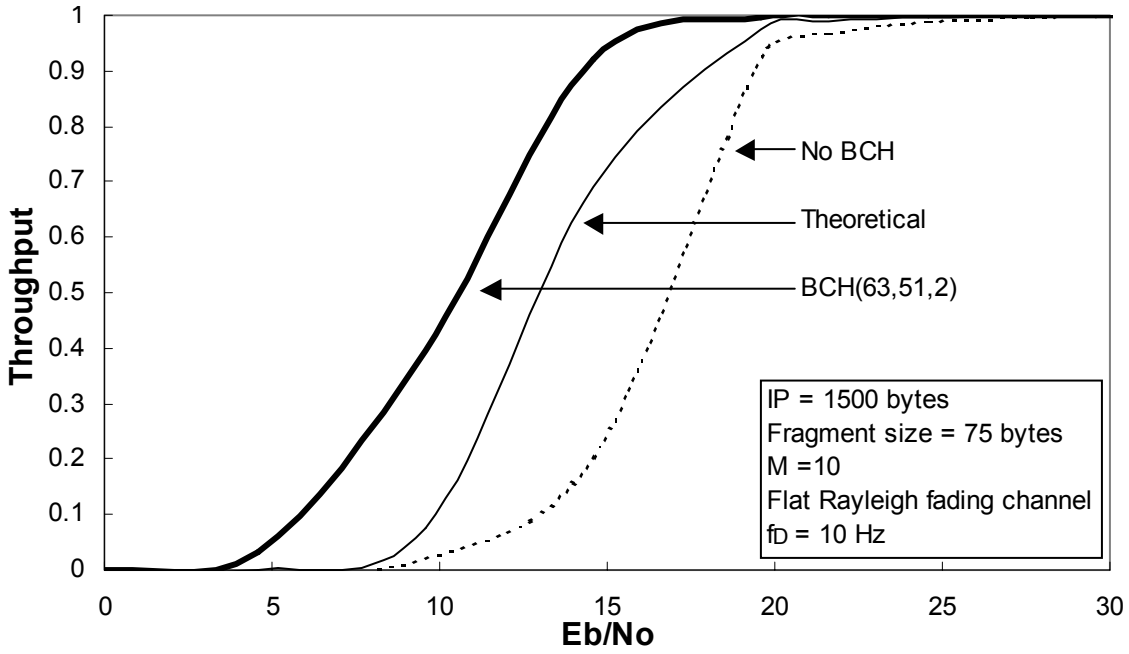


Figure 2-19 Throughput against Eb/No for proposed scheme under flat fading channel.

2.5.2 Fading Channel

Performance of Layer-2 or higher is effected by erroneous frames which in turn is related to BER and Eb/No. For calculation of throughput under fading channel the results generated by the simulation model given in Section 2.4.2 is used. BER for different Eb/No given in Figure 2-10 was used for throughput calculation in Equation (9) [6,8].

In Figure 2-19 results are given for throughput against Eb/No for the proposed ARQ with BCH(63,51), theoretical and without BCH (FEC) [6,8]. As expected the performance of the proposed ARQ is better with BCH which gives a gain of about 7dB for throughput (S) = 0.9.

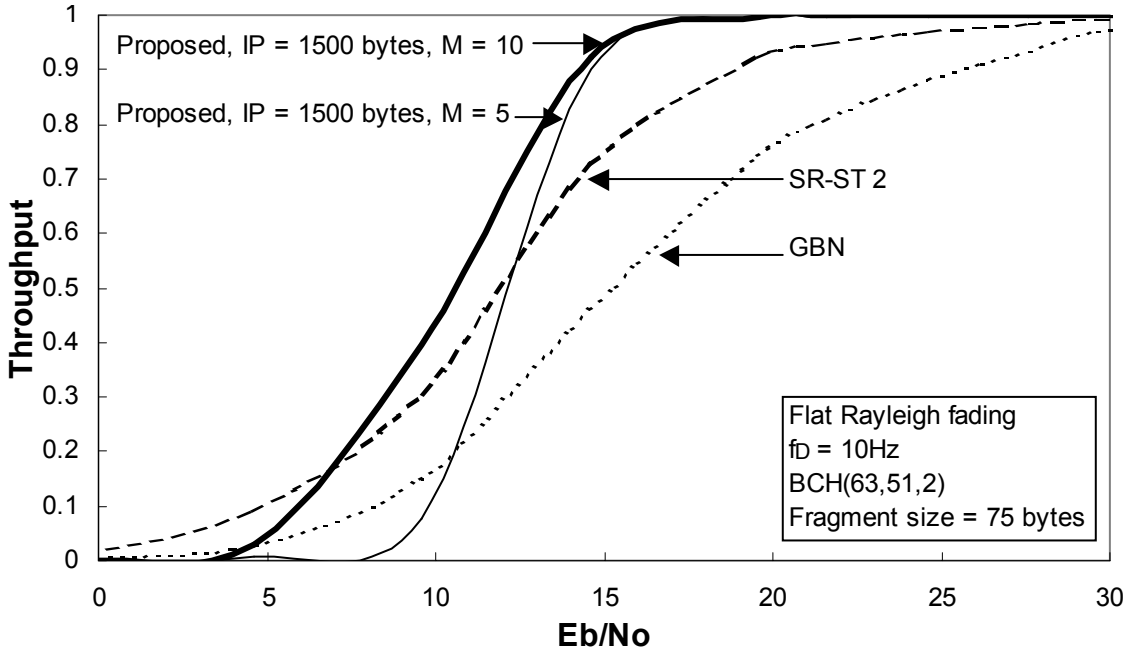


Figure 2-20 Throughput against Eb/No comparison of proposed scheme, SR+ST 2 and GBN under flat fading channel.

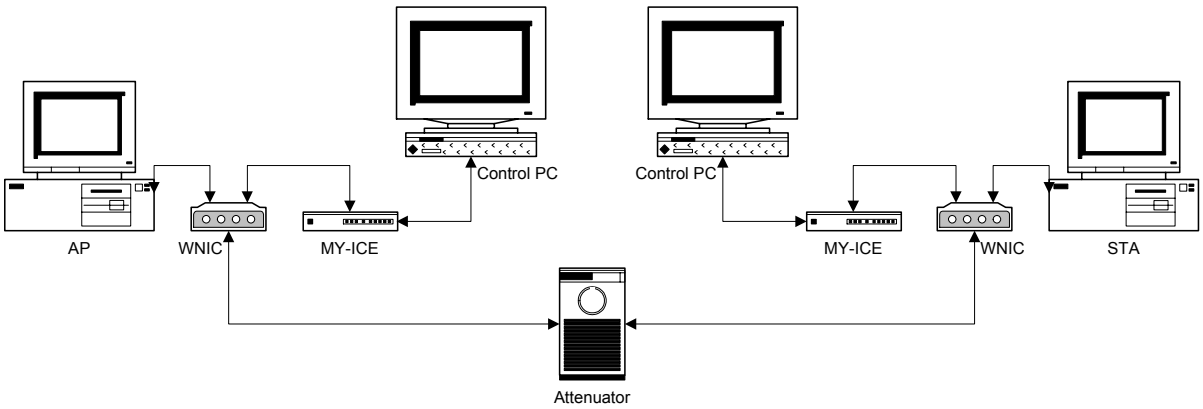


Figure 2-21 Measurement setup.

In Figure 2-20 the result of the proposed SR/MC ARQ is compared with that of the SR+ST 2 and the GBN schemes for a fragment size of 75 bytes, IP packet size of 1500 bytes and M = 5 and 10. The channel considered is a flat fading channel with Doppler frequency, f_D, of 10Hz. Similar to AWGN channel results, the proposed scheme outperforms SR+ST 2 and GBN. The proposed scheme gives better results for M = 10. For throughput of 0.9 there is an improvement of 8 dB compared to SR+ST 2 with BCH(63,51,2).

2.6 Measurement Setup and Results

In this section the performance measurement setup and results of the proposed ARQ, SR/MC, are discussed.

2.6.1 Setup

The measurement setup is given in Figure 2-21. Two similar setups were used for the throughput measurement of the ARQ. A WNIC was connected to PC; here WNIC means basically the physical layer together with the RF-part. This PC served as Access Point (AP) or, Station (STA), i.e., AP and STA protocols and control software were running in the PC. MY-ICE emulator was used for the Hitachi H8S/2246 processor [21]; this was connected to the WNIC card. MY-ICE was also connected to a PC from where the AP or, STA were controlled and results were displayed. The two WNIC card were connected using a cable with an attenuator. By varying the attenuator value different BER and throughput (S) were measured. The operating system (OS) used was μITRON 3.0 [22].

2.6.2 Results

The results were generated for a varying number of packets in the MC mode (M = 5, 10, 15). These are plotted in Figure 2-22, Figure 2-23 and Figure 2-24. The results are generated for an IP packet size of 1500 bytes.

In Figure 2-22 the results are given for M = 5. Several data are generated in odd places. These results occur because the measurements were taken even during the time the two WNICs lost their synchronization due to external interference as the measurement setup was not perfectly shielded. Similar results can be seen for M = 10 and 15 in Figure 2-23 and Figure 2-24. The dots in the three figures are the measurement results. The trendline was drawn using 'Exponential' MS Excel trendline function which uses least square method; 'Exponential' MS Excel trendline function was used because it gave the best fit. The throughput abruptly decreases at BER of 10^{-3}, although the trendline does not show that, this is similar to numerical results given in Section 2.5. Performance for M=10 is slightly better than M=5 and 15.

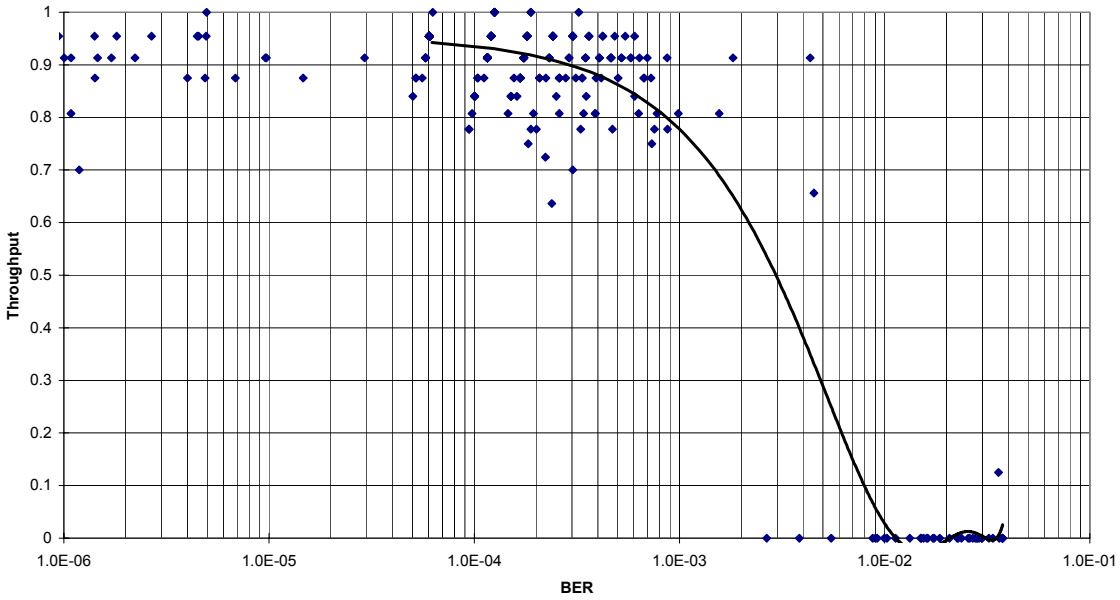


Figure 2-22 Measurement result for ARQ SR/MC for M = 5.

In theoretical calculations the ARQ was considered to stay in the MC mode until all fragments were received correctly, in practical situation this is not possible. After a certain number of cycles in the MC mode the ARQ must start transmitting the next packet or inform higher layers of a high level of interference in the medium. Higher layers also implement error correction mechanisms and will thus recover or disconnect. Another point is that, TCP also uses an ARQ retransmission time which is variable but has an upper limit. Keeping the practical limitations and TCP timer in mind, the number of cycles in the MC mode was limited to 10 for the implementation.

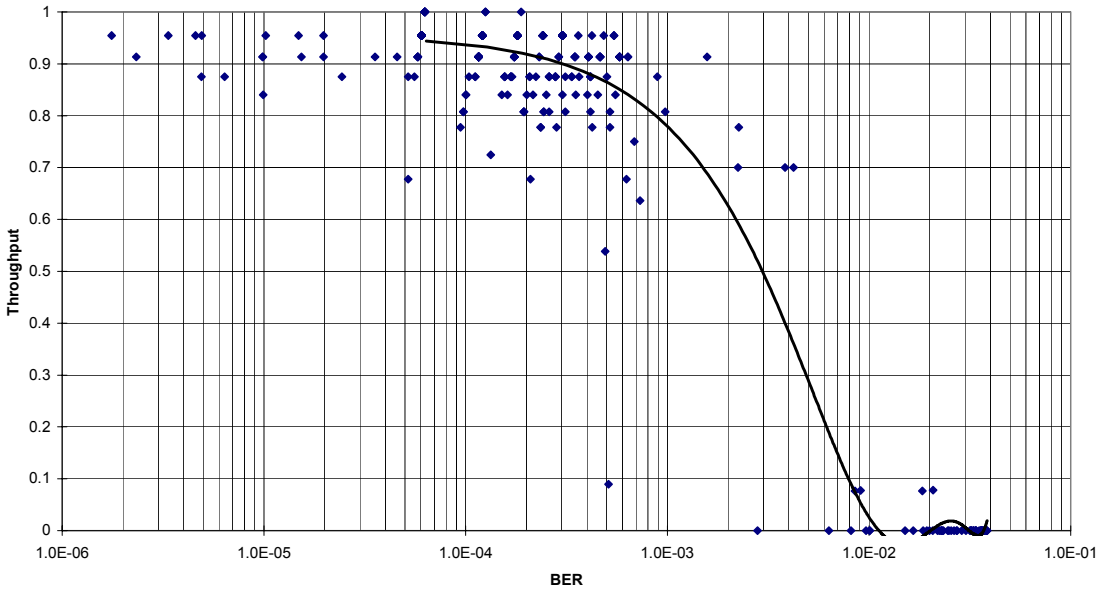


Figure 2-23 Measurement result for ARQ SR/MC for M = 10.

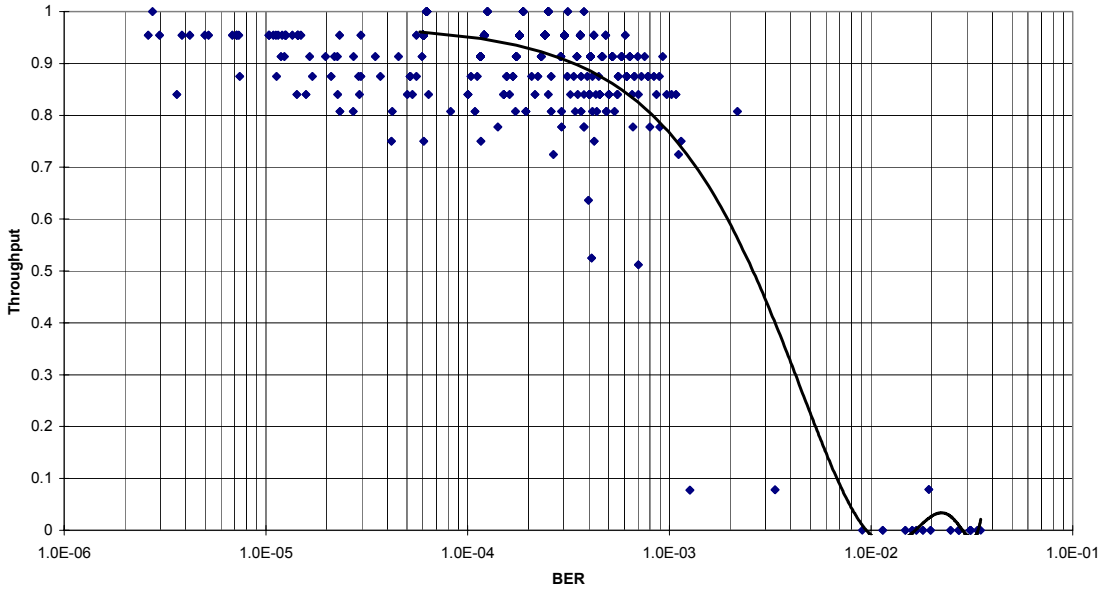


Figure 2-24 Measurement result for ARQ SR/MC for M = 15.

2.7 Conclusions

A hybrid Selective Repeat/Multicopy ARQ (SR/MC ARQ) scheme is proposed in this chapter for efficient IP packet transmission. The performance of the ARQ is given in terms of the throughput, Eb/No and BER. Numerical results of the proposed scheme are also compared with that of the SR+ST 2 scheme and the conventional Go-Back-N scheme. The results show that the proposed scheme outperforms the SR+ST 2 scheme and GBN under AWGN and flat Rayleigh fading channels for any fragment size.

The proposed scheme gives optimum performance for a fragment size of 75 bytes and number of copies in Multi-Copy mode M = 10. A fragment size of 75 bytes is a reasonable size and will not require much overhead even for large IP packet size and thus less memory management, making the transmitter and receiver structure simpler.

The proposed ARQ scheme gives a throughput higher than 0.9 for any IP packet size for much higher BER when compared with SR+ST 2 and GBN.

Throughput measurement results for the proposed ARQ are also given in this chapter; these results were the same as the numerical results. The proposed scheme gives very good performance and can be used very efficiently for IP packet transmission. As the simulation model used is very practical (flat Rayleigh fading channel and implementation loss taken in account) and as the measurement results show the proposed scheme will work very efficiently for any wireless communication systems which fits this model.

The proposed ARQ scheme is only studied for IP packet transmission, although it may as well be used elsewhere for example for wireless ATM.

In general any hybrid SR/MC scheme can be implemented either by a single (proposed SR/MC ARQ) or a series of SR-MC pairs (SR+ST 2 ARQ). Each SR-MC pair achieves higher throughput if the number of fragments to be transmitted in the SR mode is increased. The proposed scheme uses a single SR-MC pair for all IP fragments, thus the throughput increases and falls abruptly for high BER where the number of fragments in the MC mode increases.

The SR/MC ARQ scheme was applied for patent and implemented by the author for the proprietary WLAN, WNIC, developed in the Tokyo Research and Development Center (TRC) of Uniden Corporation, Tokyo, Japan. The author also implemented simple ARQs like Stop and Wait and Go-Back-N.

The C program of the ARQ implementation was about 1700 lines and the size of the file was 70KB. Processing time required by the ARQ was 1% of the total time required by the WNIC software. With fragment size of 75 bytes and a maximum IP packet size of 1500 bytes, which means 20 fragments, the memory management was simple and the buffer maximum requirement was the same as a maximum IP packet size (1.5KB).

References

[1] R. Fantacci and M. Scardi, "Performance Evaluation of Preemptive Polling Schemes and ARQ Techniques for Indoor Wireless Networks", IEEE Trans. On Vehicular Technology, vol. 45, no. 2, pp. 248-257, May 1996.

[2] S. Kumar and D.R. Vaman, "An Access Protocol for Supporting Multiple Classes of Service in a Local Wireless Environment", IEEE Transactions on Vehicular Technology, vol. 45, no. 2, pp. 288-302, May 1996.

[3] J. Walrand, *Communication Networks: A First Course*, Richard D. Irwin, Inc. and Aksen Associates, Inc., Boston, 1991.

[4] F. Halsall, *Data Communications, Computer Networks and Open Systems*. Addison Wesley, England, 1996.

[5] M. Schwartz, *Telecommunication Networks: Protocols, Modeling and Analysis*, Addison Wesley, California, 1987.

[6] A.R. Prasad, Y. Shinohara and K. Seki, "Performance of Hybrid ARQ for IP Packet Transmission on Fading Channel", IEEE Transactions Vehicular Technology, May 1999, Vol. 48, Nr. 3, pp. 900-910.

[7] A.R. Prasad and K. Seki, "Hybrid ARQ for IP Packet Transmission", ICUPC'97, pp 531-535, 12-16 October 1997.

[8] A.R. Prasad, "Optimization of Hybrid ARQ for IP Packet Transmission", International Journal on Wireless Personal Communications, Kluwer Academic Publishers, March 2001, Volume 16, issue 3, pp. 203-220.

[9] Y. Omoya, A.R. Prasad, N. Matsuoka and K. Seki, "A Wireless IP Packet Transmission Scheme", IEICE General Conference, Tokai University, Hiratsuka, Japan, B-5-305, 27-30 March 1998.

[10] A.R. Prasad and K. Seki, "Performance of Hybrid ARQ for IP Packet Transmission in Fading Channel", IEICE General Conference, Waseda University, Tokyo, Japan, B-5-84, 3-6 September 1997.

[11] A.R. Prasad and K. Seki, "Internet Protocol Packet Transmission using Hybrid SR/MC Scheme", IEICE General Conference, Kansai University, Suita, Japan, B-8-20, 24-27 March 1997.

[12] A.R. Prasad and K. Seki, "Performance of a Hybrid ARQ for IP Packet Transmission under Fading Channel", PIMRC'98, September 8-11, 1998, Boston, Massachusetts, USA.

[13] H. Tanaka, "A Performance of Selective-Repeat ARQ with Cyclical Multicopy Retransmission", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E79-A, no. 9, pp. 1386-1391, September 1996.

[14] M.J. Miller and S. Lin, "The Analysis of some Selective Repeat ARQ Schemes with Finite Receiver Buffer", IEEE Trans. on Comm., vol. COM-29, no. 9, pp. 1307-1315, September 1981.

[15] S. Lin, D. J. Costello, Jr., and M. J. Miller, "Automatic-repeat request error-control schemes," IEEE Comm. Mag., Vol. 22, pp. 5-16, Dec. 1984.

[16] International Standard ISO/IEC 8802-11:1999; IEEE Std 802.11-1999; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification.

[17] A.R. Prasad, A. Kamerman and H. Moelard, "IEEE 802.11 Standard", Chapter 3 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[18] G. Malmgren et. al., "Hiperlan type 2 – an Emerging World Wide WLAN Standard" XIIIth International Symposium on Services and Local accesS (ISSLS), Stockholm, Sweden, 18-23 June, 2000.

[19] J. Postel, "DoD Standard Transmission Control Protocol", RFC 761, January 1980.

[20] Y. Shinohara and K. Seki, "A Digital MODEM for Offset-Chip DS-SS", IEICE Technical Group Meeting on Communication Systems, Japan, RCS97-6, pp. 41-47, 25 April 1997.

[21] User's Manual, MY-ICE AE Series: Support Device H8S/2245 Series CPU, Hitachi Corporation Ultra-LSI Systems. http://www.hitachi-ul.co.jp/MYICE/pdf/users2655ae.pdf

[22] μITRON 3.0 Specifications: http://tron.um.u-tokyo.ac.jp/TRON/ITRON/spec-e.html#ITRON3

Chapter 3

Capacity Enhancement of Indoor Wireless Communication System with a Novel Channel Sharing Protocol

The Medium Access Control (MAC) protocols form the basis of efficient use of a channel, be it wireline or wireless. When numerous users desire to transmit in a channel at the same time, conflicts occur, so there must be procedures on how the available channel capacity is allocated to the user. These procedures constitute the MAC protocol rules each user has to follow in accessing the common channel [1]. The channel thus becomes a shared resource whose allocation is critical for proper functioning of the network.

This chapter starts with an explanation of the basics of MAC protocols and an explanation of IEEE 802.11 and HIPERLAN/2 MAC protocols. After this a novel MAC protocol is proposed, known as the Channel Sharing Protocol (CSP). The proposed CSP was designed for a proprietary WLAN developed by the Tokyo Research and Development Center of Uniden Corporation, Tokyo, Japan. Both numerical and simulation based performance analysis of the proposed CSP are presented in this chapter. The performance is compared with the IEEE 802.11 MAC, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The author designed the proposed CSP protocol and prepared the specifications for its implementation. The proposed CSP was also applied for patent by the author.

3.1 Medium Access Control Protocols

So as to design an appropriate MAC protocol one has to understand the wireless network under discussion [1,11,12]. The first thing that should be understood is the duplexing scheme used by a system and the network architecture. A MAC protocol is dependent on these two issues.

Duplexing refers to mechanisms for wireless devices to send and receive. There are two duplexing methods, time based or frequency based. Sending and receiving data in same frequency at different time periods is known as Time Division Duplex (TDD), while sending and receiving data in same time and different frequency is known as Frequency Division Duplex (FDD).

A wireless network can be distributed or centralized. Distributed networks are those where each device accesses the medium individually and transmits the data without any central control. A distributed network architecture requires the same frequency and thus makes use of TDD. IEEE 802.11 is an example of a distributed network architecture. On the other hand a centralized network architecture has one network element which controls the communication of various devices. Such network architecture can make use of both TDD and FDD. HIPERLAN/2 is an example of a centralized network architecture.

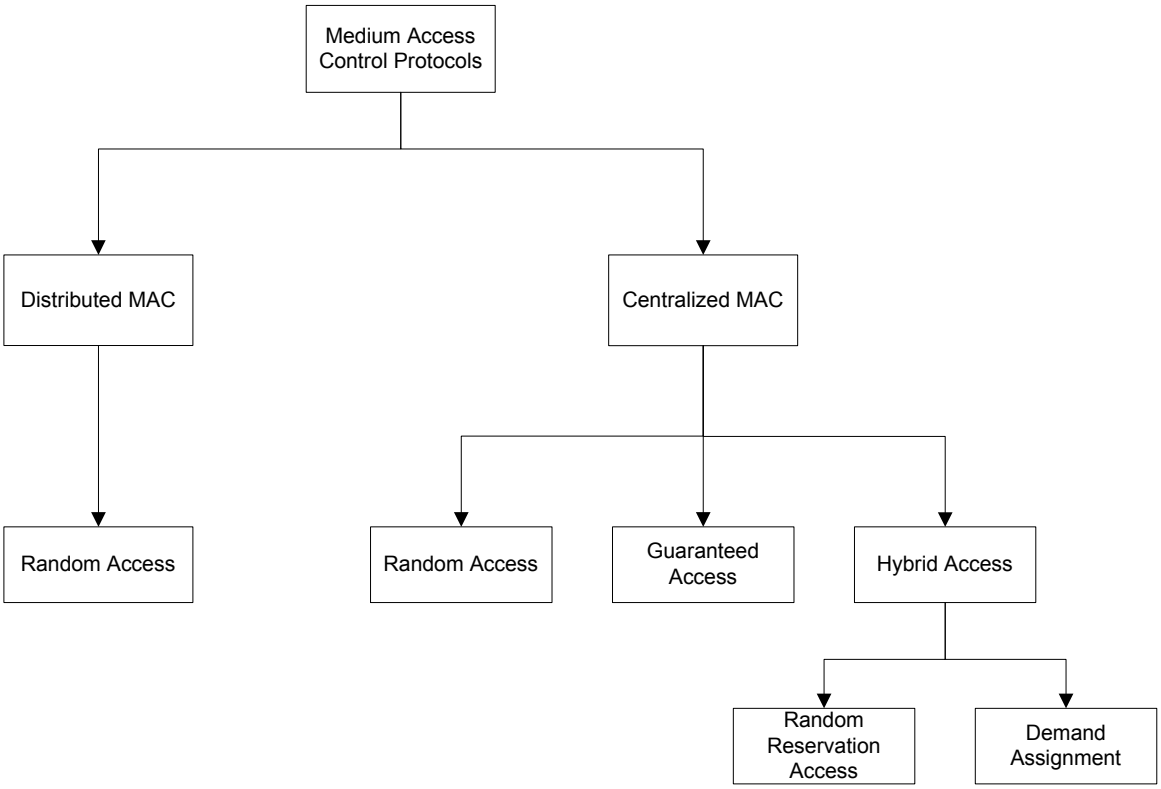


Figure 3-1 Classification of MAC protocols.

3.1.1 MAC Basics

Based on the network architecture one can divide MAC protocols in two groups, distributed and centralized, as depicted in Figure 3-1 [11]. In case of a distributed mechanism one cannot be sure if collision will happen when the channel is accessed. Thus conflicts have to be resolved when collision happens. Distributed mechanisms make use of random channel access, e.g., ALOHA or CSMA/CA. Centralized mechanisms can be divided in random access and guaranteed access protocols. In guaranteed access, nodes access the medium in an orderly manner and thus avoid collision. Another choice in centralized control is to have a hybrid of random and guaranteed access. Hybrid access protocols can further be classified in Random Reservation Access (RRA) protocols and demand assignment protocols. An example of the RRA rule is that a successful request results in periodic reservation of slots; this is where the proposed CSP falls in.

3.1.2 MAC in WLAN Standards

In this section the MAC protocols in IEEE 802.11 [3,10] and HIPERLAN/2 [13,14] are discussed. As IEEE 802.11 is the most commonly used WLAN it is explained in more detail, another reason for doing so is that the IEEE 802.11 MAC is compared with the MAC protocol proposed in this chapter.

3.1.2.1 IEEE 802.11

Standardization of IEEE 802.11 was done to satisfy the needs of wireless data networking. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) was the MAC protocol adopted by IEEE 802.11 [3,10]. Wherein, the basic channel access method is random back-off CSMA with a MAC-level acknowledgment. A CSMA protocol requires the STAtion (STA) to listen before transmitting. In this protocol only one user can access the medium at a time while the system is mostly used for low data rate applications (Internet access, e-mails etc.).

The IEEE 802.11 basic medium access behaviour allows interoperability between compatible PHYs through the use of the CSMA/CA protocol and a random back-off time following a busy medium condition. In addition, all traffic uses an immediate positive acknowledgment (ACK frame), where the sender schedules a retransmission if no ACK is received. The IEEE 802.11 CSMA/CA protocol is designed to reduce the collision probability between multiple stations accessing the medium at the point in time where collisions would most likely occur. Collisions are most likely to happen just after the medium becomes free, i.e., just after busy medium conditions. This is because multiple stations would have been waiting for the medium to become available again. Therefore, a random back-off arrangement is used to resolve medium contention conflicts. The IEEE 802.11 MAC also describes the way beacon frames are sent by the AP at regular intervals (like 100 ms) to enable stations to monitor the presence of the AP. The MAC also gives a set of management frames that allow a station to actively scan for other APs on any available channel. Based on this information the station may decide on the best-suited AP. In addition, the 802.11 MAC defines special functional behaviour for the fragmentation of packets, medium reservation via RTS/CTS (Request-To-Send/Clear-To-Send) polling interaction and point coordination (for time-bounded services) [3].

The MAC sublayer is responsible for the channel allocation procedures, protocol data unit (PDU) addressing, frame formatting, error checking, and fragmentation and reassembly. The transmission medium can operate in the contention mode exclusively, requiring all stations to contend for access to the channel for each packet transmitted. The medium can also alternate between the contention mode, known as the Contention Period (CP), and a Contention-Free Period (CFP). During the CFP, medium usage is controlled (or mediated) by the AP, thereby eliminating the need for stations to contend for channel access. IEEE 802.11 supports three different types of frames: management, control, and data. The management frames are used for station association and disassociation with the AP, timing and synchronization, and authentication and de-authentication. Control frames are used for handshaking during the CP, for positive acknowledgments during the CP, and to end the CFP. Data frames are used for the transmission of data during the CP and CFP, and can be combined with polling and acknowledgments during the CFP.

As the contention-free mode is not used, this section will discuss the contention mode of the IEEE 802.11 MAC which is also known as the Distributed Coordination Function (DCF). The RTS/CTS mechanism of IEEE 802.11 is not discussed in this chapter. The IEEE 802.11 MAC discussed here is the original MAC and not IEEE 802.11e and i these are presented in Chapter 4 and Chapter 5 respectively where work on QoS (Quality of Service) and security are presented.

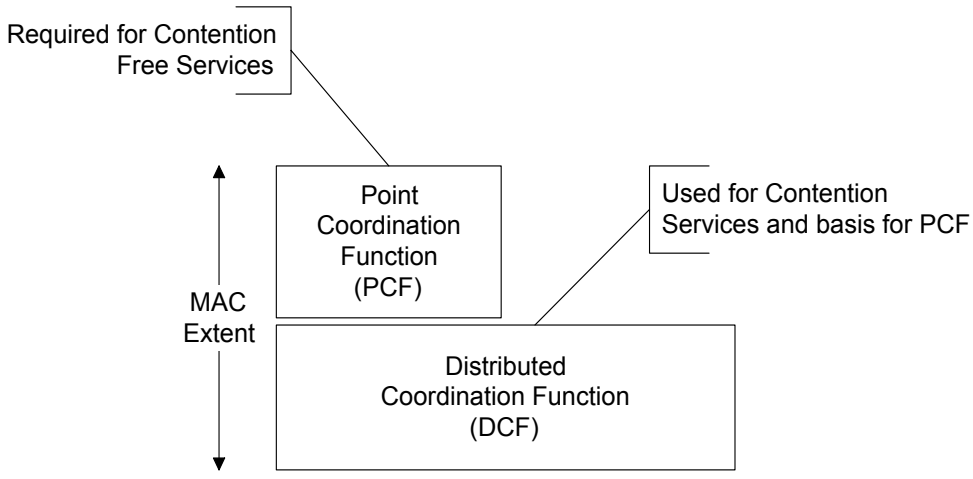


Figure 3-2 MAC architecture.

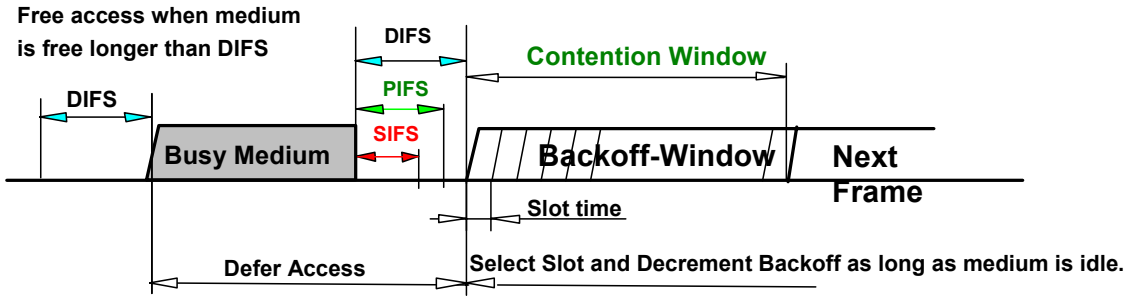


Figure 3-3 IEEE 802.11 inter frame space.

3.1.2.1.1 Distributed Coordination Function

The DCF is the fundamental access method used to support asynchronous data transfer on a best effort basis. As identified in the IEEE 802.11 specification [3,10], all stations must support the DCF. The DCF operates solely in the ad hoc network, and either operates solely or coexists with the PCF in an infrastructure network. The MAC architecture is depicted in Figure 3-2, where it is shown that the DCF sits directly on top of the physical layer and supports contention services. Contention services imply that each station with a packet queued for transmission must contend for access to the channel and, once the packet is transmitted, must recontend for access to the channel for all subsequent frames. Contention services promote fair access to the channel for all stations [3].

The DCF is based on CSMA/CA. In IEEE 802.11, carrier sensing is performed at both the air interface, referred to as physical carrier sensing, and at the MAC sublayer, referred to as virtual carrier sensing. Physical carrier sensing detects the presence of other IEEE 802.11 WLAN users by analyzing all detected packets, and also detects activity in the channel via relative signal strength from other sources.

A source station performs virtual carrier sensing by sending packet duration information in the header of RTS, CTS, and data frames. A packet is a complete data unit that is passed from the MAC sublayer to the physical layer. The packet contains header information, payload, and a 32-bit CRC. The duration field indicates the amount of time (in microseconds) after the end of the present frame the channel will be utilized to complete the successful transmission of the data or management frame. Stations in the BSS use the information in the duration field to adjust their Network Allocation Vector (NAV), which indicates the amount of time that must elapse until the current transmission session is complete and the channel can be sampled again for idle status. The channel is marked busy if either the physical or virtual carrier sensing mechanisms indicate the channel is busy.

Priority access to the wireless medium is controlled through the use of Interframe Space (IFS) time intervals between the transmission of frames. The IFS intervals are mandatory periods of idle time on the transmission medium. Three IFS intervals, see Figure 3-3, are specified in the standard: Short IFS (SIFS), Point Coordination Function IFS (PIFS), and DCF-IFS (DIFS). The SIFS interval is the smallest IFS, followed by PIFS and DIFS, respectively. Stations only required to wait a SIFS period have priority access over those stations required to wait a PIFS or DIFS period before transmitting; therefore, SIFS has the highest-priority access to the communications medium. For the basic access method, when a station senses the channel is idle, the station waits for a DIFS period and samples the channel again. If the channel is still idle, the station transmits an MPDU. The receiving station calculates the checksum and determines whether the packet was received correctly. Upon receipt of a correct packet, the receiving station waits a SIFS interval and transmits a positive ACK frame back to the source station, indicating that the transmission was successful. Figure 3-4 is a timing diagram illustrating the successful transmission of a data frame. When the data frame is transmitted, the duration field of the frame is used to let all stations in the BSS know

how long the medium will be busy. All stations hearing the data frame adjust their NAV based on the duration field value, which includes the SIFS interval and the ACK following the data frame.

The collision avoidance portion of CSMA/CA is performed through a random backoff procedure. If a station with a frame to transmit initially senses the channel to be busy; then the station waits until the channel becomes idle for a DIFS period, and then computes a random backoff time. For the IEEE 802.11, time is slotted in time periods that correspond to a Slot_Time. The Slot_Time used in IEEE 802.11 is much smaller than an MPDU and is used to define the IFS intervals and determine the backoff time for stations in the CP. The Slot_Time is different for each physical layer implementation. The random backoff time is an integer value that corresponds to a number of time slots. Initially, the station computes a backoff time in the range 0–7. After the medium becomes idle after a DIFS period, stations decrement their backoff timer until the medium becomes busy again or the timer reaches zero. If the timer has not reached zero and the medium becomes busy, the station freezes its timer. When the timer is finally decremented to zero, the station transmits its frame. If two or more stations decrement to zero at the same time, a collision will occur which lead-to missing ACKs, and each station will have to generate a new backoff time in the range 0–63 (for 802.11b, and 0-31 for 802.11a) times the Slot_Time period. The generated backoff time corresponds to a uniform distributed integer multiple of Slot_Time periods. For the next retransmission attempt, the backoff time grows to 0-127 (for 802.11b, and 0-63 for 802.11a) Slot_Time periods and so on with a maximum in the range of 0-1023. The idle period after a DIFS period is referred to as the Contention Window (CW). The advantage of this channel access method is that it promotes fairness among stations, but its weakness is that it probably could not support time bound services. Fairness is maintained because each station must recontend for the channel after every transmission of an MSDU. All stations have equal probability of gaining access to the channel after each DIFS interval. Time-bounded services typically support applications such as packetized voice or video that must be maintained with a specified minimum delay. With DCF, there is no mechanism to guarantee minimum delay to stations supporting time-bounded services.

3.1.2.2 HIPERLAN/2

The MAC in HIPERLAN/2 is a part of the Data Link Control (DLC) layer together with other functions like Error Control (EC). A brief description of the MAC layer and frames of HIPERLAN/2 are given in this chapter [13,14].

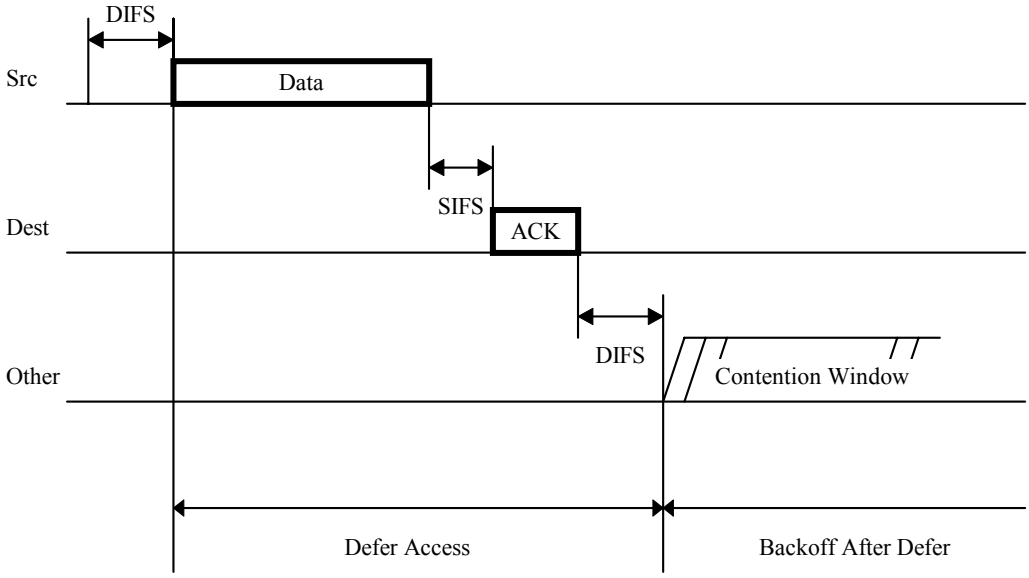


Figure 3-4 Transmission of a MPDU without RTS/CTS.

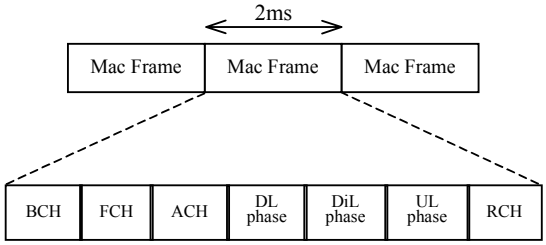


Figure 3-5 The HIPERLAN/2 MAC frame.

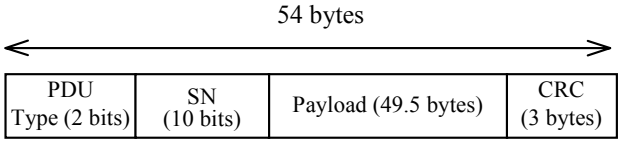


Figure 3-6 Format of the long PDUs.

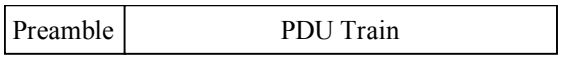


Figure 3-7 Format of PDU train.

3.1.2.2.1 MAC Layer

The MAC scheme of HIPERLAN/2 is based on a central controller, which is located at the AP. The core task of the central controller is to determine the direction of information flow between the controller and the terminal at any point of time. A MAC frame consists of control and data blocks. The central controller decides which terminal or group of terminals is allowed to transmit in a slot of the frame. The medium access scheme is classified as load adaptive Time Division Multiple Access (TDMA). Each user shall be assigned zero, one or several slots in a frame. In general, the number of slots assigned to an individual user varies from frame to frame and depends on the actual bandwidth request of the terminal. The uplink and downlink packets are sent on the same frequency channel in a TDD mode.

Random access slots are provided to allow STAs to get associated with the controller. In this "bootstrap phase" data is transmitted in a contention-based mode, collisions may occur. Therefore, a collision resolution algorithm is applied.

Uplink signalling of resource describes the state of the input queues of a STA to the central controller. The AP collects these requests from all associated STAs and uses this data to schedule the uplink access times. The results of the scheduling process are signalled via the frame control channel, i.e., a description of the exact frame structure and slot allocation is contained in the frame control channel. These control data are valid for the ongoing frame. Further tasks are: multiplexing and de-multiplexing of logical channels, service requesting and service granting and medium access control.

3.1.2.2.2 MAC Frames

The MAC frame structure (Figure 3-5) comprises time slots for Broadcast Control (BCH), Frame Control (FCH), Access Feedback Control (ACH), and data transmission in Downlink (DL), Uplink (UL), and Directlink (DiL) phases, which are allocated dynamically depending on the need

for transmission resources. An STA first has to request capacity from the AP in order to send its data. This can be done in the Random Access Channel (RCH), where contention for the same time slot is allowed.

DL, UL and DiL phases consist of two types of PDUs: long PDUs and short PDUs. The long PDUs (Figure 3-6) have a size of 54 bytes and contain control or user data. The payload is 49.5 bytes and the remaining 4.5 bytes are used for the PDU Type (2 bits), a sequence number (10 bits, SN) and a cyclic redundancy check (CRC-24). Long PDUs are referred to as the long transport channel (LCH). Short PDUs contain only control data and have a size of 9 bytes. They may contain resource requests, ARQ messages etc. and they are referred to as the Short Transport Channel (SCH).

Traffic from multiple connections to/from one STA can be multiplexed onto one PDU train, which contains long and short PDUs. A physical burst is composed of the PDU train payload and a preamble and is the unit to be transmitted via the physical layer (Figure 3-7).

3.2 Network Architecture

As explained in Section 3.1 MAC protocols are dependent on the network architecture; in this section the network architecture considered for the design of the proposed MAC protocol is described.

A centralized network architecture, as in Chapter 2, is considered in this chapter. The system is considered to be used mainly for Internet browsing and, when required, for E-mail download. The system considered is shown in Figure 3-8, there is one AP with which several STAs can communicate. STAs cannot communicate with each other. The AP is connected to the wired LAN so that users can access the Internet through the AP.

The AP can support a fixed number of physical channels. As Frequency Division Multiple Access (FDMA) is used, a channel stands for a particular frequency. The duplexing method used is TDD. Further details of the system can be found in Appendix C: WNIC Specification. The original MAC used for WNIC used to assign one channel to a user after which the channel was occupied even if it was not being used. Thus the capacity of the system was equal to the number of available channels. The goal of a new MAC design was to improve the capacity.

3.3 Channel Sharing Protocol

In this section the proposed CSP is explained in detail. For better explanation of the proposed CSP first the frame structure and the p-persistence algorithm are explained. After which the protocol description is given together with an example [6 – 9].

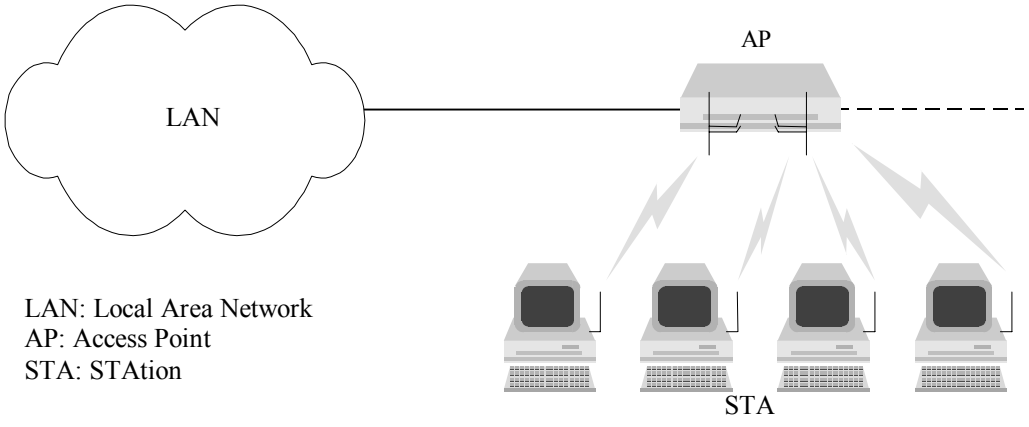


Figure 3-8 network architecture.

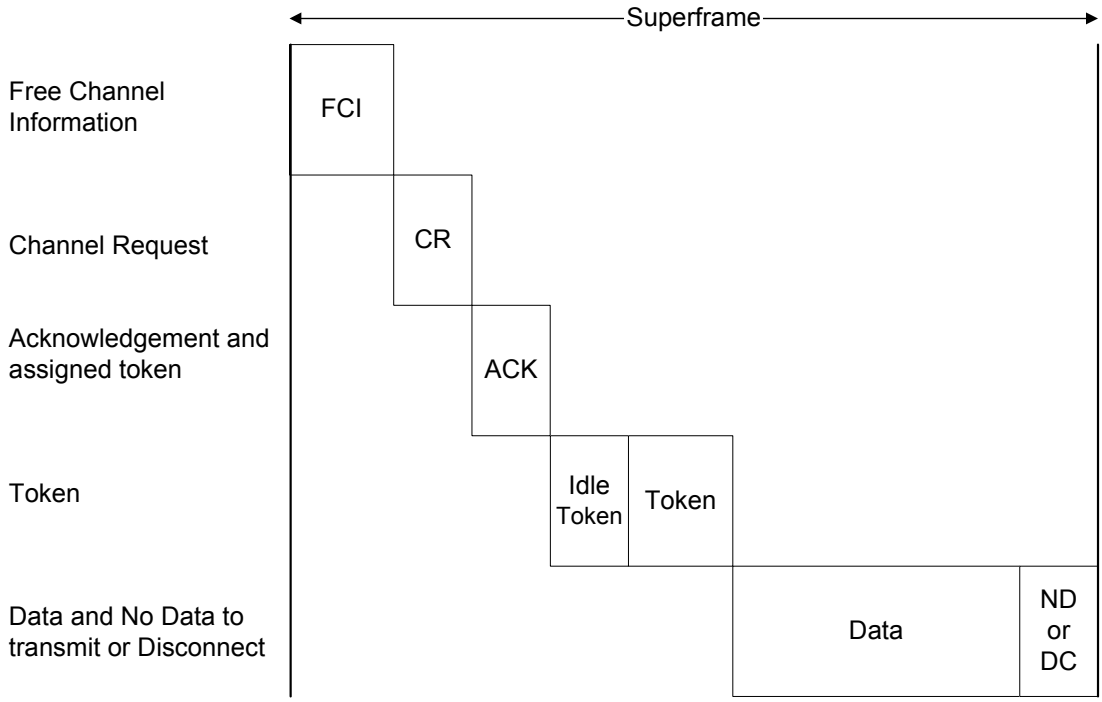


Figure 3-9 CSP Superframe.

3.3.1 Frames

For better understanding of the proposed CSP the frames used are explained in the following. The super frame structure of the proposed CSP is given in Figure 3-9 and consists of:

FCI: Free Channel Information (FCI) is transmitted periodically by the AP in every channel. So as to achieve uniform distribution the FCI contains information about the number of users in each channel. This information is used by the STA to decide which channel to join.

CR: Channel Request (CR) is transmitted by the STA to the AP to request a connection. This is usually transmitted after receiving an Idle Token or a FCI and after performing the p-persistence algorithm.

ACK: Acknowledgement together with MAC address and Token ID (ACK) is transmitted by the AP to the STA of which the CR was received correctly.

Idle Token: Idle Token is transmitted after all the assigned tokens have been transmitted. The main purpose of this token is to give STAs a chance to join a channel, this chance is necessary for the case where the channel was busy after FCI due to one reason or other. After Idle Token the first token is transmitted. A STA can join the channel after receiving the Idle Token.

Token: Token is assigned to all the STAs connected to an AP. Each channel has fixed number of tokens, i.e., each channel can support a given number of STAs at a time. The AP transmits tokens cyclically in every channel. The STA to which the token belongs can communicate with the AP.

Data: This is the data frame transmitting data from the AP to a STA or vice versa.

ND: No Data (ND) is transmitted by the STA to the AP after receiving the assigned token. This is to inform the AP that there is no data to transmit. One can see ND as a keep alive message also.

DC: Disconnect (DC) is transmitted by a STA or the AP so as to discontinue the communication and make the token available for another STA.

3.3.2 P-persistence Algorithm

In p-persistence algorithm [2,12] each STA is given a p-persistence value, p_p, between 0 and 1, the STA generates a random value, p, between 0 and 1 before it begins to transmit. If p is greater than p_p then the STA is allowed to transmit. This avoids collision by preventing multiple STAs to access a channel at the same time. This method can also be used to set priority levels. Smaller p-persistence value (high priority) will give higher chance to access the channel while higher value (low priority) will give lower chance to access the channel.

3.3.3 Protocol Description

When the AP is switched on it is initialized by setting the number of STAs in each channel equal to zero. The AP then transmits the FCI in each channel at a fixed interval and after that the Token 0. While, when a STA is switched on, a value equal to p-persistence, p_p, is given to the STA. This value is between 0 and 1. The STA then waits for a FCI from the AP. The FCI contains information of the channels that are crowded/not crowded and the number of STAs per channel. Here crowded means that all tokens in a given channel are assigned and not crowded means one or more tokens are available. After receiving the FCI the STA follows the steps given below:

1. If, all channels are free (no STA in any channel); choose any channel at random.

2. If, some channels are occupied and some are free or, one is free; choose the free channel or, one of the free channels at random.

3. If, there are STAs in all channels but, they are not crowded then choose the channel with the minimum number (STA_{min}) of STAs. If many channels have STA_{min} then choose one of them randomly.

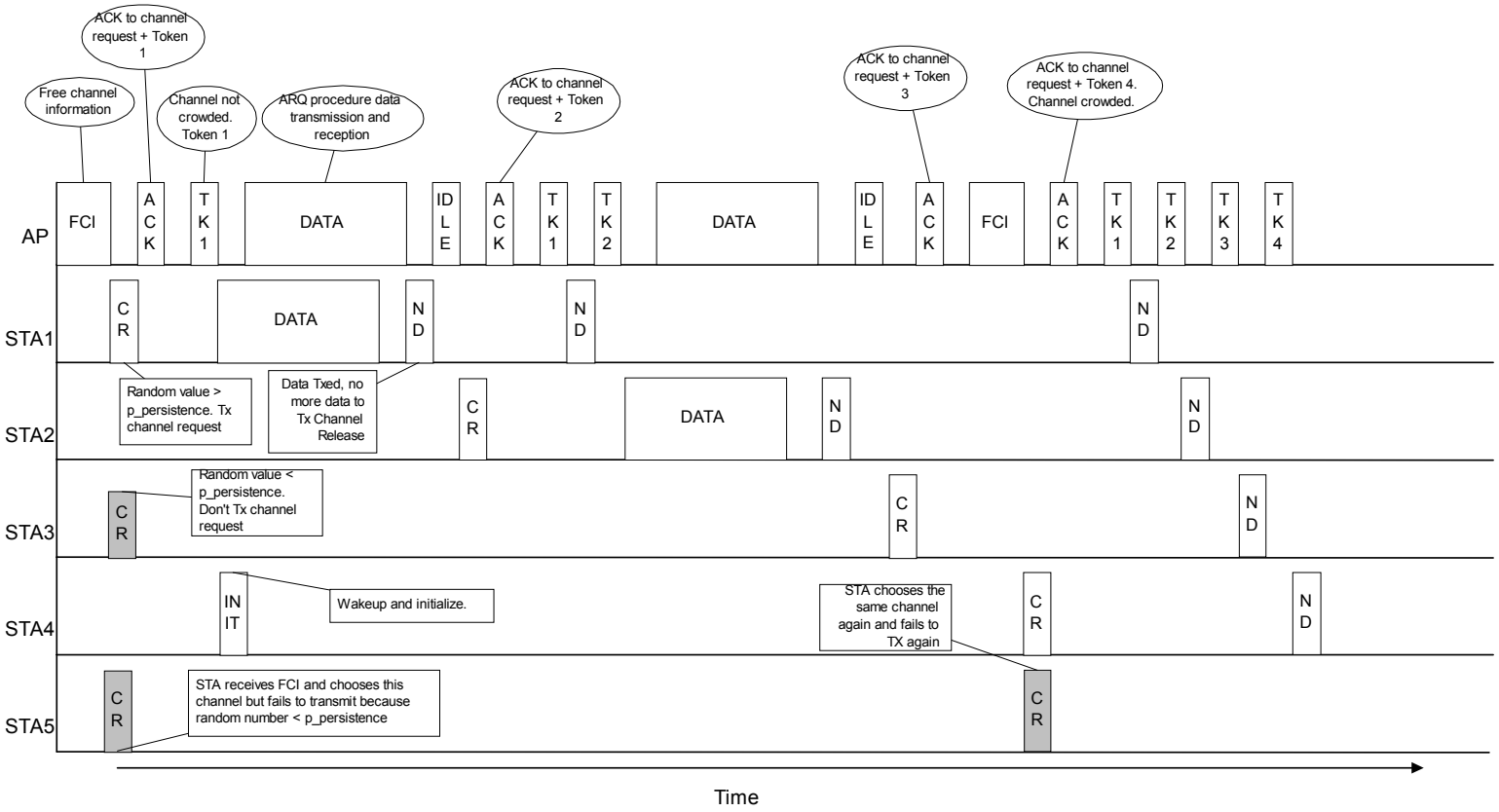
The above steps are used to obtain a uniform distribution of STAs in each channel. When a channel is chosen, the p-persistence algorithm is used to start the transmission; this is to prevent collision between two STAs trying to access the same channel simultaneously.

If a STA is not successful in getting a channel after receiving the FCI (due to p-persistence) then it chooses a channel at random and checks the token. The token is not only a field passed to the STA communicating with the AP but it also tells if a channel is crowded or, not crowded and also if a channel is idle or, not idle. If the channel is crowded then the STA chooses another channel at random and again checks the token in that channel. If the channel is not crowded then the STA checks if the channel is idle.

Once the channel is idle the STA will start transmitting to the AP based on p-persistence algorithm. The STA will first send a CR to the AP; the AP assigns a token number to the STA and responds to the STA together with an acknowledgment and the token number. If that particular STA has nothing to transmit then the next token will be sent by the AP. This cycle of token passing is continued even if none of the STAs have any data to transmit.

3.3.4 CSP Example

So as to get a better understanding of the proposed CSP, an example is given in this section As shown in Figure 3-10. This example is for one channel with several STAs trying to access the channel. A maximum of four STAs are allowed per channel and there are no collisions. Each STA sends a CR to the AP after it has received a FCI or, Idle Token from the AP. Several STAs receive the free or, idle channel information but, due to p-persistence they fail to access the channel at the same time thus avoiding collision. For example in Figure 3-10; STA5 could never access the channel. Failure in access can cause extreme delay in data transmission. Each channel request receives an ACK from the AP together with the token number assigned to the STA. When the STA ends data transmission (for example STA1) it transmits a ND to the AP, this informs the AP to transmit the next token in sequence.



FCI:	Free Channel Information.
ACK:	Acknowledge for channel request together with assigned Token number.
TK:	Token.
CR:	Channel request.
ND:	No Data to transmit.
INIT:	Wakeup and Initialize.
p_persistence value:	Random value between 0 and 1 pre-assigned or, generated at wake up.
Random value:	Random value between 0 and 1 generated before transmitting CR.

Figure 3-10 Example of the proposed CSP.

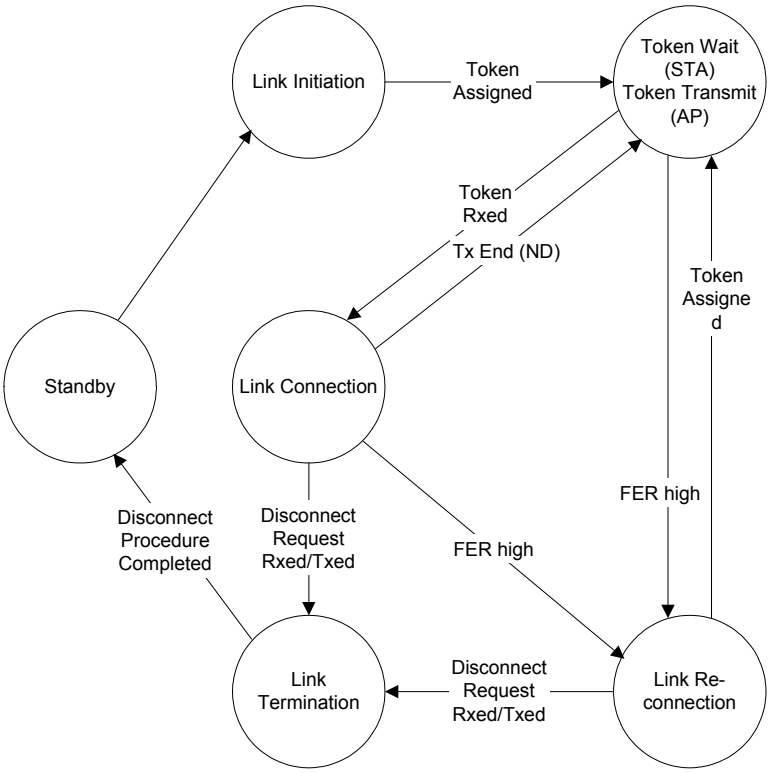


Figure 3-11 Channel Sharing Protocol phases.

3.3.5 Communication Phase

The protocol can be in 6 different phases as given in Figure 3-11. In the following the functioning of the protocol based on these phases is explained.

3.3.5.1 Standby Phase

The Standby Phase is the phase after an AP or, a STA is switched on or, re-started. The AP transmits a FCI or a Idle token in ever channel and waits for a CR from any STA. The phase of the AP is changed to Link Initiation Phase when the request frame is received successfully. A STA is only in reception mode in this phase. When a STA intends to start the communication, the phase of STA is changed to Link Initiation Phase.

3.3.5.2 Link Initiation Phase

The Link Initiation Phase is a procedure to start communication between a STA and an AP. A STA chooses a channel at random and waits for a FCI. The STA chooses a channel with the least number of users. If there are several channels with the same number of users then it chooses one of them at random. The STA then transmits a CR and the AP transmits an ACK which contains the assigned Token ID and MAC address of the STA. A p-persistence algorithm is followed before a CR is sent by the STA. After receiving the ACK, the STA goes to the Link Connection Phase. If the ACK from the AP does not contain a MAC address of the STA or the AP does not respond; the STA checks if the number of tokens in the channel is the maximum allowed per channel. If the channel already has the maximum number of tokens then the STA changes channel else it stays in the same channel for FCI or, Idle Token. When an Idle Token is received the STA follows the steps similar to that after receiving a FCI.

3.3.5.3 Token Wait/Transmission Phase

In this phase the AP transmits token and FCI cyclically in each channel. If the AP receives data from one of the STAs then it goes in the Link Connection phase. While STA waits for its token to be transmitted by AP. STA does not transmit anything without receiving it token. When STA receives token it goes to Link connection phase.

3.3.5.4 Link Connection Phase

In the Link Connection Phase the AP transmits the FCI periodically and tokens cyclically. The AP also transmits to and receives data from the communicating STAs. If a ND is received from a STA then the AP sends the next token. In case of no response from the STA; the AP transmits the token a few times then it makes the token free and transmits the next token. A STA waits for its token and transmits or receives data. When data transmission is completed the STA sends ND to the AP. If the STA does not receive the token when its turn comes then it waits for the token for a time out period after which it goes in the Link Re-Connection Phase. A STA can also go to the Link Re-Connection Phase if the frame error rate (FER) is higher than specified.

3.3.5.5 Link Re-Connection Phase

This phase is for Link Re-Connection of a suspended link. Link suspension occurs due to increase in FER in a channel or, when a STA changes channel due to failure in receiving response for channel request from the AP. The Link Re-Connection Phase is same as the Link Initiation Phase.

3.3.5.6 Link Termination Phase

In the Termination Phase the STA transmits a Disconnect frame to the AP and goes to the Standby Phase. The AP releases the token of the STA after receiving the Disconnect frame. If all STAs are disconnected, the AP goes to the Standby Phase.

3.3.6 Error State and Recovery

Any wireless system is prone to have some error state. In this section the error states and recovery from error states for the proposed CSP are discussed.

3.3.6.1 STA not Uniformly Distributed

First the term “uniform/not uniform distribution” must be defined: The wireless system has uniform distribution of STAs in all the channels if:

1. The same number of STAs are present in all the channels.

2. The number of STA in some of the channels is 1 less than in other channel, e.g., 2 STA in 10 channels and 1 STA or, 3 STA in 7 channels.

STAs must be uniformly distributed in all the channels for fair and optimum channel usage. This is achieved by giving information to the STAs of the number of STAs in each channel through the FCI but, a STA can access a channel after receiving an Idle Token also. Following are the two situations when the STAs might not be distributed uniformly:

1. If a STA accesses a channel after receiving an Idle Token; it is possible that the number of STAs in a few channels will be more than other channels.

2. It is possible that some of the STAs terminate the connection thus the distribution will not be uniform.

The first problem can be solved by Idle Token containing same information as FCI frame or, by AP requesting the new STA to another channel.

The second problem can also be solved by the AP requesting a STA to change channel. The steps to be followed by, the AP and a STA while requesting a change in channel and changing channel are given in detail in the following.

When an AP finds that the STAs are not uniformly distributed then it does the following:

1. Reserves a token in a channel with less number of STA.
2. If there are several channels with less STA then the AP chooses a channel randomly or, it checks the FER in each channel and chooses a channel with minimum FER.
3. After data transmission is finished for a STA with token in a channel with several STAs; the AP requests the STA (with token) to change channel and gives the token number and channel information.
4. The STA responds with an acknowledgment and changes channel.
5. If the STA does not respond due to interference or any other unforeseen reason the AP will request the next STA to change channel.

3.3.6.2 Interference & Shadowing

Interference and shadowing are two major problems for wireless systems. It is possible that interference is too high in a few channels at the same time it is possible that due to shadowing certain channels cannot be used. This section will discuss the two problems separately.

3.3.6.2.1 Interference

Interference is measured in terms of FER and signal level in a channel. It is possible that due to high interference a few channels cannot be used, this means several STAs cannot connect to the AP. This is an extremely severe problem.

This problem can be solved by the AP measuring the FER in all the channels. If the FER is higher than the FER_{max} and signal level is below the $Signal_{min}$ for a given time-out period then the following is done:

- Allowed number of tokens per channel is increased depending on the number of channels with high FER, this is to maintain the capacity although the delay will increase. In case the number of channels with high FER is above a limit for a given time out period, the network operator or person in charge will receive a warning.
- The FCI contains crowded information for channels with interference.
- The AP keeps on checking the channels with interference; if the FER decreases and the signal level improves for a pre-defined period then the channels are set to be idle. The system then goes back to uniform distribution of STAs as explained before in Section 3.3.6.1.
- If there are STAs in a channel with high interference then the STAs must also time-out and change channel. The measurement and decision of a STA changing channel is also based on FER and signal level.

3.3.6.2.2 Shadowing

Shadowing occurs when something comes in between the sender and the receiver disturbing the communication path. Thus, this is a situation when there is no Line-of-Sight (LOS). In such cases few STAs cannot connect to the AP.

The solution is, if there is no LOS between the AP and a STA then the STA will receive no signal or it will receive a signal with high FER; thus the STA will time-out and try to connect to some other channel. The AP will transmit the token of such STA for a given number of times. If even then the STA does not reply, then the AP will make the token free.

3.4 Numerical Throughput Analysis

In this section a numerical throughput analysis of the proposed CSP is presented [6 – 9]. A simulation of the protocol was also done to study the performance. The simulation model and results are presented in Section 3.5. Due to the difference in the assumptions the results of the numerical analysis and the simulation are different.

3.4.1 Assumptions

So as to simplify numerical calculation several assumptions were made. These assumptions are listed below:

- It was considered that there was no error in transmission.
- The time taken by token, ND, FCI, DC, CR and ACK were not considered.
- The channel selection process to get equal load in each channel is not considered.
- STAs are considered to be always available, i.e., the STA arrival process is not considered.
- DC is not considered, i.e., the process of STAs disconnecting or leaving is not considered.
- The idle time calculation is just done for the situation where there is not data to transmit but idle time due to the channel access delay is not considered.

3.4.2 Numerical Model

The throughput for the proposed CSP can be written as [1,6,7,9,12],

$$S = \frac{U}{B + I} \tag{1}$$

where S is the channel throughput, U is the expected utilized time, B is the expected busy time and I is the expected idle time.

The expected utilized time is the time during which the channel is successfully utilized. As no error or interference is considered in this analysis, data transmission is always successful. Thus, the probability that a channel is utilized is the probability that a STA receives the token and has data to transmit. The probability that a STA receives the token is [7]:

$$P_{\text{token received}} = \frac{1}{E(\text{number of users})} \tag{2}$$

The probability that i STAs are in a channel is:

$$P(i) = C_i^n \left(\frac{(1-p_p)}{NM} \right)^i \left(1 - \frac{(1-p_p)}{NM} \right)^{n-i} \tag{3}$$

where, N is the total number of STAs, M is the number of channels, n is the number of STAs allowed per channel, p_p is the p-persistence value (between 0 and 1) given to each STA and C_y^x represents the combination, i.e., $C_y^x = x!/y!(x-y)!$.

Thus, the expected number of STAs is [7]:

$$E_{STA} = \sum_{j=1}^{n} jP(j) \tag{4}$$

IP packets arrive according to a Poisson process thus, the probability that an IP packet arrives to a user is [1,7,12],

$$P_{\text{IP}} = gT \exp(-gT) \tag{5}$$

where, T is the time slot and g is the arrival rate in terms of the number of IP packets. Thus, the probability that k channels are utilized is [7],

$$\tilde{U} = C_k^M \left(\frac{G\exp(-G)}{1+E_{STA}} \right)^k \left(1 - \left(\frac{G\exp(-G)}{1+E_{STA}} \right) \right)^{M-k} \tag{6}$$

where, G = gT is the load.

Thus the expected number of utilized channels is [7],

$$\text{U} = \sum_{\text{k}=1}^{\text{M}} \text{k}\,\tilde{U} \tag{7}$$

Similarly the expected number of busy channels is the sum of the expected number of utilized channels and the expected number of channels with collision. The probability that there is collision in a channel is the probability that two or, more STAs choose the same channel and get a random value greater than p_p. Thus the probability of collision, P_C, is one minus the probability that no STA chooses the channel minus the probability that one STA chooses the channel and gets a p-persistence random value greater than p_p [7],

$$P_C = 1 - \left(1 - \frac{1-p_p}{NM} \right)^N - \frac{1-p_p}{NM} \left(1 - \frac{1-p_p}{NM} \right)^{N-1} \tag{8}$$

Thus the probability that there is collision in k channels is [7],

$$\tilde{C} = \text{C}_\text{k}^\text{M} P_C{}^k (1-P_C)^{M-k} \tag{9}$$

Knowing that the probability that k channels have a collision, the expected number of channels with collision, C, can be written as [7],

$$C = \sum_{i=1}^{M} i\,\tilde{C} \tag{10}$$

Thus the expected number of busy channels is [7],

$$B = U + C \tag{11}$$

The next step is to calculate the expected number of idle channels in the time slot T. A channel is idle when a token arrives to a STA and the STA has no data to transmit. As the data arrival is assumed to be a Poisson process, the probability that no data arrives can be given as [1,7,12],

$$P_{\text{no data arrives}} = \exp(-G) \tag{12}$$

Using Equation (4), the probability that all channels are idle can be given as [7],

$$P_{\text{channel idle}} = \left(\frac{\exp(-G)}{1 + E(\text{number of users})} \right) \tag{13}$$

Therefore the probability that k channels are idle can be given as [7],

$$\tilde{I} = C_k^M P_{\text{channel idle}}^k P_{\text{channel idle}}^{\text{M-k}} \tag{14}$$

Thus the expected value can be given as [7],

$$I = \sum_{k=1}^{M} i \tilde{I} \tag{15}$$

The throughput is 0 if all channels are idle and, if the channels are not idle, then the throughput is the ratio of the number of utilized channels and the number of busy channels. Thus the throughput for the proposed CSP can be written as [7],

$$S = \begin{cases} \dfrac{U}{B} & \text{I} < \text{M} \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

Substituting Equations (7), (11) and (15) in Equation (16) yields [7],

$$S = \begin{cases} \dfrac{\sum_{k=1}^{M} i C_k^M (\tilde{U})^k (1-\tilde{U})^{M-k}}{\sum_{k=1}^{M} i C_k^M (\tilde{U})^k (1-\tilde{U})^{M-k} + \sum_{k=1}^{M} i C_k^M (\tilde{C})^k (1-\tilde{C})^{M-k}} & \lceil \text{I} \rceil < \text{M} \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

3.4.3 Numerical Results

This section presents the numerical results of the proposed CSP. All the results are generated for T = 10 ms which was specified for WNIC. The WNIC product was specified to match the Integrated Services Digital Network (ISDN) data rate of 64kbps per user. This data rate was considered enough for the standard text e-mail download and Internet browsing. With 75 bytes of data (optimum fragment size for ARQ, see Chapter 2) in Layer-2 at 10ms a pure-data rate of 60kbps is achieved.

To reduce collisions a p-persistence algorithm is used by the proposed CSP. Thus the considered value of p_p is a very important factor. If p_p is small then the probability of accessing the channel increases which in turn increases the probability of collision and thus also the delay in transmission while if p_p is large the delay in accessing the channel increases but the collision probability decreases. Thus choosing an appropriate value of p_p is important for a proper functioning of the proposed CSP.

In Figure 3-12 the throughput results for a varying value of p_p are given. These results clearly show that a better performance for a higher value of p_p because as the value of p_p is increased the number of collisions decreases. Another reason for this result is that the idle time due to the channel access delay is not considered in the numerical analysis. Obviously from this result a p_p of 0.9 seems to be the best value but keeping in mind that the effect of the channel access delay, the rest of the results are generated for $p_p = 0.8$. Of course $p_p = 0.8$ might not be the optimum value when the channel access delay is considered but STAs with a p_p of 0.8 should have a relatively smaller delay in accessing the channel than the STAs with a p_p of 0.9. Thus for this calculation it is considered to be a close to optimum value.

In Figure 3-13 the throughput performance comparison of the proposed CSP is given with the CSMA/CA [4]. The CSMA/CA results are for N = 10 (total number of STA) and Contention Window = 0.4*Pkt_Time, where Pkt_Time = 20. The results clearly show that the larger the number of channels in the proposed CSP, the better the performance compared to CSMA/CA.

It should be noted that the throughput shown for the proposed CSP in Figure 3-13 is the aggregate throughput of all the available channels. For a small number of channels and less load the throughput of the proposed CSP is almost zero while the throughput increases sharply as the load increases for any number of channels. The reason for this behaviour of the proposed CSP is due to the use and rotation of tokens amongst the STAs in a channel. At low load the probability that a STA with a token has data to transmit is very low and thus the throughput of the system is low. As the load increases the number of STAs with data to transmit increases and thus the overall throughput increases, while as the number of channels increases the probability that STAs with a token and data to transmit increases and thus causes an earlier rise in the throughput.

Figure 3-13 also shows that the proposed CSP throughput becomes quasi constant for a larger number of channels after a sharp rise and even decreases for fewer channels. Further the maximum achievable throughput is higher for a higher number of channels. The throughput maximum is reached due to the number of collisions which increases with an increase in load; this is also the reason of the decrease in throughput for higher load. As the number of channels increases the overall probability that STAs access the channel increases thus a higher throughput is achieved for a larger number of channels.

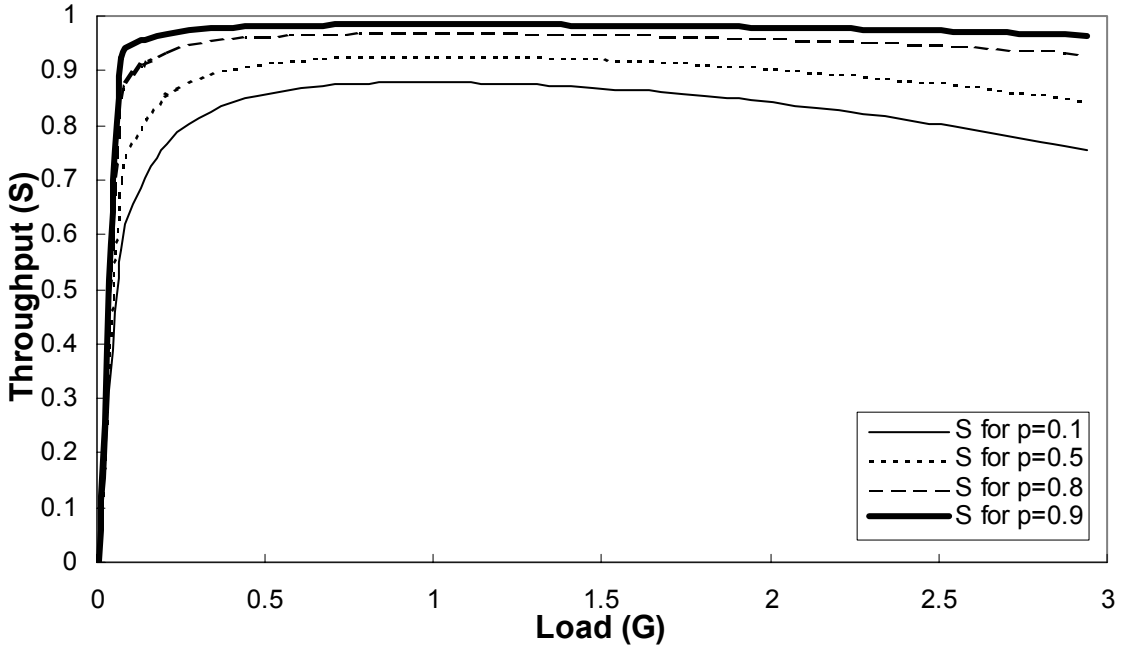


Figure 3-12 Throughput against load for the CSP with 17 channels, 68 STA and 4 STA per channel.

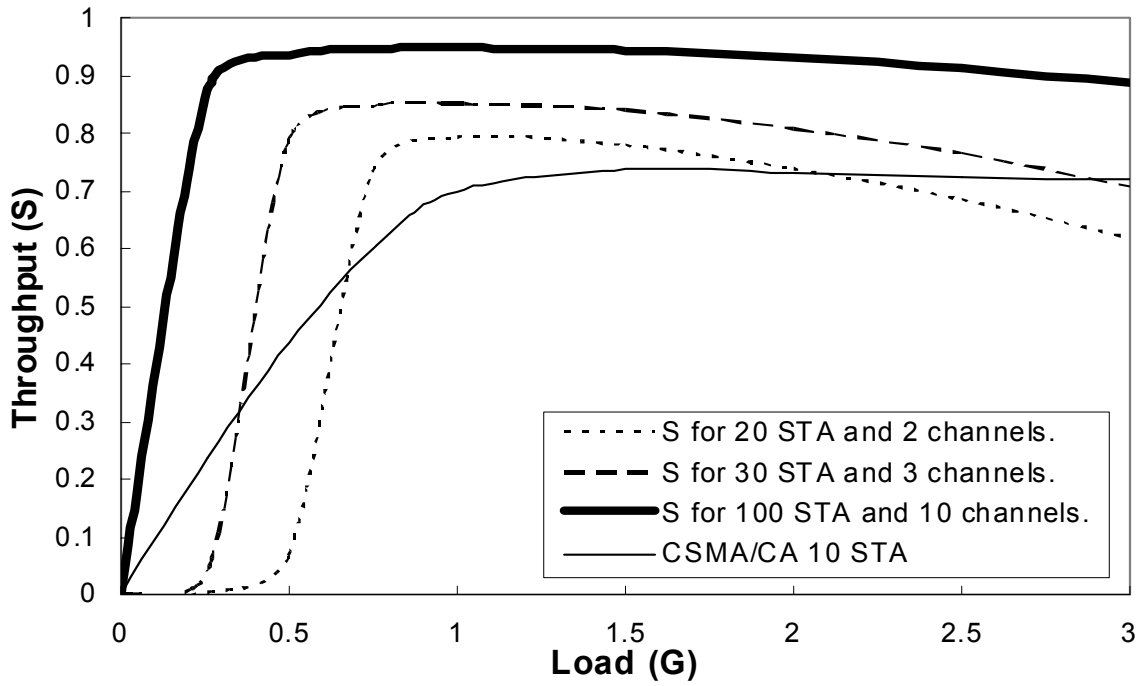


Figure 3-13 Throughput against load comparison of the CSP with CSMA/CA.

For CSMA/CA there is one channel with no token which means that all STAs try to access the same channel if and when they have data to transmit. Thus the throughput of CSMA/CA increases gradually. The throughput of CSMA/CA becomes constant after reaching a maximum because the back-off and the contention window mechanisms provide a maximum limit for collisions which stays constant even if the load increases.

Figure 3-14 presents results for a varying number of STAs per channel. The result shows that there is no effect on the performance of the proposed CSP with the number of STAs per channel. In a given channel only one STA gets the token and the probability of getting the token at the same time as having data to transmit for STAs in 17 channels does not differ much which gives this result.

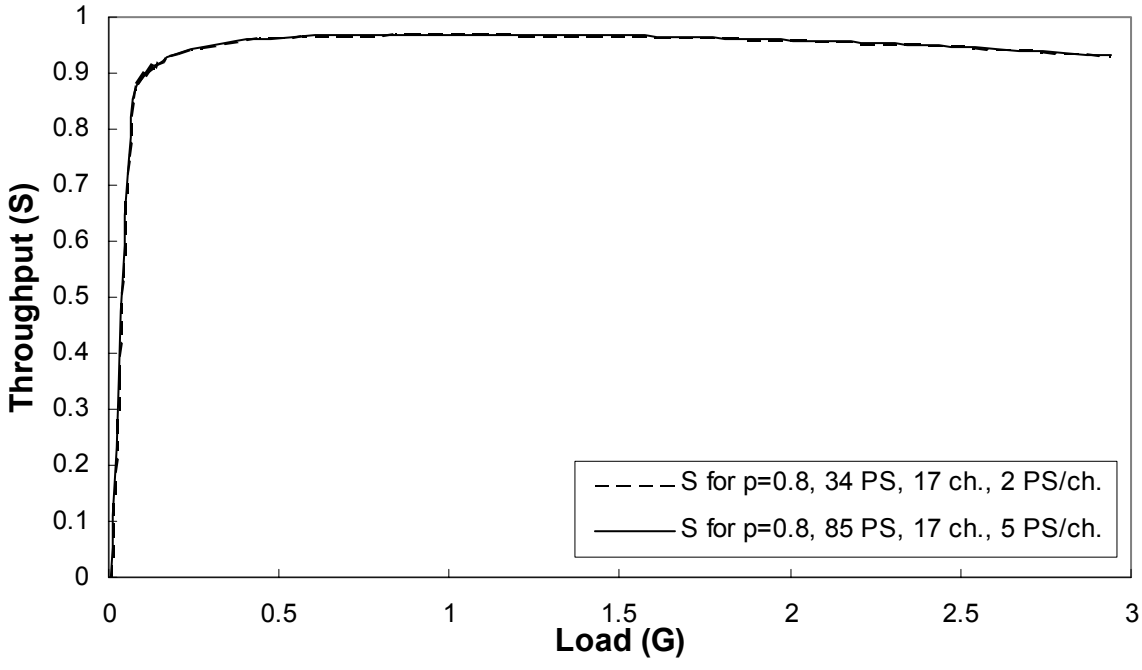


Figure 3-14 Throughput against load for 17 channels with varying number of STA per channel.

Table 3-1 Simulation Parameters.

FCI	1 per second
Token	1 per 10ms
Fragment size	75 bytes
Time-Slot (T)	10ms
Data arrival	Poisson distributed
Tokens per channel	6
Load (G)	1
P-persistence value (p_p)	0.5

3.5 Simulation Analysis

In this section a performance analysis of the proposed CSP is done by simulating the protocol. All procedures of the protocol were implemented. In all the simulation results the dot represents simulation point while the line connecting them was drawn using 'Linear' MS Excel trendline function which uses linear equation except for Figure 3-21 where 'Polynomial' MS Excel trendline function of second order was used. Linear of Polynomial MS Excel trendline function was chosen because they gave the best fit.

3.5.1 Simulation Model

The proposed CSP has three parameters which must be optimised before it can be used, these are [6]: (1) The number of channels, (2) The number of tokens and (3) The p-persistence value. Once these values were found the performance of the proposed CSP was compared with CSMA/CA. The performance was compared in terms of the throughput and the normalized load.

The simulation parameters as given in Table 3-1 were used unless otherwise specified.

The throughput (S) of the system is defined as [1,6-9,12],

$$S = \frac{U}{\text{Total run time}} \tag{1}$$

where, U is the utilized time, the time during which the channel was used for successful data transmission, i.e., there was no error or collision.

The FCI transmission of 1 per second is a reasonable value because it is used for channel access in addition to the Idle Token which is transmitted more frequently.

A 10ms token time was taken because WNIC (proprietary WLAN) was specified to provide 64kbps which was considered enough for e-mail download and web browsing. With 75 bytes of data (ARQ optimum fragment size see Chapter 2) in Layer-2 at 10ms a pure-data rate of 60kbps is achieved.

It was assumed that in every time slot (10ms) one IP packet arrived in Layer-2, this is understandable because Layer-2 will process only 1 higher layer packet at a time. Thus the considered value of load (G) = 1. This means there is one packet to transmit in every channel in every time slot. Now based on Equation (5) and definition of G as G=gT, the IP packet arrival rate (g) for G=1 is 100 per second (g=G/T).

Further, it was assumed that the stations were either sending or receiving e-mail. An average text only e-mail is 3000 bytes long. Now assuming that IP packet size is uniformly distributed between 48 and 1500 bytes, for a STA the simulation took the randomly generated IP packet size as the average IP packet size for the whole e-mail transmission. Thus the number of IP packets to be transmitted for a STA was the e-mail size divided by the average IP packet size and the arrival rate of these IP packets was Poisson distributed.

Each IP packet was divided in equal size fragment of 75 bytes.

STAs were assumed to be awake all the time. After all the IP packets were transmitted for or by a STA and there were no further IP packets to transmit then the STA left the channel and the token was made available.

The simulation was run for 1 hour which corresponds to 360,000 cycles or time-slot period.

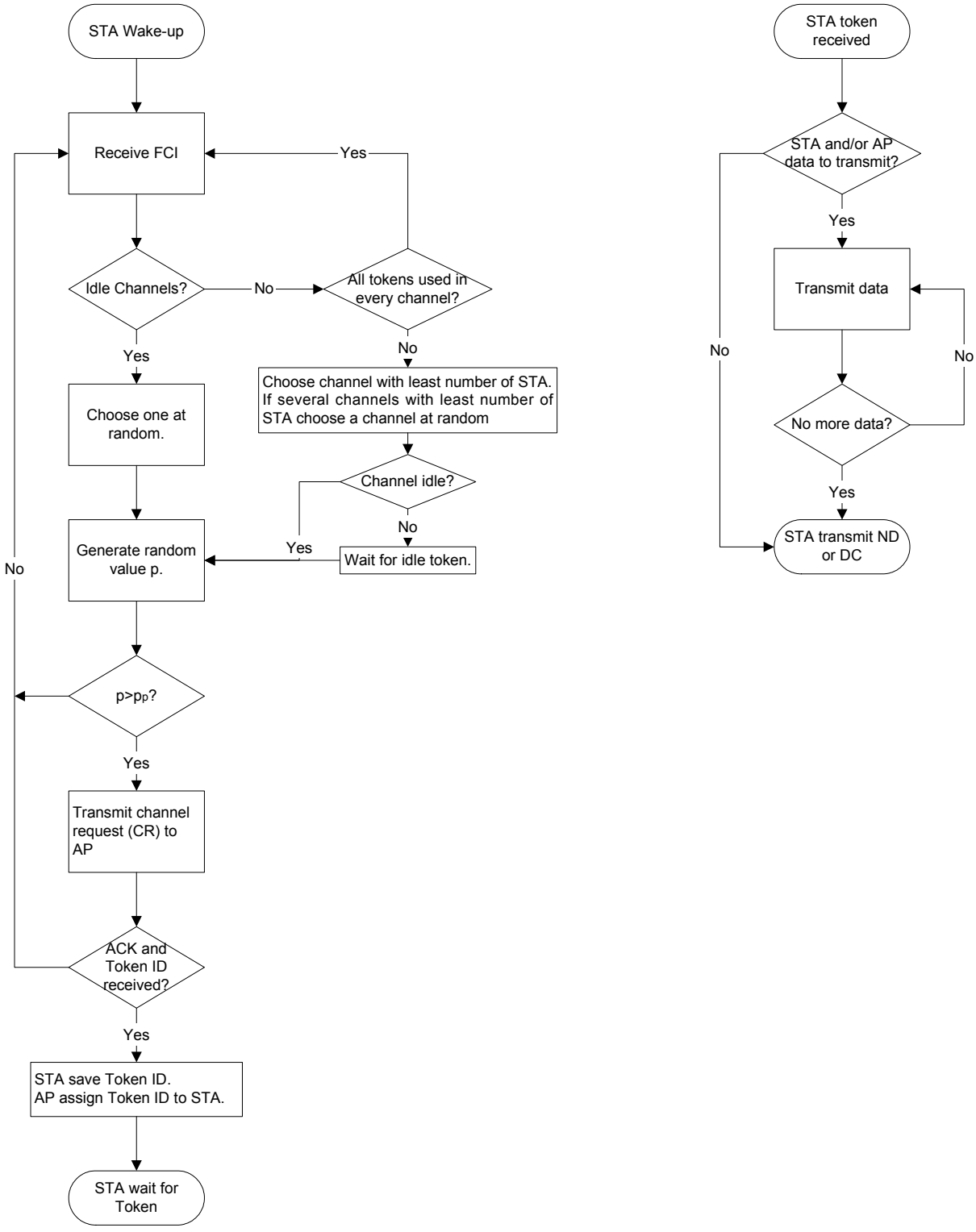


Figure 3-15 Simulation flow chart for STA.

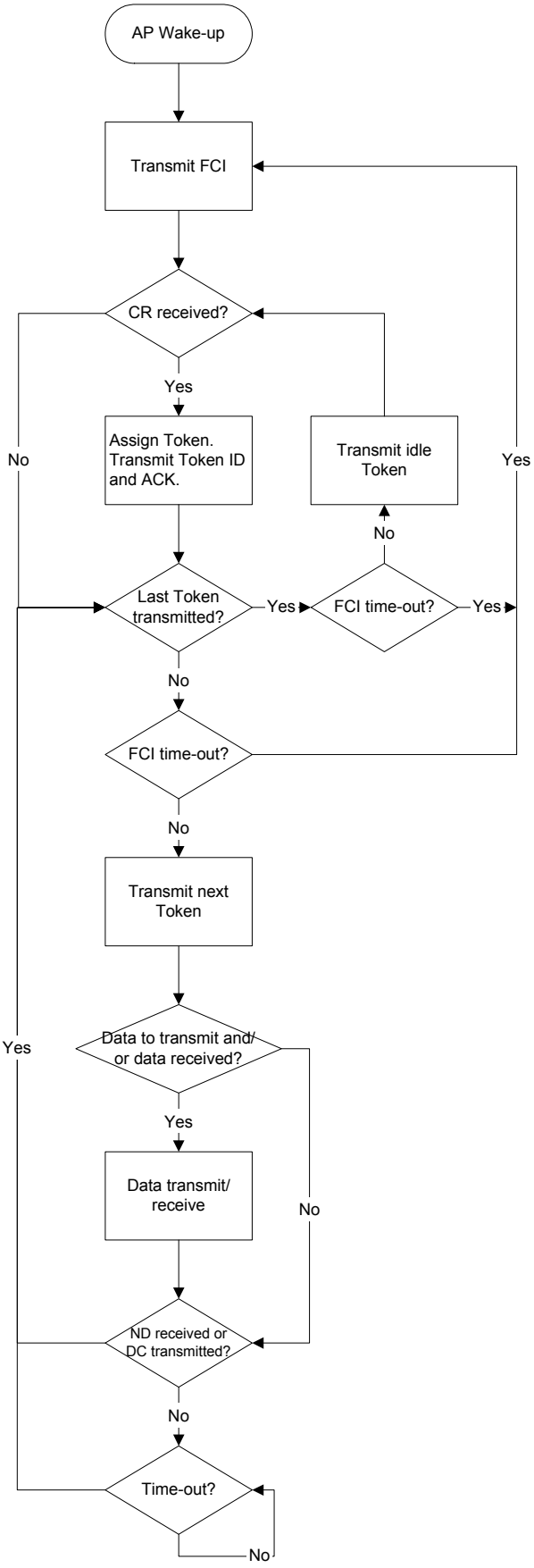


Figure 3-16 Simulation flow chart for AP.

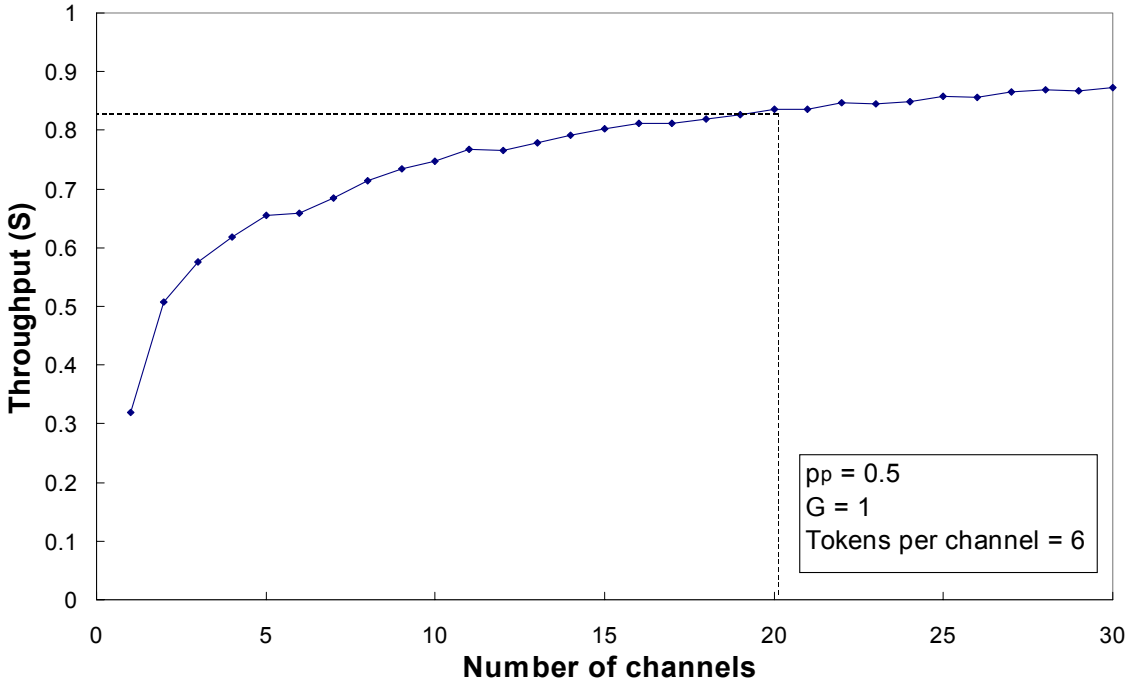


Figure 3-17 Throughput against number of channels.

Figure 3-15 and Figure 3-16 show the flow chart used for the simulation of the proposed CSP. This is the same as the explanation of the proposed CSP in Section 3.3. The part to be noted is data transmission. As explained above, the data was an e-mail of 3000 bytes divided in IP packets of equal size. IP packets were generated according to a Poisson process. Each IP packet was fragmented in equal size fragments of 75 bytes. The STA kept its token until all IP packets were transmitted, i.e., the complete e-mail. After completion of the transmission, if there were no more packets to transmit, the STA left the channel and the token was made available.

3.5.2 Simulation Results

Although there were 17 channels for WNIC, the optimum number of channels for the proposed CSP was studied. The optimum number of channels can be found in terms of the throughput (S) and the channel access delay. In Figure 3-17 simulation results for the number of channels against the throughput is given. Each dot in the figure gives the simulation point while the line joining the two consecutive dots was made by the using 'Linear' MS Excel trendline function which uses linear equation. The figure shows that a pseudo constant throughput is achieved for 20 channels onwards. A similar curve was found for other values of p_p; this happens because p_p basically affects the number of collisions and the channel access delay which can be considered relatively constant for any number of channels. Thus p_p will only affect the overall throughput but not the shape of the curve. Similarly changing the load for a given p_p will have a fixed effect on the channel idle time and will not affect the shape of the curve. Similarly changing the number of tokens per channel (i.e., the number of STAs per channel) will only affect the overall throughput but not the shape of the curve.

In Figure 3-18 the channel access delay is given for a varying number of channels. As expected the channel access delay increases with the increase in the number of channels because with an increase in number of channels the number of tokens per channel increases and thus the increase in the total number of users. For 20 channels, on average, a channel access delay of about 0.3 seconds will be faced by each STA. 0.3 seconds was not considered long for Internet browsing and e-mail download.

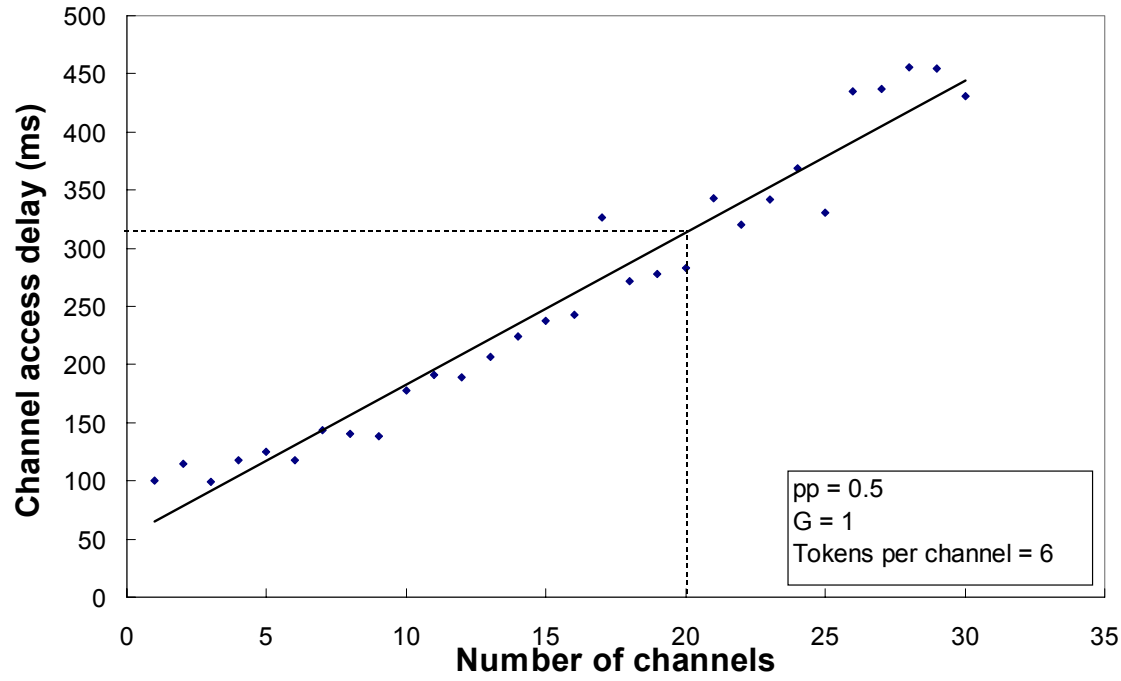


Figure 3-18 Channel access delay in terms of number of channels.

The next step is to find the optimum number of tokens per channel; this result is given in Figure 3-19. The result shows that the throughput of the system rises until 3 tokens per channel and decreases from 6 tokens per channel. Thus 6 tokens per channel is the optimum value. Once again the result is given for $p_p = 0.5$ similar results were found for other values of p_p the reason being that p_p basically affects the number of collisions and the channel access delay which can be considered relatively constant for any number of channels. Thus p_p will only affect the overall throughput but not the shape of the curve.

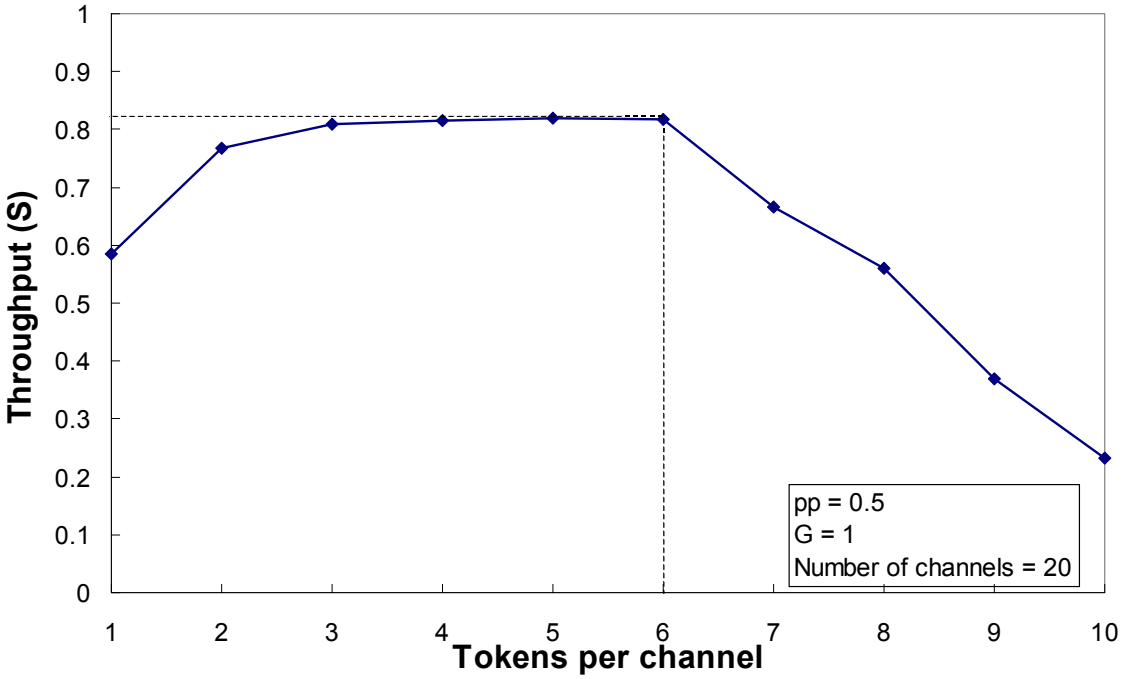


Figure 3-19 Throughput for varying number of tokens per channel.

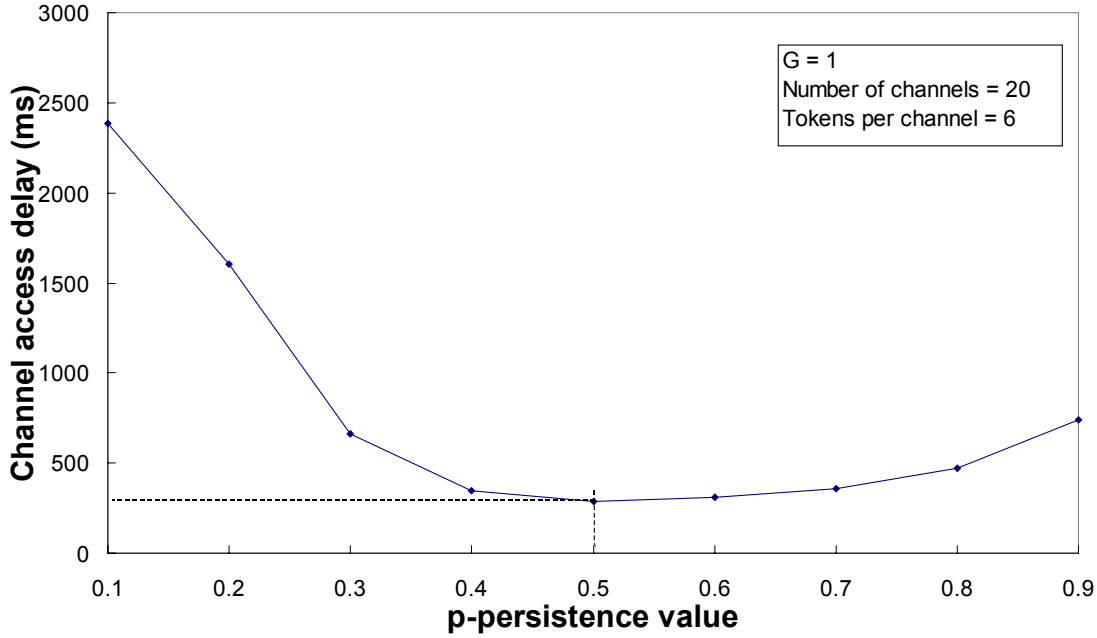


Figure 3-20 Channel access delay against p-persistence value.

Knowing the optimum number of channels and the optimum number of tokens the p-persistence, p_p, value is obtained. This is simulated for the channel access delay as shown in Figure 3-20. The optimum p_p value is 0.5. The shape of the curve is understandable; for a smaller value of p_p there are more collisions while for larger value of p_p there is less collision but the p-persistence mechanism does not allow access to the channel so often.

Now the proposed CSP is optimized, the number of channels should be 20, the tokens 6 and p_p is 0.5. The point now is to check the effect of the Frame Error Rate (FER). The result for normalized transmission time, for a given IP packet size, and FER is shown in Figure 3-21. There is a sharp increase in delay from FER of 0.1 onwards. This curve is not affected by the IP packet size because IP packet size only gives the number of fragments to transmit and will only determine the minimum normalized transmission time.

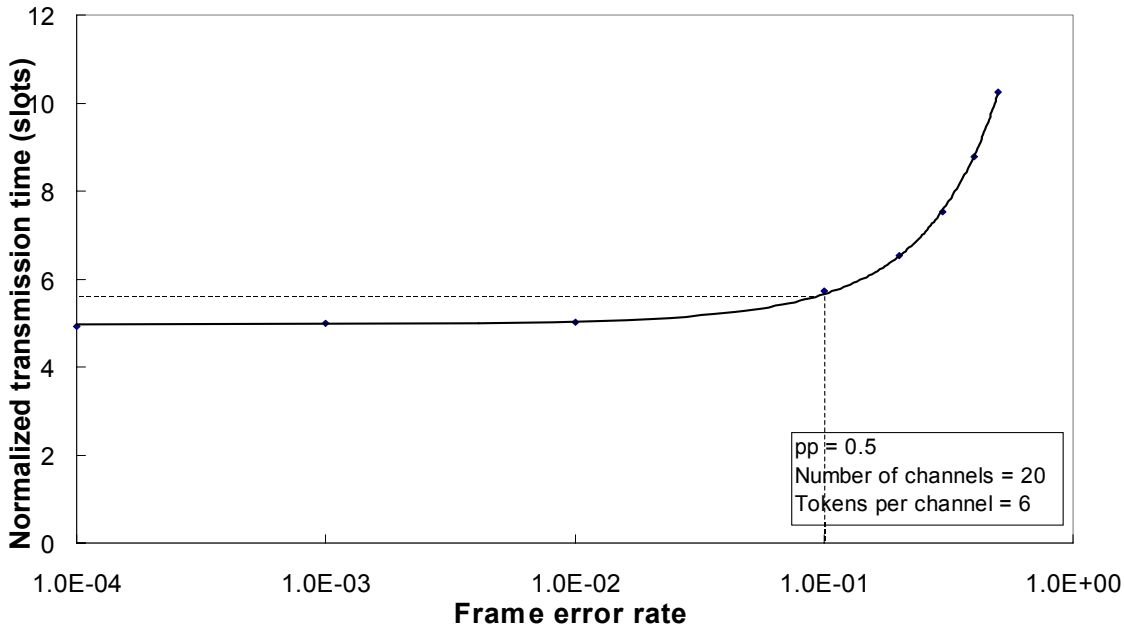


Figure 3-21 Normalized transmission time and frame error rate.

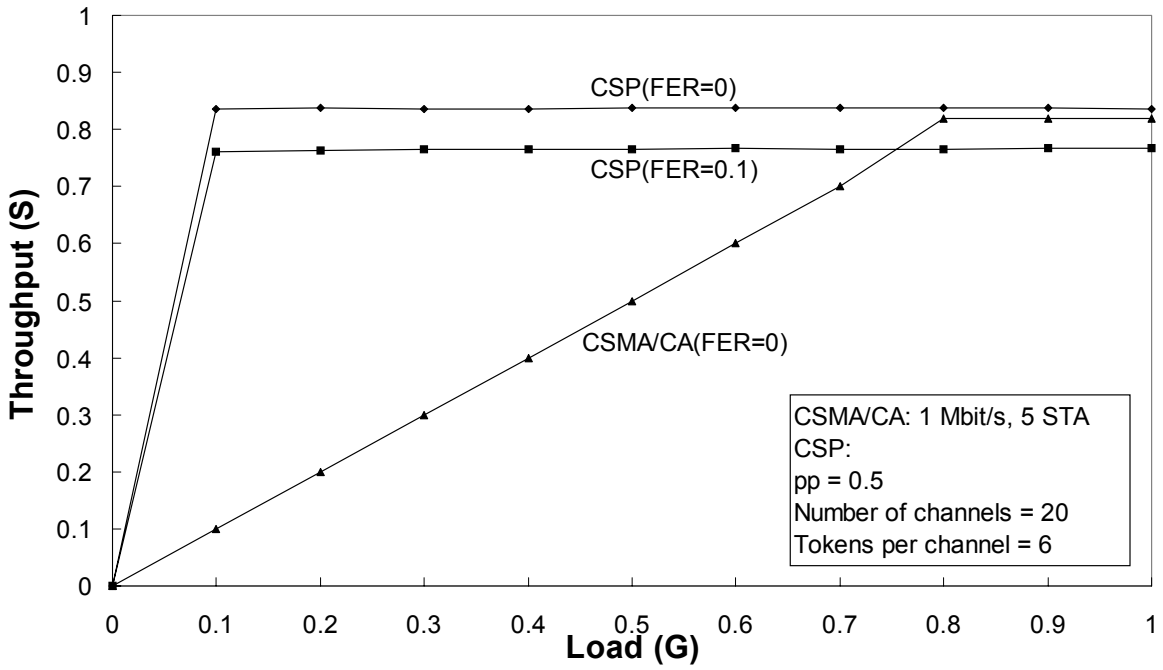


Figure 3-22 Throughput against load for varying FER compared with CSMA/CA.

The performance of the proposed CSP can now be compared with that of CSMA/CA. The result is given in Figure 3-22 for varying G and FER = 0 and 0.1 for the proposed CSP. As the load, G, was varied the arrival rate for a Poisson distribution also changed, g=G/T. It is clear from the figure that the proposed CSP outperforms the CSMA/CA even for a FER = 0.1 until load of 0.7. CSMA/CA shows a constant throughput from a load, G, of 0.8; the throughput gain by the proposed CSP (for FER = 0) from this load onwards is 0.2 as compared with CSMA/CA. The sharp increase in throughput in the proposed CSP, as explained in the numerical results discussion, is due to the probability that the stations (6 per channel) in each channel (20 channels) have data to transmit is high. In case of CSMA/CA, unlike the proposed CSP, only one station can access the channel at a time which results in lower throughput.

3.6 Conclusions

In this section conclusions are drawn from the numerical and the simulation study of the novel Channel Sharing Protocol (CSP) proposed in this chapter.

3.6.1 Numerical

The main purpose of the proposed CSP is Internet data transmission for a point to point communication system. The performance of the proposed CSP is measured in terms of throughput and load.

Numerical results show that the proposed CSP gives a quasi constant throughput, as high as 0.9, for high values of p-persistence (p_p = 0.8, 0.9) with varying load. The proposed CSP outperforms CSMA/CA if the number of channels is three or, more. The performance of the proposed CSP is better for a larger number of channels. There is no effect on the performance of the proposed CSP with the number of STAs in a channel.

The proposed scheme thus makes efficient use of the spectrum.

3.6.2 Simulation

The proposed CSP is first optimized and then the scheme is evaluated in terms of the throughput and the load. The result is also compared to that of the CSMA/CA.

Simulation results show that the proposed protocol gives quasi-constant throughput from 20 channels onwards while the channel access delay increases with an increase in the number of channels. Thus 20 channels is taken as the optimum number of channels for the proposed CSP because of the high throughput achieved and the channel access delay of 0.3ms which is acceptable for the services considered (e-mail, web browsing etc.). Next the optimum number of tokens was found. This was done by simulating the number of tokens against the throughput. It is clear from the results that 6 is the optimum number of tokens. The proposed CSP gives an optimum result for p-persistence value of 0.5.

The performance of the proposed CSP was then measured in terms of throughput and frame error rate. Results show that a quasi-constant throughput is achieved until a frame error rate of 0.1. The proposed CSP outperforms the CSMA/CA even for a frame error rate of 0.1.

The proposed scheme thus, makes efficient use of the spectrum and can be used for optimum IP packet transmission. Although not studied in this thesis, the proposed CSP can also be used to give priority to users in the wireless medium by changing the users' p-persistence values. Smaller p-persistence value (high priority) will give a higher probability to access the channel while a higher value (low priority) will give a lower probability to access the channel Of course for each p-persistence value the optimum number of users must be found, else too many users in low p-persistence value will cause a high collision rate and thus a decrease in performance.

References

[1] H.R. van As, "Media Access Techniques: The Evolution towards terabit/s LANs and MANs", Computer Networks and ISDN Systems, Vol. 26, Issue 6-8, pp. 603-656, 1994.

[2] W. Diepstraten, G. Ennis and P. Belanger, "Distributed Foundation Wireless Medium Access Control", IEEE P802.11-93/190.

[3] ISO/IEC 8802-11, ANSI/IEEE Std 802.11, First Edition 1999-00-00, 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.

[4] R. White, M. Demange, K. Doss, F. Vook, "A complete Description of Frame Prioritization in a CSMA/CA MAC Protocol", IEEE P802.11-93/208.

[5] T.S. Ho and K.C. Chen, "Performance Analysis of IEEE 802.11 CSMA/CA Medium Access Control Protocol", PIMRC'96, Taipei, Taiwan, pp. 407-410, October 15-18.

[6] K. Ogata, A.R. Prasad and K. Seki, "Performance Analysis of a Novel Channel Sharing Protocol for Wireless communication", IEICE General Conference in September 1998.

[7] A.R. Prasad and K. Seki, "Capacity Enhancement of Indoor Wireless Communication System with a Novel Channel Sharing Protocol", ICPWC'97, Mumbai, India, pp. 162-166, 16-19 December 1997.

[8] A.R. Prasad, and K. Seki, "Novel Channel Sharing Protocol for Indoor Wireless Communication", IEICE General Conference, Tokai University, Hiratsuka, Japan, B-5-306, 27-30 March 1998.

[9] N. Matsuoka, A.R. Prasad and K. Seki, "Performance Analysis of a Novel Channel Sharing Protocol for Indoor Wireless Communication", IEICE General Conference, Tokai University, Hiratsuka, Japan, B-5-307, 27-30 March 1998.

[10] A.R. Prasad, A. Kamerman and H. Moelard, "IEEE 802.11 Standard", Chapter 3 of WLAN

Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[11] A. Chandra, V. Gummalla and J.O. Limb, “Wireless Medium Access Control Protocols”, IEEE Communications Surveys, http://www.comsoc.org/pubs/surveys, Second Quarter 2000.

[12] R. Rom and M. Sidi, *Multiple Access Protocols Performance and Analysis*, Spinger-Verlag New York Inc., 1990.

[13] N.R. Prasad et al, "A state-of-the-art of HIPERLAN/2", VTC 1999 Fall, Amsterdam, The Netherlands, pp 2661-2666, 19-22 September 1999.

[14] N.R. Prasad and A.R. Prasad, “Wireless Networking and Internet Standards”, Chapter 2 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

Chapter 4

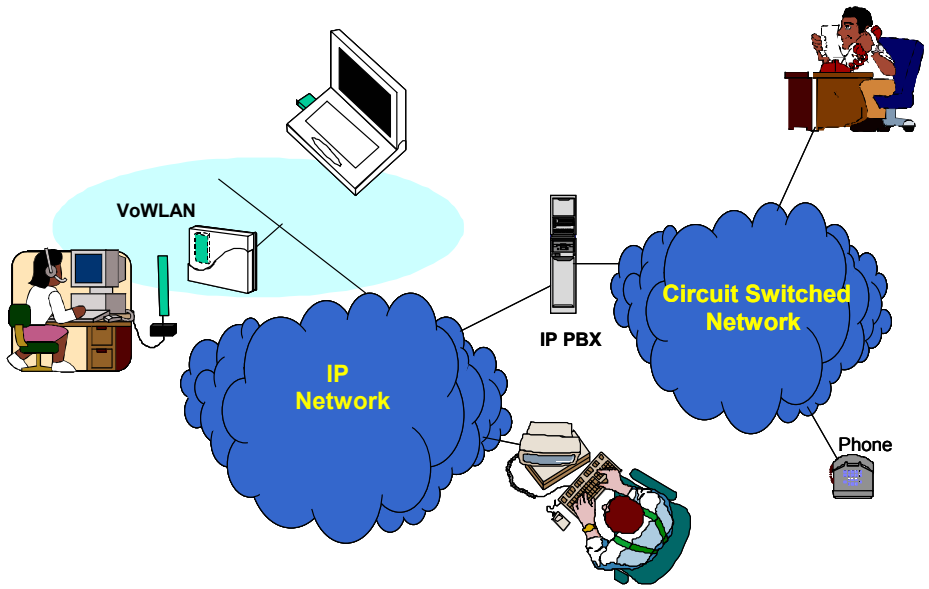
QoS over Wireless LANs

Quality of Service (QoS) is becoming an increasingly important element of any communications system. In the simplest sense, QoS means providing a consistent, predictable data delivery service, in other words, satisfying the customer application requirements. Providing QoS means providing real-time (e.g., voice) as well as non-real time services. Voice communication is the primary form of service required by the mankind. So the focus of this chapter will be on voice.

Support for voice communications using the Internet Protocol (IP), which is usually just called "Voice over IP" or VoIP, has become especially attractive given the low-cost, flat rate pricing of the public Internet. VoIP can be defined as the ability to make telephone calls (i.e., to do everything that can be done today with the Public Switched Telecommunications/Telephone Network, PSTN) over the IP-based data networks with a suitable QoS. This is desirable because of much superior cost/benefit compared to the PSTN. Equipment producers see VoIP as a new opportunity to innovate and compete. The challenge for them is turning this vision into reality by quickly developing new VoIP-enabled equipments that are capable of providing toll quality service. For Internet Service Providers (ISPs) the possibility of introducing usage-based pricing and increasing their traffic volumes is very attractive. Both the ISPs and the network manufacturers face the challenge of developing and producing solutions that can provide the required voice quality. Users are seeking new types of integrated voice/data applications as well as cost benefits.

As Wireless Local Area Networks (WLANs) are extension of the IP to the wireless, it is necessary to have a Voice over WLAN (VoWLAN) protocol which fulfils the requirement. A complete system for voice over WLAN, IP to POTS is depicted in Figure 4-1. Successfully delivering VoWLAN presents a tremendous opportunity; however, implementing the products is not as straightforward a task as it may first appear. Keeping the above in mind VoWLAN solutions are studied in this chapter. The work presented in this chapter was done for IEEE 802.11 MAC enhancements standard (IEEE 802.11e is currently in draft stage) which has the goal to enhance the IEEE 802.11 MAC by adding QoS possibilities. At the time of study four possible VoWLAN schemes existed, these were the Distributed Coordination Function (DCF) [1,2,5,6], the Point Coordination Function (PCF) [1,2,5], Priority Queuing and Balckburst scheme [3]. The best solution for QoS on 802.11 found in this chapter has been accepted by IEEE 802.11e as one of the solutions.

This chapter starts with requirements for VoWLAN as voice is the most important service. After that the four schemes that can be used for QoS in IEEE 802.11 are explained. Qualitative analyses of the four possible QoS solutions are done and a comparison is presented in this chapter. The current IEEE 802.11e draft is also explained briefly. A short section describing QoS issues for future studies is also given and finally the chapter is concluded.



VoWLAN: Voice over Wireless Local Area Network
IP: Internet Protocol
PBX: Private Branch eXchange

Figure 4-1 Voice over WLAN, IP to POTS (Plain Old Telephone Systems).

4.1 Voice Communication Requirement

Voice is a real time communication that means it has severe delay constraints [4,5,6]. Dedicated systems for voice do not face any problem considering delay but in a system made for asynchronous data transmission it will become a big issue. In the following sub-sections the challenges that will be faced while VoWLAN product development and the requirements of voice transmission are given.

4.1.1 Voice over Wireless Challenges

The goal is relatively simple: add telephone calling capabilities (both voice transfer and signalling) to WLANs with backbone IP-based networks and interconnect these to the public telephone network and to the private voice networks in such a way as to maintain current voice quality standards and preserve the features everyone expects from the telephone. The challenges for the product developer arise in five specific areas:

1. Voice quality should be comparable to what is available using the PSTN, even over networks having variable levels of QoS.
2. The underlying network must meet strict performance criteria including minimizing call refusals, network latency, packet loss, and disconnects. This is required even during congestion conditions or when multiple users must share the network resources.
3. Call control (signalling) must make the telephone calling process transparent so that the callers need not know what technology is actually implementing the service.
4. PSTN/VoIP/VoWLAN service interworking (and equipment interoperability) involves gateways between the voice and the wireline data network environments and the wireline and the wireless data networks.
5. System management, security, addressing (directories, dial plans) and accounting must be provided, preferably consolidated with the PSTN Operation Support Systems (OSSs).

4.1.2 Voice Quality and Characteristics

Providing a level of quality that at least equals that of the PSTN (this is usually referred to as "toll quality voice") is viewed as a basic requirement. It has been found that there are three factors that can profoundly impact the quality of the service [4,5,11]:

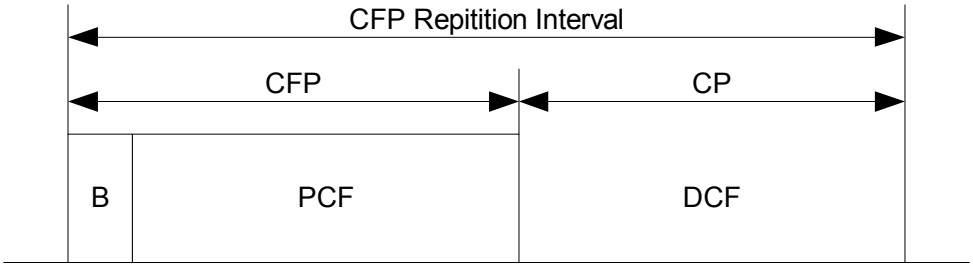
1. Delay: Talker overlap (the problem of one caller stepping on the other talker's voice) becomes significant if the one-way delay becomes greater than 250 milliseconds. The end-to-end delay budget is therefore the major constraint and driving requirement for reducing the delay through a packet network.
2. Jitter (Delay Variability): Jitter is the variation in inter-packet arrival time as introduced by the variable transmission delay over the network. Removing the jitter requires collecting packets and holding them long enough to allow the slowest packets to arrive in time to be played in the correct sequence, which causes additional delay. The jitter buffers add delay, which is used to remove the packet delay variation that each packet is subjected to as it transits the packet network.
3. Packet Loss: Wireless and IP networks cannot provide guarantee that packets will be delivered at all, much less in order. The packets will be dropped under peak loads.

The above three parameters can be used for objective voice quality measurements. The subjective voice quality measurements are given in terms of Mean Opinion Score or MOS. MOS is the average score given by a large number of users (about 100) with similar listening ability listening to the same segment of voice under the same condition [11]. This method of voice quality measurement can be very expensive [11].

4.2 IEEE 802.11 MAC Layer

IEEE 802.11 MAC, particularly the DCF, has been explained in detail in Section 3.1.2.1. In this section an explanation of the contention-free mode and the limitations of the MAC with respect to QoS are explained.

As presented in Section 3.1.2.1, the IEEE 802.11 MAC can alternate between the contention mode, known as the Contention Period (CP), and the Contention-Free Period (CFP), Figure 4-2. It has been known since long that CP although suitable for data (non real-time) transmission is unsuitable for supporting real-time (voice) applications [1].



B: Beacon
CFP: Contention Free Period
CP: Contention Period
PCF: Point Coordination Function
DCF: Distributed Coordination Function

Figure 4-2 IEEE 802.11 MAC Architecture.

In IEEE 802.11 there is only a single point of access to and from the wired LAN, i.e. the Access Points (AP). Since most wireless traffic is in fact destined for (or will at least traverse) the wired LAN, this single point of access to the wired LAN creates a natural bottleneck in the bandwidth and the throughput. As the wireless network becomes loaded, the APs will begin queuing significant amounts of traffic as they contend for the access to the medium. This queuing behaviour is also in direct opposition to the limited lifetime nature of the voice traffic.

The CFP mode based on polling was claimed to be more suitable to support real-time traffic than the CSMA/CA. However, the use of a centralized scheme imposes heavy constraints on the operation of the WLANs.

In this section the DCF and the PCF are presented as possible VoWLAN solutions. Limitations of the DCF and the PCF for VoWLAN and a qualitative comparison with other possible VoWLAN solutions are given in Section 4.5.

4.2.1 Distributed Coordination Function Limitations

The DCF (Distributed Contention Function) is the fundamental access method used to support asynchronous data transfer on a best effort basis in IEEE 802.11 [2,5,6]. As identified in the specification [7], all stations must support the DCF. The DCF operates solely in the ad hoc network, and either operates solely or coexists with the PCF in an infrastructure network. The DCF sits directly on top of the physical layer and supports contention services. Contention services imply that each station with a packet queued for transmission must contend for access to the channel and, once the packet is transmitted, must recontend for access to the channel for all subsequent frames. Contention services promote fair access to the channel for all the stations.

4.2.2 Point Coordination Function

The PCF (Point Coordination Function) [1,2,5,6] is an optional capability of IEEE 802.11, which is connection-oriented, and provides contention-free (CF) frame transfer. The PCF relies on the point coordinator (PC) to perform polling, enabling polled stations to transmit without contending for the channel. The function of the PC is performed by the AP within a network. Stations within a network that are capable of operating in the CF period (CFP) are known as CF-aware stations.

The PCF is required to coexist with the DCF. The CFP repetition interval is used to determine the frequency with which the PCF occurs. Within a repetition interval, a portion of the time is allotted to contention-free traffic and the remainder is provided for contention-based traffic. The CFP repetition interval is initiated by a beacon frame (B), which is transmitted by the AP. One of its primary functions is synchronization and timing. The duration of the CFP repetition interval is a manageable parameter that is always an integral number of the beacon frames. Once the CFP repetition interval is established, the duration of the CFP is determined. The maximum size of the CFP is determined by CFP_Max_Duration. The minimum value of CFP_Max_Duration is the time required to transmit two maximum-size MAC layer protocol data units (PDUs), including the overhead, the initial beacon frame and the CF-End frame. The maximum value of CFP_Max_Duration is the CFP repetition interval minus the time required to successfully transmit a maximum-size MAC PDU (MPDU), which is 2312 Bytes, during the CP. It is up to the AP to determine how long to operate the CFP. If traffic is very light, the AP may shorten the CFP and provide the remainder of the repetition interval for the DCF. The CFP may also be shortened if DCF traffic from the previous repetition interval carries over into the current interval.

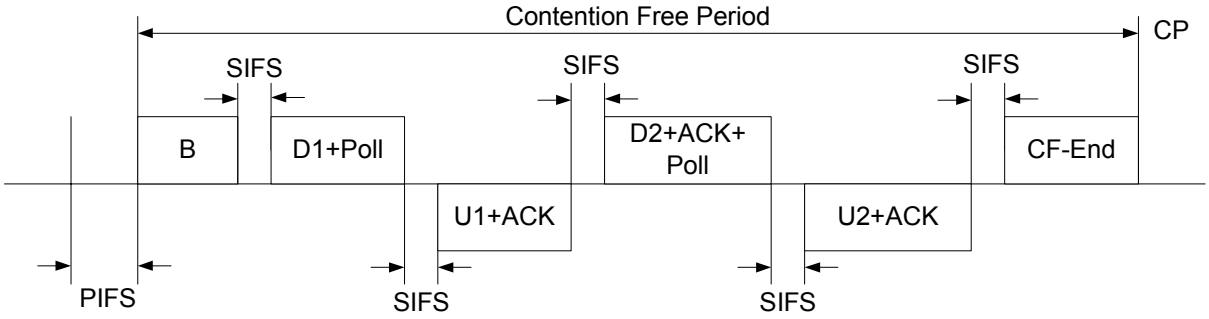


Figure 4-3 PC to Station transmission.

At the nominal beginning of each CFP repetition interval, all stations connecting the AP update their waiting period to the maximum length of the CFP (i.e., CFP_Max_Duration). During the CFP, the only time stations are permitted to transmit is in response to a poll from the PC or for transmission of an ACK a SIFS interval after the receipt of a MPDU. At the nominal start of the CFP, the PC senses the medium. If the medium remains idle for a PIFS interval, the PC transmits a beacon frame to initiate the CFP. The PC starts the CF transmission a SIFS interval after the beacon frame is transmitted by sending a CF-Poll (no data), Data, or Data+CF-Poll frame. The PC can immediately terminate the CFP by transmitting a CF-End frame, which could be a case if the network is lightly loaded and the PC has no traffic buffered. If a CF-aware station receives a CF-Poll (no data) frame from the PC, the STA can respond to the PC after a SIFS idle period, with a CF-ACK (no data) or a Data+CF-ACK frame. If the PC receives a Data+CF-ACK frame from a station, the PC can send a Data+CF-ACK+CF-Poll frame to a different station, where the CF-ACK portion of the frame is used to acknowledge receipt of the previous data frame. The ability to combine polling and acknowledgment frames with data frames, transmitted between stations and the PC, was designed to improve efficiency. If the PC transmits a CF-Poll (no data) frame and the destination station does not have a data frame to transmit, the station sends a Null Function (no data) frame back to the PC. Figure 4-3 illustrates the transmission of frames between the PC and a station, and vice versa. If the PC fails to receive an ACK for a transmitted data frame, the PC waits a PIFS interval and continues transmitting to the next station in the polling list. After receiving the poll from the PC, as described above, the station may choose to transmit a frame to another station. When the destination station receives the frame, a ACK is returned to the source station, and the PC waits a PIFS interval following the ACK frame before transmitting any additional frames. The PC may also choose to transmit a frame to a non-CF-aware station. Upon successful receipt of the frame, the station would wait a SIFS interval and reply to the PC with a standard ACK frame. Fragmentation and reassembly are also accommodated.

If, for instance, a STA starts a transmission during the DCF period which lasts longer than the remaining time between the start of the transmission and the nominal start of the next CFP, the PC has to defer the start of its transmission until the medium has been free for a PIFS period (Figure 4-4).

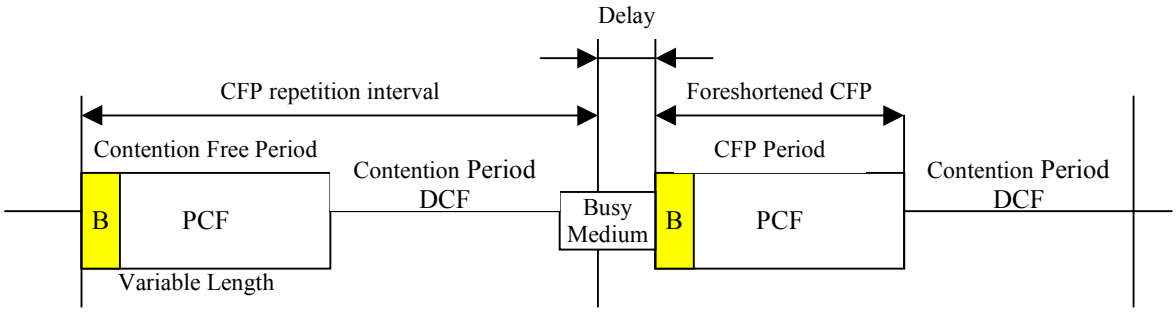


Figure 4-4 Contention Free Period, CFP and Contention Period, CP.

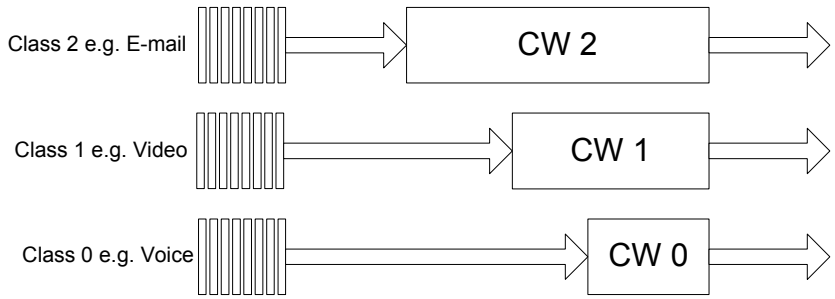


Figure 4-5 Priority queuing for different service classes.

4.3 Priority Queuing

Priority Queuing is a scheme in which the voice packets are given priority over the data packets within a system using the DCF [5]. The channel access process remains the same as in IEEE 802.11 except that the random back-off value is varied for voice and data transmission by giving a smaller contention window for voice and longer for data. This method can be used for several classes of service.

In Figure 4-5 the priority queuing method for different service classes is given. Three different service classes are given as example. For a lower value of the Contention Window (CW) the chance to access the channel is much higher as compared to a higher value of the CW. Thus the priority is given to the traffic with high QoS requirements.

4.4 Blackburst

One of the solutions for providing voice over WLANs is the Blackburst protocol [3,5]. Blackburst as discussed in [3] is described in this section.

4.4.1 Protocol Description

In Blackburst design it is considered that a mixed population of data and voice stations share a common radio channel. The data stations regulate their access to the channel according to the CSMA/CA protocol while the voice stations follow a variation of CSMA that will give them priority over the data stations.

The Blackburst design takes in consideration the propagation delay and access delay in wireless communication. For simplicity it is assumed in this section that delays are with a value in the interval $[0, \tau]$. The operation of the Blackburst requires definition of three interframe spacing, t_{short}, t_{med} and t_{long}, such that

$$t_{short} + 2\tau < t_{med} \quad (1)$$

$$t_{med} + 2\,\tau < t_{long} \quad (2)$$

t_{short} is related to acknowledgement traffic, t_{med} is related to access procedure of voice stations and t_{long} is related to access procedure of data stations. These interframe spacing can be related to SIFS (Short Inter-frame Space), PIFS (Point coordination function Inter-frame Space) and DIFS (Distributed coordination function Inter-frame Space) respectively as specified in the IEEE 802.11 standard.

4.4.2 Access Procedure of Voice Stations

The access procedure of a voice station is based on two ideas. One consists in having both the instants when the packet is formed and the number of speech bits conveyed in the packet dependent on events in the channel. The other idea consists in having the voice station contend for

access to the channel with "black" slots. A black slot is just a short burst of energy of fixed duration. An appropriate interplay of these ideas minimizes the contention among voice stations and allows them to have priority over the data stations.

The coding rate of the voice stations is denoted by r_s and speech bits delayed for transmission by more then d_{max} are discarded. A voice station has a reset instant at a given time if only the speech bits generated from that time onwards are considered for transmission; it is said to have access instant at a given time if it transmits a voice packet at that time. In the sequel a reset instant will always be equal to access instant but not conversely.

4.4.2.1 Basic Operation

Under basic operation it is assumed that the transmitted voice packets are not acknowledged by their recipients. After transmitting a packet a voice station will not care whether or not that packet suffered a collision and it will be interested in transmitting the speech bits generated from that time onwards. Therefore the reset instant coincides with the access instant.

Further it is assumed that every voice packet has fixed length of h header bits plus $r_s d_{max}$ bits. The latter bits are reserved for transmitting speech information, although the actual number of speech bits conveyed in a voice packet will depend on the congestion found in the channel.

Consider a voice station with an access instant scheduled to occur at time t. The protocol will follow the following procedure:

1. If the channel was perceived idle in the interval $(t - t_{med}, t]$ and remains idle for the ensuing t_{obs}, with $t_{obs} > 2\tau$, the station transmits a voice packet with the speech bits generated between the last access instant and the current one.
2. If the channel is not perceived idle for t_{med} consecutive units then the station enters into a black burst contention period: the station jams the channel with a number of black slots which are proportional to the time it has been waiting for the channel to be idle. Specifically, if a station has been waiting for a period d to access the channel then it transmits a black burst of duration $t_{bslot} \times \lceil d / t_{unit} \rceil$, where t_{bslot}, $t_{bslot} > 2\tau$, is the length of a black slot and t_{unit} is a system parameter.
3. After transmitting its black burst a station waits for t_{obs} to see if any other voice station is transmitting a longer burst, implying that it would have been waiting longer for access to the channel.
4. If the station is perceived idle then the voice station transmits the most recently generated speech bits, up to a maximum of $r_s d_{max}$ bits.
5. If the channel is not perceived as idle, then the station waits for t_{med} once again and repeats the algorithm from step 1 onwards.
6. Whenever a voice station has an access instant it schedules the next access instant to occur at $t_{sch} = (d_{min} - t_{obs})$ from then, with $d_{min} < d_{max}$.

The observation period t_{obs} has to be smaller than t_{bslot} so that a voice station always recognizes when its black burst is shorter than that of another station; it has to be less than t_{med}, so that the voice stations do not access the channel to transmit black burst during the observation period. In conclusion, $2\tau < t_{obs} < \min(t_{bslot}, t_{med})$.

As for t_{unit}, the reset instants of different voice sources are shifted in time by at least t_{inter}, where t_{inter} accounts for transmission time of a voice packet plus the interframe space of t_{med} plus an observation period of t_{obs}:

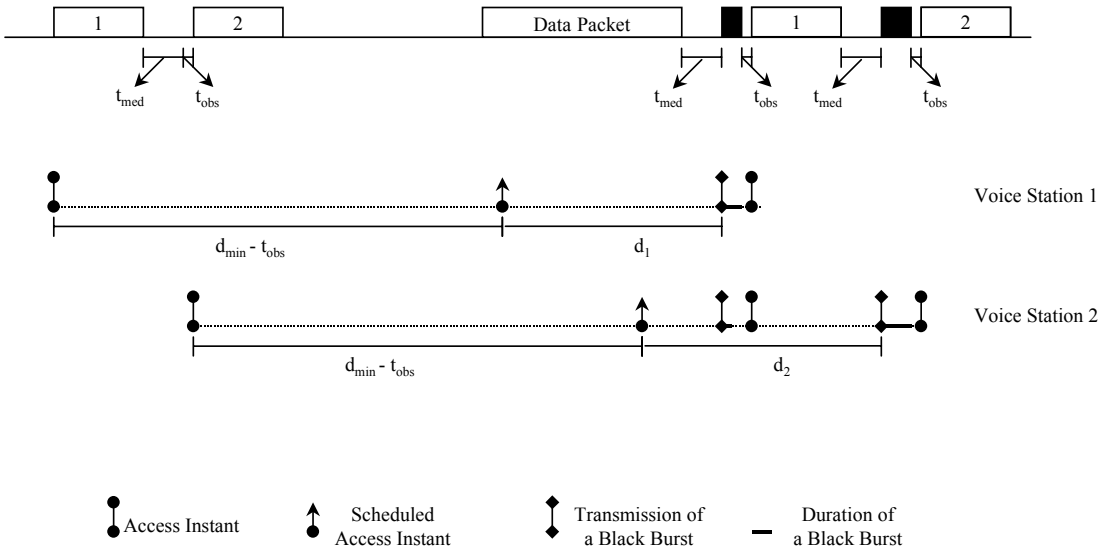


Figure 4-6 Example: Access procedure of voice stations.

$$t_{interr} = \frac{h}{r_c} + \frac{r_s}{r_c} d_{\max} + t_{med} + t_{obs} \quad (3)$$

where, $t_{pkt} = h / r_c + (r_s / r_c) d_{\max}$.

This implies that voice channels that find the channel busy will have access delays that differ by at least t_{inter}. Therefore if $t_{unit} \leq t_{inter}$, their black burst will differ by at least one black slot, implying that every black burst contention period will result in a unique winner. The winner is the voice channel that has been waiting the longest to access the channel. Collisions between a voice packet and a data packet can only occur when the channel has been idle for a long time and both packets get transmitted in a time frame of τ seconds.

To ensure that a real-time station recognizes at the beginning of a call when it has acquired undisputed access to the channel, this station can use the access procedures of data stations to transmit its first packet. When an acknowledgment is received, the station knows that its previous access instant is shifted in time from those of the other real-time stations. From that point on, the access procedures of real-time stations ensure that the packets of this station do not collide with those of other real-time stations.

Figure 4-6 shows how the protocol operates. The access instants of stations 1 and 2 get perturbed by a data packet transmission. Station 2 contends twice with black bursts, and its second black burst is longer than its first because the delay from the scheduled access instant has increased. The protocol has two important characteristics. First, the real-time station that has been waiting the longest for access to the channel wins the next black burst contention period. This effectively ensures that real-time stations access the channel to transmit their packets in a round-robin order. Second, the real-time stations get priority over the data stations, because no data station will perceive the channel idle for t_{long} consecutive units until all contending real-time stations have obtained access to the channel.

4.4.2.2 Bandwidth Control

The access procedures of the previous section are independent of the characteristics of the traffic to be transported. Whenever a station has an access instant, it is only required that it transmits for at least t_{pkt} seconds, where t_{pkt} is the same for all stations. The number of information bits actually transmitted at the access instants does not have to be fixed. Indeed, a real-time station generating information bits at a constant nominal rate will typically increase the number of information bits transmitted as a function of the delay it incurred before accessing the channel. This compensates

for the fact that the time between consecutive access instants of a real-time station may be longer than (t_{sch} + t_{obs}) seconds. By the same token, real-time stations with different bandwidth requirements can be supported by having those stations transmit different numbers of information bits when they access the channel. Deciding whether the network can support a new call with the specified bandwidth and QoS requirements is made when the call is set up.

Usually, a real-time application will produce blocks of bits, which are then enqueued in a buffer for transmission. The buffer may have finite capacity and only be able to enqueue the most recently generated blocks of information. When the station has an access instant, it will simply empty the contents of the buffer. The packets transmitted on the channel may be of fixed length, matched to the capacity of the buffer. If the buffer is not full, the fixed-length packets are filled with padding bits. Alternatively, the packets may just contain the blocks found in the buffer at the access instant, plus the required packet overhead.

The performance of the system improves if the AP groups real-time packets with different destinations into a frame and only contends for access to the channel with black bursts once for each frame, rather than once for each real-time packet.

4.4.2.3 Negative Acknowledgment Scheme

A positive acknowledgment scheme, as proposed in the IEEE 802.11 standard, incurs a penalty in channel efficiency, because every correctly received packet has to be followed by an acknowledgment minipacket. On the other hand, the specific characteristics of the real-time access procedures support a negative acknowledgment scheme, in which a receiver only notifies the transmitter when it does not get a packet that was expected. This is only possible because under the proposed procedures a receiver expects a new real-time packet (t_{sch} + t_{obs}) seconds after the previous one, plus some prespecified delay tolerance. Not receiving a new packet within that time implies that the packet is lost or unduly delayed.

Whenever a destination station operating with a negative acknowledgment scheme receives a real-time packet, it schedules the transmission of an invitation minipacket to t_{neg} seconds in the future, with $t_{neg} > (t_{sch} + t_{obs})$. After that time has elapsed, if no new real-time packet has arrived, the destination station starts contending for access to the channel to invite the source station to (re)transmit a packet. The invitation minipacket can contend for access to the channel as if it were a data packet. If a real-time packet arrives in the interim, the destination aborts its attempts to send the invitation minipacket.

The use of invitation minipackets also offers robustness against the hidden stations problem. This problem arises in CSMA wireless networks because a source station inhibits the other stations in its vicinity, rather than those in the vicinity of the destination. However, it is the latter stations that may interfere with the packet transmission from source to destination. If, instead, the destination invites the source to transmit a packet, then, by doing so, it is inhibiting the stations in its vicinity exactly those that may interfere with the ensuing real-time packet transmission from source to destination

4.5 Comparison

In this section a qualitative analysis and comparison of the four schemes are given [5]. Besides delay, jitter and packet loss; implementation difficulty, scalability and compatibility to the IEEE 802.11 standard are important parameters for comparison. MOS is not considered here because it is a subjective parameter and very expensive to measure [11]; in this comparison it is assumed that the qualitative analysis of delay and jitter will give an idea of the effect on MOS.

Packet loss basically is an issue of the channel. In the case of IEEE 802.11, packet loss can be decreased by decreasing the data rate. As Forward Error Correction (FEC) is not used by the IEEE 802.11b there is no other way to decrease packet loss [3,6]. In the case of IEEE 802.11a FEC is used but in combination of modulation it is used to vary data rate [6,13].

Jitter can be taken care of by the AP. For this purpose the AP will have to implement a scheduling scheme that can distinguish between different service classes. The service classes should not be distinguished by unwrapping the received packet until the application layer is reached but there should be mechanisms to identify the service class from the packet header. A discussion related to this issue is given in Section 4.6.

4.5.1 Distributed Coordination Function

The advantage of DCF is that it promotes fairness among stations, but its weakness is that it cannot support time bounded services [5]. Fairness is maintained because each station must recontend for the channel after every transmission of a packet. All stations have equal probability of gaining access to the channel after each DIFS interval. Time-bounded services typically support applications such as packetized voice or video that must be maintained with a specified minimum delay. With DCF, there is no mechanism to guarantee minimum delay to stations supporting time-bounded services. It might be possible to transmit voice over DCF in an isolated cell with few users but in normal conditions (data and voice traffic in a network) performance for voice communication will be relatively bad [6].

As DCF is the basic access method of the IEEE 802.11 WLANs, implementation is a non-issue; it has to be implemented and is already implemented in all the IEEE 802.11 products. The issue with the DCF, like any other QoS solution for WLAN, will be the implementation of scheduling and prioritized queue in the AP and also in the STAs. This could be very easily done for example, by delaying the non-real-time traffic from the STA and giving priority to real-time traffic and in the AP by implementing a round-robin method for transmission of real-time packets to the stations while giving low priority to non-real-time traffic.

As the basic MAC mechanism of IEEE 802.11 is dependent on the DCF, compatibility with the standard is a non-issue.

Scalability, in terms of the number of people that can use an AP is not a problem for the DCF. The standard does not define the number of users per channel using the DCF either. As the channel access is based on the CSMA/CA mechanism the overall delay will increase if a large number of users join a channel and have data to transmit at the same time. Scalability in terms of a large number of APs that use the DCF is again not a problem; such deployments are common. Neighbouring APs will use different channel, see Chapter 7, and if there is some effect of overlapping the CSMA/CA characteristics will take care of it as it takes care of channel access of the STAs to an AP.

4.5.2 Point Coordination Function

There are three issues related to real-time services and PCF as given below [5].

The first issue is that the centralized mode cannot be operated simultaneously in the neighbouring cells, this happens because there are very few independent or non-overlapping channels (3 channels) defined by the IEEE 802.11 standard [6,7]. With such few independent channels there is a very high probability of interference from the neighbouring cells. Even if the neighbouring cell is not using an overlapping or the same channel a far away cell using the same channel will cause interference. Further to it the IEEE 802.11 APs are not synchronized thus the CFP in different cells can start at the same time and thereby cause collision. Thus the overall quality will be degraded. Not only that a STA in an AP with the same frequency can also cause interference and thus degradation of quality. This issue is often known as the overlapping cell issue.

Second, as a result of the CSMA/CA protocol, the PC might be unable to gain control of the channel at the nominal beginning of the CFP. If, for instance, a station starts a transmission during the DCF period which lasts longer than the remaining time between the start of the transmission and the nominal start of the next CFP, the PC has to defer the start of its transmission until the

medium has been free for a PIFS, see Figure 4-4. This decreases the CFP period and thus the QoS will be degraded.

Third, PCF is central control based but study done in [1] show that high overhead introduced by the IEEE 802.11 WLAN standard results in a low number of possible voice conversations.

Besides the above issues, PCF is an optional feature of the IEEE 802.11 standard and is not implemented by most vendors. To the best of author's knowledge it was only implemented by one vendor and that for test purposes only. Implementation of a fully functional PCF might not be very difficult but a good implementation could be very complicated because it would require resolving all the issues discussed in this section.

PCF is defined by the standard thus its compatibility is not an issue but a good implementation will require which might make it incompatible with the IEEE 802.11 standard.

As already presented in this section, the PCF is not scalable.

4.5.3 Priority Queuing

Priority Queuing will give reasonable performance [5]. Although priority queuing gives higher priority to voice packets by decreasing the backoff period but the same benefit can be the cause of increased collisions and thus decreased quality. Of-course increased collisions will occur if there were large number of users, thus an optimum number of users for a given CW and non-real-time traffic should be found. Implementations exist with the CW set to '0' for voice services. These solutions provide from 3 to best case of 5 simultaneous voice users in a channel connected to an AP.

The implementation difficulty of this solution is of a similar level as that of the modification of the DCF to provide voice services.

As this solution makes use of the DCF the compatibility with the IEEE 802.11 standard is not an issue. The standard allows implementation of different CW size.

Scalability could be an issue because as the number of users and number of APs increase, there will be overlapping cells (cell of an AP and transmission radius of a STA). Overlapping cell will mean increased collision and thus decreased QoS.

4.5.4 Blackburst

Blackburst is especially designed for voice transmission over IEEE 802.11. The protocol will give better performance as compared to other solutions described in this chapter. Quantitative results on the performance of Blackburst are given in [3].

The scheme makes use of the standard IFS of IEEE 802.11 thus requiring a slight modification in the MAC layer. Implementation of the new features like the black burst, sensing black burst at the receiver and antenna turn around time smaller than t_{obs} will mean changes in both the MAC layer and the Physical layer.

Sending of Blackburst is not compatible with the IEEE 802.11 standard.

This solution can be used in neighbouring/overlapping cells without any problem as it uses the CSMA/CA characteristics. Thus scalability is not an issue for Blackburst.

Table 4-1 Comparison of different schemes.

	DCF	PCF	Priority Queuing	Blackburst
Channel Access Delay(number of users)	+	++	+++	++++
Implementation	++++	++	+++	++
Compatibility	++++	++++	++++	+
Scalability	++++	+	+++	++++

4.5.5 Qualitative Comparison

A qualitative comparison of the four VoWLAN schemes are given in this section and summarized in Table 4-1 [5]. In the table the number of "+" gives the extent of fulfilment of the requirement with 4 + being the maximum.

It is possible that a very good voice coding could compress voice to such extent that the voice packets become very small and thus a reasonable service could be provided even by using the DCF. Even then, using the same coding scheme the performance will vary for the 4 possible VoWLAN solutions.

For the DCF implementation, compatibility and scalability are non-issues but delay is a big problem.

In case of the PCF implementation, several changes will be required in the current implementation but compatibility is not an issue as it is a part of the standard. Compatibility becomes an issue if problems related to the PCF are taken care of. The channel access delay is an issue because of the overlapping cell problem and the shift in nominal start of the CFP period which leads to decrease in the length of the CFP period. Scalability is a major problem for the PCF.

Priority queuing is basically a simple variation of the DCF and thus is easy to implement. It can bring improvement in the quality when compared to the DCF. The solution is compatible with the IEEE 802.11 standard. Scalability could be an issue for priority queuing due to the overlapping cell problem.

Blackburst is designed for voice services and is also designed to be scalable. The issue with Balckburst is its implementation and compatibility with the standard.

Based on the discussion in this section, the previous sections and Table 4-1 it is clear that the DCF is the best solution if no changes are desired but is worst in terms of quality, while Blackburst can give better quality but its implementation and compatibility with the standard is an issue. Overall, priority queuing is the best solution.

4.6 Top-to-Bottom and End-to-End QoS

In this section a method to provide top-to-bottom QoS and end-to-end QoS are discussed [12]. Top-to-Bottom QoS means each layer in the protocol stack has QoS provision, understands QoS requirements and has either similar understanding of QoS or understands QoS parameters of the layer higher and lower. End-to-End QoS means provision of QoS from one terminal to other or more specific from the senders' application layer to the receivers' application layer. Without provision of the top-to-bottom QoS, the end-to-end QoS is not possible. In Figure 4-7 different protocol layers for the top-to-bottom QoS are given.

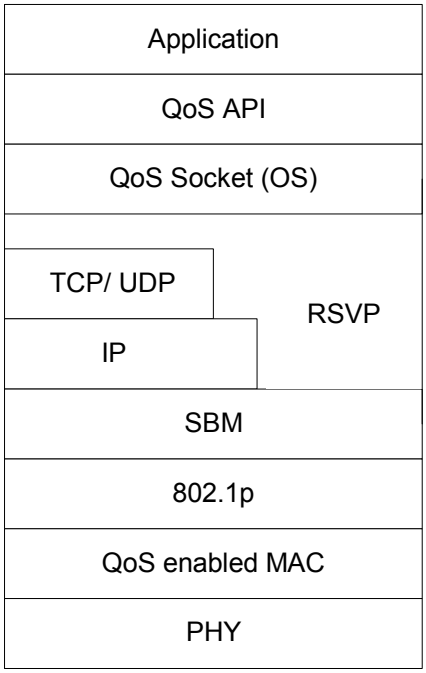


Figure 4-7 QoS protocol stack in wireless stations, top-to-bottom QoS.

An explanation of communication of top-to-bottom is given below:

1. The application should be capable to provide QoS services like video, audio or voice and should be capable of calling on a QoS based Application Program Interface (API). The API should be built such that it can call on the QoS sockets..
2. The QoS information can thus by using the API and the socket be mapped on the Resource Reservation Protocol (RSVP) protocol, [8], or another protocol.

   RSVP, [8,12], is a signaling protocol for resource reservation that permits the allocation of different levels of service to different users. RSVP can be used to offer service discrimination for delay sensitive applications by explicit allocation of resources in the network.
3. The information is then mapped to the Subnet Bandwidth Manager (SBM), [9], for bandwidth allocation and the admission control.

   SBM, [9,12], is a signaling protocol that allows communication and coordination between network nodes and switches and enables mapping to higher-layer QoS protocols. Basically SBM is a protocol for RSVP-based Admission Control over IEEE 802-style networks.
4. The SBM maps the quality needed on the IEEE 802.1p which in turn maps the required QoS on the QoS MAC.

   The IEEE 802.1p, [12,16], standard defines how Ethernet switches can classify frames in order to expedite delivery of time-critical traffic. IEEE 802.1p uses a 3-bit value that can represent an 8-level priority value.
5. The QoS MAC then performs medium access so as to provide the required QoS.

In Figure 4-8 an example of an end-to-end QoS for WLAN networks using SBM, RSVP and Differentiated Service (DiffServ) [10,12] are given. The following is an explanation of the messages given in the figure for end-to-end communication:

1. A station sends the PATH message to the AP+DSBM (Designated Subnet Bandwidth Manager). The DSBM checks the available bandwidth. Detail discussion on bandwidth allocation for RSVP and SBM is available in [8,9].

The PATH message contains traffic specific information like bandwidth, delay and jitter. It is sent by the transmitter to the receiver; network elements in between create a path-state that includes the previous source address i.e. the previous network element.

DSBM is basically the Bandwidth Allocator (BA) in a SBM network, i.e., it maintains state about allocation of resources on the subnet and performs admission control according to the resources available and other administrator-defined policy criteria.

2. The AP+DSBM send the PATH message to the router after checking the destination address.
3. The router checks for available bandwidth and performs a policy check at the directory.

   The directory contains the policy and mapping between DiffServ and RSVP parameters. The policy is dependent on network administrator but it should preferably be standard defined.
4. The router sends the packet to the Internet using DiffServ.

   DiffServ, [10,12], provides customisable QoS depending on traffic types. When using DiffServ, the IP header (the DS CodePoint) indicates the packet priority level. This also means that policy decisions are required. Differentiation of services is provided by classes of services with different priorities, which is indicated by Type-Of-Service (TOS) in a IPv4 header or priority bits of IPv6 header. The use of IP header for service prioritisation shows the biggest difference with RSVP where flows are used to reserve bandwidth.
5. The packet reaches the destination router that performs check for the available bandwidth and performs policy check at the directory.
6. The packet (now RSVP PATH message) is passed to the receiving AP+DSBM. The DSBM checks for the bandwidth availability. The RSVP PATH message is based on policy check at the directory.
7. The PATH message is then sent to the destination station.
8. After checking for the available service and application the destination station sends a RESV message to the AP+DSBM.

   The RESV is a RSVP message sent by the destination or receiver to the source of the PATH message to make resource reservation. The RSVP router that receives the RESV message authenticates the request by admission control process and allocates the required bandwidth. In case the request cannot be satisfied due to lack of resources or authorization failure, the router returns an error back to the receiver. Otherwise, the router sends the RESV to the next router. When the last router receives the RESV and accepts the request, it sends a confirmation message back to the receiver.
9. The DSBM reserves the bandwidth and sends the RESV message to the router after checking the destination.
10. The directory control is performed.
11. The router sends the packet on the Internet using DiffServ.
12. The packet reaches the transmitting LAN router where the directory control is performed.
13. The RESV message is send to the AP+DSBM which allocates the bandwidth to the service and the station.
14. The originating station receives the RESV message.

Now end-to-end QoS communication can take place.

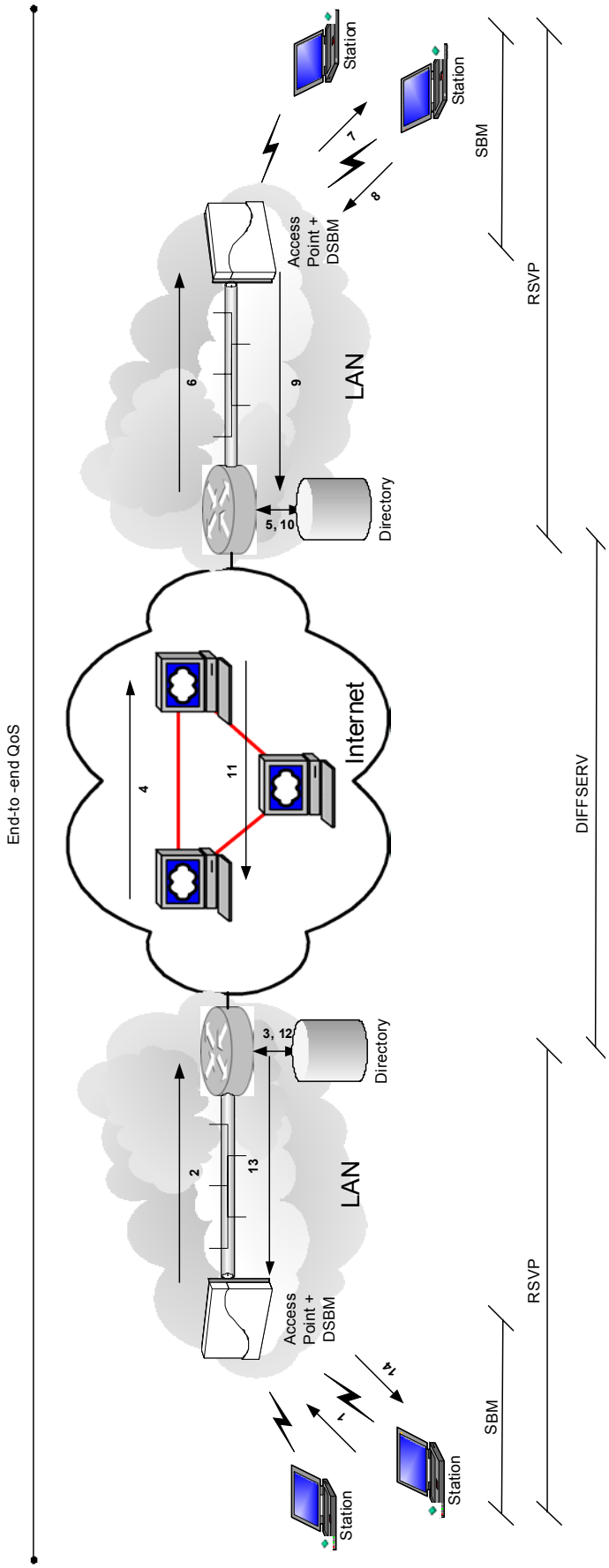


Figure 4-8 End-to-end QoS using WLAN.

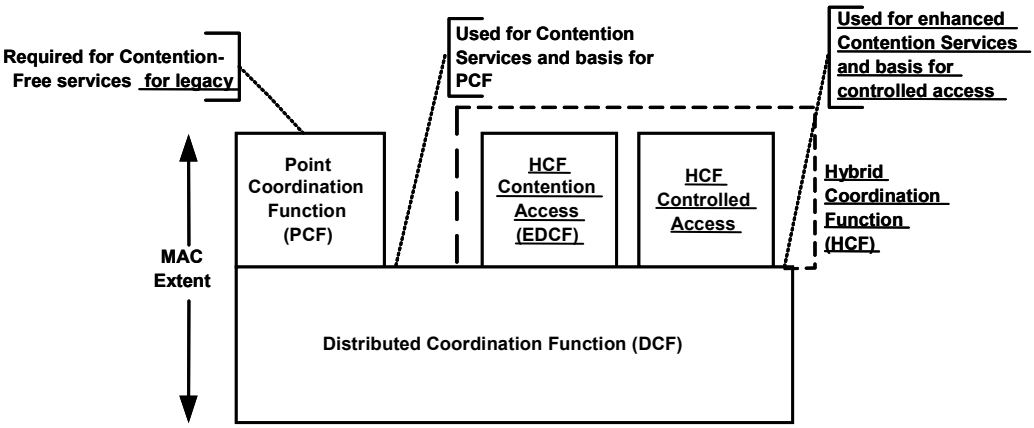


Figure 4-9 IEEE 802.11e MAC architecture.

4.7 IEEE 802.11 Draft QoS Standard

In the previous sections possible mechanisms to provide QoS in the IEEE 802.11 standard were presented together with a qualitative performance comparison. The comparison work was done at the starting phase of the IEEE 802.11 Task Group E (TGe) which is working on MAC enhancements for QoS. In this section the QoS mechanisms adopted in the present IEEE 802.11e standard is presented.

4.7.1.1 IEEE 802.11e

IEEE 802.11e provides MAC enhancements to support LAN applications with QoS requirements. The QoS enhancements are available to the QoS enhanced Stations (QSTAs) associated with a QoS enhanced Access Point (QAP) in a QoS enabled network. A subset of the QoS enhancements may be available for use between QSTAs. A QSTA may associate with a non-QoS AP in a non-QoS network [6,7]. Non-QoS STAs may associate with a QAP. In Figure 4-9 the MAC architecture of the IEEE 802.11e is given.

The enhancements that distinguish the QSTAs from non-QoS STAs and the QAPs from non-QoS APs comprise an integrated set of QoS-related formats and functions that are collectively termed the QoS facility. The quantity of certain, QoS-specific mechanisms, may vary among QoS implementations, as well as between the QSTAs and the QAPs [7]. However, all service primitives, frame formats, coordination function and frame exchange rules, and management interface functions defined as part of the QoS facility are mandatory, with the exception of the Group Acknowledgement function defined [7] which is an option separate from the core QoS facilities, and the presence of it is indicated by QSTAs separately from the core QoS facility.

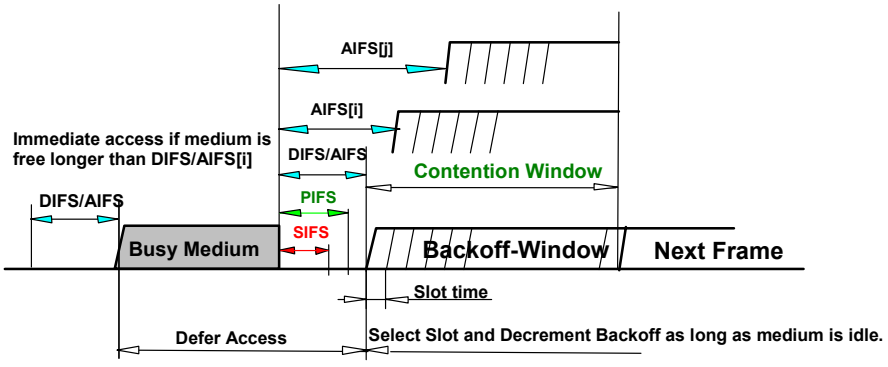


Figure 4-10 Inter frame spacing for enhanced MAC.

The IEEE 802.11e standard provides two mechanisms for the support of applications with QoS requirements.

The first mechanism, designated as the Enhanced Distributed Coordination Function (EDCF), is based on the differentiating priorities at which the traffic is to be delivered. This differentiation is achieved through varying the amount of time a station would sense the channel to be idle, the length of the contention window during a backoff or the duration a station may transmit once it has the channel access. This is similar to the Priority Queuing discussed in Section 4.5.3.

The second mechanism allows for the reservation of transmission opportunities with the Hybrid Coordinator (HC). A QSTA based on its requirements requests the HC for transmission opportunities – both for its own transmissions as well as transmissions from the HC to itself. The HC, based on an admission control policy either accepts or rejects the request. If the request is accepted, it schedules transmission opportunities for the QSTA. For transmissions from the STA, the HC polls a QSTA based on the parameters supplied by the QSTA at the time of its request. For transmissions to the QSTA, the HC queues the frames and delivers them periodically, again based on the parameters supplied by the QSTA. This mechanism is expected to be used for applications such as voice and video which may need a periodic service from the HC. This mechanism is a hybrid of several proposals studied by the standardization committee.

4.7.1.2 Inter-Frame Spacing

The time interval between the frames is called the IFS. A STA determines that the medium is idle through the use of the carrier sense function for the interval specified. Five different IFSs are defined to provide priority levels for access to the wireless media; they are listed in order, from the shortest to the longest except for the Arbitration Interframe Space (AIFS). Figure 4-10 shows some of these relationships. The different IFSs are independent of the STA data rate.

a. SIFS Short Interframe Space
b. PIFS Point Coordination Function (PCF) Interframe Space
c. DIFS Distributed Coordination Function (DCF) Interframe Space
d. AIFS Arbitration Interframe Space (used by the QoS facility)
e. EIFS Extended Interframe Space

The AIFS is to be used by QSTAs to transmit data and management frames. A QSTA using the EDCF is allowed a transmit opportunity (TxOP) for a particular Traffic Class (TC) if its carrier sense mechanism determines that the medium is idle at the T_{XAIFS}(TC) slot boundary after a correctly-received frame, and the backoff time for that TC has expired.

4.7.1.3 Other QoS Related Development

IEEE 802.11e is also looking into admission control and scheduling, this will of course complete the picture for QoS support. Besides this the IEEE 802.11 standard is also looking into overlapping cell issues which is very important for QoS especially for a system with very few and unlicensed non-overlapping channels. Another ongoing work is IEEE 802.11f which looks at the Inter Access Point Protocol or IAPP (approved as standard in July 2003) [15], transferring of context information from one AP to another will help in fast and seamless handover.

4.8 QoS Issues for Future Studies

For the wireless communications there are two major goals: to maximize the usage of the wireless resource and minimize the usage of energy. These two goals should be fulfilled while providing the best possible quality to the user. The issue of energy is of course directly linked to the radio resource when it comes to the transmit power but it is also related to the battery life time of the device.

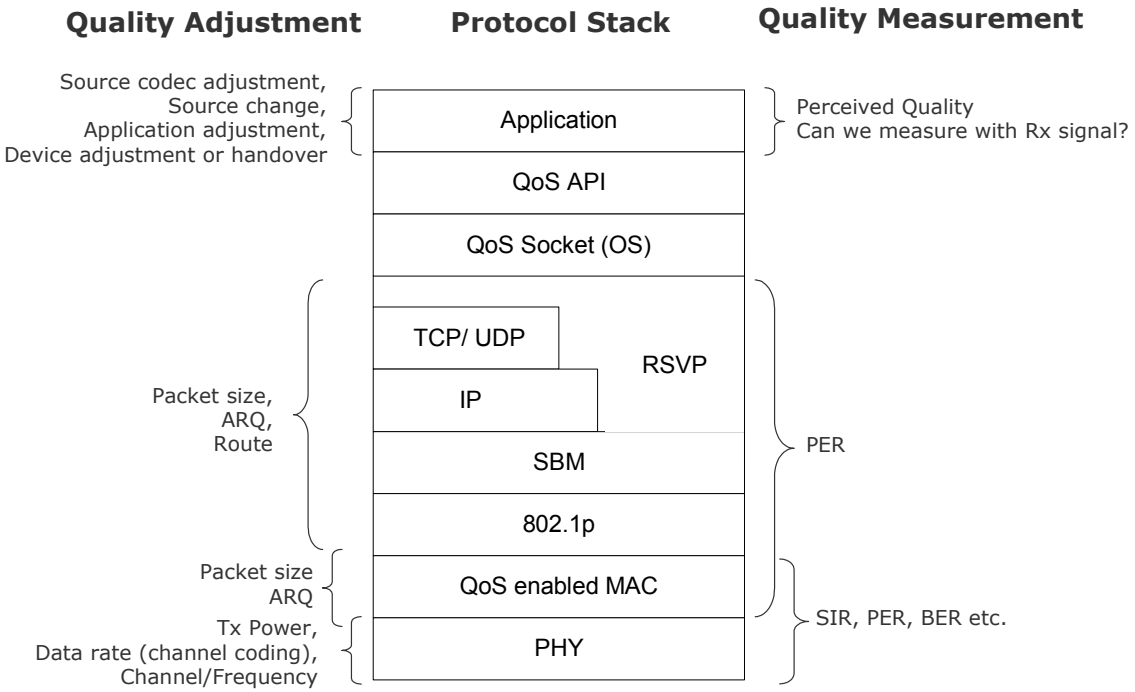


Figure 4-11 QoS protocol stack, quality measurement parameters and quality adjustment methods.

In this section first the method for quality measurement and adjustment/control is discussed after which issues related to providing good quality while fulfilling the two goals is presented.

4.8.1 Quality Measurement and Adjustment

So as to provide QoS all protocol layers must understand the quality as discussed in Section 4.6. Although quality can be understood and provided by different layers, it must be measured and adjusted during the communication. In Figure 4-11 protocol stack and quality measurement and adjustment/control parameters for different layers are given.

For Layer-1 and Layer-2 (PHY, and MAC layer) the quality is usually measured in terms of the Signal to Interference Ratio (SIR), the Packet Error Rate (PER) or the Frame Error Rate (FER) and the Bit Error Rate (BER). The adjustment of quality in Layer-1 can be done by adjusting the transmit (Tx) power, changing the data rate/channel coding and changing the channel or frequency, while for Layer-2 the packet size can be changed or Automatic Repeat Request (ARQ) mechanism can be used.

While for Layer 2.5 (Subnet Bandwidth Manager (SBM) and Layer-3 (IP, Transmission Control Protocol (TCP)/User Datagram Protocol (UDP), Resource Reservation Protcol (RSVP) etc.) the quality can be measured in terms of the PER and adjusted by varying the packet size, the ARQ or simply by changing the route or path of the communication.

The application layer quality measurement can be done by measuring the perceived quality, i.e., the objective perceived quality; of course the issue is how to measure the perceived quality just from the received (Rx) signal [11]. The adjustment of quality at the application layer can be done by changing the source codec rate or other variables in the source codec (e.g., for video coding I frame interval), it also possible to simply change the source, adjust the application by for, e.g., changing the size of application window or by adjusting the device to give a better perceived quality.

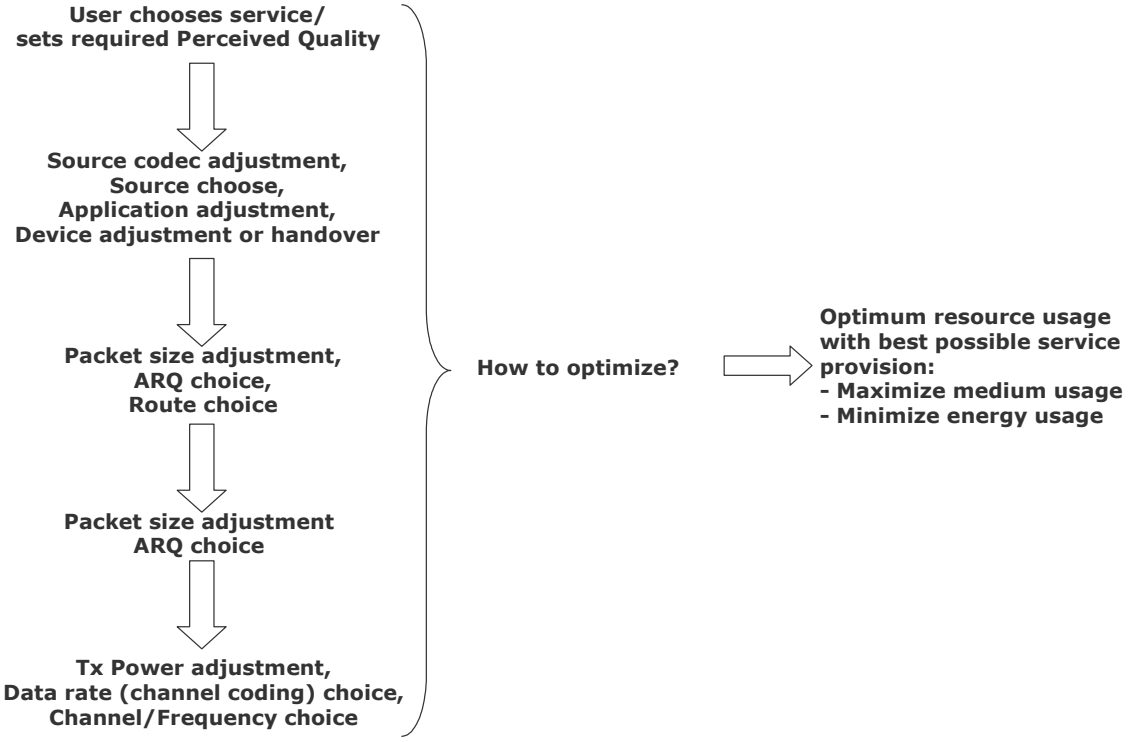


Figure 4-12 Quality adjustment issues.

4.8.2 Quality Adjustment Issues

It is understandable that the quality of the system and the resource adjustment should be done based on the application layer quality measurement. The application layer quality can be measured by measuring the perceived quality from the received signal; this is not yet done and is a very difficult but important problem to be solved [11].

Once the perceived quality is known, the quality in lower layers can be adjusted, i.e., a study should then be done on adjusting the packet size, the transmit power, the data rate etc.. Optimization of all the parameters to achieve a good QoS while maximizing resource usage and minimizing energy/power usage is a very big but important issue.

Current wireless systems mostly adjust the quality independently in different layers. The first step could be to study methods for the optimum quality adjustment in each layer. Then one can pursue towards the optimum quality adjustment in two layers (Layer-1 and 2), going to three (Layer-1, 2 and 3) and then finally to the application layer.

In Figure 4-12 the preliminary adjustment per layer based on the user quality requirement is given. Preliminary because each layer should find the optimum quality adjustment value so as to provide the requested quality. These parameters will be adjusted as the communication continues.

4.9 Conclusions

In this chapter four possible schemes for voice communication over the IEEE 802.11 WLANs are examined. These schemes are Distributed Coordination Function (DCF), Point Coordination Function (PCF), Priority Queuing and Blackburst. A qualitative analysis and comparison of the four schemes are given.

Comparison of qualitative analysis of the four schemes shows that Blackburst outperforms all the schemes in terms of quality, delay and scalability. But implementation of Blackburst is difficult and it is not compatible with the IEEE 802.11 standard. The DCF on the other hand is not a good choice because it will give very bad voice quality although it is compatible and is mandatory for

the IEEE 802.11 standard. The DCF is also a very scalable solution. The PCF will give better performance than the DCF in terms of delay but studies show that the performance will not be good enough for voice. Further the PCF is only good enough for single or a maximum of three cell solutions where each cell uses a different and non-overlapping channel, as soon as there is a channel overlap the PCF will perform very poorly. Besides that the nominal start time of the PCF is not fixed although the end time is fixed thus the QoS will degrade considerably. Priority queuing will give better performance than the DCF and the PCF and will be relatively easy to implement, the only issue with priority queuing is the extent of scalability is not of the same level as for the DCF.

There is a trade-off between the delivered QoS and the implementation complexity. If high performance is required Blackburst is advised but if a simple solution with reasonable quality is required then priority queuing is the right scheme. Current draft of IEEE 802.11e has chosen priority queuing as one of the possibilities for QoS in the MAC layer thus proving the soundness of the qualitative analysis.

The chapter also discusses protocols and methods to provide top-to-bottom QoS and end-to-end QoS. Where top-to-bottom means all protocols in the protocol stack understand QoS and end-to-end provision of QoS from the sending application to the receiving application.

Finally methods used for the quality measurement and adjustment in each protocol layer are discussed together with the issues related to quality adjustment which can be considered for future studies. The biggest issue identified is the measurement of quality at the Application layer (perceived quality) with just the received signal and the adjustment of the quality parameters in each layer based on the measured perceived quality.

References

[1] M. A. Visser and M. El Zarki, “Voice and Data Transmission over an 802.11 Network”, pp 648-652, Proc. PIMRC’95, Sept. 1995, Toronto, Canada.

[2] Draft International Standard ISO/IEC 8802-11, IEEE P802.11/D10, 14 January 1999, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Clause 8.

[3] J. L. Sabrinho and A.S. Krishnakumar, “Real-Time Traffic over the IEEE 802.11 Medium Access Control Layer”, pp 172-187, Bell labs Technical Journal, Vol. 1, No. 2, Autumn 1996, N.J., USA.

[4] K.R. Rao and J.J. Hwang, Techniques & Standards for Image, Video & Audio Coding, Prentice Hall, New Jersey, 1996.

[5] A.R. Prasad, "Performance Comparison of Voice of IEEE 802.11 Schemes", VTC 1999 Fall, pp. 2636-2640, 19-22 September 1999, Amsterdam, The Netherlands.

[6] A.R. Prasad, A. Kamerman and H. Moelard, “IEEE 802.11 Standard”, Chapter 3 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[7] IEEE P802.11e, Draft Supplement to IEEE Std 802.11, 1999 Edition, Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Medium Access Control (MAC) Enhancements for Quality of Service (QoS).

[8] Braden, R., L., Zhang, S. Berson, S. Herzog, and S. Jamin, “Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification,” IETF, RFC 2205, September 1997.

[9] Yavatkar, R., D. Hoffman, Y. Bernet, F. Baker, and M. Speer, “SBM (Subnet Bandwidth Manager): A Protocol for RSVP-based Admission Control over IEEE 802-style networks”

IETF, RFC 2814, May 2000.

[10] IETF "Differentiated Services" working group, Web URL: http://www.ietf.org/html.charters/diffserv-charter.html and http://www.ietf.org/ids.by.wg/diffserv.html, 12 July, 2001.

[11] A. R. Prasad, R. Esmailzadeh, S. Winkler, T. Ihara, B. Rohani, B. Pinguet and M. Capel, "Perceptual Quality Measurement and Control: Definition, Application and Performance", WPMC 2001, 9-12 September 2001, Aalborg, Denmark.

[12] L. Brederveld, N.R. Prasad and A.R. Prasad, "IP Networking for Wireless Networks", Chapter 4 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[13] IEEE 802.11, "Draft Supplement to Standard for Telecommunications and Information Exchange between Systems - LAN/MAN Specific Requirements - Part 11: Wireless MAC and PHY Specifications: High Speed Physical Layer in the 5 GHz Band," P802.11a/D6.0, May 1999.

[14] A. Kamerman and A.R. Prasad, "Performance Analysis", Chapter 6 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[15] IEEE 802.11f, "Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation", IEEE standard P802.11f, January 2003.

[16] IEEE 802.1p, "Media Access Control (MAC) Bridges", incorporated in IEEE 802.1D, 1998.

Chapter 5

Enhanced Security for Wireless LANs

Barely a decade ago filing cabinets with strong combination locks were replaced by computers communicating by wireline medium [1]. Communicating through a wireline medium meant the end (almost) of physical means of protecting sensitive information and a major change in requirements of information security. Now the communicating medium is becoming wireless. Wireless Local Area Networks (WLANs) [1-3,9,17,18] usage is experiencing explosive growth and the once envisaged usage environments have already been reached: the market of academia, enterprise and the public environment. Security is an issue that can cause a major setback to the growth of WLANs and all these environments have different security requirements. This chapter discusses security issues and proposes requirements and novel solutions for IEEE 802.11 based WLANs [2].

5.1 Chapter Overview

The work done in this chapter was started at the preliminary stages of the IEEE 802.11 search for improved security solutions. The purpose of this work was to propose the requirements for the environments in which WLANs were envisaged to be used (today WLANs are being used in the envisaged environments) and propose solutions which would fulfil these requirements.

This chapter starts with the basic information about general security threats and security goals for the background information of the audience. These security goals are the requirements that should be fulfilled by the security solutions so as to counter the security threats. Two of the security solutions that will be used in the rest of the chapter are the Remote Authentication Dial-In User Service or RADIUS and the Kerberos, these two solutions are also briefly discussed in the chapter.

As the goal of this chapter is to examine the security of WLANs, a description of the current IEEE 802.11 standard security solution based on the Wired Equivalent Privacy (WEP) is also given. The security issues of the current IEEE 802.11 security solution, WEP, are also discussed in this chapter.

Having identified the background of security threats, goals, solutions and WEP security issues the security requirements of the three WLAN envisaged environments are proposed in the chapter. The three envisaged environments considered in this chapter are, academic environment which uses Kerberos, corporate environment and public environment, presently also known as hot-spot, where a user uses RADIUS. At the time when this work was started the residential and the military environment were not considered to be that important, although now the WLAN growth is higher in the residential market than in the corporate market. The main reason of the lack of growth in the corporate market is the security issues related to WEP.

Security solutions for the three envisaged environments are proposed next. The primary goal of the proposed security solutions was to re-use the existing off-the-shelf techniques as far as

possible, e.g., from the Internet Engineering Task Force or IETF. Some proposals were presented by the author to the IEEE 802.11i Medium Access Control (MAC) security enhancements group [12]. The current draft reflects the acceptance of the proposals [11].

One of the common security 'holes' for each environment and proposed solutions based on off-the-shelf techniques was the issue of access control. Thus a novel access control protocol is proposed in this chapter. Although the access control protocol was proposed some time ago, the IEEE 802.11f Inter Access Point Protocol (IAPP) standardized recently is very similar to the proposed solution. Today several other standards and research work talk about 'context' and 'context transfer'; the proposed access control protocol called the context 'profile'.

After proposing the solutions a short description of the IEEE 802.11i and the IEEE 802.11f are given and the security issues of future generation communications are discussed. Then the chapter is concluded.

5.2 Security Threats and Goals

The introduction of distributed systems and the use of networks and communications facilities – wireline and now increasingly wireless– has increased the need for network security measures to protect data, here data is for both real-time and non real-time, during transmission. To assess the security needs effectively and evaluate and choose the most effective solution a systematic definition of the security goals or requirements and understanding of the threats is a necessity [1,2,16,18,23]. In this section first the security threats and then the security goals are discussed. This section also discusses which security goals will counter a given security threat.

5.2.1 Threats

Security threats or security issues can be divided in two types: passive and active threats. Passive threats are done by individuals to gain information which can be used for their benefit or maybe to perform active attacks at a latter time. Active threats are those where the intruder does some modification to the data, network or traffic in the network. In the following the most common active and passive threats are discussed for a comprehensive list see [1,16,18].

Passive Threats

A passive threat is a situation when an intruder does not do anything to the network or traffic under attack but collects information for personal benefit or for future attack purpose. Two basic passive threats are given below [1,16,18,23].

- Eavesdropping: This is a common security threat known to the human being since ages. In this attack the intruder listens to things he/she/it is not supposed to listen. This information could contain, for example, the session key used for encrypting data during the session. This kind of attack means the intruder can get information which is at times strictly confidential.
- Traffic Analysis: This is a subtle form of passive attack. It is possible that at times for the intruder knowing the location and identity of the communicating device or user is enough. An intruder might only require the information like: a message is sent, who is sending the message to whom and at what frequency or the size of the message. Such threat is known as traffic analysis.

Active Threats

An active threat arises when an intruder directly attacks the traffic and the network and causes modification of the network, data etc.. A list of common active attacks is given below [1,16,18,23].

- Masquerade: This is an attack in which an intruder pretends to be a trusted user. Such an attack is possible if the intruder captures information about the user like the authentication data,

simply the username and the password. Sometimes the term spoofing is used for masquerade [18].

- Authorization Violation: An intruder or even a trusted user uses a service or resources it is not intended to use. In case of an intruder this threat is similar to the masquerading; having had the possibility to enter the network the intruder can access services it is not authorized to access. On the other hand a trusted user can also try to access unauthorized services or resources; this could be done by the user performing active attacks on the network or simply by lack of security in the network/system.
- Denial of Service (DoS): DoS attacks are performed to prevent or inhibit normal use of communications facilities. In case of wireless communications it could be as simple as causing interference or it could be done by sending data to a device and overloading the Central Processing Unit (CPU) or draining the battery. Such attacks could also be performed on a network by, for example, flooding the network with unwanted traffic.

  Sabotage is also a form of DoS attack. A DoS attack when termed as sabotage could also mean the destruction of the system itself.
- Modification or forgery of information: An intruder creates new information in the name of a legitimate user or modifies or destroys the information being sent. It could also be that the intruder simply delays the information being sent. An example is an original message "Allow Bill Gates to read confidential Source Codes" modified to "Allow Anand Prasad to read confidential Source Codes".

5.2.2 Goals

There are five major security goals which are also known as security services and can also be used as *security requirements*. These goals are discussed below [1,16,18,23].

- Confidentiality: This is for the protection of the data from disclosure to an unauthorized person. Encryption is used to fulfil this goal. With an active attack it is possible to decrypt any form of encrypted data (given there is a good mathematician/cryptographer or a person with a powerful computers and no time limit) thus confidentiality is primarily considered a protection against passive attacks.
- Authentication: The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic (i.e., each is the entity that it claims to be). Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.
- Access Control: In the context of network security, access control is the ability to limit and control the access to the systems, the networks and the applications. Thus unauthorized users are kept out. Although given separately user authentication is often combined with access control purposes this is done because a user must be first authenticated by the given server, the network etc. so as to determine the user access rights.
- Integrity: Prevents unauthorized changes to the data. Only authorized parties are able to modify the data. Modification includes changing status, deleting, creating, and delaying or replaying of the transmitted messages.
- Non-repudiation: Neither the originator nor the receiver of the communication should be able to deny the communication and content of the message later. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a

message is received, the sender can prove that the message was in fact received by the alleged receiver.

Besides the above mentioned security requirements there are some general requirements which play an important role in developing the security solutions, these are:

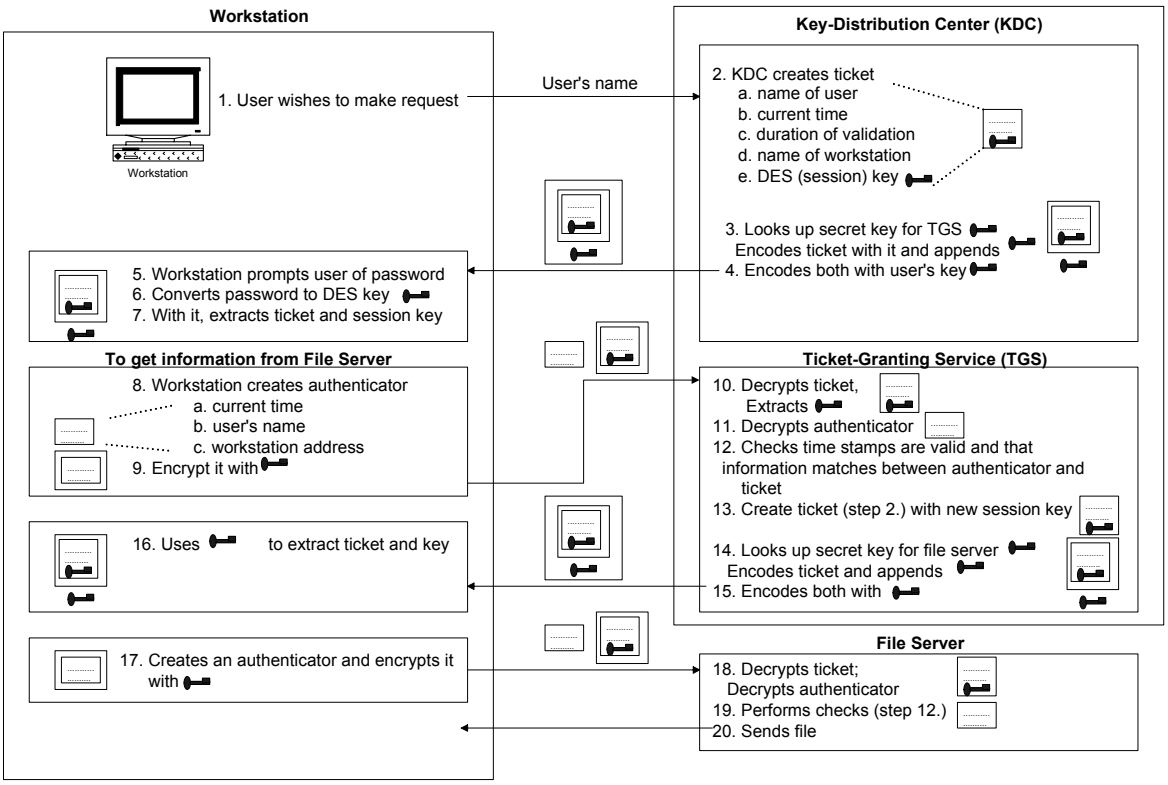
- Manageability: The load of the network administrator must not be unnecessarily increased by adding security while at the same time the deployed solutions should be easy to manage and operate in the long term.
- Scalability: A network must be scalable which requires that the security scheme deployed in the network to be equally scalable while maintaining the level of security. Here the term scalability is being used in its broadest sense, scalable in terms of the number of users and also in terms of an increase in network size, i.e., addition of new network elements or an extension to a new building.
- Implementability: A simple and easy way to implement a scheme is extremely important. Thus a security scheme must be devised which is easy to implement and still fulfils the security requirements.
- Performance: Security features must have minimum impact on the network performance. This is especially important for real-time communication where the security requirements must be met while the required quality of service is met. Performance also goes hand in hand with the resource usage of the medium, the security solutions must not, for example, cause a decrease in the overall capacity of the network.
- Availability: This goal is closure to the five goals mentioned earlier in the section. Any service or network should be available to the user. Several attacks are possible to disrupt the availability, DoS being the major one.

5.2.3 Mapping Security Threats to Goals

In this section the security threats are mapped to the security goals. Knowing which threat can be countered by which goal, the next step is to find the security solutions or mechanisms that can fulfil the security goals. The mapping of security threats and goals is given in Table 5-1 [1,16,18], X in a cell represents that the given security goal can counter the given threat. It should be noted that a security goal can fail to counter a threat sometimes.

Table 5-1 Mapping of the security threats to the security goals.

Security Goals	Security Threats					
	Eaves-dropping	**Traffic Analysis**	**Masquerade**	**Authorisat-ion violation**	**DoS**	**Modification or Forgery of Information**
Confidentiality	X	X	X	X		
Authentication			X	X		X
Access Control			X	X		X
Integrity			X	X		X
Non-repudiation			X	X		X
Availability			X	X	X	X



KDC: Key Distribution Centre; DES: Data Encryption Standard (Kerberos v4.0);
TGS: Ticket Granting Service

Figure 5-1 Kerberos example.

5.3 Security Solutions

The security solutions used commonly in current networks are discussed in this section. First part of the section discusses RADIUS and Kerberos. These two security solutions are used in environments in which WLANs are envisaged to be used. The second section discusses security solution used in current IEEE 802.11 based WLANs and its security issues.

5.3.1 General Security Solutions

In this section a short description of Kerberos and Remote Authentication Dial In User Service or RADIUS is given. This information is background information for the convenience of the reader as they proceed to later sections where these two protocols are used.

5.3.1.1 Kerberos

Kerberos provides a means of verifying the identities of principals, (e.g., a workstation user or a network server) on an open (unprotected) network [1,2,4-6]. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets travelling along the network can be read, modified, and inserted at will. Many applications use Kerberos' functions only upon the initiation of a stream-based network connection, and assume the absence of any "hijackers" who might subvert such a connection. Such use implicitly trusts the host addresses involved. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography, i.e., the shared secret key.

Kerberos is a secure protocol and fulfils all the security goals such as confidentiality, authentication, access control, integrity, non-repudiation, availability, scalability and manageability if implemented and used correctly [1]. As Kerberos is also implemented in Microsoft Windows, implementation is not an issue. In Kerberos v4, the user ID can be spoofed

and password can be guessed but this issue is solved in Kerberos v5 [1]. Further Data Encryption System (DES) used for Kerberos v4 is considered broken. Scalability and availability of Kerberos can be a problem because it requires a centralised trusted server, which constitutes a single point of failure. If the centralised trusted server is broken then everything else is broken. Other limitations of Kerberos are discussed in [22].

Kerberos protocols rely on encryption keys, known only to the appropriate parties in a transaction, to protect information sent across an open network. The example in Figure 5-1 shows the sequence that takes place when users first log in to the system and gain access to their files. Only the first exchange requires a user's password; subsequent requests rely on the session key shared by the user and the Ticket Granting Service (TGS).

5.3.1.2 RADIUS

RADIUS, "Remote Authentication Dial In User Service," is the industry standard protocol for authenticating remote users [7,16]. Today it is widely deployed in remote access servers, routers, and firewalls. RADIUS servers are strategically placed on the network to provide authentication services to all users through a common security protocol. In addition to authenticating and authorizing users, RADIUS enables accounting for the network services. A network configuration of RADIUS is given in Figure 5-2. Key features of RADIUS are:

1. Client/Server Model: A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned. RADIUS servers are responsible for receiving the user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver the service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.
2. Network Security: Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an insecure network could determine a user's password.

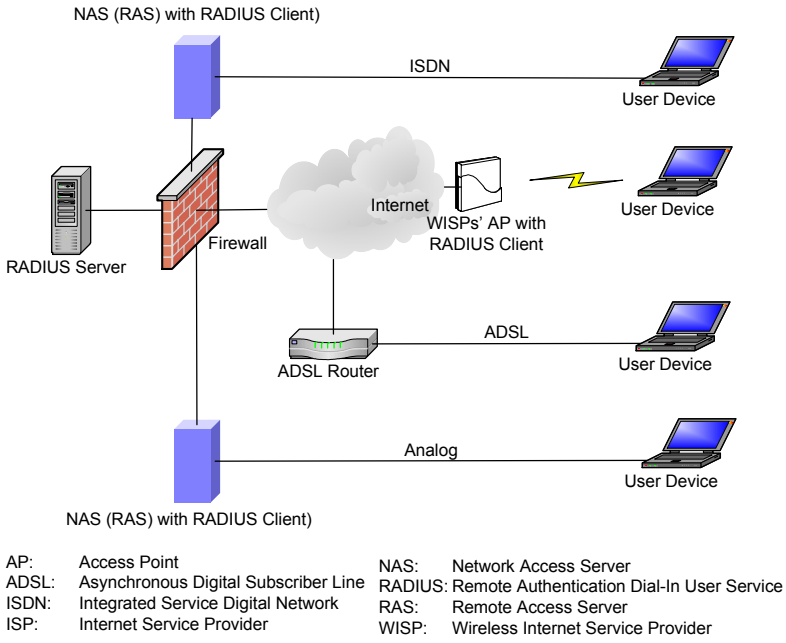


Figure 5-2 RADIUS network configuration.

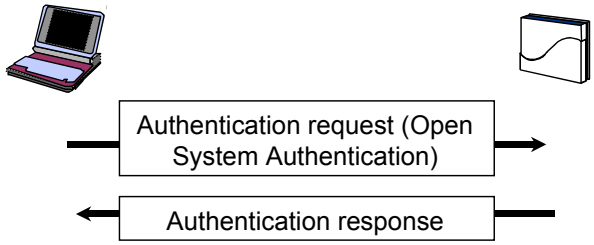


Figure 5-3 Open system authentication.

3. Flexible Authentication Mechanisms: The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the user name and the original password given by the user, it can support Point-to-Point Protocol (PPP) with Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP), UNIX login, and other authentication mechanisms.
4. Extensible Protocol: All transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.

One of the vulnerabilities of RADIUS is the use of shared secret between the client and the server. If the shared secret is known there can be lots of threat like intruder acting as a client or even a server and collecting user information. Another security issue with RADIUS is that authentication of the access request message is not done and the use of PAP and CHAP procedures is insecure. Both passive and active attacks are possible against RADIUS. The IETF has proposed solutions for the security issues arising from RADIUS.

5.3.2 Security in IEEE 802.11

IEEE 802.11 had a goal to provide three basic security services, authentication, confidentiality and integrity [2,3,8]. This section discusses the method in which these services are achieved in the current standard, i.e., the original IEEE 802.11 solution not IEEE 802.11i.

5.3.2.1 Authentication

IEEE 802.11 defines two subtypes of authentication service: Open System and Shared Key [8].

Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any STA that requests authentication with this algorithm may become authenticated if the recipient station is set to the Open System authentication Figure 5-3.

The Shared Key authentication supports authentication of the STAs as either a member of those who know a shared secret key or a member of those who do not. The IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in the clear; requiring the use of the Wired Equivalent Privacy (WEP) mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of the IEEE 802.11. During the Shared Key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the PRN (pseudorandom number) sequence for the key/IV (Initialisation Vector) pair used for the exchange. Therefore the same key/IV pair for subsequent frames should not be used. The shared key authentication process is shown in Figure 5-4.

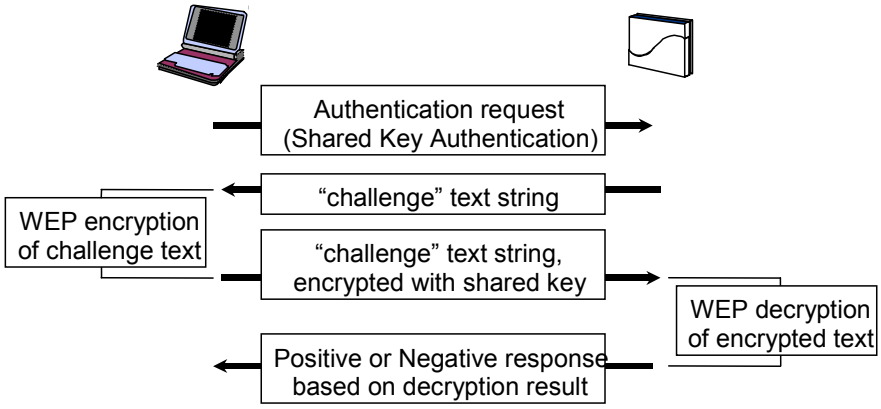


Figure 5-4 Shared key authentication.

5.3.2.2 Wired Equivalent Privacy

The WEP algorithm is a form of electronic code book in which a block of plaintext is bitwise XORed with a pseudorandom key sequence of equal length. The key sequence is generated by the WEP algorithm.

Referring to Figure 5-5 and viewing from the left to the right, the encipherment begins with a secret key that has been distributed to the cooperating STAs by an external key management service. WEP is a symmetric algorithm in which the same key is used for encipherment and decipherment.

The secret key is concatenated with an IV and the resulting seed is an input to the pseudorandom number generator (PRNG). The PRNG outputs a key sequence *k* of pseudorandom octets equal in length to the number of data octets that are to be transmitted in the Medium Access Control Protocol Data Unit (MAC PDU or MPDU) plus 4 [since the key sequence is used to protect the Integrity Check Value (ICV) as well as the data]. Two processes are applied to the plaintext MPDU. To protect against unauthorized data modification, an integrity algorithm operates on the plaintext MPDU to produce an ICV. Encipherment is then accomplished by mathematically combining the key sequence with the plaintext concatenated with the ICV. The output of the process is a message containing the IV and ciphertext.

Referring to Figure 5-6 and viewing from the left to the right, the decipherment begins with the arrival of a message. The IV of the incoming message shall be used to generate the key sequence necessary to decipher the incoming message. Combining the ciphertext with the proper key sequence yields the original plaintext and the ICV. Correct decipherment shall be verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV′ to the ICV transmitted with the message. If ICV′ is not equal to ICV, the received MPDU is in error and an error indication is sent to the MAC management.

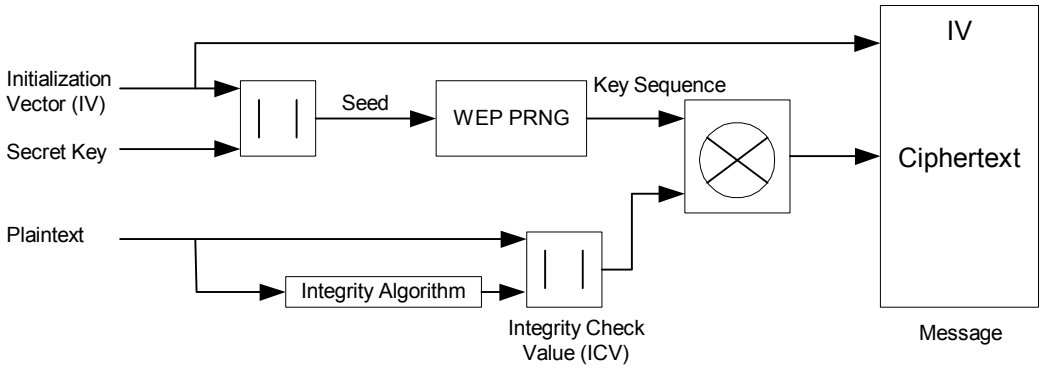


Figure 5-5 WEP encipherment block diagram.

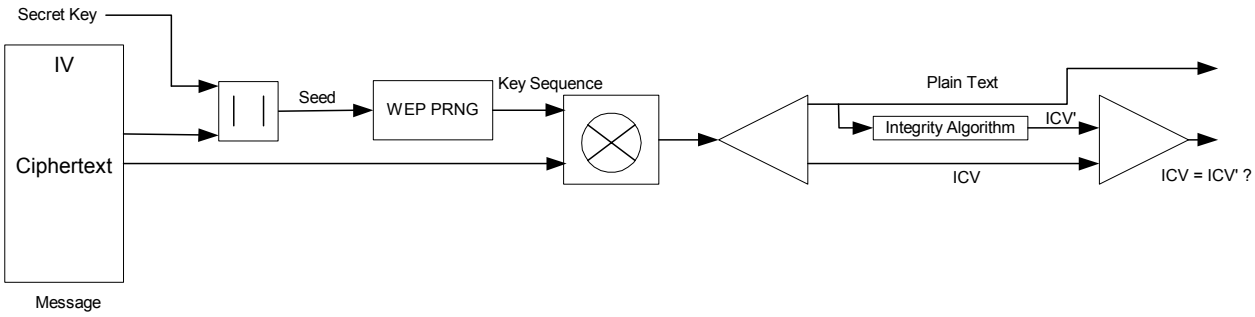


Figure 5-6 WEP decipherment block diagram.

5.3.2.3 IEEE 802.11 Security Issues

The following security issues of IEEE 802.11 were known and identified when this work was started:

1. Shared key authentication: Shared key authentication suffers a known-plaintext attack; recovering the pseudo-random string by XOR the plaintext and cipher-text of challenge, which can be eavesdropped from the air. Then the pseudo-random string can be used in a new authentication even though the "shared secret" is not recovered.
2. Mutual authentication: WEP provides no mutual authentication between the station and the access point, i.e. the AP can authenticate the station, but not vice versa.
3. Key management: There is no real key management in WEP, but two methods of using WEP keys are provided. The AP and the stationss share the usage of the four (default) keys. The compromising of each of the node means a compromise of the wireless network. A key mappings table is used at the AP. In this method, each unique MAC address can have a separate key. The size of a key mappings table should be at least ten entries according to the 802.11 specification, however, is likely chip-set dependent. The use of a separate key for each user mitigates the known cryptographic attacks, but requires more efforts on the manual key management. Since key distribution is not defined in the WEP and can be done only manually, many of the organizations deploying wireless networks use either a permanent fixed cryptographic variable, or key, or no encryption at all.
4. Other problems: Influence of the compromising WLAN, since WLAN APs are usually connected to the intranets which are protected by firewalls, a compromise of WLAN can result in a serious exposure of the intranets. Using the same key for authentication and encryption increases the possibility to be compromised.

After this work was completed several other security issues in IEEE 802.11 found [13]. One of the major issues discovered was confidentiality; it is the most discussed weakness of WEP because it is easy to recover the encryption key.

5.4 Security Requirements

In this thesis three WLAN usage environments are considered: enterprise or corporate, academia and public or commonly known as hot-spot [2]. WLANs can be and are being used in other environments also for example home or residential use which is enjoying a tremendous growth. At the time this work was started the residential market for WLAN was not there and the three envisaged environments were those which were expected to see the biggest market penetration.

In general a corporate environment has an Ethernet based LAN with Operating System (OS) related authentication procedure (Microsoft, Apple, Unix etc.). Such environment will be referred to as the enterprise environment. Enterprises have closed network environments where reasonable

security can be achieved by using network name and shared key authentication. “Reasonable” because shared key and network name based authentication are not very secure processes. Another major concern in enterprises is the rate of change in the personnel, both short and long term. Distributing keys to them and making sure they cannot misuse a key once they have left the company is a major managerial problem. Ideally, a staff member should never share any secret information with any other staff member and a person should be entered into or removed from a database only once. Enterprise customers will not accept a security system that does not meet or come close to these management requirements.

Besides enterprises there are academic and other institutions where either OS based authentication is used or in certain cases Kerberos is used. Kerberos is Unix based (now also available in MS Windows); it includes authentication, access control and session encryption. The authentication is decoupled from access control so that the resource owners can decide who has access to their resources. In this sense, Kerberos meets the managerial needs given above [4-6]. For such institutions, the WLAN system must be compatible with Kerberos with the wireless part giving the same level of security as Kerberos.

The public or dial up environment users make use of the untrusted communications facilities to remote access systems of their employer or an Internet Service Provider (ISP). Therefore both authentication and session security are needed. This environment is dominated by the users using Microsoft platforms. Operators and service provider frequently use RADIUS [7]. RADIUS services are used especially when people are mobile and require access to their enterprise network or when people want to access an Internet Service Provider (ISP) from home. WLAN system like Public LAN will require compatibility to RADIUS and added extra security for the wireless part.

In this section requirements for the three identified environments are proposed [2]. Manageability, implementation and performance, although not mentioned below, are required for all three envisaged scenarios an explanation of these three requirements is given in Section 5.2.2.

5.4.1 Enterprise Environment

An enterprise network is usually a closed network giving remote access to the employees by RADIUS. People within an enterprise network usually access their files, e-mails, or World Wide Web (WWW). The access to the server is usually done by OS based authentication and access control processes. In the following requirements are proposed for the WLAN usage in an enterprise network security requirements arising from remote access or of any other form are not considered. One of the major assumptions here is that the system is a closed system thereby meaning that the users and machines are assumed to be trusted. As users and machines are assumed to be trusted, integrity and non-repudiation were assumed to be fulfilled at higher layer and are not considered as necessary requirement for this study [2].

1. Confidentiality: This means that information exchanged between a user and the system is not visible to third parties.
2. Authentication: All users entering the network must also be authenticated at the wireless level. Without authentication a user is not given access to any part of network. This is a requirement of IEEE 802.11.
3. Access Control: It is the job of the network administrator to restrict the access privileges of a user. At wireless level a user might get access to a certain set of services depending on his/her privileges, e.g., a network administrator will have full access giving him or her the possibilities to upload a new firmware in the APs while a guest user might be allowed to be associated to an AP but he/she might not get access to the underlying the network. This kind of requirement will vary from enterprise to enterprise.

   When using minimum or no security at the wireless or network level it might be required to secure the files storing the password and login name (even if good security mechanism is used,

this is recommended) to prevent misuse of network by wrong hands. Users often save these information in their machines.

4. Scalability: A security system deployed within an enterprise network must be scalable. Scalable both in the sense of the number of users that can use it and the network size. A scalable security solution should maintain the level of security with the change in number of users and the network size.
5. Security Level: Certain users/applications will require higher level of security than others. Different levels of security can be provided by using different key sizes or by partitioning the network based on the level of security required.

5.4.2 Academic Environment

A distributed environment in which users wish to access services on servers distributed throughout the network using Kerberos is assumed to be an academic environment. Kerberos provides centralized authentication, distributed access control and secure communication for such environments.

Any system being deployed in academic environment should fulfil the following proposed requirements [2]:

1. Confidentiality: This is provided on a user-by-user basis (session encryption).
2. Encryption: The data being transmitted in a wireless medium should be encrypted by different keys for each user. Although encryption is a method to provide confidentiality it is put as a separate requirement here so as to stress the need of per user encryption while the confidentiality requirement stresses the need of per session encryption.
3. Authentication/Access Control: Although the authentication and the access control are provided by Kerberos they must also be done at the wireless level. Once an AP authenticates a user he/she will have access to the wireless part of the network. The authentication protocol must be such that information is not disclosed to a bogus (fake) AP. Kerberos provides user-based authentication, which must also be provided at the wireless level.
4. Scalability: The system must be capable of serving a large numbers of users in a distributed environment. The system must be scalable both in terms of the number of users and the network size.
5. Compatibility: The deployed network must be compatible to and must give at-least the level of security achievable by Kerberos.
6. Impact on Network: System deployed on Kerberos must be either “plug and play” or must require minimal impact on the Kerberos system being used (minimum meaning slight change in the network based on Kerberos rules/methods).

5.4.3 Public Environment

In the Public environment usually the user calls in to the server from a remote location. For this purpose RADIUS is used [1,7,16]. It is assumed that a user will use RADIUS when accessing through a public WLAN network. The proposed requirements of an access network using a RADIUS based authentication protocol are [2]:

1. Confidentiality: The wireless connection between the AP and the STA must be encrypted with a key per user, i.e., per user encryption.

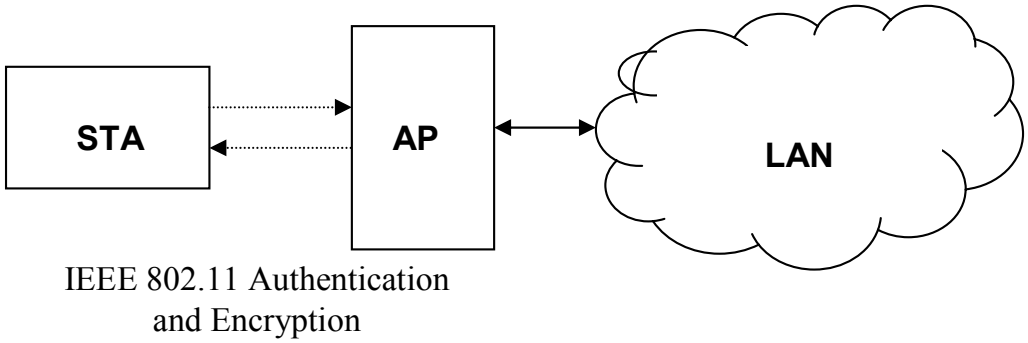


Figure 5-7 Enterprise security and IEEE 802.11.

2. Authentication/Access Control: Authentication and access control must be provided at the wireless level and the backbone network level also such that the secret information (password, etc.) is not disclosed to a bogus gateway to the public network.
3. Scalability: In public environment the user population (number of users) can vary a lot. The solution should provide scalability in terms of the number of users while maintaining the level of security.
4. Compatibility: The network must be compatible to RADIUS. As RADIUS is a standard protocol it must not be modified at all. There must not be any impact on the RADIUS based system.
5. Impact on the Network: The network should not require several changes.

5.5 Proposed Solutions

In this section solutions for the environments discussed in Section 5.4 are proposed. The most preferred solution would be the one that can be applied to all the environments without any compromise to the security. A qualitative analysis of the security solutions presented in this section is done in Section 5.6 [2].

5.5.1 Enterprise Security Schemes

The current enterprise security structure consists of an Ethernet LAN with a server that gives access to a user based on Login and Password, Figure 5-7. As the enterprise network is a closed environment, the standard IEEE 802.11 security scheme discussed in Section 5.3.2 is proposed as the solution. IEEE 802.11 provides two methods of authentication: the open system and the shared-key. The open system authentication means anyone is authenticated by the AP while in case of the shared-key a challenge is sent by the AP to the station which can only be encrypted correctly if the station has the right key. The key used for authentication is also used for the encryption, WEP, see Section 5.3.2 [2].

The biggest problem with WEP, as identified in Section 0, is authentication which is related to the encryption key. The best solution for it is to rotate the key as often as possible. IEEE 802.11 allows usage of four keys in a network which means each station and AP can have 4 keys at a given time.

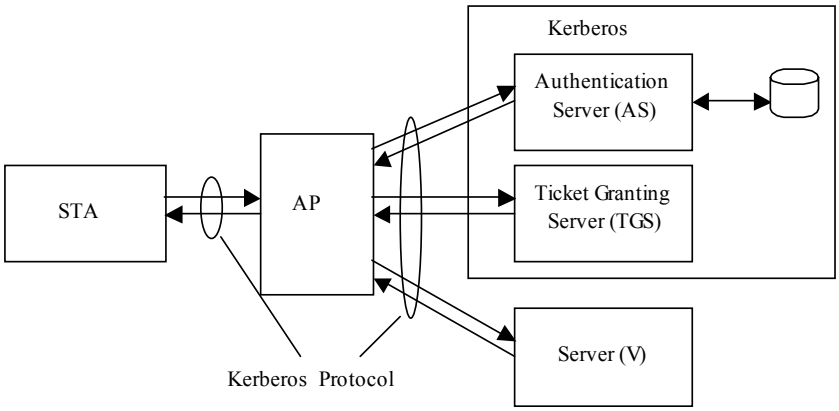


Figure 5-8 End-to-end authentication with Kerberos.

As the assumption for the enterprise environment is that it is a closed environment it is correct to assume that the preliminary key put in each AP and station will be secure. The preliminary key distribution could be done manually or by any other way considered to be safe by the network manager. Once the first set of 4 keys have been safely loaded, keys can be changed as frequently as the network manager wants. Automatic key roll-over and addition of new key in the list of course will require implementation by the vendors.

Other possible solutions for enterprise environment, also used currently, is to use MAC address list as Access Control List (ACL), i.e., only the MAC addresses in the ACL are allowed access to the network. Another solution being used currently is RADIUS with AP as the RADIUS client. Similarly it is possible to uses a Firewall at the AP.

Although using the MAC address ACL, RADIUS and Firewall are possible solutions for WLAN network security the proposal in this thesis is to use WEP with key roll-over as explained earlier in this section. The reason being that several security issues with the WEP including the weakness of RC4 was still unknown when this work was done. It was considered that WEP provided strong encryption and that using longer keys, 104 bits, would give a even better security.

The enterprise environment can also make use of the academic security solutions as discussed in Section 5.5.2 or the public security solutions discussed in Section 5.5.3.

5.5.2 Academic Security Schemes

It was assumed that in academia Kerberos is used. Two ways of applying security for WLAN with Kerberos proposed in this chapter are [2]:

1. End to end authentication: In this case Kerberos is simply used as is, with the AP as a wireless bridge. WLAN authentication takes place with current authentication methods: the open system and the shared key. As Kerberos is being used it will not make sense to use encryption at the MAC layer.
2. AP level authentication: Here the AP becomes a part of the Kerberos network, thus the station is authenticated by the AP and the Kerberos based network using Kerberos protocol.

In the following these two proposals are explained in detail.

5.5.2.1 End to End Authentication

In the end-to-end authentication case the procedure is exactly the same as Kerberos [2,4,5], the AP acts simply as a bridge. So as to comply with the IEEE 802.11 standard requirement, the AP level authentication will be used, i.e., either the open system authentication or the shared key authentication will be used. As can be understood, the shared key and WEP option should be turned off because it will only create extra overhead when used with Kerberos.

The communication between a STA and the Kerberos network is given below and in Figure 5-8. Notations and abbreviations used are given in Table 5-2; these legends and method of representing the communication is taken from [1].

Authentication service exchange: to obtain ticket-granting ticket

The station sends the request to the AP which forwards it to the Authentication Server (AS). The request contains the ID of the STA, the ID of the Ticket Granting Server (TGS) and the Time Stamp (TS).

1. STA → AP → AS: $ID_{STA} \parallel ID_{TGS} \parallel TS_1$

The AS responds to the STA via the AP. The response contains an encrypted message using the encryption key of the STA. The encrypted message is: the key for the TGS to be used by the STA, the ID of the TGS, the Time Stamp for the response, the lifetime of the response and the ticket to access the TGS.

The ticket always contains the username, the current time, the duration or the life-time of the ticket, the name of the workstation the user is using and the session key. It is encrypted by the key of the receiving side, e.g., the TGS.

2. AS → AP → STA: $E_{K_{STA}}[K_{STA,TGS} \parallel ID_{TGS} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{TGS}]$

Ticket-granting service exchange: to obtain service-granting ticket

With the ticket of the TGS the STA now contacts the TGS via the AP. This message contains the ID of V or the server STA wants to contact, the ticket for the TGS and an authenticator. The authenticator is encrypted by the STAs' key and consists of the current time, the username and the workstations address.

3. STA → AP → TGS: $ID_V \parallel Ticket_{TGS} \parallel Authenticator_{STA}$

The TGS responds to the request by sending a message encrypted by the key of the STA meant for the TGS sent by the AS in step 1. This message contains key for server V meant for STA, ID of V, the Time Stamp and a ticket for V.

4. TGS → AP → STA: $E_{K_{STA,TGS}}[K_{STA,V} \parallel ID_V \parallel TS_4 \parallel Ticket_V]$

STA/Server Authentication exchange: to obtain service

Now the STA sends the ticket and its authenticator to the server.

5. STA → AP → Server: $Ticket_V \parallel Authenticator_{STA}$

Table 5-2 Legends used.

$\parallel$	Concatenated data/information.
AD	Address
AS	Authentication Server
E_j	Encrypt using Key j
ID	Identity
$K_{k,l}$	Key for k to access l
TGS	Ticket Granting Server
TS_n	Time Stamp n
V	Server from which STA wants service
X→Y	From X to Y: data/information

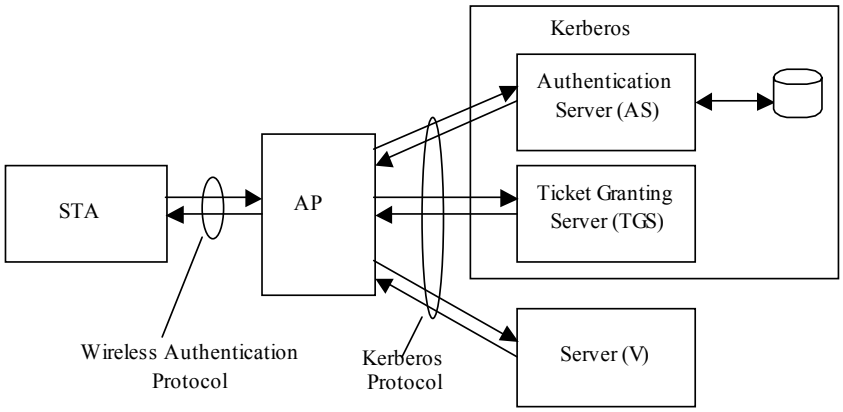


Figure 5-9 AP-level authentication.

The server responds with a Time Stamp +1 encrypted by the key meant for communication between the STA and the server, V. After this the STA can access the server.

6. Server → AP → STA: $E_{K_{STA,V}}[TS_5 + 1]$

Explanation/Definition:

$Ticket_{TGS} = E_{K_{TGS}}[K_{STA,TGS} \| ID_{STA} \| AD_{STA} \| ID_{TGS} \| TS_2 \| Lifetime_2]$

$Ticket_V = E_{K_V}[K_{STA,V} \| ID_{STA} \| AD_{STA} \| ID_V \| TS_4 \| Lifetime_4]$

$Authenticator_{STA} = E_{K_{STA,i}}[ID_{STA} \| AD_{STA} \| TS_5]$ where i = V or TGS.

5.5.2.2 AP Level Authentication

In this section two methods for authentication with the AP are proposed, see Figure 5-9:

1. Normal procedure: The AP authenticates the STA, the STA then proceeds with Kerberos authentication.
2. AP as Kerberos Element: In this case AP is a trusted element of the Kerberos network.

These two proposals are described in the following.

5.5.2.2.1 Normal Procedure

STA to AP authentication can take place by any of the following IEEE 802.11 authentication methods:

1. Open system authentication
2. Shared Key authentication

This solution is exactly the same as end-to-end authentication mechanism discussed in previous section, Section 5.5.2.1.

5.5.2.2.2 AP as Kerberos Element

The solution proposed in this section assumes that the APs in the network are known to Kerberos as authorized server [2]. Kerberos based authentication takes place first after which the AP allows data communication. In this sense the solution is somewhat similar to the IEEE 802.1X, see Section 5.8.1.3.

Kerberos Authentication service exchange: to obtain ticket-granting ticket

The station sends the request to the AP which forwards it to the AS. The request contains the ID of the STA, ID of the TGS and the Time Stamp.

1. STA → AP → AS: $ID_{STA} \parallel ID_{TGS} \parallel TS_1$

The AS responds to the STA via the AP. The response contains an encrypted message using encryption key of the STA. The response contains the key for the TGS to be used by the STA, the ID of the TGS, the Time Stamp for the response, the lifetime of the response and the ticket to access the TGS.

2. AS → AP → STA: $E_{K_{STA}}[K_{STA,TGS} \parallel ID_{TGS} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{TGS}]$

AP ticket-granting service exchange: to obtain STA/AP ticket

The STA now contacts the TGS to get access to the AP. For this purpose it sends, through the AP, the ID of the AP, the ticket that it had received of the TGS and an authenticator.

3. STA → AP → TGS: $ID_{AP} \parallel Ticket_{TGS} \parallel Authenticator_{STA}$

The TGS in return sends an encrypted message with the key for the STA to be used with the AP, the ID of the AP, the Time Stamp and the ticket for the AP.

4. TGS → AP → STA: $E_{K_{STA,TGS}}[K_{STA,AP} \parallel ID_{AP} \parallel TS_4 \parallel Ticket_{AP}]$

STA/AP Authentication service exchange: to obtain AP authentication

The STA can now authenticate itself to the AP by sending the ticket of the AP it received from the TGS and an authenticator.

5. STA → AP: $Ticket_{AP} \parallel Authenticator_{STA}$

The AP in return accepts the authentication by sending an encrypted ACK or an encrypted Time Stamp+1.

6. AP → STA: $E_{K_{STA,AP}}[TS_5 + 1]$ or, $E_{K_{STA,AP}}[ACK]$

Ticket-granting service exchange: to obtain service-granting ticket

With the ticket of the TGS the STA now contacts the TGS via the AP. This message contains the ID of the server STA wants to contact, the ticket for TGS and an authenticator. The authenticator is encrypted by the STAs' key and consists of the current time, the username and the workstations address.

7. STA → AP → TGS: $ID_{SERVER} \parallel Ticket_{TGS} \parallel Authenticator_{STA}$

TGS responds to the request by sending a message encrypted by the key of STA meant for the TGS sent by the AS in step 1. This message contains key for the server meant for the STA, the ID of the server, the Time Stamp and a ticket for the server.

8. TGS → AP → STA: $E_{K_{STA,TGS}}[K_{STA,SERVER} \parallel ID_{SERVER} \parallel TS_4 \parallel Ticket_{SERVER}]$

STA/Server Authentication exchange: to obtain service

Now the STA sends the ticket and its authenticator to the server.

9. STA → AP → Server: $Ticket_{SERVER} \parallel Authenticator_{STA}$

The server responds with a Time Stamp +1 encrypted by the key meant for communication between the STA and the server. After this the STA can access the server.

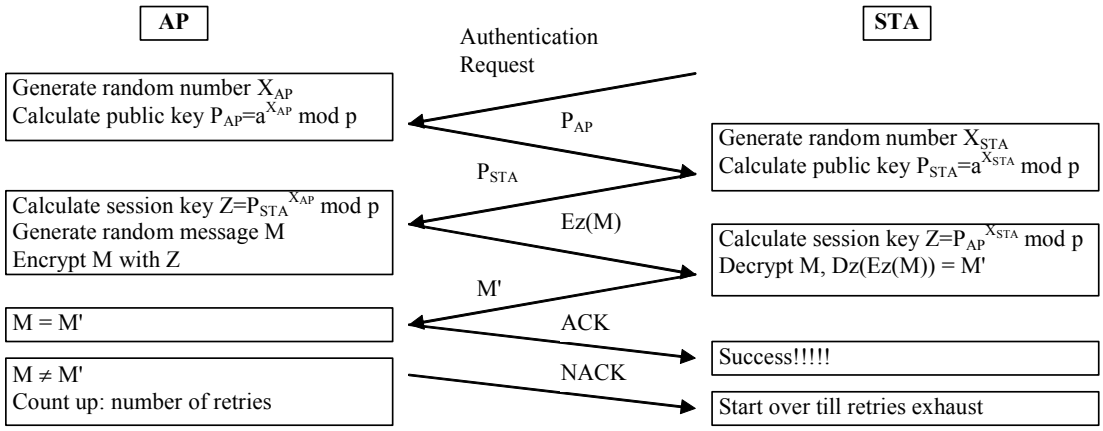


Figure 5-10 Diffie-Hellman key exchange.

10. Server → AP → STA: $E_{K_{STA,SERVER}}[TS_6 + 1]$

Explanation/Definition:

$Ticket_{TGS} = E_{K_{TGS}}[K_{STA,TGS} \| ID_{STA} \| AD_{STA} \| ID_{TGS} \| TS_2 \| Lifetime_2]$

$Ticket_j = E_{K_j}[K_{STA,j} \| ID_{STA} \| AD_{STA} \| ID_j \| TS_4 \| Lifetime_4]$ where j = AP or TGS.

$Authenticator_{STA} = E_{K_{STA,i}}[ID_{STA} \| AD_{STA} \| TS_5]$ where i = AP, TGS or SERVER.

5.5.3 Public Security Schemes

Two methods of authentication in the public environment are proposed in the following:

1. Access Point authentication: This is a wireless system level (AP/STA) authentication. The AP can provide authentication by the public key method or by using the IEEE 802.11 authentication procedures as given in Section 5.3.2.
2. Client authentication: This is the RADIUS server level authentication. When the RADIUS authentication is used the AP will work as Point to Point Protocol (PPP) server and the RADIUS client and the STA as the PPP client. Thus the CHAP/PAP process takes place directly between the PPP client and the PPP server in one hand and the RADIUS client and the RADIUS server in the back end.

The combination of the two proposals can also be used for the WLANs. The encryption can be done by using the WEP as given in the IEEE 802.11 standard or with 104 bits key (current IEEE 802.11 standard allows usage of 104 bits key). In the following a solution is discussed that combines the two proposals.

In the public key case the Diffie-Hellman key exchange procedure, [1,2], is proposed as shown in Figure 5-10. At the AP and the STA the Diffie-Hellman root number 'a' is used and modulus 'p' is used. The STA sends an authentication request to the AP on reception of which the AP generates a random number X_{AP} and calculates the public key $P_{AP}=a^{X_{AP}}$. On receiving the P_{AP} the STA calculates the $P_{STA}=a^{X_{STA}}$ and send it to the AP. The AP now calculates a session key $Z=P_{STA}^{X_{AP}}$ mod p, generates a random message M and sends $E_z(M)$ to the STA. The STA also generates the session key Z, decrypts M and sends M', the decrypted M, to the AP. If M=M' then the AP sends an Acknowledgement (ACK) to the STA else the STA tries for a given number of times, the AP also counts the number of times the STA has tried to access the AP.

The above proposal is just a basic mechanism with no protection against replay attack; time-stamp or similar method can be used to make the proposal more secure. This procedure does provide a session key.

In the procedure given in Figure 5-10 RC4 can be used for encryption as it is already defined by the IEEE 802.11 standard. With the ACK an AP can also send the shared key to be used by the WEP (RC4) for further communication. After these steps the RADIUS procedure can be used for authenticating the user with the RADIUS server. All RADIUS messages in the wireless link can be encrypted by using the session key. Once the user is authenticated by the RADIUS server the RADIUS client, the AP, will allow the user to access the network.

5.6 Qualitative Analysis of Proposed Solutions

A qualitative analysis of the proposed security solutions is done in this section. The analysis performed shows the extent to which a given solution fulfils the security requirements given in Section 5.4. Note that a threat analysis is not done in this study also, as mentioned in 5.3.2.3, several other security issues in IEEE 802.11 were found after this work was done.

5.6.1 Enterprise

In the following the requirements and the extent to which they are fulfilled by the proposed security solution for enterprise environment, Section 5.5.1, are discussed:

1. Confidentiality: Confidentiality is provided by RC4 encryption and is dependent on the freshness of the key used for the encryption. At the time this work was done RC4 with 40 bits was still considered reasonably good encryption. Encryption with 104 bits was also possible and is often used nowadays.
2. Authentication: This is taken care of by the shared key authentication process with the IV being changed every packet, see Section 5.3.2.1. A closed system (hidden SSID) can also be used together with the shared key authentication.
3. Access Control: This solution does not provide access control. Access control is only available as authentication, i.e., if a station is authenticated it is allowed to access the network.
4. Scalability: Scalability is not an issue for this solution. The same key is used by the whole system and it is up to the network administrator to add/remove users. Although, depending on key distribution mechanism used, it could be a tedious task for the network administrator.
5. Security level: The level of security can be varied depending on the user by using 104 bit key for high security and 40 bit key for low security. A mixed environment can also exist but it will mean that the level of security of the network is the same as the weakest link, i.e., limited by the 40 bits key.

Other requirements and their extent of fulfilment are discussed below.

1. Manageability: Managing the key is a very time consuming job for the network administrator. This because the network administrator will either have to manually feed the key in each AP and station or will have to ask the users to do so for their own stations. It is likely that the situation arises where the users have the wrong key.
2. Implementation: As this proposal is same as the standard IEEE 802.11 security solution, implementation is not an issue. Of course if automatic key roll-over is required then it should be implemented by the vendor. Simple implementation of automatic key roll-over is possible by allowing the manager to put the life-time of each key in the network management tool. The network management tool will invoke a new key at the end of the life-time of the key being used. Key roll-over is of course limited to 4 keys as per the standard [8]. A new set of keys can be sent encrypted by the last key (not secure), by manual means or by any other secure means.
3. Performance: There is no impact on performance as this solution is a standard implementation.

The closed system assumption could be a major issue in this environment; this issue could be taken care of by using the academic environment solutions (Kerberos based) or the public environment security solutions in this environment also. Of course Kerberos solutions will require major changes in the network while the public solutions will require some changes in the AP and the STA. Although not done here, before implementation, it is important to study the benefits of using the Kerberos and the public environment solutions in the corporate environment.

All the requirements and the extent to which they are fulfilled are summarized in Table 5-3.

From the above discussion it is clear that the solution does not fulfil the requirement of access control. The known problem of WEP concerning key refreshing is left in the hands of the network administrator or to the implementation of the key roll-over mechanism which can be done quite easily. 104 bits key should be used for better confidentiality.

5.6.2 Academic

This section discusses the extent to which the requirements are fulfilled by the solutions discussed in Section 5.5.2.

5.6.2.1 End to End Authentication

1. Confidentiality: A per session encryption is provided by the session key used in Kerberos.
2. Encryption: The encryption is provided by the DES algorithm in Kerberos v4. Kerberos v5 allows a choice of different encryption algorithms.
3. Authentication/Access Control: The AP level authentication is taken care of by using open system authentication this gives the STA access to the AP which means the issue of a rogue AP remains. The authentication and the access control at the network level are taken care of by Kerberos.
4. Scalability: The scalability is not a problem for the wireless part. It depends totally on the Kerberos protocol.
5. Compatibility: This scheme follows the Kerberos method totally thus it is compatible with the Kerberos except for the point that the AP is not authenticated/registered at the Kerberos.
6. Impact on Network: The only impact on the existing network will be that of adding the APs, i.e., no impact.

Table 5-3 Enterprise Solution

Requirement	Extent fulfilled
Confidentiality	++
Authentication	+
Access Control	-
Scalability	+++
Security Level	+
Manageability	-
Implementation	+++
Performance	+++
Legends used	
Excellent	+++
Good	++
OK	+
Does not fulfil	-

Other requirements:

1. Manageability: This is not a big issue in this solution as each STA is working as any other Kerberos client and the network is not changed. No added management overhead is there beyond what is needed for the deployment of a WLAN network.
2. Implementation: A standard Kerberos protocol can be implemented in each STA which requires negligible implementation effort in terms of security. With Microsoft Windows being shipped with Kerberos implementation, this requirement can be considered fulfilled almost always.
3. Performance: Overall there will be no effect on the performance of the network, this is with the initial assumption that academic environment will use Kerberos. Looking from the point of view of the wired network part of the network, the performance will be as good as any Kerberos client with some effect due to the wireless channel. With the WEP turned off, there will be no effect on the performance due to the encryption used by Kerberos. Looking from the point of view of the wireless part of the network, the performance will be affected slightly because the number of messages that are sent and received when using Kerberos is far more than that when using the IEEE 802.11 security solution. Such performance and security trade-off should be acceptable.

The biggest problem of this proposal, as mentioned in some of the points above, is the authentication of the AP to the Kerberos and the STA and the AP to each other. This makes the network vulnerable to attacks by unregistered APs. A fake AP can be put in the network that can collect all the information making it easier for an intruder to enter the network. An intruder can also try to simply enter the network by guessing the passwords while physically being outside the campus (the academic environment) in which the network is installed.

IEEE 802.11 issue of authentication at the AP level is not solved with this proposal.

5.6.2.2 AP level Authentication: AP as Kerberos Element

1. Confidentiality: A per session encryption is provided by the session key used in Kerberos.
2. Encryption: The encryption is provided by the DES algorithm in Kerberos v4. Kerberos v5 allows a choice of different encryption algorithms.
3. Authentication/Access Control: The authentication and the access control takes place according to Kerberos both at the AP and Kerberos (wireless and wireline) level. The AP is part of the Kerberos thus the STA also needs a ticket to access the AP thus providing the AP level authentication. The AP will allow preliminary messages to be sent to the TGS. After the preliminary messages the STA should authenticate itself to the AP with the ticket without which no further communication will be allowed.
4. Scalability: The solution proposed is as scalable as the Kerberos protocol; it does not affect the scalability of the Kerberos based network both in terms of number of users and the network size. The limitation might be the number of APs the Kerberos server can handle.
5. Compatibility: This scheme is totally compatible with Kerberos. The APs should be made a Kerberos element. The APs will be required to check the Kerberos messages so as to authenticate the STAs and control the authentication and the data traffic.
6. Impact on the Network: New APs must be added and Kerberos server must be informed of the APs as server.

Other requirements:

1. Manageability: Once all the APs are defined as servers the level of manageability will be the same as that of the normal Kerberos network assuming that there is no Kerberos related problems with the APs once they are implemented in the network.

2. Implementation: Kerberos must be installed in all STAs (this does not require any change in WLANs) and the APs where the STAs will be as a client and the APs as server. The APs should be able to check the traffic of each STA going through it so as to know when to allow the data traffic.
3. Performance: Overall there will be no effect on the performance of the network; this is with the initial assumption that the academic environment will use Kerberos. Compared to the end-to-end authentication proposal there is extra signalling required for the authentication of the STA to the AP. Looking from the point of view of the wired part of the network the performance will be as good as any Kerberos client with some effect due to the wireless channel. With the WEP turned off, there will be no effect on the performance due to the encryption used by Kerberos. Looking from the point of view of the wireless part of the network, the performance will be affected slightly because of the number of messages that are sent and received when using Kerberos is far more than that when using the IEEE 802.11 security solution. Such performance and security trade-off should be acceptable.

This proposal solves the issue of rogue AP as identified in end-to-end case in Section 5.5.2.1 by making the APs an element of the Kerberos network. The key distribution issue and the authentication issue of IEEE 802.11, see Section 5.3.2.3, is also solved by this proposal.

5.6.2.3 Comparison

Table 5-4 gives a comparison for the Kerberos based proposals.

As the end-to-end authentication and the normal procedure for authentication with the AP were discovered to be the same, their results are given together. For these two proposals the result is discussed for both the shared key and the open system based IEEE 802.11 authentication mechanisms. The open system authentication looks at first sight like a good solution but the issue of the authentication and the access control is too big. A rogue AP is possible in this proposal. The shared key authentication simply creates extra overhead and the need for increased management without any improvement in the level of security.

The AP as a Kerberos element solves the issues of the end-to-end authentication. This solution can be considered as the best solution but the issue here is the impact on the network in terms of adding APs as Kerberos element and implementation of Kerberos on APs. Still this trade-off should be acceptable seeing from the point of view of the impact on the network and the implementation on one side and the security on the other side.

Table 5-4 Kerberos Solutions Comparison.

Requirement	**End-to-End & Normal Procedure**		**AP as Kerberos Element**
	Shared Key Authentication	*Open System Authentication*	
Confidentiality	++	++	+++
Encryption	+++	+++	+++
Authentication / Access Control	-	-	+++
Scalability	+++	+++	+++
Compatibility	+++	+++	+++
Impact on Network	+++	+++	++
Manageability	+	+++	+++
Implementation	+++	+++	+
Performance	++	+++	+++
Legends used			
Excellent	+++		
Good	++		
OK	+		

5.6.3 Public

One of the problems with the proposed solution is the bogus or rogue AP. In case of Diffie-Hellman procedure bogus AP can be placed in the network if the values 'a' and 'p' are known. If only RADIUS is used then the bogus AP can be very easily used because the RADIUS does not authenticate the AP to the STA neither is there any trust relation between the AP and the STA as in the Diffie-Hellman case.

1. Confidentiality: The bogus AP, as explained above, will be the only limitation for confidentiality else the system will be as secure as a WEP system.
2. Authentication/Access Control: Here the problem of the bogus AP will be faced. As there is no mutual authentication between the AP and the STA a bogus AP can be placed which can easily collect the username and the password of anyone trying to login the network.
3. Compatibility: The scheme (with or without Diffie-Hellman) uses the standard RADIUS process which is totally compatible with the public WLAN. The Diffie-Hellman procedure is not compatible to the IEEE 802.11 standard but if implemented above the MAC layer there will be no compatibility issue.
4. Scalability: The solution is scalable in terms of the number of users at the same time the solution is scaleable in terms of the network size. If there is any limitation then it will be on the part of RADIUS.
5. Impact on Network: As RADIUS is commonly used there will be no impact on the network.

Other requirements:

1. Manageability: RADIUS being a common and widely used, there will be no extra extra management required than that which comes with the deployment of the WLAN.
2. Implementation: Diffie-Hellman will have to be implemented on the WLAN APs and the STAs. Passing of key from Diffie-Hellman to the WEP should also be implemented. As the Diffie-Hellman procedure is very simple the implementation will not be much work. The RADIUS client should be implemented on the APs. As the APs often have a RADIUS client, implementation concerning RADIUS is a non-issue.
3. Performance: With the addition of the Diffie-Hellman procedures at least six extra messages will have to be transmitted on the wireless link while with RADIUS there will be at least four more messages. A total of 10 extra messages will be sent over the wireless medium which will not have much impact on the performance.

Table 5-5 summarizes the extent of the fulfilment of requirements.

Table 5-5 Public Solution.

Requirement	Extent fulfilled
Confidentiality	++
Authentication / Access Control	-
Compatibility	+++
Scalability	+++
Impact on Network	+++
Manageability	+++
Implementation	+
Performance	++
Legends used	
Excellent	+++
Good	++
OK	+

5.6.4 Proposal Acceptance by IEEE 802.11i

Based on the security solutions proposed in Section 5.5, some ideas were proposed to IEEE 802.11i [12] and the use of these solutions on the MAC layer was patented. One of the main points of the proposal was to align the IEEE 802.11 standard with the IETF and thus avoid re-inventing the wheel; this is also reflected in all proposed solutions in Section 5.5.

Comparing the draft standard, given in Section 5.8, and the proposals discussed in Section 5.5, the first thing one observes is that the members of the IEEE 802.11i agreed with 'not re-inventing' the wheel and using the upper layer solutions. By using the upper layer solutions the standard becomes more scalable. The proposal of using higher layer for key exchange was also accepted, while certification is also possible using variation of the EAP.

5.7 Novel Access Control Protocol

Most of the proposed solutions in Section 5.5 do not fulfil the access control requirement. So as to solve the issue of the access control a novel access control protocol is proposed in this section. This solution was patented by the author.

A major part of this proposal is also used by the IEEE 802.11f standard although the solution was never proposed by the author to the standard [10]. Several other studies recently going on in the field of seamless handover and context transfer use very similar thoughts as proposed in this section.

As explained in Section 5.8.2, the IEEE 802.11f draft standard makes use of proactive context transfer. The context is basically similar to the profile discussed in the proposed access control protocol. The proactive context transfer is similar to the transfer of profile to the neighbouring APs so as to avoid re-authentication from the server. In the proposal it is a must to have key distribution to the APs which is also reflected in the draft standard [10].

In the following requirements for access control protocol are given, see also Figure 5-11:

1. Allow valid users to access all the APs and the files (depending on the user access rights and the organization regulations) in the server.
2. Give a network administrator full access to the APs including the right to load new firmware.
3. Give limited access (e.g., controlled roaming, limited access to services/servers) to certain users (e.g., guests, test).
4. Present a solution which can be used with most existing security schemes for the WLANs.

5.7.1 Proposed Access Control Protocol

So as to fulfil the above mentioned requirements an access control protocol is proposed in this section. The proposed access control protocol makes use of different profiles depending on type of users, e.g., guest, test etc. The profiles are encrypted by a key which is the same throughout the network, i.e., all the APs and the Server have the same key. Any encryption algorithm can be used. Profiles can also be given different levels of priority thus providing distinction within a profile set also, e.g., a researcher is given higher priority than the CEO of the company.

The first step is to give all the users a profile, for e.g., 0 = default profile, i.e., no rights at all, 1 = normal user profile, 2 = test profile, 3 = master, 4 = guest etc.. Each profile is related to certain set of APs, for e.g., normal user gets access to all APs but the user cannot perform test or make changes in the AP; master has access to all the APs and can modify them by uploading new software etc.; test profile will give access to the APs in test area the user with this profile will be a normal user when accessing other APs; guest will have access to the APs in guest area only. Further each profile is associated with a set of services/servers. The following sections describe the working of the proposed access control protocol. A Message Sequence Chart (MSC) is given in Figure 5-12.

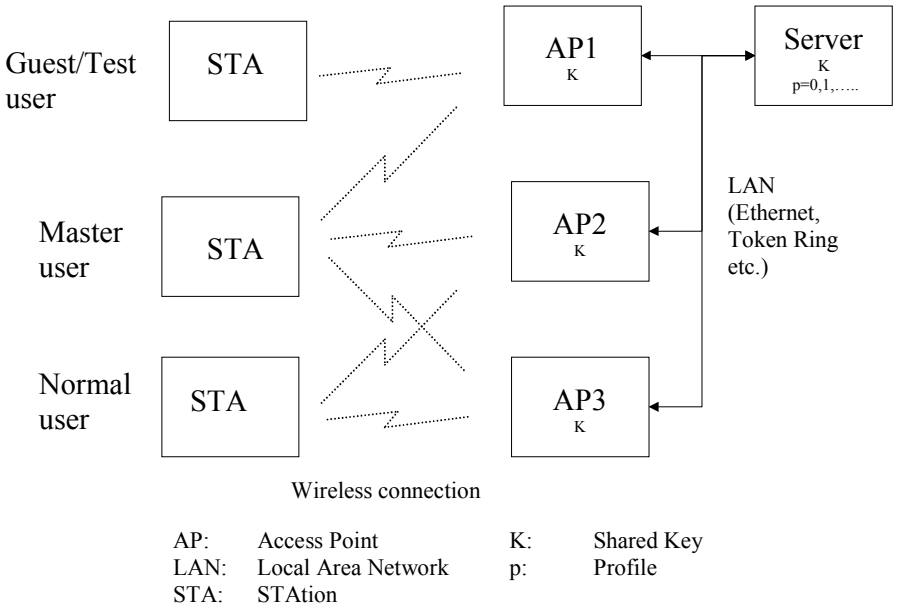


Figure 5-11 A wireless LAN network.

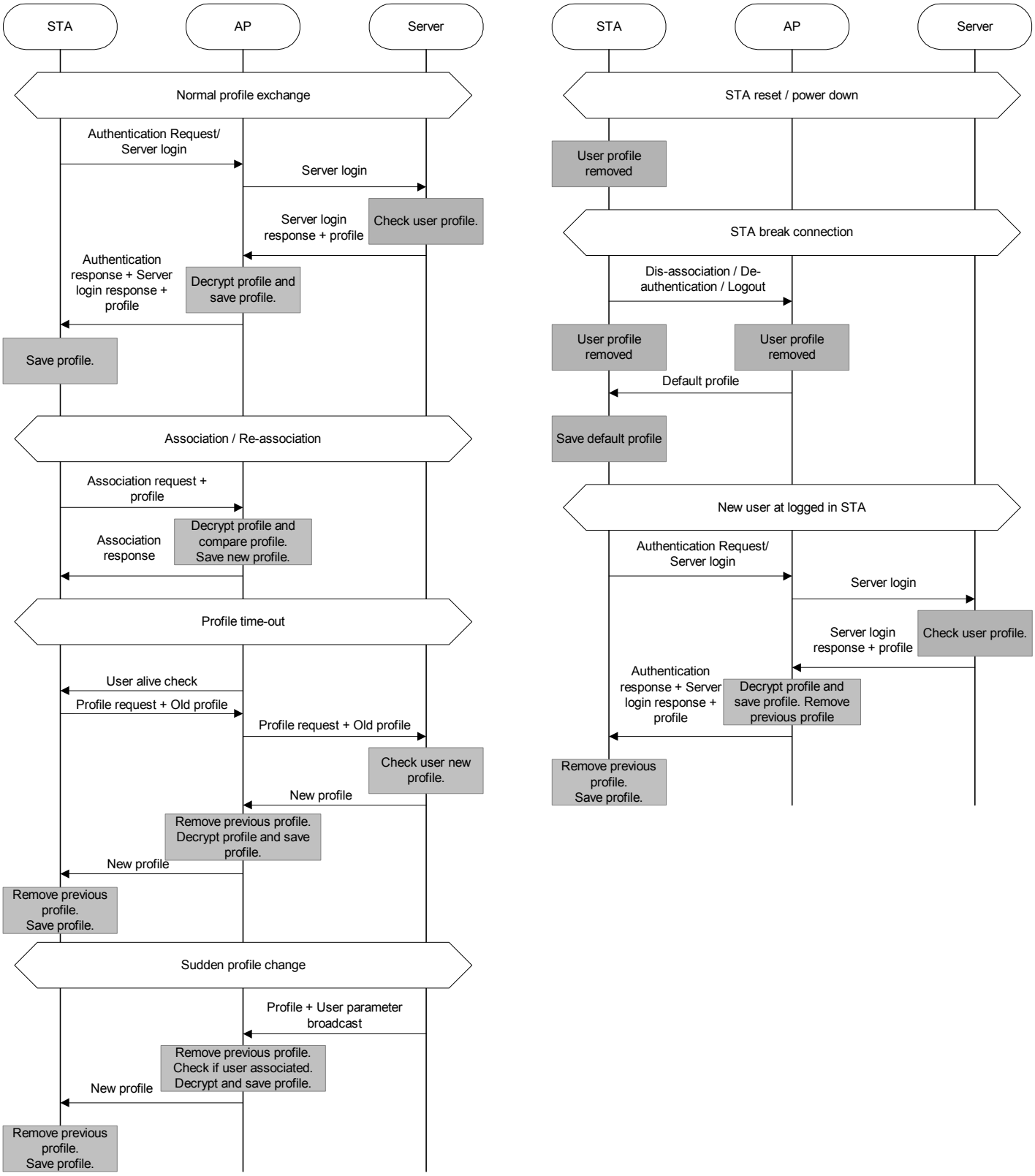


Figure 5-12 Access control MSC.

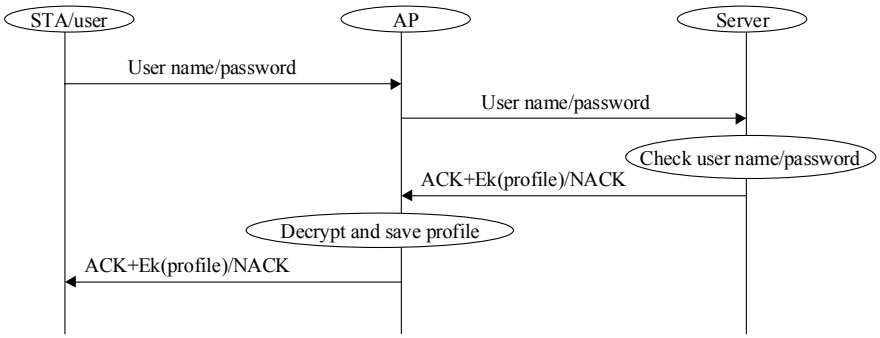


Figure 5-13 User login.

5.7.1.1 Normal Procedure

The normal protocol procedure is explained in following steps.

1. The user requests for authentication to the AP which is sent to the server. At the server, the profile of the user will be related to the user password, the login name or any kind of identification used by the server to recognize the user.
2. The server sends the login response with the user profile if the authentication is successful. Note that any form of authentication mechanism can be used including, for example, RADIUS.

   The AP also decrypts and saves the profile.

   The server informs all the 'related APs' in the network of the users' profile. This can be done by encrypting the profile by a shared key known to all the APs in the network and the server that stores the profiles. The network manager can change the shared key in all the APs in one go by using a network management tool or any other key exchange/distribution mechanism can be used. For stronger security the key must be changed frequently, the frequency will depend on the network manager and security policy of the network. Some mechanism of authentication and key distribution between the APs and the server could be implemented for example RADIUS or Kerberos.

   'Related APs' can be the APs near the current AP being accessed by the STA or most likely the APs where the user will move to. Different methods can be used for creating/finding the related APs.

   Steps 1 and 2 are also given in Figure 5-13.

3. The STA saves the profile.

   The encrypted profile is stored in the STA only while it is switched on, it is removed when the STA is switched off or the user logs out.

   When a user logs out either the STA can remove the profile or the server can send a default profile that is common to all the users and provides no access privileges. Similarly the AP can either remove the profile and the STA from its list or copy the default profile for that particular STA.

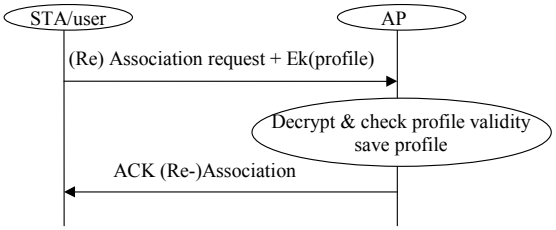


Figure 5-14 Successful association.

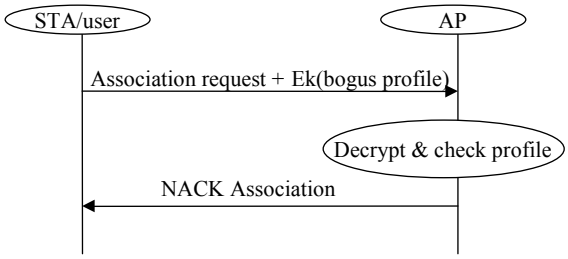


Figure 5-15 Association attempt with bogus profile.

4. When a STA (Re-)Associates with a AP the encrypted profile is sent to the AP during association, Figure 5-14.
    a. The AP decrypts the profile and thus knows the extent of access allowed to the particular user/STA and the APs to which the user is allowed to access. As the AP most probably has the profile already (sent by the server), the profile sent by the user/STA is a form of quick authentication.
    b. An AP will not accept ((re-) associate) a user/ STA without a profile or with a bogus profile, Figure 5-15.
    c. A (re-) association request must always have an encrypted profile.

    APs can be modified to provide multiple users per STA. This means the AP must have a STAs' MAC address, the user names and the profile of each user
5. When a STA is reset or the power is turned off the profile is removed from the STA and depending on the situation a default profile is saved. The default profile does not give access to the network.
6. Similar to point 5, if the STA wants to break connection the profile is removed in both the STA and the AP and the default profile is saved in both places.
7. If a new user logs in through a STA being used by another user (still logged in), the profile of the previous user can be removed or, both the profiles can be kept. In the present AP the profile with highest priority or, least priority (depending on organization) will be kept. When one of the user logs out his profile will be removed from the STA only if two or more profiles are being maintained. When such STA moves to a new AP the profile with highest priority or, least priority (depending on organization) is sent during association.

    The most preferred case is with only one profile per STA.

5.7.1.2 Profile Time-out or Aging

In general profiles will be changed and modified when the password expires but for security reasons the network manager would like to modify the profile more often. This means there must be some kind of aging parameter in the profiles to notify the concerned of the expiry. Of-course the aging process is related to timing and can be solved as follows:

1. Set a time-out period for the profiles (individually, depending on type of profile or, same for all profiles). The time-out period is maintained both at the AP and the STA.
2. Give an encrypted and an un-encrypted time-stamp and time-out period together with the profile. The un-encrypted time-stamp and the time-out pair will be used by the STA to know when to ask the new profile. Encrypted part will be kept by the AP to validate a new profile request from the STA.
3. When a profile time-out occurs the STA will request for a new profile.

4. The AP will check the time-out of the profile for the particular STA/user. If the request is valid the AP will forward the new profile request to the server. If the request is not valid an alarm will be sent to the server together with the available STA/user information.
5. The server will send the new profile on the APs request.

5.7.1.3 Sudden Profile Change

It is possible that the profile must be changed without aging. This type of profile change is called as sudden profile change. When a sudden change in profile occurs; the APs and the STAs must be informed of this change, the solution for this is given in the following:

1. The server broadcasts the profile change to all the APs.
2. The AP associated to the STA reads the profile.
3. The AP sends the profile to the STA.
4. The STA changes the profile.

5.7.1.4 Controlled Roaming

It is possible that users must be contained in certain areas depending on their profile. Examples would be guests allowed to access the network only from the showroom or the test engineers allowed to access the network for test purposes only in assigned areas. This is called controlled roaming which can be done as follows:

1. Each profile is given a number of MAC addresses of the APs to which it is allowed to communicate. For the master and the normal users this field might not be there as such profiles give right to access all the APs in the network.
2. When a STA (re-)associates or in any other case if it send its profile to a AP the AP will check if it is listed in the MAC address list of the profile; the AP will also have the profile sent by the server. For the master and the normal users this might not be needed.

5.7.2 Access Control Proposal Benefits and Drawbacks

The proposed scheme requires the present system to maintain the user profiles at the server. If each user is assigned a fixed STA then a STA/user profile can be maintained at the server. The scheme is very secure as the profiles are encrypted by a key known only to the APs and the Server which are part of the network. The network manager has full control to change the encryption key when required. The scheme described can be used not only to limit the access of a user to the network but also to contain a certain set of users to a limited area and the APs. The problem of roaming is also solved by the proposed access control protocol.

The proposed access control protocol solves the following:

1. The network manager will have full control on the accessibility of the network by the user
2. It gives access control at the AP level.
3. It distinguished between the types of users.
4. The users cannot change their own profile.
5. The profile can be decrypted only by the trusted APs and the server, i.e., the bogus APs cannot work in a network using the proposed access control protocol.
6. The user can roam from one AP to other without logging in (giving password/username) to the server every time thus better service can be provided as the handover delay is decreased.
7. The aging process makes the system more secure.

8. The “sudden change in profile procedure” also gives extra security, e.g., from a guest who has left the building, an employ who has resigned, etc.
9. The proposed scheme gives access control at the AP for a given user. This access control is for the services, the servers etc. to which a user is allowed to access.
10. This proposal can also be used for inter-stakeholder handover and in vertical handover to maintain the security, the service quality, provide seamless mobility etc.

As a whole the scheme is very secure and can be implemented (flexible) on any WLAN system. The use of this scheme can be extended to other wireless systems for example, mobile communications. There are of course some drawbacks in the proposal as given below:

1. A common encryption key is used in the network between the server and the APs. If this key is compromised then the network will be in the control of the intruder. The solution for this is to use good negotiation procedures between the server and the APs and to change the key as often as possible.
2. Putting the profiles in the STAs could mean that an intruder could somehow copy this profile and reuse it. There are solutions proposed to refresh the profile in case there is a stolen profile and it is known by the network administrator. One of the solutions could be simply not to use profiles in the STAs but to transfer the profile between the APs in a network.

5.8 IEEE 802.11i and IEEE 802.11f

In this section an overview of IEEE 802.11i, security enhancements of IEEE 802.11, and IEEE 802.11f, Inter Access Point Protocol, are given. IEEE 802.11f was recently accepted as a standard. A short description of IEEE 802.1X is also given as it plays an important role in future WLAN security solutions.

5.8.1 IEEE 802.11i

The IEEE 802.11i is a security enhancement standard currently in draft stage.

As the IEEE 802.11i standard is not yet available, the IEEE 802.11 vendors are giving some security solutions to bridge the gap. These solutions started with extended WEP key size, which was adopted by the standard, providing RADIUS and MAC address based authentication, the IEEE 802.1X port based user authentication and the AES based encryption.

Seeing the market situation, Wi-Fi, the IEEE 802.11 interoperability industry alliance, is introducing the Temporal Key Integrity Protocol (TKIP) as a simple but secure intermediary solution [11]. This solution is usually known as the Wi-Fi Protected Access (WPA) and is already available from some vendors. The WPA provides enhanced data encryption through the Temporal Key Integrity Protocol (TKIP), the user authentication via IEEE 802.1X and EAP, mutual authentication and, for ease of transition, Wi-Fi certified products are software upgradeable.

This section gives an overview of the current IEEE 802.11i draft.

5.8.1.1 The Robust Security Network

IEEE 802.11i defines a Robust Security Network (RSN). A RSN provides a number of additional security features not present in the basic IEEE 802.11 architecture. These features include:

- enhanced authentication mechanisms for both the APs and the STAs;
- key management algorithms;
- dynamic, association-specific cryptographic keys; and
- an enhanced data encapsulation mechanism, called WRAP.

A RSN makes extensive use of protocols above the IEEE 802.11 MAC layer to provide the authentication and the key management. This allows the IEEE 802.11 standard to both take advantage of the work already done by other standardization bodies as well as to avoid duplicating functions at the MAC layer that are already performed at the higher layers. A RSN introduces several new components into the IEEE 802.11architecture, these are:

- IEEE 802.1X Port: Present on all the STAs in a RSN and resides above the 802.11 MAC. All data traffic that flows through the RSN MAC also passes through the IEEE 802.1X Port.
- Authentication Agent (AA): This component resides on top of the IEEE 802.1X Port at each STA and provides for the authentication and the key management.
- Authentication Server (AS): The AS is an entity that resides in the network that participates in the authentication of all STAs (including the APs). It may authenticate the elements of the RSN itself or it may provide material that the RSN elements can use to authenticate each other.

As the IEEE 802.1X plays an important role in the IEEE 802.11i, it is explained separately in Section 5.8.1.3.

5.8.1.2 Security Goals

A RSN does not directly provide the services. Instead, a RSN uses the IEEE 802.1X to provide the access control and the key distribution, and the confidentiality is provided as a side effect of the key distribution. Some of the security goals of the IEEE 802.11i are:

- Authentication: A RSN-capable IEEE 802.11 network also supports the Upper Layer Authentication, based on the IEEE 802.1X. The Upper Layer Authentication utilizes the protocols above the MAC layer to authenticate the STAs and the network with one another.
- Deauthentication: In a RSN using the Upper Layer Authentication, the deauthentication may result in the IEEE 802.1X controlled port for the station being disabled.

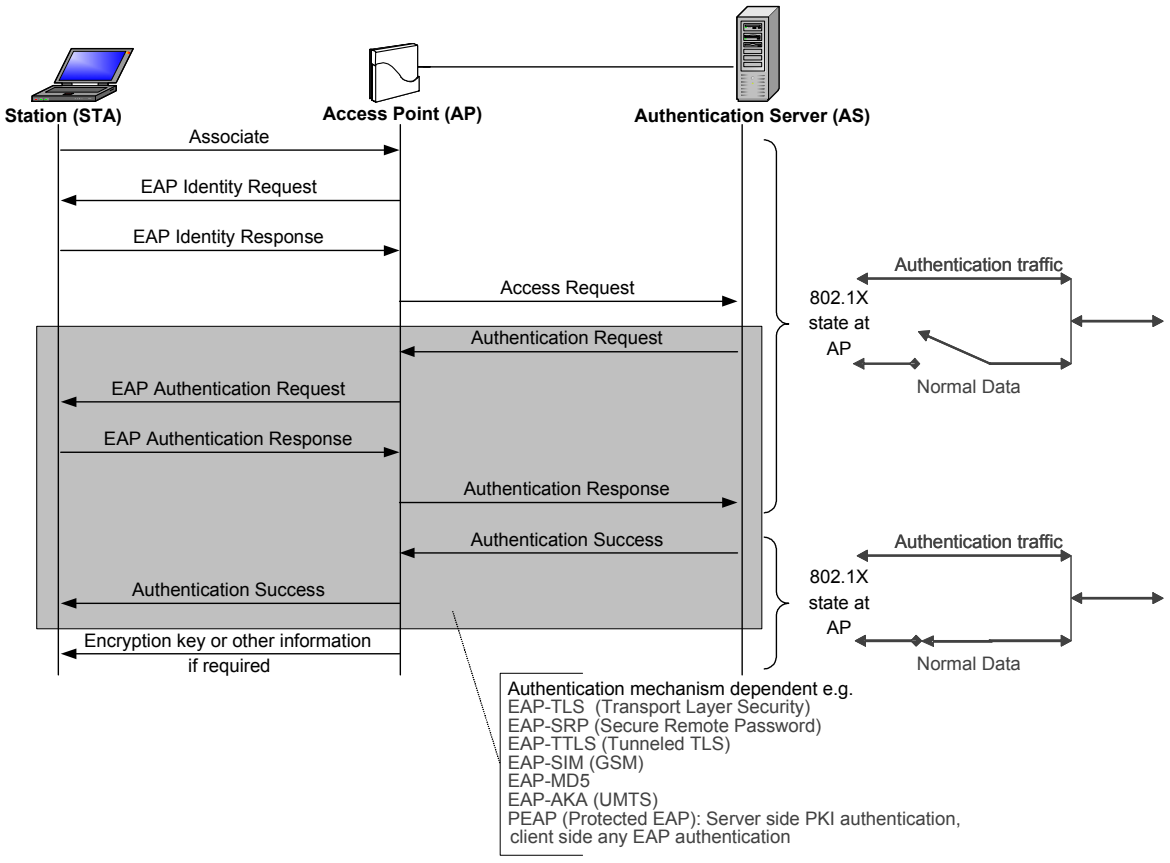


Figure 5-16 IEEE 802.1X EAPOL message sequence chart.

- Privacy: The IEEE 802.11i provides three cryptographic algorithms to protect the data traffic. Two are based on the RC4 algorithm defined by RSA and the third is based on the Advanced Encryption Standard (AES). This standard refers to these as WEP, as TKIP and as WRAP. A means is provided for the stations to select the algorithm to be used for a given association.

  The Wireless Robust Authenticated Protocol (WRAP), adopted by IEEE 802.11i, is based on the Advanced Encryption Standard (AES) and the Offset Codebook (OCB).

- Key distribution: The IEEE 802.11i supports two key distribution mechanisms. The first is the manual key distribution. The second is the automatic key distribution, and is available only in a RSN that uses the IEEE 802.1X to provide the key distribution services. A RSN allows a number of authentication algorithms to be utilized. The standard does not specify a mandatory-to-implement Upper Layer Authentication protocol.

- Data Origin Authentication: This mechanism is available only to stations using the WRAP and the TKIP. The data origin authenticity is only applicable to the unicast traffic.

- Replay Detection: This mechanism is also available only to stations using the WRAP and the TKIP.

5.8.1.3 IEEE 802.1X

IEEE 802.1X is the Standard for Port based Network Access Control which applies to the IEEE 802.3 Ethernet, the Token Ring and the WLAN [14]. Based on the Point to Point Protocol (PPP) Extensible Authentication Protocol (EAP) [15], IEEE 802.1X Extends the EAP from PPP to the LAN Applications. This standard defines the Extensible Application Protocol over LANs (EAPOL), a protocol which provides a framework for negotiating the authentication method. It defines no explicit authentication protocol itself, the EAPOL is extensible to many authentication protocols. It must be made clear that, IEEE 802.1X is not an authentication protocol or a guarantee of a secure authentication algorithm for the wireless applications.

Some of the terms used in the IEEE 802.1X and its relation with the WLAN are explained below.

- IEEE 802.1X Supplicant: The entity at one end of the point-to-point LAN segment that is being authenticated. The software on the STA which implements the EAP.

- Authenticator: The entity that facilitates authentication of the entity attached to the other end of that link. The software on the AP which forwards the EAP control packets to the Authentication Server, enables/blocks the port, uses received information.

- Authentication Server: The entity that provides an Authentication Service to the Authenticator. The Radius Server, the Kerberos Server, or the Diameter Server. It can be integrated into the AP.

The Message Sequence Chart (MSC) of the IEEE 802.1X is given in Figure 5-16. The IEEE 802.1X has two ports; the data port at the authenticator is open until the supplicant is authenticated by the authentication server. Once the supplicant is authenticated the data port is closed and normal data communication can take place. The IEEE 802.1X together with the EAP allows several different methods of authentication some of which are also mentioned in the figure, these are:

1. EAP-Transport Layered Security (TLS)
2. EAP-Secure Remote Password (SRP)
3. EAP-Tunnelled TLS (TTLS)
4. EAP-Subscriber Identity Module (SIM) of Global System for Mobile Communications (GSM)
5. EAP-Authentication and Key Agreement (AKA) of Universal Mobile Telecommunications System (UMTS)

6. EAP-Message Digest 5 (MD5) and
7. PEAP or Protected EAP

5.8.2 IEEE 802.11f

The IEEE 802.11f Inter Access Point Protocol (IAPP) is a communication protocol, used by one AP to communicate with the other APs. It is a part of a communication system comprising the APs, the STAs, a backbone network and the RADIUS infrastructure [10].

The RADIUS servers provide two functions:

1. mapping the ID of an AP to its IP address and
2. distribution of keys to the APs to allow the encryption of the communications between the APs.

The function of the IAPP is to facilitate the creation and maintenance of the wireless network, support the mobility of the STAs and enable the APs to enforce the requirement of a single association for each STA at a given time.

One of the services the IAPP provides is proactive caching. Proactive caching is a method that supports fast roaming by caching the context of a STA in the APs to which the STA may roam. The next AP's are identified dynamically, i.e., without management pre-configuration, by learning the identities of neighbouring the APs.

5.9 Future Generation Systems and Security Needs

The current trend in the wireless industry is towards heterogeneous networks, the most visible example is the work going on towards WLANs and 2.5G/3G interworking. The future will see further development of such interworking which brings heterogeneity in networks.

In case of the heterogeneous networks the first thing to understand is the trust level required for inter-domain (or inter-stakeholder) and the vertical handover, issues of authentication in case of the handover, the key management, the accounting and billing, the location privacy, the infrastructure security, the secure attachment and detachment, the lawful interception, the scalability and the management. Besides requirements from security issues, other requirements like: maintaining the security level during mobility, impact on the network and impact of the security solution on the resources of the network and the device must also be considered. The whole dimension of security issue changes when the issue of more than one stakeholder is considered, i.e., 3G can be operated by one stakeholder and the WLAN by another stakeholder. Some of these issues are discussed in further detail below.

Handover can happen between different technologies and even between unknown operators. This will require the creation of trust between the two operators. Creation of trust can be done before hand or on-the-fly during the handover.

Authentication mechanisms may vary depending on the heterogeneous technologies and/or on the network policies. When a device is handed over, authentication will take place once again this may be very bad for some types of services. Similarly different key management mechanisms will be deployed by different networks, how to handle it and how to do key management is a major issue especially for a devices moving from place to place.

When a user moves from one network to the other the Service Level Agreement (SLA) must be communicated between the two networks. This negotiation phase can give the possibility to an intruder to cause changes or even highjack a connection. The SLA will be related to cost of the service also thus bringing in the issues related to the accounting during handover and the billing. If handover happens during an active session of a service especially between different administrative domains, some questions arise, like how to keep the integrity and the consistence of accounting record and how to assure non-repudiation.

A firewall is often used by the networks and it becomes especially an issue for IPSec, Mobile IP and Network Address Translator (NAT) [19]. NAT is considered to be of use for IPv4 and in the future IPv6 will be used but it will be long before IPv4 is completely replaced by IPv6.

Lawful interception in a operators' network is required by several countries and is based on laws of the country. Location Privacy on the other hand is a double edged sword; the users do not want their location to be known while the governments are setting requirements on the location information for emergency cases.

Although not necessarily related directly to the security, it will be very important that security mechanisms at different layers talk to each other and maybe share the security needs. During handover it will be necessary that lower layers inform, for example, layer 3 when handover is taking place.

Header compression is important for efficient use of the wireless medium. A malicious header compressor could cause the header decompressor to reconstitute packets that do not match the original packets but still have valid IP, UDP and RTP headers and possibly also valid UDP checksums. Such corruption may be detected with the end-to-end authentication and the integrity mechanisms which will not be affected by the compression. The denial-of-service attacks are possible if an intruder can introduce packets onto the link. The encrypted or the authenticated packets cannot be compressed. Compressing such packets will not provide end-to-end security but will lead to network-to-end or network-to-network security. Also, most protocols available for the security and the mobility for example IPSec and any Mobile IP will require a lot of message exchange which uses valuable capacity and battery life. Especially if the user is very mobile the total message exchange will too much. This again needs to be studied while keeping the security requirements in mind [20].

Besides a security attack, it is possible that an authorized user can misuse the resources, this brings in the need for the secure access control, monitoring of the use of the resources and the management of resources. There is also a need for security of the infrastructure, which means security of the network elements like router, the server, the customer information etc.. An attack on these elements of the network can lead to crashing of the whole network and the business [21].

Attaching securely to a network is a very important issue. When one first tries to attach to a network lot of information is sent and received. Normally the username and the password are communicated but besides issues to such well know items one of the major security issues for the IP network is the Dynamic Host Configuration Protocol (DHCP) which is not secure. Another point is the secure detachment from network. It is possible that an intruder can simply observe (sniff) the detachment process or can simply continue using the connection after a user has left. This can lead to misuse of the network resources, an increase in the cost for the legitimate user, etc..

Negotiation of the service; be it in terms of the quality requirement or the payment, should be done securely. Intruding in this phase can lead to overcharging or a decrease in quality or even denial of service. The negotiation of service will also lead to a SLA and this should be maintained throughout the communication period.

A network needs to be managed and security holes exist in management solutions. Insecure management methods can lead to control of a network by an intruder.

The scalability of the security solutions is very important. High mobility will require that the security solutions are not only limited to a place or number of people. The scalability also means that the security solution should be flexible enough to modify and to fulfil the security needs as the network changes.

Ad-hoc networks are expected to play an important role in the future. There are several security issues that the ad-hoc networks will face; they also face issues related to variety of devices that can communicate with each some of them might have a powerful CPU, a lot of memory etc. while others might exist which have severely restricted (peanut) CPU and battery power.

5.10 Conclusions

The chapter gives background information on security threats and goals. The security solutions like RADIUS and Kerberos are also discussed in the chapter. The current IEEE 802.11 security solution and the security issues related to it are also presented in the chapter.

This chapter presents three envisaged WLAN usage environments, academia, enterprise and public and proposes their security requirements. Some of the common security requirements are backward compatibility to existing security solutions, scaleability, manageability, authentication, confidentiality and access control.

For the enterprise environment the existing security solution of the IEEE 802.11 is found to be good enough, if the key management is done correctly, although the access control remains an issue. The academic environment makes use of Kerberos based security solution. Two solutions are proposed in this chapter for the academic environment. The best solution is the one providing authentication at the Kerberos and also at the AP level. In the public environment a Diffie-Hellman based public key solution together with RADIUS is proposed, it does fulfil most of the requirements but not all of them and the issue related to bogus AP also remains.

Some ideas for security in the WLANs were also presented to the IEEE 802.11i committee; parts of this idea were accepted by the standardization committee. The accepted points are the use of higher layers as much as possible and the use of the IEEE 802.1X standard.

For the three considered WLAN usage environments the access control is the main problem. For this purpose a novel access control protocol based on the user profile is proposed (applied for patent by the author). The profile is stored at the server together with the username, the password etc.. The proposed solution on the access control is very secure. When combined with the security solutions presented for the three envisaged environments all security requirements are fulfilled. The access control protocol proposed in this chapter can also be used for seamless handover during the vertical and the inter-stakeholder handover to provide seamless mobility while maintaining the security level and the service quality.

The access control protocol was proposed prior to the IEEE 802.11f standard. Although never presented to the standardization committee, the proposed access control protocol is very similar to the IEEE 802.11f standard. The biggest similarity is the use of context transfer which in the case of the proposed access control solution is the profile. Other similarities are the key distribution to APs which is also done in the proposed solution and the distribution of context, in the proposed case profile, to the neighbouring APs.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, July 1998.

[2] A.R. Prasad, H. Moelard and J. Kruys, “Security Architecture for Wireless LANs: Corporate & Public Environment”, VTC 2000 Spring, May 2000, pp. 283-287.

[3] A.R. Prasad, A. Kamerman and H. Moelard, “IEEE 802.11 Standard”, Chapter 3 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[4] D. Borman, “Telnet Authentication: Kerberos Version 4”, RFC 1411, January 1993.

[5] J. Kohl and C. Neuman, “The Kerberos Network Authentication Service (V5)”, September 1993.

[6] Armando Fox and Steven D. Gribble, “Security on the Move: Indirect Authentication using Kerberos”, Proceedings of the 2nd ACM International Conference on Mobile Computing and Networking (MobiCom ‘96), Rye, New York, November 10-12, 1996.

[7] A. Rubens, C. Rigney, W. Simpson and S. Willens, “Remote Authentication Dial In User

Service (RADIUS)", RFC 2138, April 1997.

[8] IEEE 802.11, "Wireless LAN Medium Access Control (MAC) and Physical (PHY) Layer Specifications", ANSI/IEEE, 1999.

[9] N.R Prasad and A.R. Prasad, editors, WLAN Systems and Wireless IP for Next Generation Communications, Artech House, January 2002.

[10] IEEE P802.11f, "Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation", D5, January 2003.

[11] IEEE P802.11i, "Draft Supplement to IEEE Std 802.11, 1999 Edition, Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security", D5, August 2003.

[12] A. Prasad and A. Raji, "A Proposal for IEEE 802.11e Security", IEEE 802.11e, 00/178, July 2000.

[13] William A. Arbaugh: http://www.cs.umd.edu/~waa/wireless.html.

[14] IEEE Std 802.1X-2001 "IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control", 14 June 2001.

[15] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[16] U. Black, *Internet Security Protocols: Protecting IP Traffic*, Prentice Hall, 2000.

[17] L. Brederveld, N.R. Prasad and A.R. Prasad, "IP Networking for Wireless Networks", Chapter 4 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[18] M. Bishop, *Computer Security: Art and Science*, Addison Wesley, 2003.

[19] A.R. Prasad, H. Wang and P. Schoo, "Network Operator's Security Requirements on Systems Beyond 3G", WWRF #9, 1-2 July, Zurich, Switzerland.

[20] A.R. Prasad and P. Schoo, "IP Security for Beyond 3G towards 4G", WWRF #7, 3-4 December 2002, Eindhoven, the Netherlands.

[21] A.R. Prasad, H. Wang and P. Schoo, "Infrastrucutre Security for Future Mobile Communications Systems", October 19-22, 2003, Yokosuka, Japan.

[22] S.M. Bellovin and M. Merritt, "Limitations of the Kerberos Authentication System", ACM SIGCOMM Computer Comm. Review, vol. 20, iss. 5, Oct. 1990, pp. 119-132.

[23] R. Shirey, "Internet Security Glossary", RFC 2828, May 2000.

Chapter 6

Wireless LANs System Design and Deployment

The radio-based modes of current Wireless Local Area Network (WLAN) devices typically employ spread spectrum technology [1-8,17,20-23]. Spread spectrum *spreads* the signal power over a wide band of frequencies which makes the data much less susceptible to the electromagnetic noise than the conventional radio modulation techniques. The spread spectrum modulators use one of the two methods to spread the signal over a wider area: Direct Sequence Spread Spectrum, DSSS or Frequency Hopping Spread Spectrum, FHSS.

The present generation of WLAN products are implemented as Personal Computer Memory Card International Association or PCMCIA cards (also called PC cards) that are used in personal computers and portable devices [1,4,17,20-23]. The technical issues for the WLAN systems are the size, the power consumption, the data rate, the aggregate throughput, the coverage and the interference robustness. A system design must consider all these issues so as to make optimum use of the scarce wireless medium with the limitations of the standard requirements.

Once an appropriate system design has been chosen, the challenge is to deploy the network in such a way so as to serve the largest number of users with a specified system quality [6,7,17,20]. For this purpose the network deployment and the study thereof plays a very important role.

The main contributions of this chapter are two-fold, first being a study of the system design considerations of the IEEE 802.11 based WLANs and second being the deployment considerations for the IEEE 802.11 and the performance results of the IEEE 802.11b.

The IEEE 802.11 standard leaves several open issues; these issues can have adverse effects on the final product if not considered carefully and will finally affect the deployment. Such important open issues are identified and solutions are proposed in this chapter for the IEEE 802.11 based WLAN system design. This will help the WLAN system architects to better design their products. The solutions for some of the open issues are also studied and proposed in this chapter. For deployment purposes the coverage and the propagation results in various WLAN usage environments is presented in this chapter; measurement results are also presented on interference and throughput of IEEE 802.11b product. A cell and frequency planning method is proposed for the IEEE 802.11b WLANs.

The system design and deployment methods proposed in this chapter were used for the ORiNOCO products of Lucent Technologies.

6.1 System Design Issues

A system design of a wireless system must take the size, the power consumption, the bit rate, the aggregate throughput, the coverage and the interference robustness in consideration [6,7,17,20-23].

The IEEE 802.11 standard leaves several open issues which are not defined and thus are system design dependent [1]. These open issues help differentiate the products but also require a good product design. For example, although the IEEE 802.11 allows roaming there is no standard process defined for it. Another example is the data-rate control; there are several data rates at which the IEEE 802.11 standard can work but the standard does not describe the method for changing the data rates while a device is being used.

In this section three main system design considerations, roaming, automatic data rate control and issues arising from the definition of various threshold levels are studied. Power management as described by the standard is also given so as to better understand the results on power management presented in the latter part of the chapter.

6.1.1 Roaming

The IEEE 802.11 standard does not define how roaming should be performed in an infrastructure network. The standard only says that the IEEE 802.11 WLANs should provide roaming within the coverage boundaries of a set of APs that are interconnected via a (wired) distribution system. The APs send beacon messages at regular intervals. In this subsection a basic solution to perform roaming within the IEEE 802.11 infrastructure network is proposed. Note that roaming in the IEEE 802.11 sense does not have the same meaning as in the mobile communications world. Here roaming is the same as handover in the mobile communications; roaming in the mobile communications would mean moving to a different operator without service continuity [3,17,20].

The proposed roaming method is to allow the stations to keep track of the conditions at which the beacons are received per Access Point (AP). The receive conditions can be determined by a communications quality (CQ) indicator, see Figure 6-1. The different zones within the full range of CQ scale refer to various states of activities at which a station can track or try to find an AP. When the CQ is poor, then the station has to spend more effort to quickly find another AP that gives a better CQ.

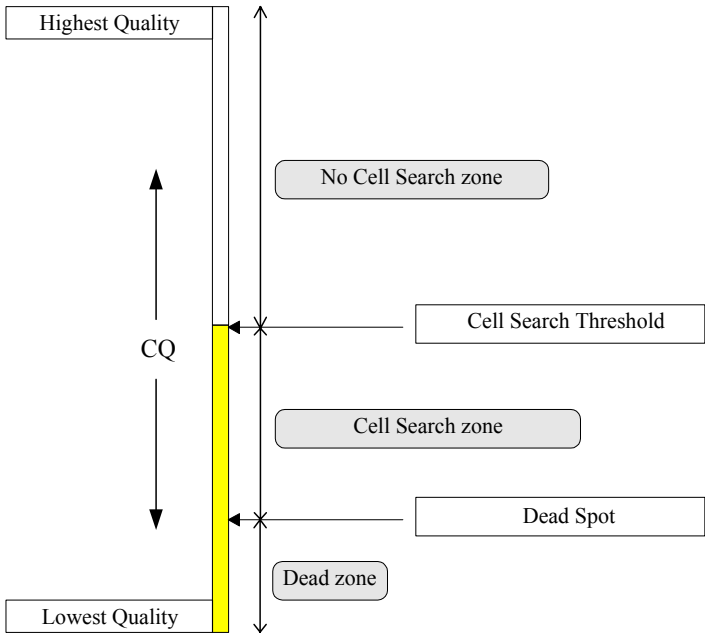


Figure 6-1 Comms Quality scale and Cell Search zones.

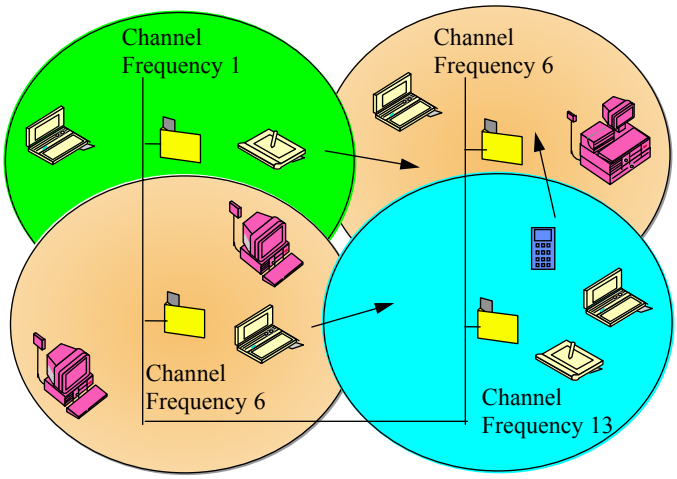


Figure 6-2 Wired infrastructure between access points and multi-channel operation with three different channel frequencies.

The APs, which are interconnected by a wired distribution system, can use channel frequencies from a basic set within all supported channel frequencies of the IEEE 802.11 DSSS standard [1], see Figure 6-2. A station can search for an AP giving a better CQ by looking at all the channel frequencies selected for the interconnected APs. The searching station can initiate an active mode by sending a probe request message (such messages are allowed by the 802.11 standard) referencing the target set of the interconnected APs. Each AP will respond to a probe request with a probe response message. This will serve as a "solicited" beacon.

For example, assuming a station at first has a good signal quality and is working in 'no cell search zone' of the CQ indicator. As the station moves away from the AP the signal quality deteriorates and the CQ indicator indicates that the signal quality is reached or is below the cell search threshold. Now the station is in 'cell search zone' of the CQ indicator and starts searching for new APs. If a new AP is found with better CQ level then the station will roam to it. In case that there are several APs with better CQ level then the station moves to the best one. It can happen that there are no APs in the area the station is moving; in this case the station will reach the 'dead zone' this is the CQ level where communication cannot take place.

6.1.2 Power Management

For battery powered devices, the power consumption of a WLAN card is a critical factor. The IEEE 802.11 standard defines the power management protocols that can be used by the stations [1]. The power management schemes result in a lower consumption of (battery) power compared to traditional operation where a station is always monitoring the medium during idle periods. To achieve savings in power consumption, a WLAN card in a station must have a low power state of operation called DOZE state. In this state the WLAN card will not monitor the medium and will be unable to receive a frame. This state differs from the OFF state in the sense that the card must be able to make a transition from DOZE state to fully operational receive (AWAKE) state in a very short time. In the DOZE state the station stays associated and synchronized with the AP. A transition from the OFF to the AWAKE state will take much more time, this is because the loading of parameters and the association procedure takes time.

Power Management allows a station to spend most of its idle time in the DOZE state, while still maintaining connection to the rest of the network to receive unsolicited messages. For the latter requirement, the other stations or the AP must temporarily buffer the messages that are destined to a station operating in a power management scheme, and such a station must "wakeup" on regular intervals to check if there are messages buffered for it [6,7,17,20].

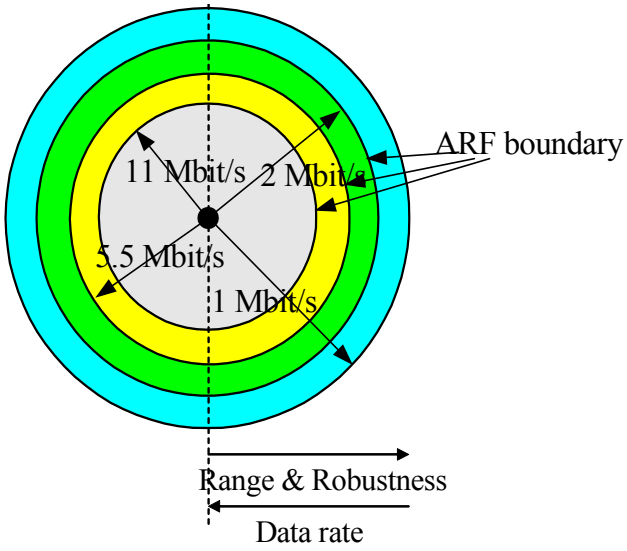


Figure 6-3 Relation between data rate and cell regions.

6.1.3 Automatic Data Rate Control Algorithm

The different modulation techniques used for the different data rates of the IEEE 802.11 can be characterized by more robust communication at the lower rate. This translates into different reliable communication ranges for the different rates, 1 Mbit/s giving the largest range. Figure 6-3 shows the four concentric cell regions associated with the four data rates of IEEE 802.11b. Stations moving around in such a large cell will be capable of higher speed operation in the inner regions of the cell. To ensure usage of the highest practicable data rate at each moment an automatic rate fallback (ARF) algorithm is proposed in this section; this solution was also applied for patent by the author. Although the name ARF means decreasing the data rate, this algorithm also increases the data rate automatically as the situation changes. The IEEE 802.11 standard does not define any data rate control algorithm [1].

The ARF algorithm causes a fallback to the lower data rate when a station wanders to the outer regions or has high level of interference and should increase the data rate when it moves back into the inner region or in better channel conditions [6,7,20-23]. The fallback algorithm prevents a ping-pong effect. The ARF functions come into play when the ARF boundary is crossed in either direction. These boundaries are the result of the fallback scheme with a fallback in data rate after a few successive retries in transmission of a frame and after a number of successful frame transfers an attempt to a higher data rate. In this way the data rate shows a Carrier to Interference (C/I) dependent behaviour and leads to a difference in coverage range. The upgrade in the data rate will be done step-wise, i.e., if in 1 Mbit/s the WLAN will go to 2 Mbit/s but not to 5.5 or 11 Mbit/s. Besides resulting in a bigger range, the lower rates will also be more robust against other interfering conditions like high path loss, high background noise, and extreme multipath effects.

Introduction of different data rates means the CQ indicator mechanism used for roaming must be modified and levels for each data rate must be introduced. Although the data rate control algorithm, ARF, is based on Medium Access Control (MAC) frames, in certain deployments it will not make sense to fallback to lower data rates. For example an office scenario where 11 Mbit/s data rate is required and thus dense deployment of AP is done. ‘Cell search zone’ in this case should start when the CQ is barely good enough to maintain 11 Mbit/s. While in the case of warehouse where 1 Mbit/s is sufficient the ‘cell search zone’ should start at the level where CQ is coming to a level below which 1 Mbit/s can barely be maintained.

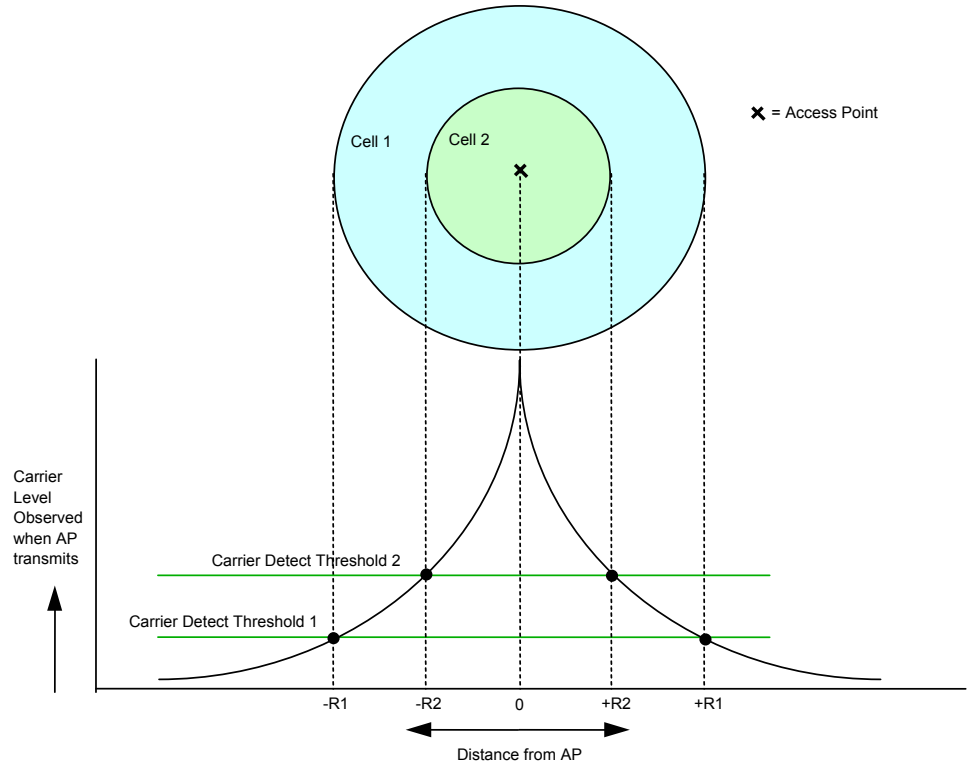


Figure 6-4 Carrier detect threshold (CDT) impact on cell size.

6.1.4 Thresholds and System Scalability

A WLAN system can be deployable in a broad variety of situations, posing different and often conflicting requirements on the system behaviour. In particular, the situation of a stand-alone single cell network versus an infrastructure network consisting of multiple overlapping cells will have different requirements on both transmit and receive behaviour. To accommodate these varying operational situations, some WLAN products have a number of built-in provisions to create scaleable systems, optimized for environment and network usage needs [17].

When an AP transmits, the observed levels of the carrier signal by a station will decrease with the distance. Figure 6-4 illustrates the typical curve for the signal level in two opposite directions. In this section threshold values that should be understood for the system design and deployment are discussed. These values can either be fixed by the vendor or can be left for the user to control.

6.1.4.1 Carrier Detect Threshold

The Carrier Detect Threshold (CDT) is defined as: “the carrier signal level, below which the WLAN receiver will not receive.” Figure 6-4 shows that the CDT at level 1 crosses the curves at distances -R1 and +R1. This implies that an associated cell size for this CDT value with radius R1. This is shown as the dark ring area above the curves. The other example at level 2, which is higher (less sensitive) than level 1, shows a smaller cell (radius R2). The range for meaningful CDT levels has a lower boundary determined by the sensitivity of the WLAN receiver circuitry. Setting the CDT to a lower value will result in a number of meaningless receive attempts, which will have a high failure rate. The importance of configurable carrier detection is that it allows the WLAN cards to be configured at smaller cell sizes than the receiver is capable of handling. Small cell sizes play an important role when considering the possibilities for re-use of the same channel in a relatively small area, see Section 6.8.

6.1.4.2 Defer Threshold

The 802.11 medium access rules (CSMA/CA) are based on defer and random backoff behaviour of all the stations within range of each other as discussed in Chapter 3 and Chapter 4. The defer decision is based on a configuration entity called the Defer Threshold (DT). When a carrier signal level is observed above the DT level, the WLAN card will hold up a pending transmission request.

Taking the example of the CDT level 2 (Cell 2) from Figure 6-4, the ideal value of the DT is such that it produces the double radius. This means that a station on one edge of the cell defers for a station at the other edge. This is shown by plotting the curve for one edge station and ensuring that the DT level crosses this curve at the other cell edge. Choosing this relation between the CDT and the DT level gives a cell in which all stations defer for each other, and where each station can communicate with the AP.

The range for the DT level has a lower boundary determined by the sensitivity of the WLAN carrier detect circuitry. Below a certain level, the signal will not be detected and no defer will be done, however, this can be a little lower than the receiver sensitivity which marks the level for reliable data reception. The ideal relation shown in Figure 6-5 cannot be achieved in the case where the CDT is set to the lowest (and most sensitive) level. In that case the lowest meaningful DT will not guarantee the wanted deferral between the two “edge stations”. If a low CDT value is chosen, a large cell size with radius R is created; this is shown with the large circle in Figure 6-6. The lowest meaningful DT level has a smaller size; this is shown with the smaller and light grey circle with radius R'. The outer area of the cell (dark ring) will not have guaranteed deferral.

Similar to the CDT, the DT plays an important role when considering the possibilities to re-use the same channel. If a station is at the edge of a cell it will differ from signal received from a station or an AP which is working on the same frequency and is a cell away. Cell planning is discussed in Section 6.8.

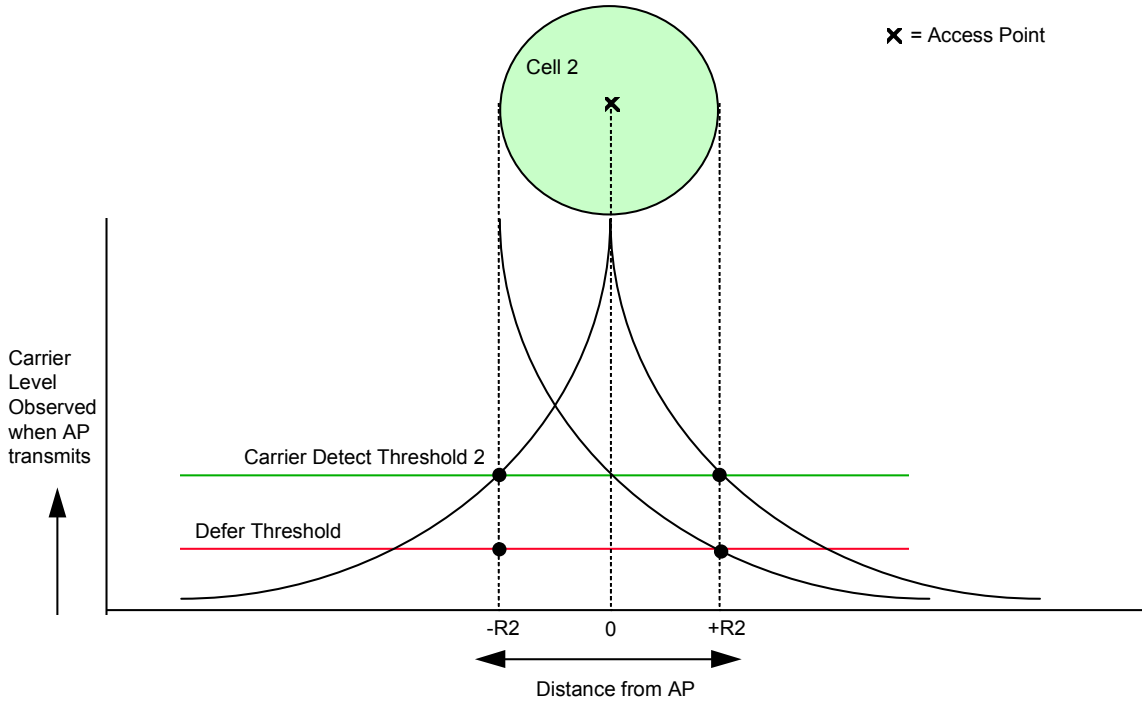


Figure 6-5 Ideal relation between defer threshold (DT) and carrier detect threshold (CDT).

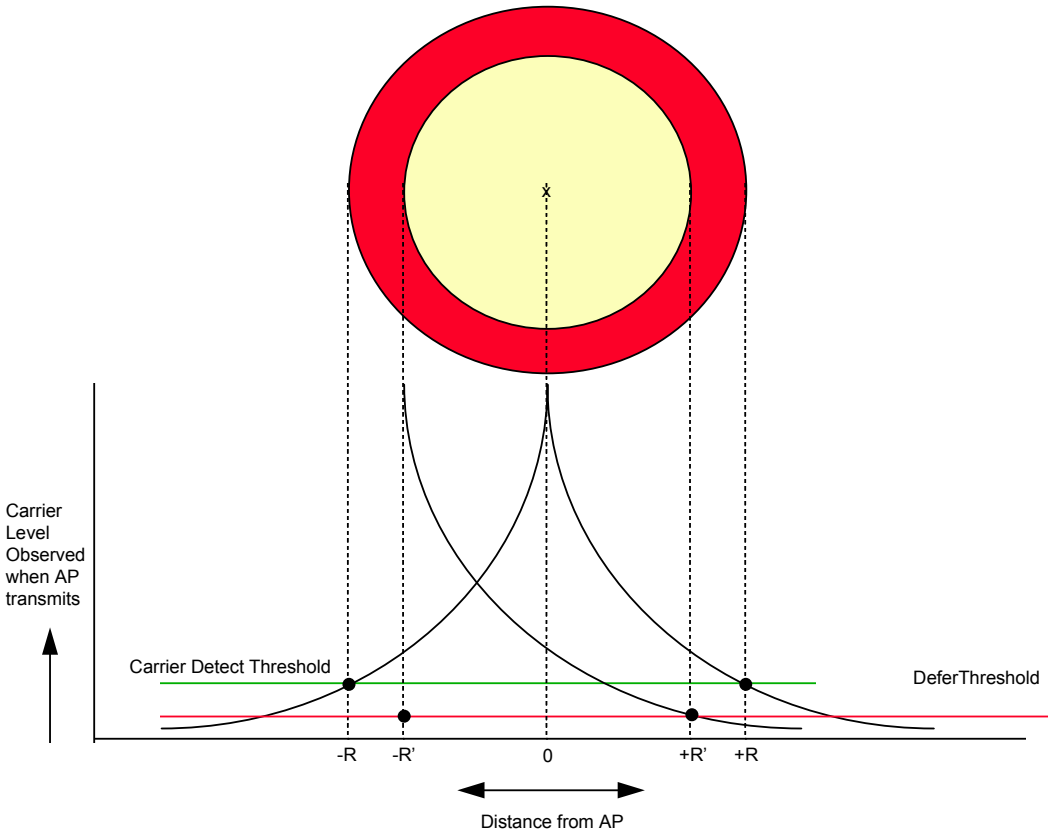


Figure 6-6 Large cell characteristics.

6.1.4.3 Roaming Thresholds

When creating a cellular infrastructure system with the above defined thresholds for the low-level receiver and transmitter control, there must be a proper balance with the earlier discussed roaming thresholds. While the CDT and the DT determine the transmit/receive behaviour of the stations and the APs which belong to the same cell, the roaming thresholds determine the moments for deciding to start or stop participation in a cell. A station should base its handover decisions on the currently configured capabilities of the receiver. In particular when small cell sizes are required, the roaming thresholds must be set such that stations will start searching for a new (better) AP in advance of the moment that the receiver becomes physically incapable of receiving messages from the current access point.

6.2 Deployment Considerations

Planning a network which fulfils the requirements of the user is a major issue. In this section some critical points are discussed for WLAN deployment, details of which are given in latter sections. Some of the deployment criteria discussed below requires measurement results; the system considered and the measurement setup used is also discussed in this section [6,7,17,23].

6.2.1 Critical Deployment Issues

Critical deployment issues are discussed in the following, details and results for each issue are given in latter sections.

- *Utilization*: Deployment of WLANs depends also on the kind of users and the kind of application they will run. This issue will not be discussed further although a point related to this issue is discussed in Section 6.3.

- *Security*: One cannot be blind to this issue. Hackers breaking into the networks are common; this can be even more dangerous when data is transmitted in a wireless medium that can be accessed by anyone with ease. This topic and requirements for different environments is discussed in detail in Chapter 5, [8].
- *Data rate*: This is a very important issue for WLANs. Factors such as the available bandwidth and the frequency restrict the maximum achievable data rate. The data rate is further restricted by the interference in the system. The optimum choice of the data rate depending on the channel conditions and the communicating devices is extremely important. The IEEE 802.11b WLANs can communicate at data rates of 1, 2, 5.5 and 11 Mbit/s. A rate control algorithm and the threshold levels are discussed in Section 6.1 and the throughput results for the different data rates are given in Section 6.4.
- *Coverage*: Factors like band restrictions and output power controlled by regulatory bodies effect the coverage. The coverage is also affected by the interference and the type of building. The material used in a building effect the propagation of the radio waves which in turn affect the wireless network. As WLANs are used in a variety of businesses, the propagation characteristics must be taken into account during the network deployment. The coverage is directly related to the propagation environment, both the propagation and the coverage are discussed in Section 6.5.
- *Interference (Coexistence/Interoperability)*: In any wireless system one is haunted by the interference from other systems working at the same frequency this becomes an even more important issue when discussing systems working in the ISM band. Thus, the study on the interference for the coexistence of different devices in the ISM band and the interoperability among WLANs following the same standard is bread and butter for a network deployment engineer. This issue and more are dealt with in Section 6.6.
- *Power management*: The battery life is a major issue for wireless communications devices. The size and the weight of the wireless systems depend on the power consumption. For optimum battery usage power management is used in the WLANs which means the station goes to sleep mode when not in use. This can save the battery but in certain situations increase the delay and decrease the system throughput, thus the optimum power management setting should be done depending on the user and the traffic in the system. The power management depends on the system design, this is further discussed in Section 6.1.2; results of the power management are given in Section 6.7.
- *Cell planning (Cell size/Frequency planning/Capacity)*: This factor is dependent on the density of the users, the base stations and last but not least the available bandwidth. As given in Section 6.1 the cell planning is also dependent on the threshold values. A good network deployment will require an adequate cell size planning which in turn will give an optimum capacity. Thus a good cell planning must make optimal use of the already scarce wireless spectrum for which several points must be taken care of together with the frequency planning. A good planning is extremely important to increase the coverage and the capacity. The cell planning is also dependent on the part of the world where the WLAN is being deployed because the regulatory bodies control the frequency band allocation. This issue is discussed in Section 6.8.

Measurements should be done for some of the deployment criteria discussed above. The system model and the measurement setup used in this chapter are given in the following sub-section.

6.2.2 System Model and Measurement Setup

Before further discussion it is important to know which WLAN is considered. This section discusses briefly the WLAN standard used and the measurement setup.

Table 6-1 Frequency bands and power levels for wireless LANs.

Location	Regulatory Range	Maximum Output Power
North America	2.401-2.4835 GHz	1000 mW
Europe	2.401-2.4835 GHz	100 mW (EIRP)
Japan	2.401-2.495 GHz	10 mW/MHz

6.2.2.1 System Model

In this chapter WLANs based on DSSS technology as given by the IEEE 802.11 standard is considered. The IEEE 802.11 WLAN based on DSSS is initially aimed for the 2.4 GHz band designated for the ISM applications as provided by the regulatory bodies worldwide [1-3,5,17].

The DSSS system provides a WLAN with 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s and 11 Mbit/s data payload communication capability. According to the FCC regulations, the DSSS system shall provide a processing gain of at least 10 dB. This shall be accomplished by chipping the baseband signal at 11 MHz with an 11-chip pseudo random, PN, code (Barker sequence) [1,5,17]

The DSSS system uses baseband modulations of Differential Binary Phase Shift Keying (DBPSK) and Differential Quadrature Phase Shift Keying (DQPSK) to provide the 1 and 2 Mbit/s data rates, respectively. Complementary Code Keying (CCK) is used to provide 5.5 and 11 Mbit/s.

The regulatory bodies in each country govern the ISM band. Table 6-1 lists the available frequency bands and the restrictions to devices which use this band for communications [1,5,17]. In the USA, the radiated emissions should also conform to the ANSI uncontrolled radiation emission standards (IEEE Std C95.1-1991).

6.2.2.2 Measurement Setup

Throughout the chapter for measurement purpose a simple setup was used as given in Figure 6-7. A server was used to transmit packet of 1500 bytes cyclically using TCP/IP. An AP was connected to the server via the 10Mbit/s Ethernet connection to which one or more stations were connected. Measurement was done by the Lucent Technologies Wireless Communications and Networking Division (WCND) test team.

6.3 User Requirements and Utilization

Before one starts deploying the WLANs it is important to study the target environment. Analysis of the environment should lead to the study which will finally give the required number of APs. While the maximum range of the WLAN (as measured from point-to-point) determines the number of APs required. In the following the criteria which determine the maximum range are given [6,7,17,20]:

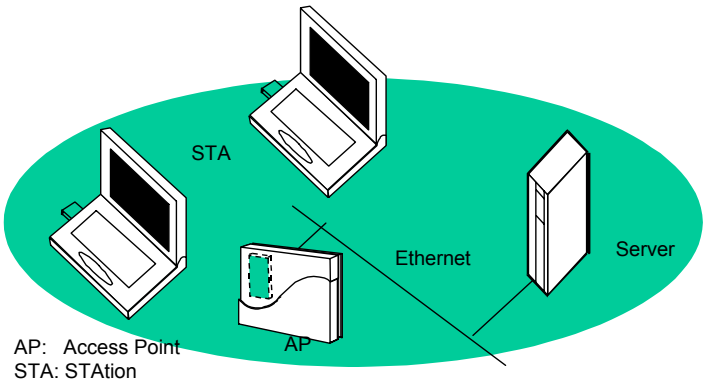


Figure 6-7 Measurement setup.

- The Access Point Density.
- The environment the WLAN equipment will be installed.

In this section these two points are explained.

6.3.1 User Need and Access Point Density

In the networking environments where there are either data intensive users, or a large number of users in a small area, one may wish to balance the throughput performance versus the cost of the investments. Three different AP density, low, medium and high, which fulfil different user requirements are considered below [6,7,20,23].

- **Low AP Density** provides a maximum wireless coverage with a minimum number of access points. This option that is typically used for single-cell networks and Point-to-Point link, will also provide an efficient and cost effective solution for most networks that include multiple wireless cells.
- **Medium AP Density** can be used for environments where the stations experience slow network response times even though the quality of the radio communications is rated as excellent. The slow response times might be experienced in areas where:
    - A high number of the wireless stations are located close to one another, causing other stations within the same cell around the AP to defer the data transmissions.
    - A number of wireless stations engaged in heavy network traffic are causing other stations to defer the data transmissions.
- **High AP Density** can be used when one is designing a wireless infrastructure where the total cost of the hardware investments is less critical than the maximum data throughput per cell. Per definition, a High Density network will include the highest concentration of APs.

6.3.2 Type of Radio Environment

Subject to the type and nature of the building materials, the WLAN radio signals may either pass obstacles in the radio signal path, or be absorbed or reflected by the RF barriers. According to the number and severity of the RF barriers in the radio signal path, the wireless networking environments can be classified as one (or combination) of the following type of radio environments [6,7,17,20,23]:

- Free Space — No physical obstruction in the signal path
- Open Office — Similar to free space but obstruction can occur sometimes
- Semi-open Office — Shoulder-height partitions of wood or synthetic material
- Closed Office — Floor to ceiling walls of brick and plaster

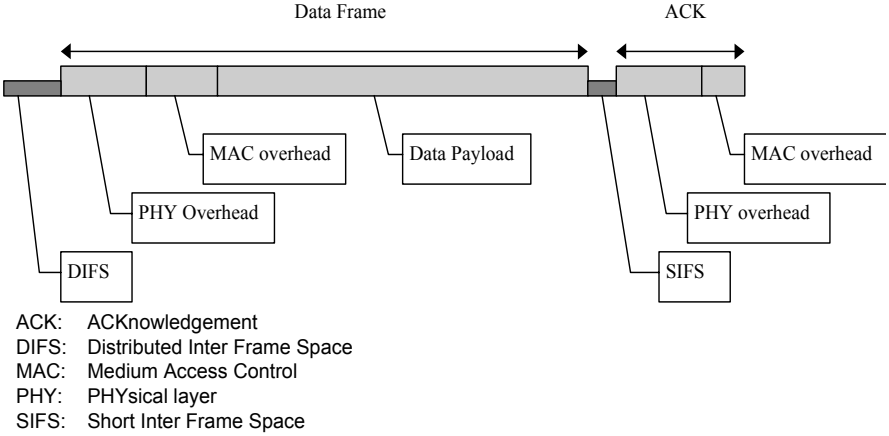


Figure 6-8 Packet/frame structure of 802.11.

Metal for example, is a high severity barrier. Environments with metal constructions or large metal objects, such as elevator shafts or machinery, require extra attention when performing an analysis. One should first determine which environment the building represents. Then using reliable values the network deployment can be done.

6.4 Throughput Results

For the deployment it is very important to understand the actual throughput that is achievable for a given data rate. Throughput can be measured based on the amount of transferred net data and the required transfer time. A typical method of measuring the throughput is by copying a file between a wireless station and a server connected to the wired infrastructure. The effective net throughput depends on the data rate at which the wireless station communicates to its AP, but there are a lot of overhead like the data frame preamble, the MAC header, the ACK (acknowledgement) frame, the transmission protocol overhead (per packet and by request/response packets), the processing delay in local/remote computer, the forwarding around the AP. The packet/frame structure of the IEEE 802.11 is given in Figure 6-8. Table 6-2 gives the frame overhead and the impact on the net data throughput [6,7,17,20,23].

The results in Table 6-2 are given for a 1500 bytes payload, the PHY overhead (preamble) is transmitted at 1 Mbit/s. The results are calculated for the minimum Inter Frame Space (IFS) of 50μs. First the time required to transmit different parts of the data frame and the ACK frame are given, these are calculated using the following equation [6,7,20,23],

$$\text{Transmission time required} = \frac{\text{Size in bits}}{\text{Data rate in bits/s}} * 10^6 \ \ \mu s \qquad (6\text{-}1)$$

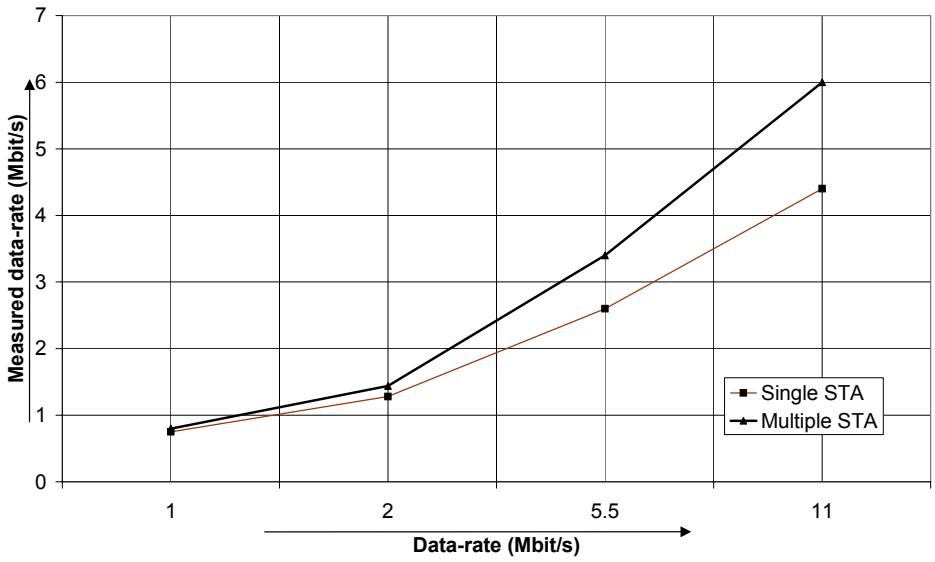
The data throughput is given by [6,7,20,23],

$$\text{Data throughput} = \begin{cases} \dfrac{\text{Payload transmission time}}{\text{Total tranmisison time required}} \% \\ \text{Data rate} * \dfrac{\text{Payload transmission time}}{\text{Total tranmisison time required}} \ \text{Mbit/s} \end{cases} \qquad (6\text{-}2)$$

Figure 6-9 gives the net throughput results as can be found with the file copying between a server connected through the Ethernet to an AP and one or more (multiple, maximum 6) wireless client stations. A 1 Mbyte file was transmitted cyclically. The net throughput difference between two or more stations is negligible. Results in Figure 6-9 are given for actual data throughput, i.e., the overhead from TCP and IP headers are also considered thus the difference from the result given in Table 6-2 in which the overhead from TCP and IP headers are not considered.

Table 6-2 Frame overhead with DSSS at different bit rates and impact on throughput.

Data Rate (Mbit/s)	Frame				ACK			Total (μs)	Data Throughput (Mbit/s)	Data Throughput (%)
	Minimum IFS (μs)	Preamble (μs)	MAC overhead (μs)	Payload (μs)	IFS (μs)	Preamble (μs)	MAC overhead (μs)			
1	50	192	272	12000	10	192	112	1282	0.94	93.5
2	50	192	136	6000	10	192	56	6636	1.81	90.4
5.5	50	192	49	2182	10	192	56	2732	4.39	79.8
11	50	192	25	1091	10	192	56	1616	7.43	67.5



STA: STAtion

Figure 6-9 Net throughput (file copy time).

The reliable coverage range, see Section 6.5, will be influenced by the interference and the data rate. In Figure 6-10 measured throughput results for different receive levels are given. The receive level for a given data rate can be used to determine the coverage as discussed in Section 6.5.2. IEEE 802.11 defines the minimum required receive level. The throughput in Figure 6-10 was measured based on the cyclic transmission of 1500 byte frames while the signal level at the receiver was adjusted by the controlled set up using a step attenuator. The ARF scheme is discussed in Section 6.1.3.

To consider throughput measurement with multiple stations divided over more than one AP one has to look into other aspects like the adjacent channel interference (Section 6.6) and medium reuse effects.

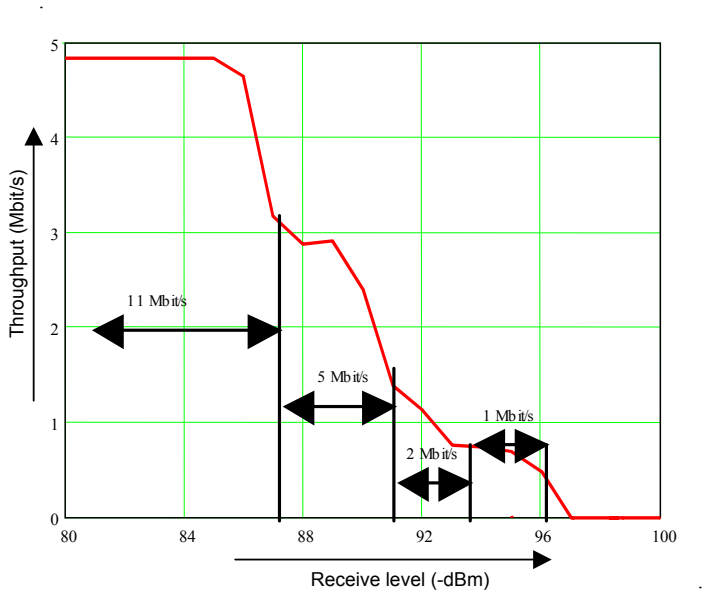


Figure 6-10 Throughput against receive level for 802.11 PC card with ARF.

6.5 Propagation and Coverage

The success of any communication system depends on the understanding of the influence of the propagation medium. Propagation in a medium is affected by the atmosphere and the terrain [10]. The degree of influence depends primarily on the frequency of the wave. It is a must to understand the propagation characteristics of the frequency assigned for the WLANs being studied, 2.4 GHz. The propagation results can also be used to find the coverage in different environments for different data rates.

In this section the propagation characteristics of the 2.4 GHz band is studied and results are presented for different path loss models together with the coverage results [6,7,17,20-23].

6.5.1 Path Loss Models

The free space propagation, L_f, is frequently given as [6,7,10-13,20,23,24],

$$L_f = 20 \log f + 20 \log d \ -10 \log G_t -10 \log G_r - 27.6 \ \ dB \qquad (6\text{-}3)$$

where $20 \log f$ gives the frequency (f) dependent contribution and f is in MHz; $20 \log d$ gives the distance (d) dependent term for free space propagation, it has to be replaced by $10\ \gamma \log d$ for non free space propagation ($\gamma \neq 2$) and γ is the path loss coefficient; G_t and G_r are the directive antenna gains for the transmit (t) and the receive (r) antennas respectively ($G_t = G_r = 1$; 0 dBi for isotropic antennas). This equation is derived from the known path loss equation [10-13],

$$L_f = 10 \log(P_t/P_r) = -10 \log [(G_t G_r \lambda^2)/(4\pi d)^2] \qquad (6\text{-}4)$$

where P_t and P_r are the transmitted and the received power respectively and λ is the wavelength.

The received power in decibels can be simply written as [6,7,10-13,20,23,24],

$$P_r = P_t - L_f \qquad (6\text{-}5)$$

The free space propagation model defined by equation (1) is not applicable to many practical situations. However, due to its simplicity, it is a common practice to use it for estimates, in which case γ is changed to better match the practical situations. A breakpoint model can be applied for obstructed conditions, where $\gamma = 2$ is used till the breakpoint (b) and for the distance above the breakpoint (d_{br}) a larger value for γ is used. The path loss model for 2.4 GHz and isotropic antennas can be represented by [6,7,20,23,24],

$$\begin{aligned} L(2.4\ GHz) &= 40 + 20 \log(d) \ \ dB & d \leq d_{br} \\ &= 40 + 20 \log(b) + 10\ \gamma \log (d / b) \ \ dB & d > d_{br} \end{aligned} \qquad (6\text{-}6)$$

For indoor environments the propagation losses resulting from obstacles such as floors and walls are described simply by adding a certain number of dB of loss per obstacle, i.e., the path loss is [6,7,20,23,24],

$$L(2.4\ GHz) = 40 + 20 \log d + k f + p\ w \ \ dB \qquad (6\text{-}7)$$

where k and p are the number of floors and walls between the transmitter and the receiver and f and w are the attenuation factors in dB, per floor and per wall, respectively.

6.5.2 Coverage Results

In Figure 6-11 results are given for different path loss models [10,11]. The reliable coverage analysis is based on the path loss modelling for environments like the Open Office, the Semi-Open Office and the Closed Office with respectively γ of 2.2, 3.3 and 4.5 above a 5 meter breakpoint (up to 5 meter free space propagation with path loss coefficient equal to 2) [6,7,20,23]. On top of this modelling, with path loss dependent on the TX-RX (Transmit-Receive) distance, there will be a margin of 10 dB required in relation to variation due to fading. The 10 dB margin reflects a reliability of 99% [10-14,19].

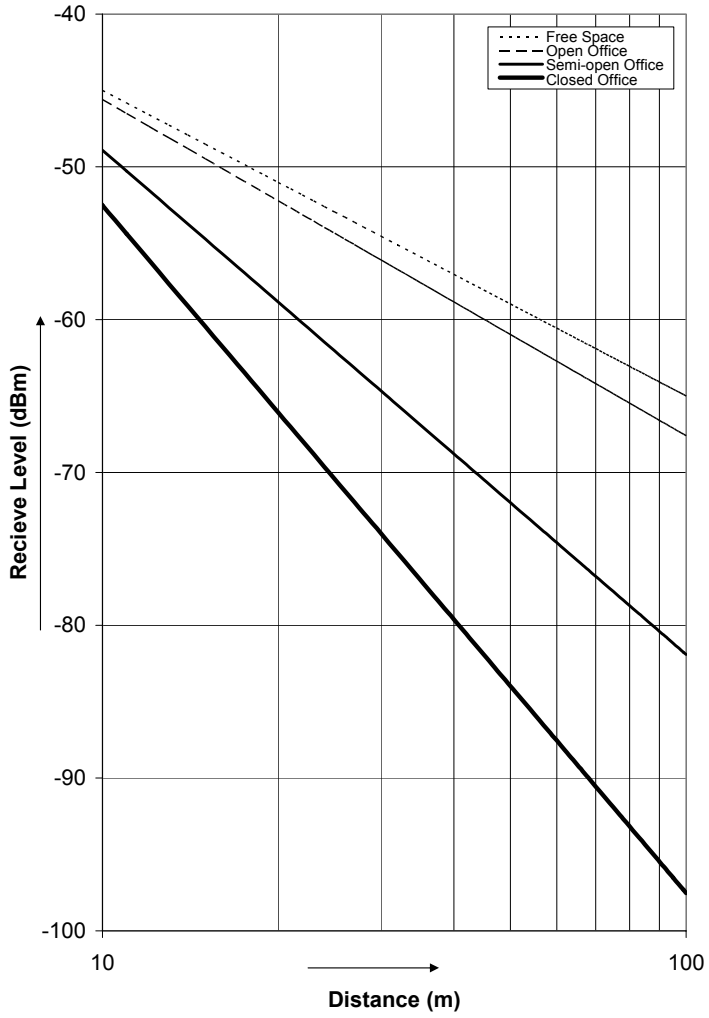


Figure 6-11 Typical receive signal vs. distance for different path loss models.

Results of Figure 6-11 can be used to find the range covered for a given receiver sensitivity. In Table 6-3 the receiver sensitivity for different data rates at a transmit power of 15 dBm. This combined with Figure 6-11 can give us the achievable distance for different data rates. For example to find the range for 11 Mbit/s the –84 dBm with a 10 dB fading margin gives –74 dBm. This gives, for closed office (coefficient 4.5), a cutting point at the distance of 29 meter.

Figure 6-11 can also give us the cell size for the CDT and the DT values discussed in Section 6.1.4. Thus the result can be used for cell planning based on the data rates and the user needs as discussed in Sections 6.1, 6.4 and 6.3.

Table 6-3 Reliable ranges according to path loss models.

Data rate (Mbit/s)	**1**	**2**	**5.5**	**11**
Receiver sensitivity for BER 10^{-5} (dBm)	**-93**	**-90**	**-87**	**-84**
Range covered 99% point TX power 15 dBm (m)				
Open Plan Building	485	354	259	189
Semi Open Office	105	85	69	56
Closed Office	46	40	34	29

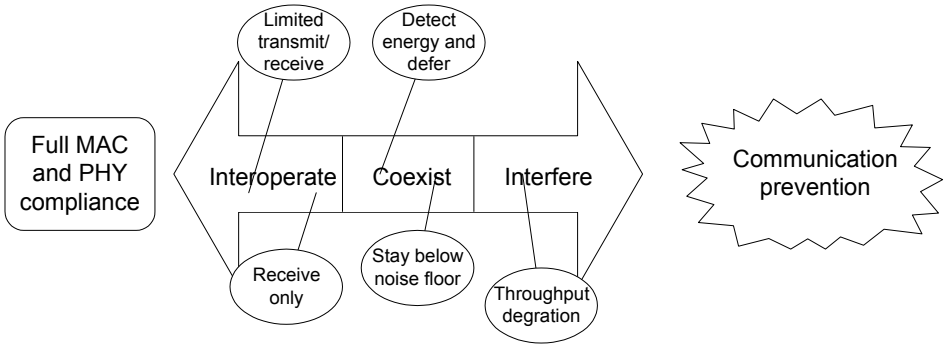


Figure 6-12 Interoperability and Coexistence, [16].

6.6 Interference and Coexistence

If a certain frequency band is allocated for a wireless radio system, a fundamental requirement in the efficient use of the band is to re-use the frequencies at as small a separation as possible [3,9-11,24]. Whenever a band of frequencies is used the interference effects have to be taken into account. These can be mainly classified as co-channel and adjacent channel. At the same time in the ISM band there is an issue of coexistence with other systems working at the same frequency. There are several technologies which are available for use in the ISM band. This brings forward the need of study of the Interference and the Coexistence.

In Figure 6-12, [16], the complexity of the coexistence is depicted. The rectangle on the left represents a perfect world in terms of two independent communications systems that share the same wireless medium. Full interoperation means that if they chose, they would fully comprehend each other's protocols and take steps to avoid adversely affecting each other. The opposite end of the scale is where the two systems conflict to such an extent that they prevent any communication.

This section explains and gives the results for the interference and the coexistence for the IEEE 802.11 WLAN [6,7,20,23].

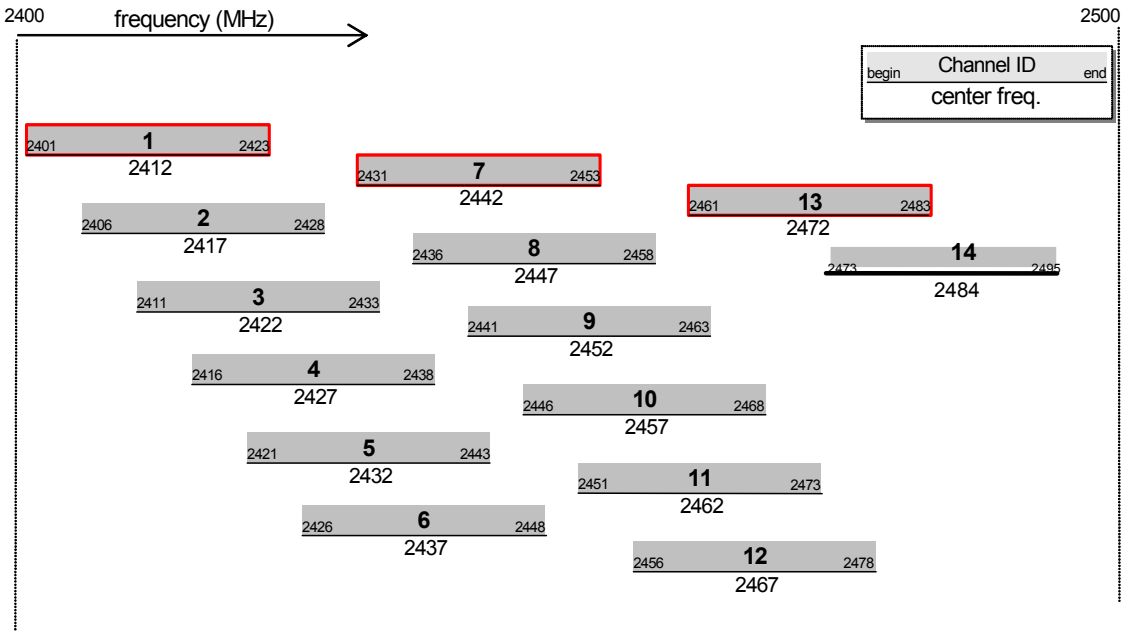


Figure 6-13 2.4 GHz channels for IEEE 802.11.

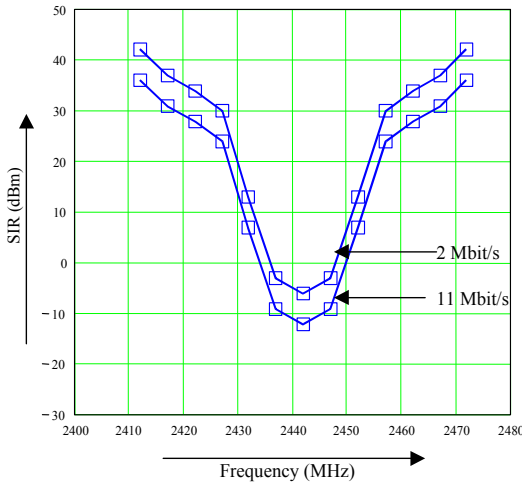


Figure 6-14 Tolerable adjacent channel interference with centre frequency at 2442 MHz.

6.6.1 Co-channel and Adjacent Channel Interference

The radio frequency interference is one of the most important issues to be addressed in the design, the operation and the maintenance of the wireless communications systems. Although both the intermodulation and the intersymbol interferences also constitute problems to account for in the system planning, a wireless radio system designer is mostly concerned with the adjacent channel and the co-channel interference.

Co-channel interference lies within the bandwidth of the victim receiver and arises principally from the transmitters using the same band. Adjacent channel interference arises from the same sources and causes problems because the receiver filters do not have perfect selectivity.

Adjacent cells with no overlap will not interfere with each other when the channel spacing use channel centre frequencies that are 15 MHz separated [1]. With fully overlapping cells, the separation has to be 25 MHz to avoid interference [1]. This can be seen from the channel assignment in the 2.4 GHz band by IEEE 802.11 as depicted in Figure 6-13. The required capture ratio [1], for 2 Mbit/s is 6dB while for 11 Mbit/s is 12dB, is fundamental in terms of how robust the scheme is with respect to the co-channel interference from neighbour cell, the defer threshold gives the point from where to allow channel reuse [1,6,7,20,23].

Defer threshold level and the required capture ratio gives the basis of the medium reuse planning, see Section 6.1.4. The focus could be among others smaller cells with a more dense reuse which needs more APs, or larger cells to limit the number of APs, Section 6.3. At 2 Mbit/s the channel frequency can be reused when there is one other cell in between which is not using that channel frequency.

Figure 6-14 gives the adjacent channel and the co-channel Signal to Interference Ratio, SIR, for the considered WLAN system. Measurement is made in a controlled set up to control the SIR (signal to adjacent channel interference) level. The SIR is measured based on the frame error ratio of 12% with 1500 byte frame reflecting a BER of 10^{-5}. A BER of 10^{-5} is a reasonable value for a LAN system and is a requirement set by the IEEE 802.11 standard for receiver sensitivity of different data rates [1].

6.6.2 Microwave Oven Interference

Microwave ovens also work in the ISM band which creates a lot of noise. Measurement result for WLAN working at 11 Mbit/s in presence of a microwave oven (Samsung RF-570D) with an AP and a station 3 m apart and a microwave oven and a station at 1 m is given in Figure 6-15 [6,7,17,20].

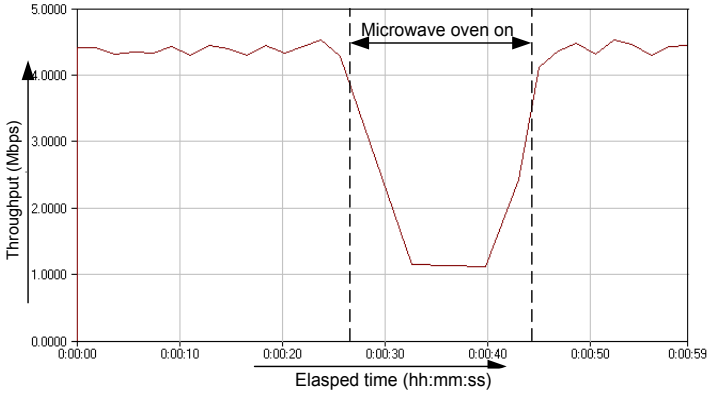


Figure 6-15 Throughput against elapsed time for microwave oven interference.

In this test cyclically 1 Mbyte file was transferred from the server through an AP to a receiving station. When the microwave oven is turned on and it is in active periods, around 8 ms every 20 ms (50 Hz of mains power cycle) with an emission of 2450-2458 MHz, the signal blocks the receiving station operating at a centre frequency of 2452 MHz. During microwave idle periods of 12 ms out of the 20 ms cycle the frames can reach the receiving station. A frame will be received correctly only if it totally falls within the microwave idle period thus with such interference a higher data rates will perform better.

6.6.3 Coexistence

Coexistence is a major issue for wireless communication systems working in the ISM band. In this section coexistence study of the IEEE 802.11 WLAN with FHSS IEEE 802.11 and Bluetooth are presented [15-18,20,23].

The FHSS IEEE 802.11 WLAN stations send one or more data packets at one carrier frequency, hop to another frequency and send one or more packets and continue this hop-transmit sequence (slow frequency hopping). The time these FHSS radios dwell on each frequency is typically fixed at around 20 ms. The FHSS 802.11 has, as modulation technique, Gaussian Frequency Shift Keying (FSK) with a low modulation index (Gaussian frequency shaping, BT product = 0.5, modulation index, h = 0.34 and 0.15 at 1 and 2 Mbit/s respectively), which gives a relatively narrow spectrum and allows 1 and 2 Mbit/s bit rate in the 1 MHz wide hop bands [1]. However, these FSK conditions results in more sensitivity for noise and other impairments.

Bluetooth applies the same modulation scheme as 802.11 FHSS at 1 Mbit/s, however, it hops faster, every 0.625 ms after a period of activity of 0.366 ms and silence of 0.259 ms. The same SIR requirement as in the previous section is applicable, except that the Bluetooth transmit power is 1 mW. System degradation in practice will depend on the actual load and the traffic process [15].

Co-located DSSS and FHSS systems interfere with each other in case of channel overlap (11 MHz DSSS channel and the 1 MHz FHSS channel) [12-14,17,20]. DSSS is more robust against in-channel interference because of its despreading (correlation) process. FHSS rejects much of the DSSS signals by its narrower filtering however it is sensitive to in-channel interference. With single cell DSSS and FHSS systems, the channel overlap risk is limited because FHSS hops through the whole 2.4 GHz band. Roughly the tolerable interference for both systems in case of channel overlap is 10 dB [18].

6.7 Impact of Power Management

Using Power Management will reduce the amount of current drawn from the battery needed to execute wireless transmissions [6,7,20,23]. The effect of this is an improvement in the battery life. Measurement results show that in the idle power save mode 15 mA is utilized in contrast to 165

mA in receive mode and 280 mA in the transmit mode for an ORiNOCO WLAN. Power usage differs from implementation to implementation.

A system that already consumes a significant amount of battery power for basic components may experience less benefit from the power management as opposed to a system where the power needed for the basic platform is low.

On the downside, using the Power Management will reduce the overall throughput, as the station has to wake up first to pick up a message that is buffered at the AP. Thus it is important to decide the DOZE time depending on the usage; in an office usage where data is often accessed from the network it might be better not to use the power management while in a warehouse it is better to let the station sleep as long as possible so as to save the battery life.

6.8 Cell Planning

In general, networks deployed with coverage as a primary requirement must have larger cells that in turn will give a low aggregate throughput. Such network deployment will require lesser APs and thus will be cheaper. The cell size can be varied by choosing the appropriate data rate which reflects in receiver sensitivity level. On the other hand networks deployed with a primary requirement being the throughput will have a smaller cell size (still giving full coverage), requiring more APs, see Sections 6.3 and 6.5. In this section cell planning is discussed together with cell overlap and frequency planning.

6.8.1 Cell Overlap

Cell overlap can be either horizontal or vertical or in occasions both. Horizontal and vertical overlaps are discussed in this section.

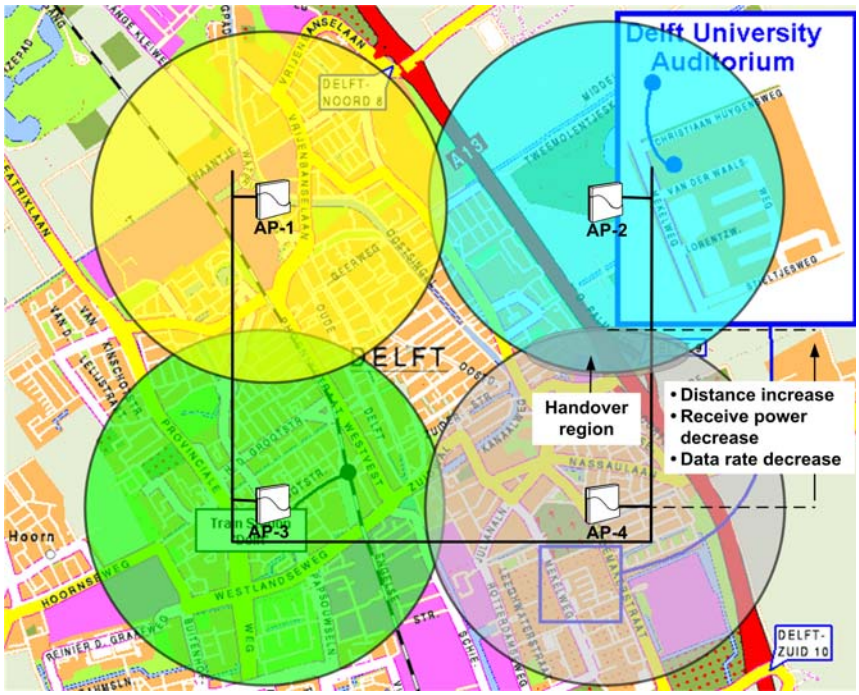


Figure 6-16 A normal deployment example.

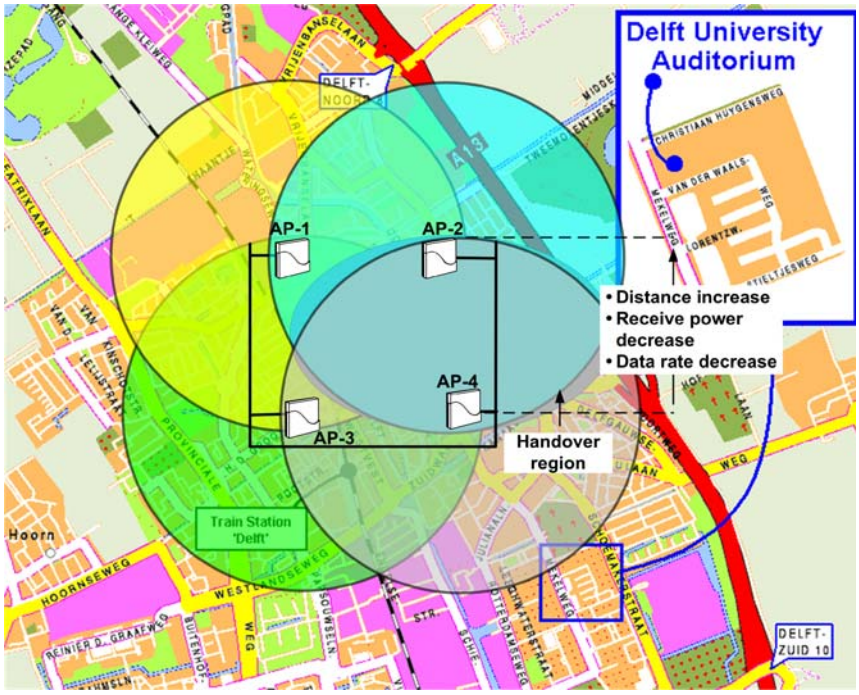


Figure 6-17 High capacity deployment example.

6.8.1.1 Horizontal Overlap

With the results in previous sections it is possible to find the point-to-point distance. If the location includes multiple types of construction materials, for example a combination of shoulder-height partitions and floor-to-ceiling brick walls one must identify the range associated with the type of RF obstacle(s). For stations to roam between various locations, they should be able to detect other APs prior to leaving the coverage area. To avoid out of range situations, the network should be designed in such a way that the wireless coverage areas of the individual APs overlap one another slightly.

For normal deployment slight overlap is considered to be enough, as depicted in Figure 6-16. This type of density pattern provides satisfactory results in normal density networks, where the stations roam at a pedestrian speed.

Increasing the overlap, as depicted in Figure 6-17, enables one to create a high capacity network, where numerous mobile wireless stations can engage in heavy traffic loads, or roam at velocities higher than the pedestrian speed.

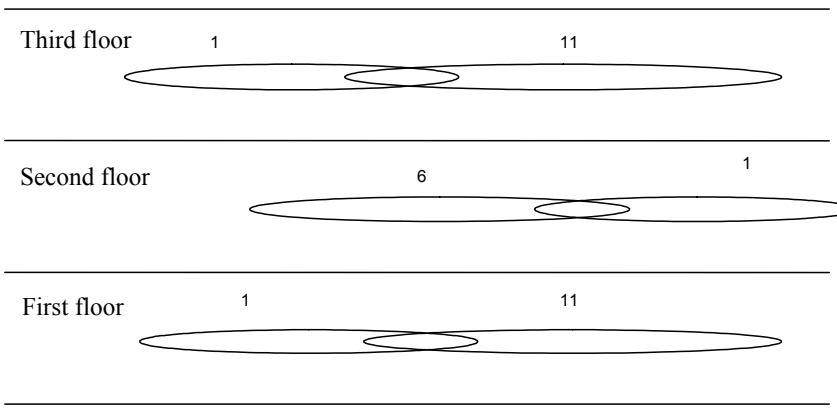


Figure 6-18 IEEE 802.11 in multifloor building.

Table 6-4 Number of Channels for Different Regions

Region	Channels Available	Number of Channels for Planning
US	2412, 2417, …. 2462 MHz (11 channels)	4 channels with 15 MHz spacing
Europe	2412, 2417, …2472 MHz (13 channels)	5 channels with 15 MHz spacing
Japan	2412, 2417, …2484 MHz (14 channels)	5 channels with 15 MHz spacing

6.8.1.2 Vertical Overlap

So as to deploy a WLAN network in a multi-story building the APs must not be placed on top of one another. One will leverage far more cost/throughput efficiency with alternate placement of APs across the various floors, in combination with smart radio channel allocation. In this way APs with the same frequency cannot hear each other. In multi-story buildings, one can also identify the vertical point-to-point distance, to determine the range of APs across multiple floors. An example of multifloor building deployment is given in Figure 6-18.

6.8.2 Frequency Planning

Cell planning which is focussed on a certain data rate can be designed based on the coverage range values as given in Table 6-3. For the case of IEEE 802.11 there is freedom to vary the CDT and the DT so as to vary the cell size this can also be found from Figure 6-11. Thus instead of cell dimensions based on the maximum coverage range one could also design a network with cell radius allowing reliable operation at the higher data rate, or a larger cell that requires fallback to lower data rates. The IEEE 802.11b adjacent channel rejection allows usage of channel with a spacing of 25 MHz with full cell overlap. For open environments (open air and open-plan buildings), neighbouring cells with channel spacing of 15 MHz can also be used. Thereby the number of available channel frequencies in the 2.4 GHz is sufficient to fill up the two-dimensional space.

The channels and the number of channels available for different regions of the world are given in Table 6-4 and Figure 6-13.

Enhanced provisions like load balancing and dynamic frequency selection provide an automatic selection of the optimum setting depending on the actual transmission conditions within a cluster of cells.

6.9 Conclusions

In this chapter system design and deployment issues for the IEEE 802.11 DSSS WLAN are given. Some performance results of the IEEE 802.11b are also given for the purpose of deployment.

Although the IEEE 802.11 is a standard, it does not provide solution for many issues which have direct effect on the system design and hence the performance and the deployment of the WLANs. These issues are roaming, the data rate control and the optimum solution for security. In this chapter, proposals for roaming, the automatic rate fallback and an explanation of power management are presented. Discussion and effect of different threshold values – the Carrier Detect Threshold and the Defer Threshold – which affect the system design and the deployment are also given. After the system design of the WLAN is explained, issues related to the deployment are presented.

Both numerical and measurement results of the MAC throughput are presented. Lower data rates have relatively higher data throughput (1 Mbit/s data throughput is 0.94 Mbit/s) than higher data rates (11 Mbit/s data throughput is 7.43 Mbit/s). Measurement results show that the throughput for two or more stations is same. Similar to numerical, the data throughput of lower data rates is relatively higher than the higher data rates. For one station at 11 Mbit/s the data throughput achieved is 4.5 Mbit/s while for multiple stations it is 6 Mbit/s. At 1 Mbit/s, the data throughput achieved for one or multiple stations is the same, 0.9 Mbit/s.

The chapter then presents results for the propagation and the coverage with different path loss models: free space, open office, semi-open office and closed office. These results are presented graphically in terms of the received signal power and the range. Results for an indoor environment with multiple floors, is also given. These results can be used to find the coverage for a given data rate based on the receiver sensitivity. Measured throughput results in terms of the received power for a WLAN using automatic rate fallback scheme is also presented.

Interference and coexistence study for the ISM band is extremely important. Results are given in this chapter for adjacent channel and co-channel interference, microwave oven interference and coexistence with Bluetooth and IEEE 802.11 FHSS (Frequency Hopping Spread Spectrum). Channels with a centre frequency separation of 15MHz can be used in adjacent cells while channels with 25 MHz centre frequency separation can be used for totally overlapped cells. Of course defer threshold and capture ratio (receiver sensitivity) are the basis for medium reuse planning. Microwave ovens are a big cause of interference in the 2.4 GHz ISM band. A packet must be received completely in the microwave oven idle period, thus higher data rates and fragmentation will give better performance in the presence of microwave interference.

Measurement results using the power management shows that in the idle power save mode 15 mA is utilized in contrast to 165 mA in the receive mode and 280 mA in the transmit mode. Although throughput when using the power save mode will be much lower.

Finally a cell planning method is presented using several results given throughout the chapter. One of the things that can be seen is that the number of channels usable is much higher than normally expected. It is a common thinking that totally separated channels must be used, which would mean, for example, three channels for Europe while, practically, 5 channels can be used for Europe.

This chapter has presented results on several issues related to the IEEE 802.11 DSSS (Direct Sequence Spread Spectrum) WLANs.

The system design presented in this thesis was used for the WLAN product (ORiNOCO) development in Lucent Technologies and the deployment method was also used within the company.

References

[1] IEEE, “802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” November 1997.

[2] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Artech House, 2000, ISBN 0-89006-530-6.

[3] A. Kamerman and L. Monteban, “WaveLAN-II: A High-Performance Wireless LAN for the Unlicensed Band”, Bell Labs Technical Journal, vol. 2, no. 3, 1997, pp. 118–133.

[4] K. Pahlavan and A.H. Levesque, *Wireless Information Networks*, Wiley, 1995, ISBN 0-471-1067-0

[5] R. van Nee, G. Awater, M. Morikura, H. Takanashi, M. Webster and K. Halford, “New High Rate Wireless LAN Standards”, IEEE Communications Magazine, Dec. 1999, pp. 82 – 88.

[6] A.R. Prasad, N.R. Prasad, A. Kamerman, H. Moelard and A. Eikelenboom, “Indoor Wireless LANs Deployment”, Proceedings of VTC 2000 Spring, Tokyo, Japan, 15-18 May 2000, pp. 1562-1566.

[7] A.R. Prasad, A. Eikelenboom, H. Moelard, A. Kamerman & N.R. Prasad, "Wireless LANs Deployment in Practice", chapter of Wireless Network Deployments, edited by R. Ganesh and K. Pahelvan, Kluwer Publications, 2000.

[8] A.R. Prasad, H. Moelard and J. Kruys, "Security Architecture for Wireless LANs: Corporate

& Public Environment", VTC 2000 Spring, Tokyo, Japan, 15-18 May 2000, pp. 283-287.

[9] K.C. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, September/October 1994, pp. 50-63.

[10] M.P.M. Hall and L.W. Barclay, *Radiowave Propagation*, IEE Electromagnetic Waves Series 30, London, 1991.

[11] T.S. Rappaport, *Wireless Communications: Principles & Practice*, Prentice Hall, 1996, ISBN 0-7803-1167-1.

[12] R. Prasad, *Universal Wireless Personal Communications*, Artech House, Norwood, MA, USA, 1998.

[13] A. Mehrotra, *Cellular Radio Performance Engineering*, Artech House, 1994, ISBN 0-89006-748-1.

[14] J.B. Andersen, T. Aulin, C.-E. Sundberg, *Digital Phase Modulation*, Plenum Press, 1986, ISBN 0-306-42195-X.

[15] J.C. Haartsen, "The Bluetooth Radio System", IEEE Personal Communications, vol. 7, nr. 1, February 2000, pp. 28 - 36.

[16] T.M. Siep, I.C. Gifford, R.C. Braley and R.F. Heile, "Paving the Way for Personal Area Network Standard: An Overview of the IEEE 802.15 Working Group for Wireless Personal Area Networks", IEEE Personal Communications, February 2000, Issue: 2000; 7:1.

[17] A.R. Prasad, A. Kamerman and H. Moelard, "IEEE 802.11 Standard", Chapter 3 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[18] A. Kamerman, "Coexistence between Bluetooth and IEEE 802.11 CCK: Solutions to avoid mutual interference", IEEE 802.11-00/162.

[19] J.B. Andersen, T.S. Rappaport and S. Yoshida, "Propagation Measurements and Models for Wireless Communications Channels", IEEE Communications Magazine, pp. 42-49, January 1995.

[20] A.R. Prasad, N.R. Prasad, A. Kamerman, H. Moelard, & A. Eikelenboom, "Performance Evaluation, System Design and Network Deployment of IEEE 802.11", International Journal on Wireless Personal Communications, Kluwer Academic Publishers, October 2001, Vol. 19, Nr. 1, pp. 57-79.

[21] H. Moelard, A. Kamerman, A.R. Prasad and N.R. Prasad, "System Design and Implementation Aspects", Chapter 5 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[22] A. Kamerman and A.R. Prasad, "Performance Analysis", Chapter 6 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[23] A. Kamerman, A.R. Prasad, N.R. Prasad, L. Brederveld and H. Moeleard, "Deployment" Chapter 7 of WLAN Systems and Wireless IP for Next Generation Communications, N.R Prasad and A.R. Prasad, editors, Artech House, January 2002.

[24] W.C.Y. Lee, *Mobile Cellular Telecommunications: Analog and Digital Systems*, Second Edition, McGraw-Hill, NY, USA, 1995.

Chapter 7

Conclusions and Future Directions

The thesis presents some challenges in the field of Wireless Local Area Networks (WLANs) and gives solutions for them. The work presented in this thesis was first done for proprietary WLANs at the time when no standardized WLANs existed in the market. The work was then continued and finalized in the IEEE 802.11 based WLANs. In this chapter the thesis work is concluded and a discussion on future directions of the wireless communications is given.

7.1 ARQ Scheme

Automatic Repeat reQuest (ARQ) schemes provides error correction based on time diversity. ARQ is often used for error correction because it requires less redundant bits than Forward Error Correction or FEC. One of the fundamental drawbacks of time diversity is the delay needed to collect the repeated transmission. In this thesis the ARQ work is focused on Internet Protocol (IP) packet transmission in the wireless medium. It was considered that the WLAN was being used for Internet access and E-mailing where delay is not an important factor.

In Chapter 2 a novel ARQ scheme is proposed for IP packet transmission. The proposed ARQ scheme is known as Selective Repeat + Multi Copy (SR/MC) ARQ. The basic idea of the proposed SR/MC ARQ scheme is to send fragments of IP packets in the SR mode until the last fragment is transmitted. If there are erroneous fragments after the last fragment is transmitted the scheme goes to the MC mode. In the MC mode multiple copies of erroneous fragments are transmitted cyclically.

The proposed SR/MC ARQ scheme gives optimum performance for a fragment size of 75 bytes and with the number of copies in the MC mode being M = 10. A fragment size of 75 bytes is large enough thus requiring low overhead and less memory management making the transmitter and the receiver structure simpler. The scheme gives a throughput higher than 0.9 for any IP packet size for much higher BER when compared with the Selective Repeat and Stutter 2 (SR+ST 2) –Stutter is similar to MC mode with the difference that a fragment is sent continuously until an ACK for it is received– and the Go-Back N (GBN) ARQs.

The proposed SR/MC ARQ was applied for patent and implemented by the author in the proprietary WLAN developed by Uniden Corporation. The implementation worked efficiently. Measurement result of the implemented ARQ gave similar performance as the numerical results.

Knowing, the above one can say that the proposed SR/MC ARQ scheme gives a very good performance and can be used for efficient IP packet transmission. As the simulation model used is a very practical one (implementation loss was also considered) and as shown by measurement results the proposed scheme should work very efficiently for other wireless communications systems than IP based WLANs.

7.2 Channel Sharing Protocol

The increase in the demand for the wireless communications services is causing further scarcity of the inherently limited spectrum. This raises the need for efficient use of the spectrum. Also, when numerous users desire to transmit in a channel at the same time, conflicts occur, so there must be procedures on how the available channel capacity is efficiently allocated to the users. These procedures constitute the Medium Access Control (MAC) protocol rules each user has to follow in accessing the common channel.

Chapter 3 proposes a novel MAC protocol named as Channel Sharing Protocol (CSP). So as to combat the collision problem faced by multiple access protocols during the channel access the proposed CSP makes use of the p-persistence algorithm. To use the channel efficiently the proposed CSP makes use of tokens so that several Stations (STAs) can join a single channel. The number of STAs per channel is fixed. In the p-persistence algorithm each STA is given a value, p_p, between 0 and 1, the STA generates a random value, p, between 0 and 1 before it begins to transmit. If p is greater than p_p then the STA can transmit. Once a STA has been assigned a channel it is given a token number. The STA then waits for its token number to be transmitted by the AP. Once the correct token is received the STA can start transmission.

Numerical results show that the proposed CSP gives a quasi constant throughput, as high as 0.9, for high value of p-persistence (p_p = 0.8, 0.9) with varying load. The proposed CSP outperforms CSMA/CA if the number of channels is three or more. The performance of the proposed CSP is better for larger number of channels. There is no effect on the performance of the proposed CSP with a varying number of STAs in a channel.

Simulation results show that the proposed CSP gives quasi constant throughput from 20 channels onwards while the channel access delay increases with the increase in number of channels. 20 is the optimum number of channels for the proposed CSP. Next the number of tokens that will give the optimum result was studied. This was done by simulating the proposed CSP for the number of tokens against the throughput. The result shows that 6 is the optimum number of tokens. The proposed CSP gives an optimum performance for a p-persistence value of 0.5.

The performance of the proposed CSP was then studied in terms of throughput and the Frame Error Rate (FER). Results show that a quasi constant throughput is achieved till the FER reaches 0.1. The proposed CSP outperforms the CSMA/CA even for a FER of 0.1.

The proposed CSP thus, makes efficient use of the spectrum and can be used for optimum IP packet transmission. A detailed implementation design was made by the author for Uniden Corporations' proprietary WLAN product. The proposed CSP was also applied for patent by the author.

7.3 QoS over Wireless LANs

Until now WLANs were only used for non real-time data but recent requirements for real-time synchronous traffic have brought about development in this field. These are normally known as providing Quality of Service (QoS). Different data types, voice, video etc., have different QoS requirements. Due to these developments the IEEE 802.11 standard started a MAC enhancement group. The purpose of this group is to enhance the MAC so as to provide QoS over IEEE 802.11.

In Chapter 4 QoS schemes for WLANs are studied, the work was done at the preliminary stage of IEEE 802.11 MAC enhancements. The chapter presents requirements for voice and qualitative analysis of four solutions for providing voice over WLANs (VoWLANs). These protocols are Blackburst, the Distributed Coordination Function (DCF), the Point Coordination Function (PCF) and priority queuing.

Qualitative analysis shows that Blackburst outperforms all the schemes in terms of delay as number of users increase. But implementation of Blackburst is difficult and it is not totally compatible with IEEE 802.11. The DCF will give very bad voice quality although it is compatible and is mandatory for IEEE 802.11. The PCF will give better performance than the DCF in terms of

delay but still studies show that the performance will not be as required. Priority queuing will give better performance than the DCF and the PCF and will be relatively easy to implement.

The above discussion shows that there is a trade-off between delivered QoS and implementation difficulty.

Blackburst has been implemented in some test system but never deployed in real products. The DCF based VoWLANs has been deployed by some companies but as expected the results are far from what a customer would expect. The PCF based VoWLAN is not deployed by any vendors of IEEE 802.11. Priority queuing with backoff for voice traffic less than that for data traffic is the most widely deployed scheme.

IEEE 802.11e has accepted priority queuing as one of the options thus proving that the study done in this thesis was accurate.

This thesis also presents possible solution for the end-to-end and the top-to-bottom QoS. By the top-to-bottom it is meant that all the protocols in the protocol stack understand and have similar understanding of the QoS. This is important to provide the required level of service. For the end-to-end QoS purpose the quality is mostly measured in terms of the physical and the MAC layer parameters which do not make much sense. The obvious way to control the QoS in different layers is by measuring the quality at the application layer and controlling the variables in each layer. The quality measured and the control based on application layer parameters remains a topic for future study.

7.4 Security

WLANs are envisaged to be used in various environments; in this thesis three WLAN usage environments are considered: academic, enterprise and public environments. These environments have different security requirements, as presented in Chapter 5. It is important that all solutions must be compatible with existing wireline security solutions. Moreover they should be scaleable, manageable and provide authentication, confidentiality and access control.

For an enterprise environment the existing security solution of the IEEE 802.11 is found to be good enough although the access control remains an issue. The academic environment makes use of Kerberos based security solution. Several solutions are studied in this chapter for the academic environment. The best solution is the one providing authentication at Kerberos and also at the AP level. In the public environment a Diffie-Hellman based public key solution is presented, it does fulfil most of the requirements but not all of them and the issue related to bogus AP also remains.

For most of the environments and solutions presented, access control is the main problem. For this purpose an access control protocol based on profile is proposed. The profile is stored at the server together with the username and the password. The proposed solution on access control is very secure. When combined with the security solutions presented for the two environments it fulfils all the security requirements. The proposed access control protocol was applied for patent by the author.

Some of the ideas were presented to the IEEE 802.11 standardization committee and as can be seen from current IEEE 802.11i and IEEE 802.11f drafts, these ideas were accepted.

7.5 Wireless LANs System Design and Deployment

The challenge of a wireless system is to serve the largest number of users with a specified system quality within the available medium. For this purpose the network deployment and study thereof plays a very important role. Before looking at the network deployment one has to consider the system design because the IEEE 802.11 standard allows several implementation options. In Chapter 6 a study is done on the system design of IEEE 802.11 based WLAN and critical issues related to the network deployment.

There are two basic requirements for a WLAN network deployment: the throughput and the coverage. On the one hand a network can be deployed with the primary requirement being the coverage. Such network will have low aggregate throughput and larger cells. Such network deployment will require lesser APs and thus will be cheaper. On the other hand the primary requirement can be the throughput. This means smaller cell size (still giving full coverage), requiring more APs and thus more expensive.

Based on the results given in Chapter 6 for the coverage, the interference and the throughput and understanding of the system design, the network deployment can be done. Frequency planning of each world region should be looked at separately as the same ISM band is not available everywhere.

If fully overlapped cells are deployed then centre frequencies spaced 25 MHz apart must be used while for adjacent cells channel frequencies with 15 MHz separation should be used. Of-course besides all this the interference sources must be isolated and the deployment environment must be carefully studied.

The results of this research was used for Lucent Technologies ORiNOCO product development and the deployment methodology was also used by the company.

7.6 Wireless Technologies in Future

Today basically three wireless technologies, besides satellite communications, have made an impact: WLANs, WPANs and WWANs. WLANs complement LANs while WPANs are used for short distance communications and WWANs cover wide area and is most commonly known as mobile or cellular communications. Recently the WLANs are being seen as threat to the WWANs but in-fact these two are complementary technologies. Another set of technology is the Fixed Wireless Access (FWA) or Broadband Wireless Access (BWA). Current standardization trend shows that the FWA technologies will get mobility functionalities; if this happens then FWA can be a threat to the WWANs. Development of 802.20 a Mobile BWA (MBWA) could surely be a threat for the WWANs in future. In the following future direction of WLANs, WWANs and WPANs are presented; an overview of wireless technology standards is given in Table 7-1.

7.6.1 WLANs

LANs (Local Area Networks) mostly make use of the Internet Protocols (IP). The growth in wireless and the benefits it provides has brought forward changes in the world of LANs in recent years. WLANs provide much higher data rates as compared to WWANs for slow mobile or static systems. The IEEE 802.11b based WLANs (Wireless LANs) are already widely being used while the IEEE 802.11g and IEEE 802.11a are also available in market.

WLAN technologies are mainly used for wireless transmission of IP packets. Until now, in contrast to the WWANs, the WLANs provided network access as a complement to the wireline LANs. In near future QoS based WLANs are expected to come in the market.

Table 7-1 Wireless Technologies.

Cellular Technology (WWAN)	**WLAN**	**WPAN**	**Cordless Technology**	**FWA/BWA**
GSM -HCSD, GPRS, EDGE- (WAP)	IEEE 802.11	IEEE 802.15	PHS	IEEE 802.16, IEEE 802.20 (MBWA)
IS-95	HIPERLAN/2	Bluetooth	DECT	HIPERACCESS
IS-54/IS-136	MMAC Ethernet WG & ATM WG (HiSWAN)	HIPERPAN	CT2/CT2+	High Speed Wireless Access
PDC (I-mode)	MBS			BWIF
3G	MMAC Wireless Homelink			LMDS
	HomeRF 1.0 & 2.0			MMDS

IEEE 802.11e is working towards MAC enhancements. The purpose of the MAC enhancement is to enable the present MAC, CSMA/CA, to provide QoS. The current draft has accepted two variations for QoS enhancements these are central control and distributed control based. For security, IEEE 802.11i, the main direction is towards applying IEEE 802.1X like solution with stronger and more choice of encryption algorithms. The IEEE 802.11 Working Group (WG) has also accepted a mobility solution known as Inter Access Point Protocol (IAPP), IEEE 802.11f. Another group in IEEE 802.11 is working on radio resource management (IEEE 802.11j); The IEEE 802.11 committee has approved IEEE 802.11h, dynamic frequency assignment and transmit power control. Due to the success of the standard there are several other study groups looking at higher data rate solutions (IEEE 802.11n 110Mbps+) and next generation technologies including standardization work with 3G standardization committees.

WiFi Alliance, an industry alliance, is providing interoperability specification and tests of the IEEE 802.11 products for better acceptance in the market. This alliance also provides recommendations for roaming between different Wireless Internet Service Providers (WISPs) so that a user, customer of one WISP, can access WLAN services when in another WISPs' hot-spot and still receive one bill.

Other known WLAN technologies are HIPERLAN Type 2 and HomeRF. HIPERLAN Type 2 is already standardized; it provides hooks for QoS and security for different environments. HomeRF developed several solutions but since beginning of 2003 HomeRF is announced to be dead.

The direction for WLANs at present would be to move towards a common international standard. Harmonization in 5GHz band technologies is a must so as to avoid making the 5GHz band a garbage band. Although harmonization is a solution it is possible that the market will be a deciding factor and choose one technology. For the time being the success of a standard will depend on pricing, performance [1], availability and marketing of the standards.

Besides the work being done by the standardization committees there should be study on providing top-to-bottom mapping. The correct mapping of higher layer protocols to lower layers protocols is a must to provide optimum service. Especially in the case of IEEE 802.11 where the standard only defines the bottom two layer, relations must be created with IETF, the committee developing layer three and some higher layer protocols

Basically most of the current development will lead to providing users different services within WLANs, in other words it is integration of services within one system. Another step currently becoming visible is towards integration with WWAN technologies like 3G.

7.6.2 WWANs

Growth in the field of Wireless Wide Area Network (WWAN) or more commonly known as mobile communications has been tremendous in the past decade. Second generation (2G), 2.5G and Third Generations (3G) standards of mobile systems are being used while efforts are going on towards development and standardization of Beyond 3G (B3G) systems. The existing (2G) systems are mainly for voice purposes. Due to the tremendous growth in Internet some support for data services like WAP (Wireless Application Protocol) and I-mode have been developed [2,3]. 2G supplement systems, 2.5G, like GPRS (General Packet Radio Systems) and now 3G systems provide further possibilities for data services with varying QoS requirements.

At present the main application for data services over mobile communications systems is Internet access. The future is towards a full multimedia type applications providing various levels of QoS (Quality of Service) using an IP (Internet Protocol) based backbone. Thus WWAN is also moving towards integration of services.

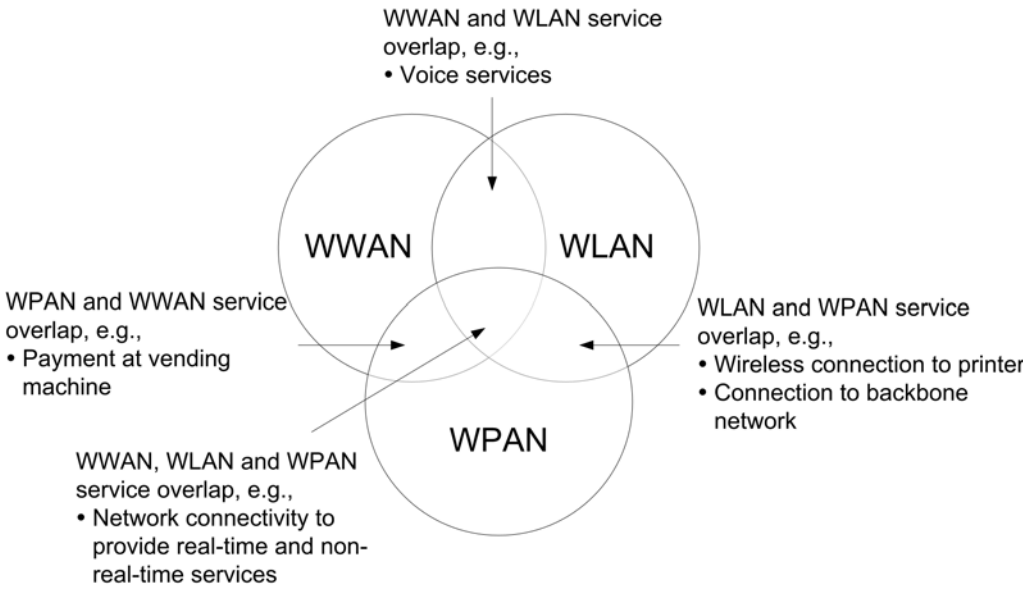


Figure 7-1 WWAN, WPAN and WLAN overlap.

Further works are being done by the standardization committees to integrate WLANs with 3G. Another development in the standardization of WWAN is towards an IP network. All this shows us that the WWANs are moving towards packet switched solutions and integration of technologies now that integration of services is almost achieved.

7.6.3 WPANs

Besides the WLANs, the Wireless Personal Area Networks (WPANs) like BLUETOOTH, HIPERPAN, and IEEE 802.15 are standardized. These technologies will be used for short distance (~10m) communications with low data rates for different QoS service. It is envisaged that the WPANs will exist in all the mobile terminals in the near future. The WPAN standards, IEEE 802.15.3 and .3a, have developed and work isgoing on higher data rates of about 55 Mbps thus paving path towards Broadband WPANs. IEEE 802.15.4 is focusing on very low data rate solutions which will work at a few or a few hundred kbps which is a first step towards the development of Body Area Networks. Several companies have reached consensus on Ultra Wide Band (UWB) as a solution for low data rate solution for IEEE 802.15.

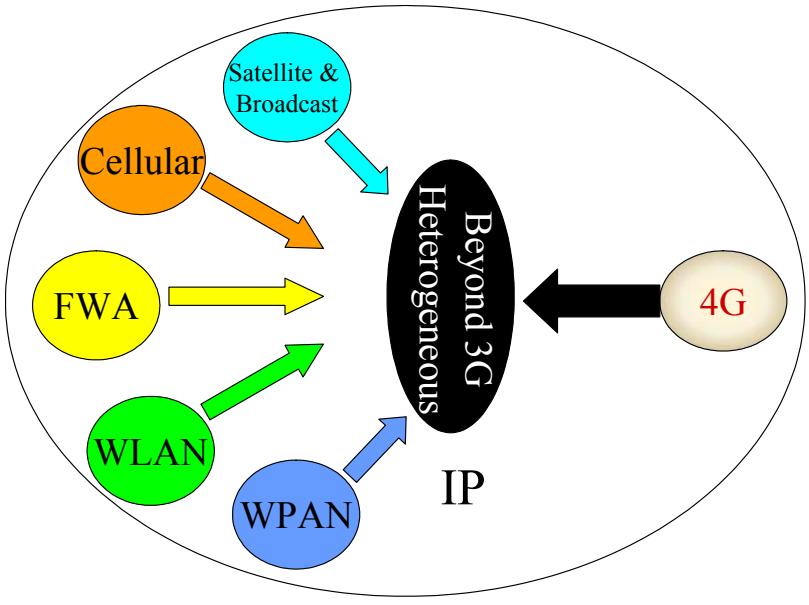


Figure 7-2 Future of telecommunications.

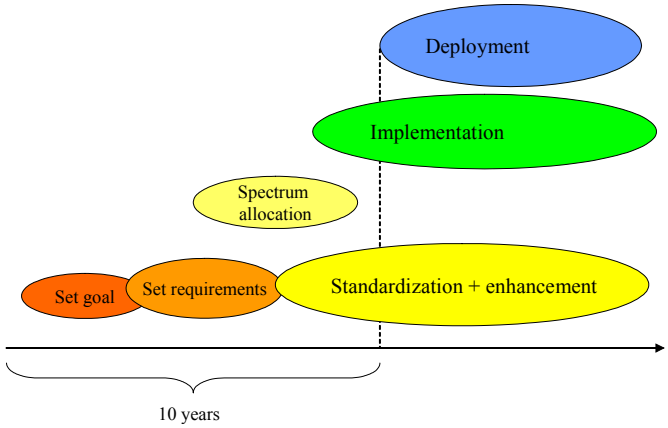


Figure 7-3 Time required for new technology development and deployment.

7.7 The Next Generation

Each wireless technology is moving towards future standardization. These standardization works are mainly focusing on wireless IP based QoS provision for any type of data. Here data is everything, be it audio, video, games or any other application. Basically this means an integration of services. All these technologies overlap each others areas of services to some extent. This is illustrated in Figure 7-1. Thus a move towards integration of technology is a logical next step to provide service continuity and higher user experience (Quality of Experience), see Figure 7-2.

The ITU-R vision for 4G also calls for integration of technologies which is commonly known as heterogeneous systems or beyond 3G or B3G systems (to some people B3G could mean any standard or technology developed after 3G). Integration of technology will provide adequate services to a user depending on mobility and availability. Of course this brings along several new challenges, for example, handover/handoff or mobility, security and QoS. These issues should be resolved without changing the existing standards. Seamless handover should be provided while a user moves form the network of one access technology to the other and domain of one stakeholder to the other. Seamless handover means provision of seamless service while the user is mobile, i.e., the user does not perceive any disruption in service or quality even during handover. IEEE 802 Handoff Executive Committee Study Group (ECSG) is working on the issue of handover for 802 based technologies.

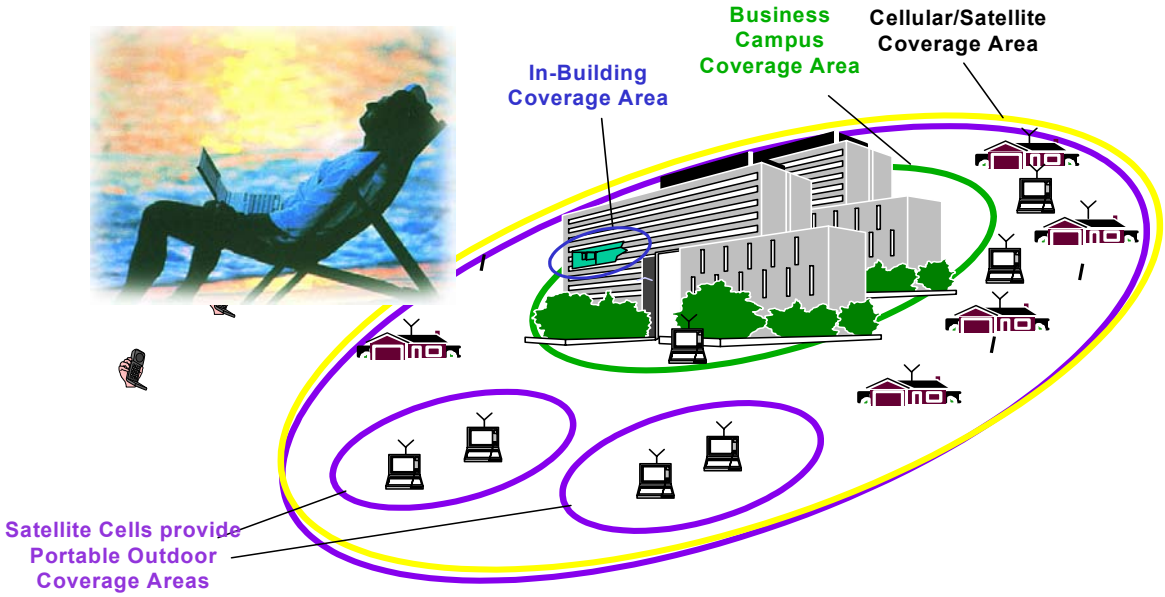


Figure 7-4 Future of wireless.

Table 7-2 Envisaged technology development in short, mid and long term.

	Stakeholder (of one or more access networks)	**IP**	**Broadcast** (DVB-T,DAB etc.)	**WPAN** (3G, 2.5G etc.)	**WLAN** (IEEE 802.11)	**Fixed** (FWA, ISDN etc.)	**WPAN and Ad-hoc** (IEEE 802 .15 etc.)
Short Term (2-3 yrs.)	Same (not broadcast)	v4	Similar to TV or Radio	3G and 2.5G, handover: maybe	b,g,a		
Mid Term (3-5 yrs.)	Same (maybe few different, surely not broadcast)	v4&6	As above	3G → 3.5G and 2.5G, handover: possible	g,a,n, NG, QoS		
Long Term (5-10 yrs.)	Same and Different	v4&6	SDR	2.5G, 3G, 3.5G and 4G handover: must	g,a,n, NG,QoS		

NG(+) Next Generation and beyond
↔ Handover
Gray For handover (arrows in 3 levels) it signifies the expected extent of handover. Darker the arrow the more common the handover between the concerned technologies.
For technologies (e.g. **2.5G**) it signifies lesser or decreased used of technology.

The ITU-R vision also talks about a new air interface, also known as 4G. As any new system takes about 10 years to develop and deploy, (see Figure 7-3), work on B3G and 4G has already started, a possible solution is given in [4]. Current market shows that 3G is going through trouble hopefully lessons will be learnt from it while developing 4G [5].

A possible future scenario is given in Figure 7-4. All technologies working together while at the same time providing all the services to the users anywhere and anytime.

Table 7-2 shows the envisaged development in stakeholder of various networks and technological development for short, mid and long term future. The table also points out several technological issues that should be worked on. Arrows between two cells of the table shows possibility of handover between the two technologies while the shade of the arrow (gray scale) shows the expected extent of handover. Research work should be done on seamless handover which brings in study of several issues like security and QoS which should be done at each protocol layer and network element. This topic itself will require further study on development methods and technologies including hardware, software and firmware and technologies like Application Specific Integrated Circuits (ASICs). Another important research topic is Software Defined Radio (SDR) which includes reconfigurability at every protocol layer.

WLANs provide roaming within LANs and work is going on towards further enhancement in this field. While WWANs provide roaming too, the challenge now is to provide seamless roaming from one system to other from one location to other and from one network provider to other. In terms of security again both WLANs and WWANs have their own approach. The challenge is to provide the level of security required by the user while roaming from one system to other. User must get end-to-end security independent of any system, service provider or location. Security also incorporates user authentication that can be related to another important issue: billing. Both security and roaming must be based on the kind of service a user is accessing. The required QoS must be maintained when a user roams from one system to other. Besides maintaining the QoS it should be possible to know the kind of service that can be provided by a particular system, service provider and location. Work on integration of the WLANs and the WPANs must also be done. The biggest technical challenge here will be the coexistence of the two devices as both of them work in the same frequency band. FWA is a technology that should be watched as it develops, depending on its market penetration and development of standards it should also be integrated together with other technologies.

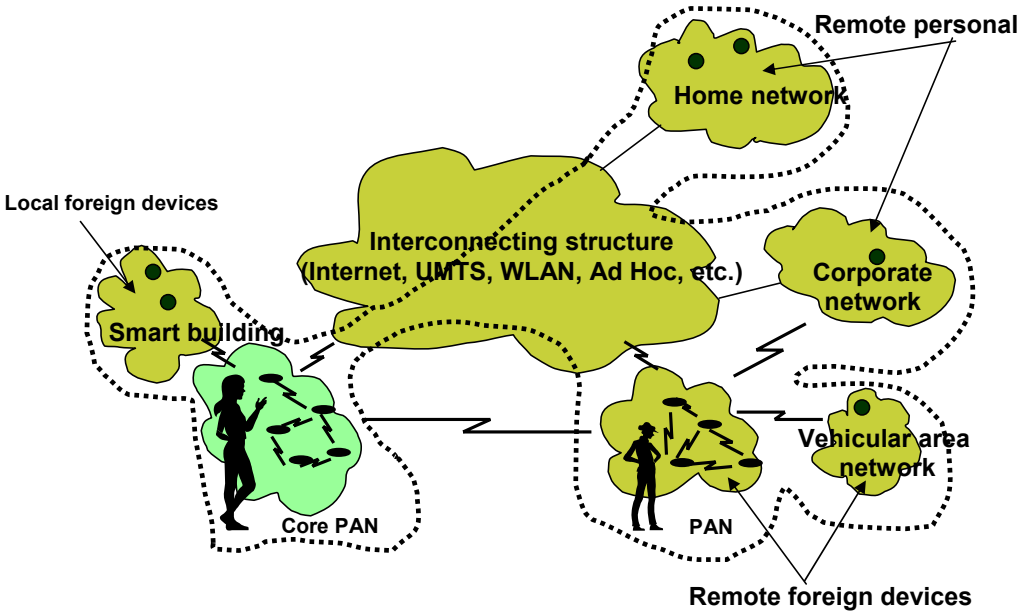


Figure 7-5 Personal Network [6].

Another area of research for the next generation communications will be in the field of Personal Networks (PNs) [6]. PN provides a virtual space to the users that spans over a variety of infrastructure technologies and ad-hoc networks. In other words PNs provide a personal distributed environment where people interact with various companions, embedded or invisible computers not only in their vicinity but potentially anywhere. Figure 7-5 portrays the concept of PNs. Several technical challenges arise with PNs, besides interworking between different technologies, some of which are security, self-organization, service discovery and resource discovery [6].

References

[1] A. Kamerman and A.R. Prasad, "IEEE 802.11 and HIPERLAN/2 Performance and Applications", ECWT 2000, 2-6 October 2000, Paris, France.

[2] http://www.nttdocomo.com/i/

[3] http://www.wapforum.org/

[4] J.Farserotu, G. Kotrotsios, I. Kjelberg and A.R. Prasad, "Scalable, Hybrid Optical-RF Wireless Communication System for Broadband and Multimedia Service to Fixed and Mobile Users", Invited Paper, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, Jan 2003, Vol 24, Nr. 2, pp. 327-339.

[5] O.M. Lauridsen and A.R. Prasad, "User needs for services in UMTS", Invited Paper, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, August 2002, Vol 22, Nr. 2, pp. 187-197.

[6] I.G. Niemegeers and S.M. Heemstra de Groot. "Research Issues in Ad-Hoc Distributed Personal Networks", International Journal on Wireless Personal Communications, Kluwer Academic Publishers, September 2003.

Appendix A: License Exempt Frequency Bands

Location	Regulatory Range	Maximum Output Power	Standard
Europe	2400 – 2483.5 MHz	10 mW/MHz (max 100 mW)	IEEE 802.11b,g, HomeRF, WBFH, Bluetooth
	5150 – 5350 MHz 5470 – 5725 MHz	200 mW 1000 mW	HIPERLAN/2 HIPERACCESS (FWA<11GHz) IEEE 802.11a
North America	2400 – 2483.5 MHz	1000 mW	IEEE 802.11b,g, HomeRF, WBFH, Bluetooth
	5150 – 5250 MHz 5250 – 5350 MHz 5725 – 5825 MHz	2.5 mW/MHz (max. 50 mW) 12.5 mW/MHz (max 250 mW) 50 mW/MHz (max 1000 mW)	HIPERLAN Type 2 BWIF, IEEE 802.16 HUMAN IEEE 802.11a
Japan	2400 – 2497 MHz	10 mW/MHz (max 100 mW)	IEEE 802.11b,g, HomeRF, WBFH, Bluetooth
	5150 - 5250 MHz 4900 – 5000 MHz (until 2007) 5030 – 5091 MHz (from 2007)	Indoor 200 mW	HIPERLAN Type 2 (MMAC HiSWAN) IEEE 802.11a (MMAC)

Appendix B: Comparison WLANs and WPANs Standards

Standard	IEEE 802.11/b	IEEE 802.11a/g	HIPERLAN/2	IEEE 802.15 1.0 and Bluetooth	HomeRF
Mobile Frequency Range (MHz)	2400-2483 (North America/ Europe) 2470-2499 (Japan)	a: 5150 – 5250 (Europe, North America, Japan) 5250 – 5350 (Europe, North America) 5470 – 5725 (Europe) 5725 – 5825 (North America) 4900 – 5000 (Japan) g: same as IEEE 802.11/b	Same as 802.11a	2400-2483 (North America/ Europe) 2470-2499 (Japan)	2400-2483 (North America/ Europe) 2470-2499 (Japan)
Multiple Access Method	CSMA/CA (Distributed and Centralized)	CSMA/CA (Distributed and Centralized)	TDMA (Centralized)	TDMA (Centralized)	TDMA (Distributed) / CSMA (Centralized)
Duplex Method	TDD	TDD	TDD	FDD	TDD
Number of independent Channels	FHSS:79 DSSS:3 to 5	a: 12 g: 3 to 5	12	FHSS: 79	FHSS: 79
Modulation	FHSS GFSK (0.5 Gaussian Filter) DSSS DBPSK (1MB/s), DQSK (2MB/s) b DSSS: CCK	a/g: OFDM 48 carriers 6 Mbps BPSK 1/2 9 Mbps BPSK 3/4 12 Mbps QPSK 1/2 18 Mbps QPSK 3/4 24 Mbps 16QAM 1/2 36 Mbps 16QAM 3/4 48 Mbps 64QAM 2/3 54 Mbps 64QAM 3/4 g PBCC and DSSS OFDM optional	OFDM 48 carriers 6 Mbps BPSK 1/2 9 Mbps BPSK 3/4 12 Mbps QPSK 1/2 18 Mbps QPSK 3/4 24 Mbps 16QAM 1/2 36 Mbps 16QAM 9/16 48 Mbps 64QAM 3/4 54 Mbps 64QAM 3/4	FHSS GFSK (0.5 Gaussian Filter)	FHSS GFSK (0.5 Gaussian Filter)
Channel Bit Rate (Mbps)	1 or 2 b 5.5 or 11	a/g: 6, 9, 12, 18, 24, 36, 48 and 54	6, 9, 12, 18, 24, 36, 48 and 54	1	1 or 2

Appendix C: WNIC Specification

System Specification

Size	77mm(W) × 120mm(L) × 14mm(H)
Weight	250g
Power Consumption	500mW
Power Supply	DC 5V

Radio Characteristics

Frequency Range	902-928MHz
Bandwidth	26MHz
Channels	17
Bandwidth per Channel	1.5MHZ
Chip Rate	1 Mcps
Bit Rate	181kbps
Data Rate	64 kbps uplink 64 kbps downlink
Transmitter Power	10mW/MHz
Peak Power	10dBm
Antenna Gain (Transmitter and Receiver)	2.15dBi
Antenna Body Loss	0
Receiver Sensitivity (BER 10^{-3})	-107dBm
Receiver Noise Figure	6.5dB
Cable/Connectors Losses	0.5dB
Isolator + Filter Losses	2.5dB
Communication Range	300 feet indoor LOS 1500 feet outdoor LOS
1st Modulation	DQPSK
2nd Modulation	Offset Chip DS-SS
SS Code	11 bit Barker Sequence
Multiple Access Scheme	FDMA/TDD
TDD Frame Time	10ms/frame
Digital Filter	Root Roll-off (α=0.5)
Error Control	BCH(63,51,2) and Hybrid ARQ (SR/MC)

Network Characteristics

Ethernet Interface	RJ45
Wireless Protocol	Uniden Proprietary
LAN Protocol	IEEE 802.3 (CS 8900)

Appendix D: List of Abbreviations

ACK	Acknowledgement
AD	Address
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
ANSI	American National Standards Institute
AP	Access Point
API	Application Program Interface
ARF	Automatic Rate Fallback
ARQ	Automatic Repeat Request
AS	Authentication Server
ATM	Asynchronous Transfer Mode
AWGN	Additive White Gaussian Noise
B	Broadcast
BCH	Bose Chaudhuri Hocquenghem
BER	Bit Error Rate
BS	Base Station
BWA	Broadband Wireless Access
BWIF	Broadband Wireless Internet Forum
CCK	Complementary Code Keying
CFP	Contention Free Period
CHAP	Challenge Handshake
CP	Contention Period
CQ	Communications Quality
CR	Channel Request
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA/Collision Avoidance
CSMA/CD	CSMA/Collision Detection
CSP	Channel Sharing Protocol
CTS	Clear To Send
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DHA	Diffie-Hellman Authentication
DIFS	Distributed Inter Frame Space
DQPSK	Differential Quadrature Phase Shift Keying
DS	Direct Sequence
DSBM	Designated Subnet Bandwidth Manager
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over Local Area Network
EIRP	Effective Isotropic Radiated Power
ETE	End To End
ETS	European Telecommunications Standard
FCC	Federal Communications Commission

FCI	Free Channel Information
FEC	Forward Error Correction
FER	Frame Error Rate
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FWA	Fixed Wireless Access
GBN	Go Back-N
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HIPERACCESS	High Performance Radio Access
HIPERLAN	High Performance Radio Local Area Network
HUMAN	High-Speed Unlicensed Metropolitan Area Networks
IEEE	Institute of Electrical and Electronic Engineering
IETF	Internet Engineering Task Force
IFS	Inter Frame Space
IKE	Internet Key Exchange
IKMP	Internet Key Management Protocol
IP	Internet Protocol
IPSec	IP Security
ISA	Instruction Set Architecture
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Industry Scientific Medical
ISP	Internet Service Provider
IS-XX	Interim Standard – XX
ITU	International Telecommunications Union
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LMDS	Local multipoint distribution system
MAC	Medium Access Control
MBWA	Mobile Broadband Wireless Access
MC	Multi-Copy
MD5	Message Digest 5
MMAC	Multimedia Mobile Access Communication
MMDS	Multichannel Multipoint Distribution Service
NACK	Negative ACK
NC	Network Computer
ND	No Data
NG	Next Generation
OS	Operating System
OSS	Operation Support System
PAP	Password Authentication Protocol
PC	Point Coordinator
PCF	Point Coordination Function
PCI	Personal Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDC	Personal Digital Cellular
PEAP	Protected Extensible Authentication Protocol
PGP	Pretty Good Privacy
PHS	Personal Handy phone System
PHY	PHYsical layer
PIFS	PCF Inter Frame Space
PKI	Public Key Infrastructure
POTS	Plain Old Telephone System
PPP	Point to Point Protocol

PPTP	Point to Point Tunneling Protocol
PS	Personal Station
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Access Dial In User Service
RF	Radio Frequency
RFC	Request For Comments
RSVP	Resource Reservation Protocol
RTD	Round Trip Delay
RTS	Request To Send
S/MIME	Secure/Multipurpose Internet Mail Extension
SAW	Surface Acoustic Wave
SBM	Subnet Bandwidth Manager
ShKA	Shared Key Authentication
SIFS	Short Inter Frame Space
SIR	Signal Interference Ratio
SKA	STA-Kerberos-AP
SR	Selective Repeat
SR+ST	Selective Repeat + Stutter
SS	Spread Spectrum
SSH	Secure Shell
SSL	Secure Sockets Layer
STA	STAtion
SW	Stop and Wait
TDD	Time Division Duplex
TGS	Ticket Granting Server
TLS	Transport Layer Security
TTLS	Tunnelled TLS
UMTS	Universal Mobile Telecommunications System
USA	United States of America
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Card

Appendix E: List of Symbols

$\lfloor X \rfloor$	Round down
$\lceil X \rceil$	Round up
μs	Micro second
A	Diffie-Hellman root number
$Authenticator_X$	Authenticator for X
B	Expected number of busy channels / time
BCH(n,k,t)	k: Number of bits in a BCH block before coding, n: Total number of bits after BCH coding, t: Number of bits that can be corrected
C	Expected number of channels with collision
$\widetilde{C}$	Probability of number of channels with collision
D	Total IP packet transmission delay for ARQ Waiting period for channel access by a station for blackburst
D_{max}	Maximum delay in transmission
D_X	Decrypt with X
dB	Decibels
E_b/N_0	Ratio of energy per bit to noise
E_{PS}	Number of PS
E_X	Encrypt with key X
$E_{K\,j,i}[X]$	Encrypt X using key of j for I
f_D	Doppler Frequency
G	Arrival rate
G	Load
GHz	Giga Hertz
H	Header length
I	Expected number of idle channels / time
$\widetilde{I}$	Probability of number of channels are idle
ID	Identity
IP_S	IP packet size
$K_{j,I}$	Key of j for I
kbps or kbit/s	Kilobits per second
M	Number of copies sent in multicopy mode for ARQ (Chapter 2) Number of channels for CSP (Chapter 3)
m	Size of fragment in bits (Chapter 2) Meter (Chapter 6)
MA	Milli Ampere
Mbit/s or Mbps	Mega bits per second
MHz	Mega Hertz
Ms	Millisecond
MW	Milli Watt
N	Number of fragments for ARQ (Chapter 2)

	Total number of PS allowed per channel for CSP (Chapter 3)
N_{MC}	Number of fragments in Multi Copy mode
N_{SR}	Number of fragments in Selective Repeat mode
O	Overhead
P	Probability of bit error (BER)
	Diffie Hellman modulus
P	Probability of frame error (FER)
$P_{channel\ idle}$	Probability of an idle channel
P_{IP}	Probability that a IP packet arrives
Pkt_Time	Time to transmit packet
$P_{no\ data\ arrives}$	Probability that no data arrives
p_p	p-persistence value
$P_{token\ received}$	Probability that a token is received
P_X	Public key of X
q_{ij}	Probability that i. Out of j fragments are erroneous
r_c	Data rate
r_s	Coding rate of voice stations
S	Throughput
S_D	Data throughput
T	TDD time slot
t_{bslot}	Blackburst slot duration
$Ticket_X$	Ticket for X
t_{inter}	Minimum channel access delay
t_{long}	Time for long interframe space
t_{med}	Time for medium interframe space
t_{neg}	Retransmission request time
t_{obs}	Channel observation time
t_{sch}	Scheduled time for next packet
t_{short}	Time for short interframe space
TS_X	Time Stamp X
t_{unit}	System parameter (slot time of IEEE 802.11)
U	Expected number of utilized time / channels
$\widetilde{U}$	Probability of number of channels utilized
V	Server from which STA wants service (Kerberos)

Appendix F: Publications and Contributions Per Chapter

F1 Chapter 2

Product and Application

Wireless Network Interface Card (WNIC) for Uniden Corporation, Tokyo, Japan.

Designed, studied performance, implemented and tested till the product was ready for Engineering Pre Production.

Publications

Journal

[1] A.R. Prasad, "Optimization of Hybrid ARQ for IP Packet Transmission", International Journal on Wireless Personal Communications, Kluwer Academic Publishers, March 2001, Volume 16, issue 3, pp. 203-220.

[2] A.R. Prasad, Y. Shinohara and K. Seki, "Performance of Hybrid ARQ for IP Packet Transmission on Fading Channel", IEEE Transactions Vehicular Technology, May 1999, Vol. 48, Nr. 3, pp. 900-910.

International Conferences

[1] A.R. Prasad and K. Seki, "Performance of a Hybrid ARQ for IP Packet Transmission under Fading Channel", PIMRC'98, September 8-11, Boston, Massachusetts, USA.

[2] A.R. Prasad and K. Seki, "Hybrid ARQ for IP Packet Transmission", ICUPC'97, San Diego, USA, pp. 531-535, 12-16 October 1997.

National Conferences Japan

[1] Y. Omoya, A.R. Prasad, N. Matsuoka and K. Seki, "A Wireless IP Packet Transmission Scheme", IEICE General Conference, Tokai University, Hiratsuka, Japan, B-5-305, 27-30 March 1998.

[2] A.R. Prasad and K. Seki, "Performance of Hybrid ARQ for IP Packet Transmission in Fading Channel", IEICE General Conference, Waseda University, Tokyo, Japan, B-5-84, 3-6 September 1997.

[3] A.R. Prasad and K. Seki, "Internet Protocol Packet Transmission using Hybrid SR/MC Scheme", IEICE General Conference, Kansai University, Suita, Japan, B-8-20, 24-27 March 1997.

Patents Applied

[1] "Packet Transfer Scheme in Unbalanced Channel", November 1996.

[2] "A Wireless IP Packet Transmission Scheme", January 1998.

Company Internal Reports

[3] SR/MC ARQ Design Document

[4] ARQ Performance

[5] SR/MC ARQ Functions Descriptions

[6] WNIC Protocol

Other Achievements

Trained a summer intern and a fresh man on ARQ schemes.

Presented in Victoria University, Canada.

F2 Chapter 3

Product and Application

Wireless Network Interface Card (WNIC) for Uniden Corporation, Tokyo, Japan.

Designed, studied performance and prepared implementation documents.

Publications

International Conferences

[1] A.R. Prasad and K. Seki, "Capacity Enhancement of Indoor Wireless Communication System with a Novel Channel Sharing Protocol", ICPWC'97, Mumbai, India, pp. 162-166, 16-19 December 1997.

National Conferences Japan

[1] K. Ogata, A.R. Prasad and K. Seki, "Performance Analysis of a Novel Channel Sharing Protocol for Wireless communication", IEICE General Conference in September 1998.

[2] A.R. Prasad, and K. Seki, "Novel Channel Sharing Protocol for Indoor Wireless Communication", IEICE General Conference, Tokai University, Hiratsuka, Japan, B-5-306, 27-30 March 1998.

[3] N. Matsuoka, A.R. Prasad and K. Seki, "Performance Analysis of a Novel Channel Sharing Protocol for Indoor Wireless Communication", IEICE General Conference, Tokai University, Hiratsuka, Japan, B-5-307, 27-30 March 1998.

Patents Applied

[1] "Channel Sharing Protocol", August 1997.

Company Internal Reports

[1] CSP Design Document

[2] WNIC Protocol

Other Achievements

Trained a summer intern and a freshman.

Presented in Victoria University, Canada.

F3 Chapter 4

Product and Application

ORiNOCO, IEEE 802.11 WLAN of Lucent Technologies, The Netherlands.

Studied for IEEE 802.11 standard.

Priority queuing type system designed; implemented as the first voice over ORiNOCO product.

Publications

International Conferences

[1] A.R. Prasad, "Performance Comparison of Voice of IEEE 802.11 Schemes", VTC 1999 Fall, 19-22 September 1999, Amsterdam, The Netherlands.

Company Internal Reports

[1] HIPERLAN Type 2 RLC and DLC.

[2] MAC Enhancement Requirements for IEEE 802.11.

[3] Quality of Service Solution for IP.

[4] Blackburst Architecture for WaveLAN.

[5] H.323.

[6] Subnet Bandwidth Manager.

[7] Priority Queuing Architecture.

[8] Voice over WaveLAN.

F4 Chapter 5

Product and Application

ORiNOCO, IEEE 802.11 WLAN of Lucent Technologies, The Netherlands.

Proposed security solution for IEEE 802.11 standard.

Implementation design for ORiNOCO.

Publications

Standards Proposal

[1] A. Prasad and A. Raji, "A Proposal for IEEE 802.11e Security", IEEE 802.11e, 00/178, July 2000.

Books

[1] N.R Prasad and A.R. Prasad, editors, *WLAN Systems and Wireless IP for Next Generation Communications*, Artech House, December 2001.

International Conferences

[1] A.R. Prasad, H. Moelard and J. Kruys, "Security Architecture for Wireless LANs: Corporate & Public Environment", VTC 2000 Spring, May 2000, pp.283-287.

Patents Applied

[1] "Enhanced Security with Flexible Handshake", June 2000.

[2] "Access Control for Wireless LANs", February 2000.

Company Internal Reports

[1] MAC Enhancement Requirements for IEEE 802.11.

[2] Security Proposal for IEEE 802.11.

[3] Available Security Solutions.

[4] User based Authentication via RADIUS.

[5] Wired Equivalent Privacy Architecture.

[6] Authentication Schemes.

[7] Key Roll-over

[8] Common Security Architecture.

[9] X.509

Other Achievements

Proposed solution to IEEE 802.11 standard.

F5 Chapter 6

Product and Application

ORiNOCO, IEEE 802.11 WLAN of Lucent Technologies, The Netherlands.

Document used as Lucent WLAN deployment guide.

Publications

Books

[1] N.R Prasad and A.R. Prasad, editors, *WLAN Systems and Wireless IP for Next Generation Communications*, Artech House, December 2001.

Journal

[1] A.R. Prasad, A. Eikelenboom, H. Moelard, A. Kamerman & N.R. Prasad, "Performance Evaluation, System Design and Network Deployment of IEEE 802.11", accepted for publication, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, October 2001, Vol. 19, Nr. 1, pp. 57-79.

Chapter

[1] A.R. Prasad, A. Eikelenboom, H. Moelard, A. Kamerman & N.R. Prasad, "Wireless LANs Deployment in Practice", chapter of Wireless Network Deployments, edited by R. Ganesh and K. Pahelvan, Kluwer Publications, June 2000.

International Conferences

[1] A.R. Prasad, N.R. Prasad, A. Kamerman, H. Moelard and A. Eikelenboom, "Indoor Wireless LANs Deployment", VTC 2000 Spring, May 2000, pp. 1562-1566.

Patents Applied

[1] "Enhanced Data Rate Control for Wireless LANs", January 1999.

Company Internal Reports

[1] ORinOCO Deployment.

F6 Chapter 7

Product and Application

ORiNOCO, IEEE 802.11 WLAN of Lucent Technologies, The Netherlands.

Publications

Books

[1] N.R Prasad and A.R. Prasad, editors, *WLAN Systems and Wireless IP for Next Generation Communications*, Artech House, December 2001.

Journals

[2] J.Farserotu, G. Kotrotsios, I. Kjelberg and A.R. Prasad, "Scalable, Hybrid Optical-RF Wireless Communication System for Broadband and Multimedia Service to Fixed and Mobile Users", Invited Paper, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, Jan 2003, Vol 24, Nr. 2, pp. 327-339.

[1] O.M. Lauridsen and A.R. Prasad, "User needs for services in UMTS", Invited Paper, International Journal on Wireless Personal Communications, Kluwer Academic Publishers, August 2002, Vol 22, Nr. 2, pp. 187-197.

International Conferences

[1] A. Kamerman and A.R. Prasad, "IEEE 802.11 and HIPERLAN/2 Performance and Applications", ECWT 2000, 2-6 October 2000, Paris, France.

Company Internal Reports

[1] WLANs and WWANs Interworking.

Other Achievements

Coordinated a project on WLANs and WWANs interworking.

F7 Other Topics

Publications

Books and Chapters

[1] A.R. Prasad, "Perceptual QoS for Wireless and Internet", chapter of Wireless Internet, editors: S. Dixit and R. Prasad, Artech House, October 2002.

[2] N.R Prasad and A.R. Prasad, editors, *WLAN Systems and Wireless IP for Next Generation Communications*, Artech House, December 2001.

[3] A.R. Prasad, A. Eikelenboom, H. Moelard, A. Kamerman & N.R. Prasad, "Wireless LANs Deployment in Practice", chapter of Wireless Network Deployments, edited by R. Ganesh and K. Pahelvan, Kluwer Publications, 2000.

International Conferences

[1] A.R. Prasad, P. Schoo and H. Wang, “An Evolutionary Step towards Ubiquitous Communications: A Security Perspective”, SAINT 2004, January 26 – 30, 2004, Tokyo, Japan.

[2] A.R. Prasad, H. Wang and P. Schoo, “Infrastructure Security for Future Mobile Communications Systems”, WPMC 2003, October 19-22, 2003, Yokosuka, Japan.

[3] H. Wang and A.R. Prasad, “Security Context Transfer in Vertical Handover”, PIMRC 2003, September 7-10, 2003, Beijing, China.

[4] A.R. Prasad and H. Wang, “Network Operator’s Security Requirements on Systems Beyond 3G”, WWRF #9, 1-2 July 2003, Zurich, Switzerland.

[5] A.R. Prasad and P. Schoo, “IP Security for Beyond 3G towards 4G”, WWRF #7, 3-4 December 2002, Eindhoven, the Netherlands.

[6] H. Wang, A.R. Prasad, P. Schoo, S. Tessier and O. Tirla “A domain model approach to network security”, IST-MIND International Workshop, London, England, 7 October 2002 and Budapest, Hungary, 18 November 2002.

[7] A.R. Prasad and S. Andresen, “Integrated Approach to Low Latency in mixed Wired and Wireless Environments”, WPMC 2002, 26-30 October 2002, Honolulu, Hawaii, USA.

[8] A. R. Prasad, R. Esmailzadeh, S. Winkler, T. Ihara, B. Rohani, B. Pinguet and M. Capel, “Perceptual Quality Measurement and Control: Definition, Application and Performance”, WPMC 2001, 9-12 September 2001, Aalborg, Denmark.

[9] M. Imine and A.R. Prasad, "Audio Coding using Parametric Piecewise Modeling", ICPWC'99, 17-19 February, 1999, Jaipur, India, pp. 414-418.

[10] M. Imine and A.R. Prasad, “Parametric Piecewise Modeling as a Novel Coding Scheme”, WPMC'98, 4-6 November 1998, Yokosuka, Japan, pp. 170-175.

[11] A.R. Prasad et al, “Generation and Testing of Self-Similar Traffic in ATM Networks”, 2nd IEEE International Conference on Personal Wireless Communication, Delhi, India, pp. 200-205, 19-22 February 1996.

[12] A.R. Prasad, “Asynchronous Transfer Mode Based Mobile Broadband System”, IEEE Third Symposium on Communications and Vehicular Technology, Eindhoven, pp. 143-148, 26-27 October 1995.

Patents Applied

[1] “Seamless Handover Mechanisms: Inter-Stakeholder, -Technology and -Network”, September 2003.

[2] “Seamless Handover Decision”, September 2003.

[3] “Context Transfer in Seamless Handover”, September 2003.

[4] “Perceptual QoS based Link Adaptation”, December 2001.

[5] “Call Admission Control for Wireless Multimedia Systems”, February 2001.

[6] “Call-back for Mobile Networks”, February 2001.

Appendix G: About the Author

Anand Raghawa Prasad (The Netherlands), Senior Researcher, DoCoMo Euro-Labs, Munich, Germany was born in Ranchi, India. He received M.Sc. (Ir.) degree in E.E. from Delft University of Technology, The Netherlands, in the field of Self Similarity of ATM Network Traffic in 1996. From 1996 to 1998 November he worked as Research Engineer and later Project Leader in Uniden Corporation, Tokyo, Japan. From 1998 till 2000 he worked as Systems Architect for Wireless LANs in the Wireless Communications and Networking Division of Lucent Technologies (now Agere Systems) in The Netherlands. Subsequently, he was Technical Director at Genista Corporation, Tokyo, Japan. In addition to his publications in journals, international conferences and chapters in books, he has several patent applications in the field of wireless communications and has co-edited a book titled "WLAN Systems and Wireless IP for Next Generation Communications" published by Artech House. He plans to write a book on "Wireless LANs and Wireless IP: Security, Mobility, QoS and Mobile Network Integration" and is a guest editor of a Special Issue on "Security for Next Generation Communications" of Kluwer International Journal on Wireless Personal Communications. His research interests include software radio, next generation wireless systems, networks and access, security and QoS for WLANs, WPANs, mobile communications and IP networking.