Mixed Contention and Contention Free MAC Layer Scheduling Techniques in Multi-Cluster WLAN

Md. Shahidul Hoq Akond

A Thesis
in
The Department
of
Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Applied Science at
Concordia University
Montreal, Quebec, Canada

July 2004

Your file Votre référence
ISBN: 0-612-94689-4
Our file Notre référence
ISBN: 0-612-94689-4

ABSTRACT

Mixed Contention and Contention Free MAC Layer Scheduling Techniques for Multi-Cluster WLAN

Md. Shahidul Hoq Akond

The ever developing wireless LAN standardization and research activities worldwide along with the recent successful deployment of WLAN in numerous hotspots makes it clear that WLAN technology will play a key rule in providing broadband data coverage and as a complement for the existing cellular networks. Keeping this in mind, a lot of work has been done to address WLAN/WAN integration, development of mobile IP, hand off mechanism between WLAN and other wireless networks. However, another important issue, large scale deployment of WLAN has got less attention.

In this thesis, we have developed two networks models of multi-cluster wireless LANs. One is infrastructure based standard multi-cluster WLAN and another is multi-cluster WLAN with gratuitous capability. We have also devised a MAC layer implementation which can be efficiently employed on both standard and gratuitous multi-cluster WLAN. We have developed a generic simulation software using C++ to simulate the performances of these networks. Our simulation results show that our network models along with the MAC layer implementation can be an effective solution to solve large-scale WLAN deployment issues.

ACKNOWLEDGEMENTS

First of all I would like to express my deepest gratitude to my thesis supervisor, Dr. Ahmed K. Elhakeem, for his continuous guidance and support throughout my thesis work. His vast experience, immense knowledge and great personality are always the source of great inspiration, which have made the completion of this thesis possible.

I want to acknowledge those people who helped me a lot during my thesis work. Faridul Islam and Salekul Islam in the department of Computer Science, Concordia University, have provided me many practical advices during the development of simulation software. I have always received continuous support from my following friends in our department: Mahmud Hossain, Ejaj Mahfuz, Rajib Ullah and Asif Iqbal.

I also want to acknowledge the faculty members, staff, system administrators and the fellow graduate students of the department of Electrical and Computer Engineering for their cooperation.

I am forever indebted to my parents, my wife and daughter. Specially, I shall always remember the stress suffered by our little daughter Marija Shahid during my research involvement.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ABO	Average Buffer Overflow
ACK	Acknowledgement
AGPD	Average Gratuitous Packet Drop
AP	Access Point
APD	Average end-to-end Packet Delay
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
ATP	Average ThroughPut
ATTP	Average Throughput of Time-bounded Packets
BSA	Basic Service Area
BSS	Basic Service Set
CFP	Contention Free Period
CP	Contention Period
CPS	Contention free Parameter Set
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DBPSK	Differential Binary Phase Shift Keying
DCF	Distribution Coordination Function
DIFS	DCF InterFrame Space
DN	Dependent Node
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSM	Distribution System Medium
DSSS	Direct Sequence Spread Spectrum

ESS	Extended Service Set
FCC	Federal Communication Commission
FHSS	Frequency Hoping Spread Spectrum
FIFO	First In First Out
GFSK	Gaussian Frequency Shift Keying
GN	Gratuitous Node
HIPERLAN2	High Performance Radio Local Area Network Type 2
IBSS	Independent Basic Service Set
IEC	International Engineering Consortium
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Taskforce
IFS	InterFrame Space
IN	Independent Node
IP	Internet Protocol
IR	InfraRed
ISM	Industrial Scientific and Medical
ISO	International Organization for Standardization
LAN	Local Area Network
LLC	Logical Link Control
MAC	Medium Access Control
MBW	Maximum Backoff Window
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
MT	Mersenne Twister
NAV	Network Allocation Vector
NIC	Network Interface Card
OSI	Open System Interconnection
PCF	Point Coordination Function
PDU	Protocol Data Unit
PG	Processing Gain
PHY	Physical

PIFS	PCF InterFrame Space
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
PN	Pseudo-Noise
RAM	Random Access Memory
RF	Radio Frequency
RFC	Request For Comments
RN	Regular Node
RR	Round Robin
RTS	Request To Send
SAP	Service Access Point
SIFS	Short InterFrame Space
TBTT	Target Beacon Transmission Time
TCP	Transmission Control Protocol
VBO	Variance of Buffer Overflow
VGPD	Variance of Gratuitous Packet Drop
VPD	Variance of end-to-end Packet Delay
VPN	Virtual Private Network
VTP	Variance of ThroughPut
VTTP	Variance of Throughput of Time-bounded Packets
WEP	Wired Equivalent Privacy
WG	Working Group
WLAN	Wireless Local Area Network

Chapter 1

Introduction

1.1. Background

Mobility, installation speed, simplicity, scalability, less vulnerability to point-of-break problem and superior bandwidth make WLAN radio technology more preferable for data and real time communications compared to conventional cellular technology. In the near future, WLAN will offer high-speed hotspot extensions to conventional cellular radio access networks [1]. This objective can be achieved by deploying multi-cell WLAN. Among the various WLAN standards, IEEE 802.11 due to its compatibility with IEEE 802 protocol suite, has become the dominating standard.

IEEE 802.11 standard defines two network topologies. One is infrastructure network, and another is ad hoc network. By integrating infrastructure and ad hoc WLAN, a hybrid network can be developed which will exploit the advantages of both networks. A lot of research works have been done so far to evaluate and improve the performances of ad hoc and infrastructure networks. However, a very few articles can be found in the literature which address the integration issues between an ad-hoc and an infrastructure network [2][3].

To deploy WLAN for hotspots, a whole geographical area should come under the coverage of several small clusters of WLANs. However, in reality, uniform coverage by multi-cell WLANs may not be feasible. Some portions of this area might not be accessible by Access Point (AP) and the node density might be so low that installation of AP is not cost effective. To solve this problem, we have proposed a gratuitous infrastructure network which is basically the hybrid of infrastructure and ad hoc network. A gratuitous WLAN exhibits all the advantages of an infrastructure network but still can provide gratuitous service to the nodes outside of the coverage area via a gratuitous node. Several gratuitous WLANs can be interconnected to form a gratuitous multi-cluster WLANs.

A proper MAC layer implementation mechanism must be presented to support gratuitous multi-cluster WLANs. We have devised a MAC layer scheduling mechanism which can be efficiently applied to both standard and gratuitous multi-cluster WLANs. Many research activities in WLAN target the evaluation and improvement of the performances of an individual cell [4]-[7]. It is a matter of great importance to observe, how our proposed MAC layer implementation performs in a multi-cluster WLANs which have received less attention.

1.2. Objective

The main objectives of this thesis are as follows:

- To ensure the continuous coverage of roaming nodes in multi-clustered wireless LANs.
- To increase the flexibility of the movement of a mobile nodes.
- To minimize the number of access points to make the network more cost effective.

- To minimize the end-to-end packet delay in the network.
- To maximize the throughput of the network.
- Studying the buffer congestion to get the optimum buffer size which can be used to minimize the packet loss due to congestion at the buffers.
- To observe the behaviour of channel condition so that appropriate measures can be taken to improve the throughput and end-to-end delay performance.
- To optimize the maximum number of retransmissions required under ARQ mechanism.
- Setting up of the maximum size of the backoff window, so that unnecessary delay due to random backoff can be minimized.
- To design simulation routines, modify the MAC protocol and setting up appropriate procedures for the efficient operation of the multi-cluster wireless LANs.

To keep the above mentioned objectives in mind, the following works are performed in our thesis:

- Design of a multi-cluster WLAN, which uniformly covers a geographical area under consideration: The design implies:
- Design of a gratuitous multi-cluster WLAN.
- Design of a MAC layer scheduling mechanism which will support both gratuitous and uniformly covered multi-cluster WLAN.
- Studying the performances of mixed contention and contention free medium access layer scheduling in gratuitous and uniformly covered multi-cluster WLAN.

1.3. Organization

The remaining chapters of this thesis are organized as follows:

Chapter 2 provides a brief overview of wireless Local Area Network. Different topologies of wireless LAN are presented. A hybrid infrastructure ad hoc network is introduced. The IEEE 802.11 standard is discussed.

Chapter 3 describes the main contribution of this thesis. A uniformly covered standard ESS and a gratuitous ESS is presented. The detailed descriptions of mixed contention and contention free MAC layer scheduling mechanism and their simulations are presented.

Chapter 4 shows the performance results of the simulations of two models: uniformly distributed AP (uniformly covered ESS) and randomly distributed AP (gratuitous ESS).

Chapter 5 summarizes the performance results and outcome of the thesis. It also provides some suggestions for future works.

Chapter 2

Overview of Wireless LAN

A Wireless Local Area Network (WLAN) is a flexible data communication system which transmits and receives data over the air and works as a supplement of, or an alternative to a wired Local Area Network (LAN). The wireless approach to the local area access, wireless LAN (WLAN), is becoming increasingly attractive, mainly because of its simpler deployment, continuous coverage, availability of ad hoc connectivity, and user/terminal mobility, together with inherent flexibility for delivering full broad band services to end users [8]. There exists several standards of wireless LAN, these are IEEE 802.11 standard [9], HIPERLAN2 [10], and Home RF [11]. Among them IEEE 802.11 standard is the most widely used WLAN standard today [12].

2.1. Wireless LAN Topology

IEEE 802.11 standard defines two types of wireless LAN topologies: infrastructure wireless LAN and ad hoc wireless LAN.

2.1.1. Infrastructure Wireless LAN

Currently most corporate wireless networks are the infrastructure network [13]. The infrastructure network is a wireless cell which consists of mobile nodes (MN), a stationary

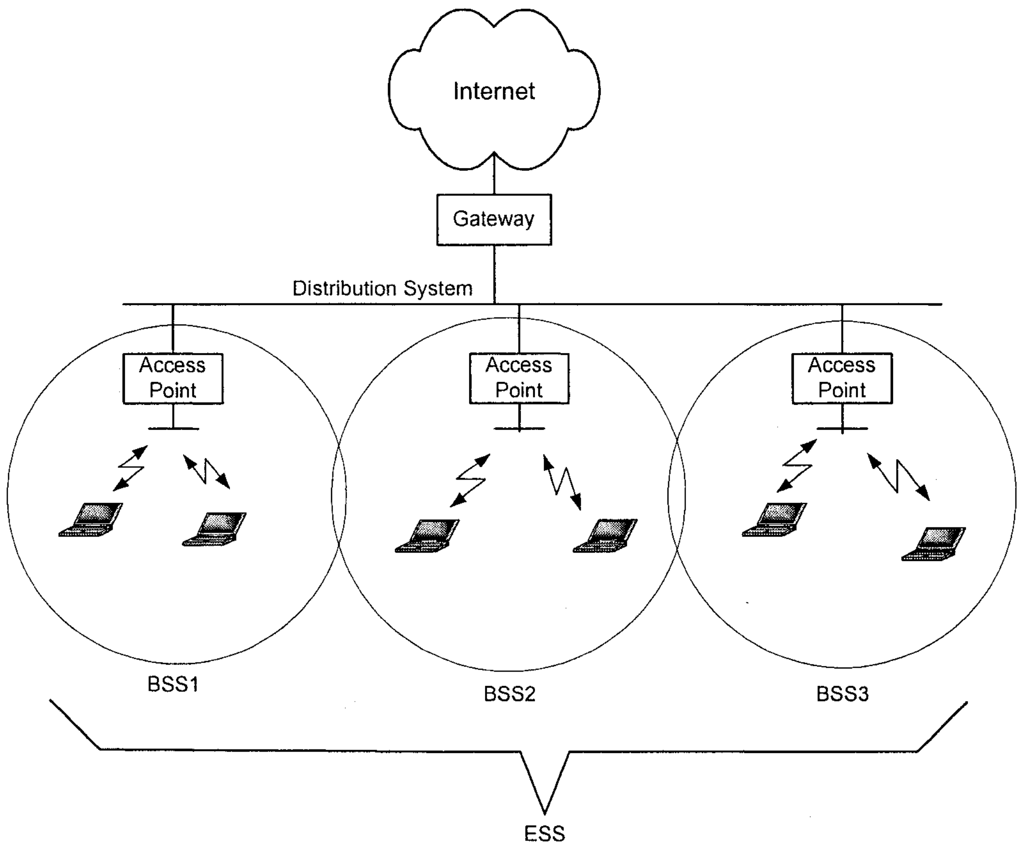


Figure 2.1: An example of infrastructure WLANs with multiple BSSs.

Access Point (AP). Each mobile node is equipped with a wireless Network Interface Card (NIC). The wireless NIC interfaces the node with a wireless network, and the AP interfaces with a wired network. A cell is covered by the AP and is termed as Basic Service Set (BSS). The geographical area covered by a BSS is known as Basic Service Area (BSA). The APs of multiple BSSs can be interconnected by a Distribution System (DS) and form an Extended Service Set (ESS). An ESS can also provide gateway access of wireless users to a wired network via a portal. For continuous coverage, APs may be placed in such a way that adjacent BSSs slightly overlap. Figure 2.1 shows an example of the infrastructure WLAN with multiple BSSs.

2.1.2. Ad Hoc Wireless LAN

An ad hoc network is a group of wireless mobile hosts that can dynamically establish routing among themselves to form a network "on the fly" [14]. Ad hoc network is temporary in nature. It can be formed any where without the need of existing infrastructure. As there is no AP, each node has the capability of forwarding packets to another node. The Basic Service Set (BSS) of an ad hoc network is termed as Independent Basic Service Set (IBSS). Figure 2.2 shows an example of an IBSS.

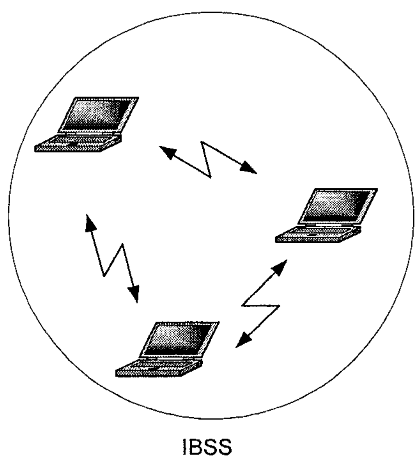


Figure 2.2: An example of ad hoc WLAN.

2.1.3. Hybrid Infrastructure Ad Hoc Wireless LAN

Though not defined by IEEE 802.11 standard, it is possible to create a hybrid infrastructure ad hoc network [2][15]. Figure 2.3 shows an example of hybrid infrastructure ad hoc wireless LAN.

Although infrastructure and wireless network shares some similar characteristics, they differ in the following points: (i) In Infrastructure network AP has continuous power and

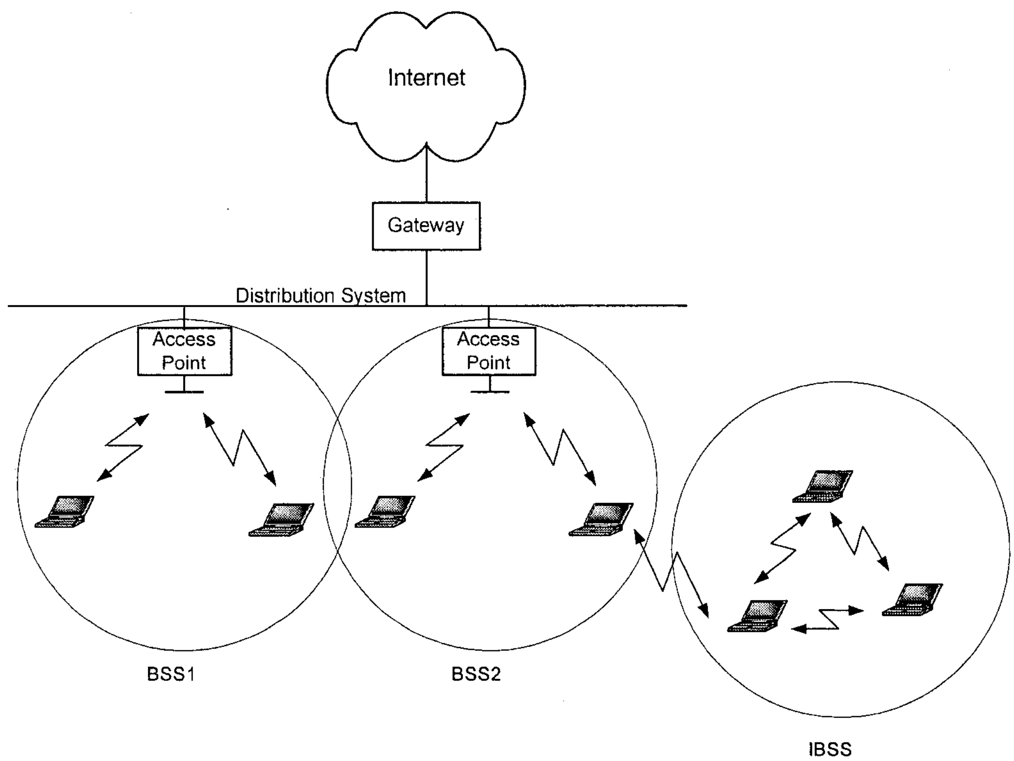


Figure 2.3: An example of Hybrid infrastructure Ad Hoc WLAN.

and is supported by back bone network. (ii) Power saving is a great concern in an ad-hoc network. (iii) Though AP supports range extension by providing the integration points necessary for network connectivity between multiple BSSs, that do not happen spontaneously. Ad hoc network can support quick change in topology due to the mobility of the nodes. (iv) Ad-hoc WLAN can have a larger diameter and transmission range than that of infrastructure WLAN [15]. (v) Paths in ad hoc network typically are involved with multiple hops, hence traditional routing protocol does not give good performance. In such a network, ad hoc routing is used to extend the range of infrastructure wireless networks that covers a larger area. Special routing protocol is needed to create such a network.

2.2. Wireless LAN Transmission Approaches

Based on transmission technique, three types of wireless LAN technologies are now available.

2.2.1. Radio Frequency (RF)

This is the most widely used WLAN technology. Spread spectrum modulation is used for radio based WLAN. The great advantage of radio-based wireless LAN over its other wireless counterparts is that radio wave can propagate through non-line of sight distance, penetrate through walls and other obstructions with a little attenuation and hence most suitable for mobile applications.

2.2.2. Infrared (IR)

Infrared light LAN products operate around 820 nanometer wavelengths, because air offers the least attenuation at that point in the infrared spectrum [16]. In comparison to radio-based WLAN, infrared based WLAN offers higher security and performance. However, because of its limited range it is not as suitable as radio based WLAN for mobile communication.

2.2.3. Carrier Current

This approach uses power lines as a medium of transmission. It is easy to install, because power line is already there. The main disadvantage is the presence of power transformer which is designed to couple 60 Hz signals, will block higher frequency signals.

2.3. ISM Frequency Bands

In 1985 Federal Communication Commission (FCC) modified Part 15 of the spectrum regulation which allowed wireless network products to operate in the Industrial Scientific and Medical (ISM) bands. ISM spectrum allocation is shown in Figure 2.4.

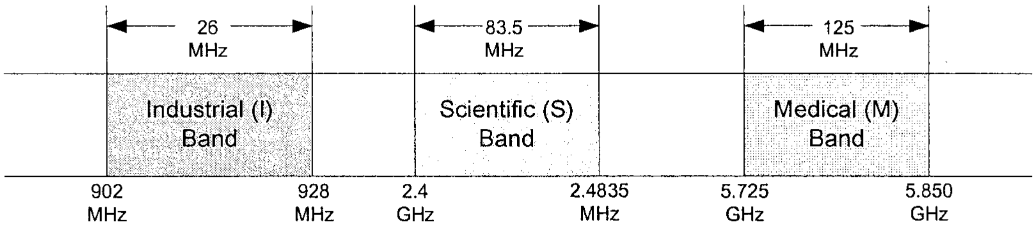


Figure 2.4: Industrial Scientific and Medical (ISM) Bands.

2.4. Spread Spectrum Communication in Wireless LAN

Most radio-based wireless LANs operate in ISM bands using spread spectrum modulation technique. In Spread spectrum transmission, the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band split is accomplished by means of a code which is independent of the data, and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery

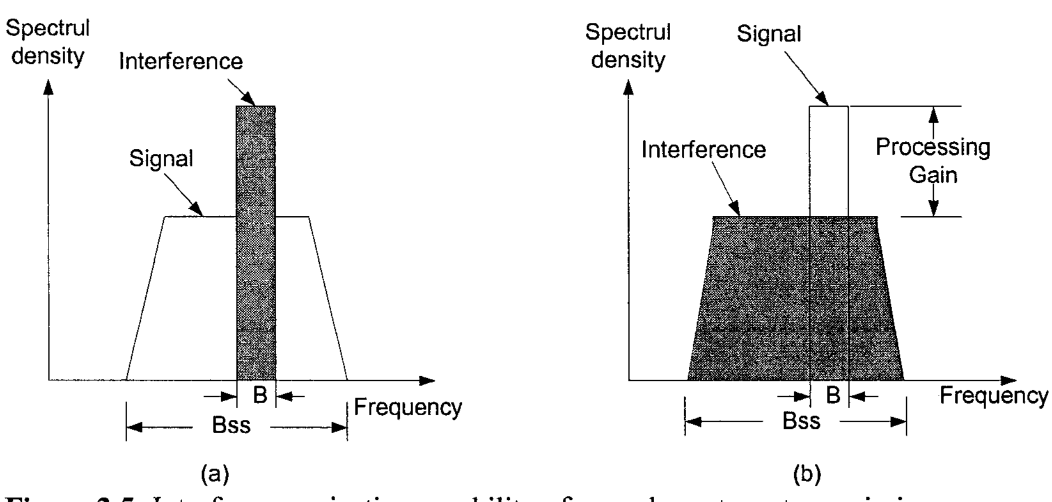


Figure 2.5: Interference rejection capability of spread spectrum transmission: (a) wide band received signal; (b) received signal after dispreading.

[17]. The spreading process makes the data signal less susceptible to electrical noise than that of conventional narrow band transmission. Spread Spectrum system has the inherent security, multi-access capability, and interference and jamming resistance [18]. Figure 2.5 shows the interference rejection capability of a spread spectrum transmission. Figure 2.5(a) shows the received spectra of the spread spectrum signal along with the interference, where B is the bandwidth of the interference and Bss is the bandwidth of the signal. As the interference occupies only a part of the bigger bandwidth, it is easy to minimize the interference. Figure 2.15(b) shows the received signal after despreading . The signal bandwidth is reduced to B, while the interference energy is spread over an RF exceeding Bss. The interference rejection capability can be described by the Processing Gain (PG) defined as

$$PG = \frac{Rc}{Rs}\frac{Bss}{B} \tag{2.1}$$

Here Rs is the symbol rate and Rc is the chip rate. There are two types of spread spectrum transmissions: (1) Direct Sequence Spread Spectrum (DSSS); (2) Frequency Hoping Spread Spectrum (FHSS).

2.4.1. Direct Sequence Spread Spectrum (DSSS)

In a DSSS transmitter, incoming data bits are first converted to data symbols. These symbols are converted into complex signals which are fed to the spreader. The spreader multiplies its input signal with a high speed Pseudo-Noise (PN) sequence. As a result the output is a signal with a wider bandwidth. The receiver again multiplies the spread signal with the same Pseudo-Noise (PN) sequence to dispread the received signal and recovers the original data.

2.4 GHz Industrial, Scientific and Medical (ISM) band (2.4 – 2.4835 GHz) is used for DSSS implementation. The 802.11 standard specifies division of the 2.4 GHz band up to 14 different channels out of which U.S. and Canada use 11 channels. Each channel is of 11 MHz bandwidth. 11 chip Barker sequence is used as PN sequence. For example, a 1 Mbps data rate will result in 11 Mbps spread signal rate. With Differential Binary Phase Shift Keying (DBPSK) the data rate is 1 Mbps (basic access rate) and with Differential Qudrature Phase Shift Keying (DQPSK) the data rate is 2 Mbps.

2.4.2. Frequency Hoping Spread Spectrum (FHSS)

Frequency hopping involves a periodic change of transmission frequency. In Frequency Hoping Spread Spectrum (FHSS) system, a station hopes from one narrow band to another narrow band within a wide band range. FHSS wireless LAN stations send data at one carrier frequency and then hop to another frequency to send more data and continue this hop and transmit sequence. Frequency hopping signal may be regarded as a sequence of modulated data bursts with time-varying, pseudorandom carrier. The bandwidth of a channel used by this hop set is called instantaneous frequency. FHSS radios dwell on each frequency for a fixed time, and its hopping sequence appeared as random but actually known to the transmitter and receiver.

The 802.11 standard specifies a set of evenly divided 1 MHz wide channels in 2.4 GHz ISM band. The standard defines three separate hopping sequence sets, each set contains 26 sequences. Hoping sequences are chosen in each set such that interference among the BSSs would be minimized. 2-level Gaussian Frequency Shift Keying (2-

GFSK) provides 1 Mbps data rate while 4-level Gaussian Frequency Shift Keying (4-GFSK) provides 2 Mbps data rate.

2.5. IEEE 802 Standard Family

The IEEE 802.11 wireless LAN standard is part of family of local and metropolitan networking standards. IEEE formed the "IEEE 802 Local and Metropolitan Area Network Standards Committee" to create, maintain and encourage the use of IEEE and equivalent IEC/ISO standard. The IEEE 802 family of standards fall within the scope of layer 1 and 2 of the OSI reference model. Figure 2.6 shows the IEEE standard family. Logical Link Control (LLC) protocol specifies the mechanisms for addressing stations across the medium and for controlling the exchange of data between two stations; whereas, the MAC and PHY Layer provide medium access and transmission functions [9][19].

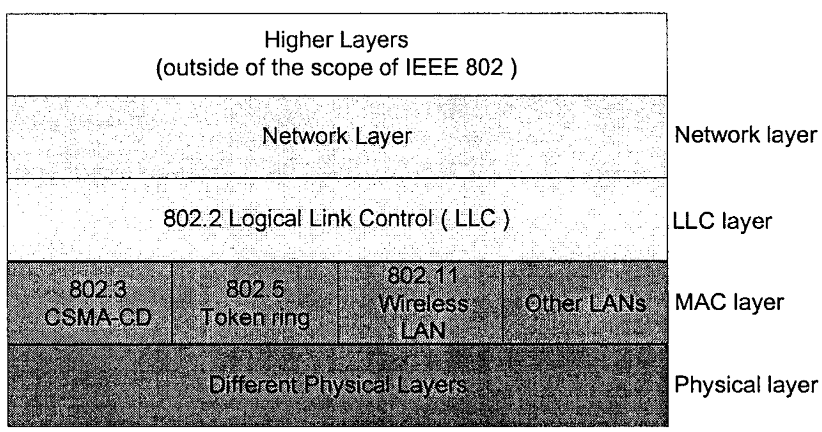


Figure 2.6: IEEE 802 standard family.

2.6. IEEE 802.11 Standard

The scope of this standard is to develop a Medium Access Control (MAC) and physical layer specification for wireless connectivity for fixed, portable, and moving stations within a local area. The purpose of this standard is to provide wireless connectivity to automatic machinery and equipment or stations that require rapid deployment, which may be portable, handheld, or which may be mounted on moving vehicles within local area [9].

2.6.1. IEEE 802.11 Features

Specific features of the 802.11 standard include the following [9][17][20]-[23]:

1. Support of asynchronous and time-bounded delivery service.
2. Continuity of service within extended areas via a distribution system, such as Ethernet.
3. Accommodation of transmission rates of 1 and 2 Mbps.
4. Support of most market applications.
5. Multi-cast (including broadcast) services.
6. Network management services.
7. Registration and authentication services.
8. Target environments for the use of the standard include:
    a) Inside buildings, such as airport lounge, bus terminal, hospital, ware house, offices, malls, banks residences, manufacturing plants.
    b) Outdoor areas such as parking lots, campus, open stadium, building complexes.

The 802.11 standard taking into account the following significant difference between wired and wireless LANs:

- ***Power Management:*** The 802.11 Working Group (WG) found techniques enabling wireless NICs to periodically switch to "sleep mode" to conserve battery while not transmitting.

- ***Bandwidth:*** The IEEE 802.11 working group suggests to compress data, making the best use of available bandwidth.

- ***Security:*** Due to its inherent nature, wireless LAN is vulnerable to eavesdropping. Wired Equivalent Privacy (WEP) is used to protect the privacy of the wireless users.

- ***Addressing:*** Because of dynamic wireless network topology, the destination address always does not corresponds to the destination location. This raises problem when routing a packets through the networks to the intended destination. The use of TCP/IP over wireless LAN offers significant problem. IETF's RFC 2002 defines Mobile IP, an enhancement to the standard IP protocol to solve this problem.

2.6.2. IEEE 802.11 Topology

The IEEE 802.11 topology consists of components, interacting to provide a wireless LAN that enables station mobility transparent to higher protocol such as LLC.

The 802.11 standard supports the following two topologies:

- Independent Basic Service Set (IBSS)
- Extended Service Set (ESS)

2.6.3. IEEE 802.11 Services

The 802.11 standard defines services that are required by the LLC Layer for sending MAC Service Data Unit (MSDU) between to entities on the network. These services are classified into two broad categories [9][16]:

2.6.3.1. Station Services: These services are necessary for providing functions among stations:

- ***Authentication:*** All 802.11 stations whether they are part of an IBSS or ESS must use the authentication service before establishing a connection with another station.
- ***Deauthentication:*** When a station wishes to diassociate with another station, it invokes the deauthentication service. Deauthentication is a notification and cannot be refused.
- ***Privacy:*** *Wired Equivalent Privacy (WEP)* algorithm significantly reduces the risk of eavesdropping.

2.6.3.2. Distribution System Services

Distribution system services provide functionality across a distribution system. AP is responsible for providing distribution functions:

- ***Association:*** Prior to any data communication, each station invokes association service to get associated with the distribution system via an AP. Each station can associate with only one AP but one AP can associate with more than one stations.
- ***Disassociation:*** A station or AP may invoke disassociation service to terminate an existing association and neither party can refuse it.
- ***Distribution:*** A station requires distribution service when it sends MAC frames across a distribution system.

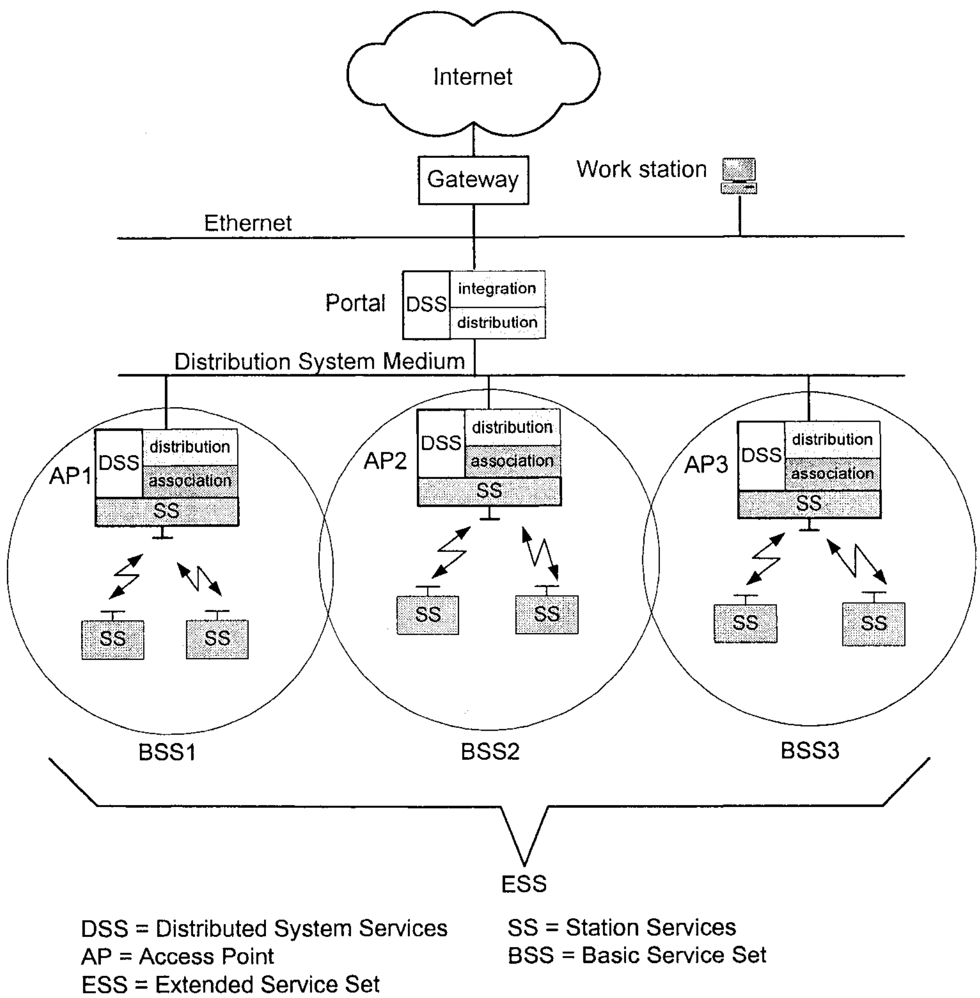


Figure 2.7: Infrastructure network logical services.

- ***Integration:*** The integration service enables the delivery of MAC frames through a portal between a distribution system and a non-802.11 LAN.
- ***Reassociation:*** Reassociation provides additional functionality to support BSS transition mobility for associated stations. The re-association service enables a station for transition its association from one access point to another.

2.6.4. IEEE 802.11 Logical Architecture

A topology explains the necessary physical components of a network, but the logical architecture defines the operation of that network. Figure 2.8 illustrates the logical architecture of 802.11 standard where Logical Link Control (LLC) layer sits on the top of MAC layer. Each station consists of a single MAC and one of multiple PHYs, FHSS, DSSS and IR.

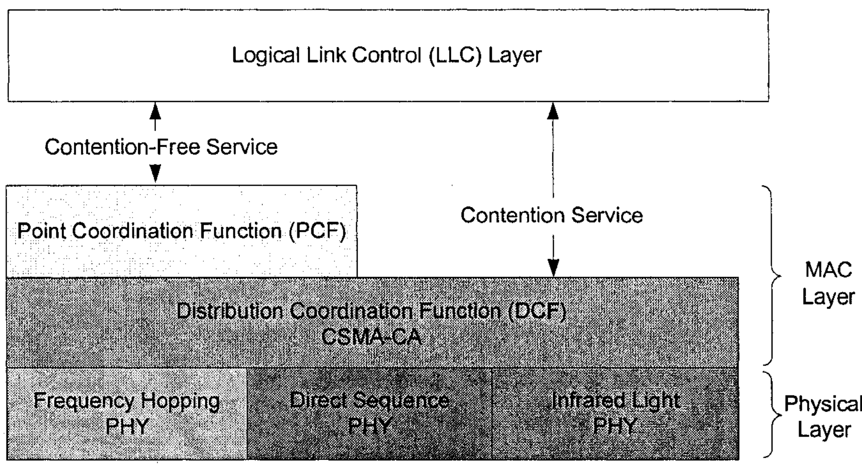


Figure 2.8 IEEE 802.11 logical architecture.

2.6.5. Medium Access Control (MAC) Layer

The MAC sublayer is responsible for the channel access procedures, Protocol Data Unit (PDU), addressing, frame formatting, error checking, and fragmentation and reassembly of MSDUs. The MAC layer also provides options to support security services through authentication and privacy mechanism [9][20][21]. Each station and AP on an 802.11 wireless LAN implements the MAC layer services, which provides the capability for peer LLC entities to exchange MAC Service Data Units (MSDUs) between MAC Service

Access Points (SAPs). The transmission medium can be accessed using the contention mode exclusively, requiring all stations to contend for the transmission of each packet. IEEE 802.11 defines Distribution Coordination Function (DCF) to provide supports for contention mode. The medium can also alternate between Contention Period (CP) and Contention Free Period (CFP). During the CFP the medium usage is controlled by AP. IEEE 802.11 defines Point Coordination Function (PCF) to support Contention Free Period (CFP) which may be implemented by an AP.

2.6.5.1. Distributed Coordination Function

The DCF is the primary access method used to support asynchronous data transfer on a best effort basis. All stations must support the DCF. Figure 2.8 shows that DCF sits directly on the top of the physical layer and supports contention services.

The DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. Carrier sensing involved monitoring the channel to determine whether the channel is idle or busy. 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 stations by analyzing all detected packets and also by analyzing the relative signal strength of the channel.

In virtual carrier sensing, source station informs all other stations in the BSS, how long the present transmission of MAC Protocol Data Unit (MPDU) will take place. Figure 2.9 shows the implementation algorithm of basic CSMA/CA. All the stations are obliged to remain quiet for a certain period after a transmission has been completed, called the InterFrame Space (IFS). The length of the IFS depends on the priority of the frame that the station is about to transmit. The frame with the highest priority waits a Short InteFrame Space (SIFS). These types of frames include ACKnowledgement (ACK) frames, Clear To Send (CTS) frames, data frames of segmented MSDUs, frames from a stations that are responding to a poll from an AP, from any AP during Contention Free Period (CFP). Point Coordination Function InterFrame Space (PIFS) is intermediate in

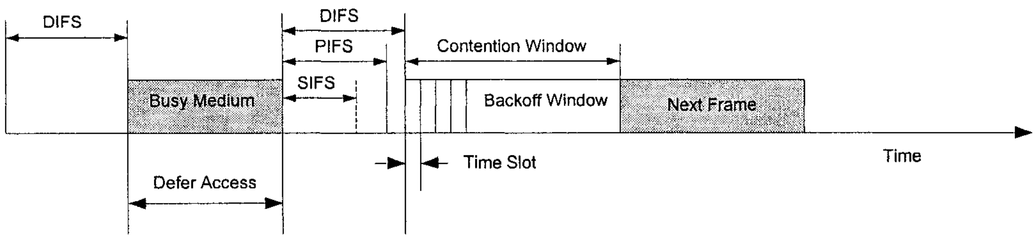


Figure 2.9: Transmission of MPDU using basic CSMA/CA.

duration and used by Point Coordination Function (PCF) to get priority access to the transmission medium. Distributed Coordination Function InterFrame Space (DIFS) is the largest in duration and is used by Distributed Coordination Function (DCF) to transmit data and management MPDUs.

2.6.5.1.1. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. The flowchart in Figure 2.10 illustrates the implementation of CSMA/CA. Whenever a packet is ready for transmission the station looks for the

Network Allocation Vector(NAV) from the recently transmitted packets by other nodes in the network. NAV gives the advance information when the network will be idle. The node waits and NAV continues to go down until becomes zero. Whenever NAV becomes zero, the node senses the medium for a DIFS period. When a node finds that the medium is not idle, it again looks back to the latest NAV information and waits until NAV becomes zero. If the medium is idle for a DIFS period, the node starts countdown from a random number within a backoff window size. The minimum backoff window size is Wmin. During countdown the node checks for the idle status of the medium. If the station finds that the medium is busy, it freezes countdown and looks for the NAV again. When the node countdowns to zero, it begins transmission. During this time other nodes waiting for transmission listen to the medium. They get the NAV of the network from the recently transmitted packets and wait until NAV becomes zero. When the transmission by a particular node is done, NAV becomes zero and other packets begin to sense the medium and contend for the channel using a backoff mechanism. If the two contending nodes countdown to zero simultaneously, a collision takes place. Both nodes will not receive ACK to their packets, they then take a new backoff window which is twice the size of the previous one. So after each collision, the backoff window doubles its size. This is called binary exponential backoff. The formulae is as follows:

$$CW_j = 2^{k+j} \tag{2.2}$$

Where j is the number of collisions and k is a constant defining minimum contention window W_{min}. The backoff window size will increase up to the maximum window size CWmax. After a successful transmission the backoff window size resets to CW_{min}.

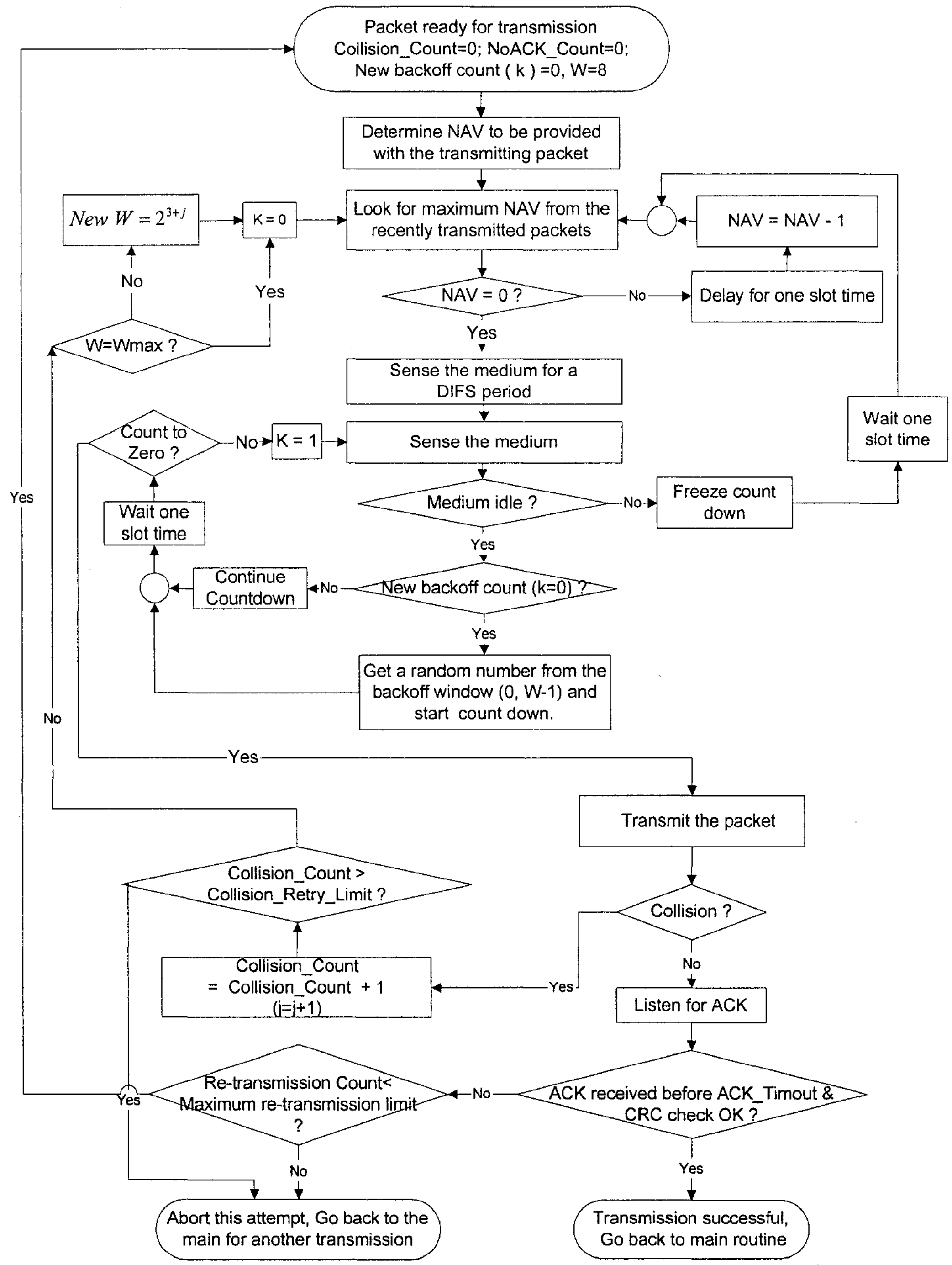


Figure 2.10: Basic CSMA/CA operation.

2.6.5.1.2. The Hidden Node Problem

Because of the possibility of partial network connectivity, wireless LAN protocols must account for potential hidden stations. Hidden node problem happens when a station attempts to access the medium because it will not be able to detect another transmitting station. The problem comes from the fact that every wireless node has

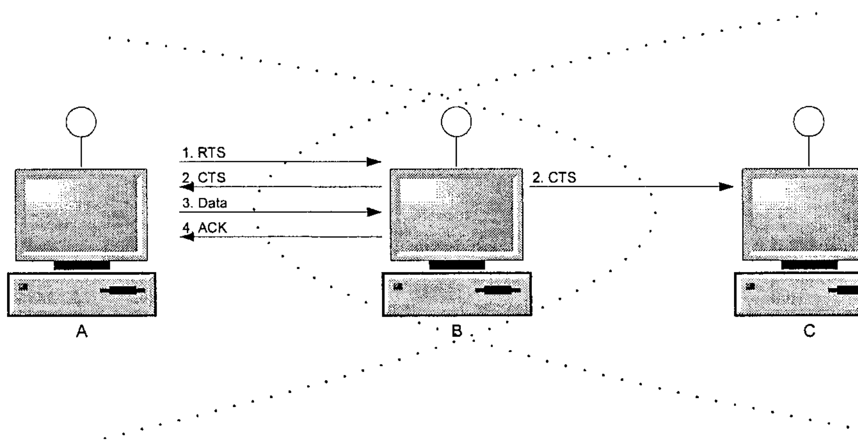


Figure 2.11: RTS/CTS scheme to overcome hidden node problem.

limited transmitting range, there might be also a barrier between two nodes and thus every node is not expected to "hear" another node in the network. A handshake procedure called RTS/CTS operation provides much better performance over basic access when there is high probability of hidden stations [16].

Figure 2.11 shows the hidden node situation and Figure 2.12 shows the timing diagram of packet transmission using RTS/CTS. If station A wants to send data frame to station B, station A sends a Request to Send (RTS) frame to station B. All stations within the range of A are aware that A is going to occupy the channel for the period specified in NAV with the RTS frame. If station B correctly receives the RTS frame, it will send Clear to Send (CTS) frame. Thus all stations within the range of B are also aware that A has been given permission to transmit and the channel will

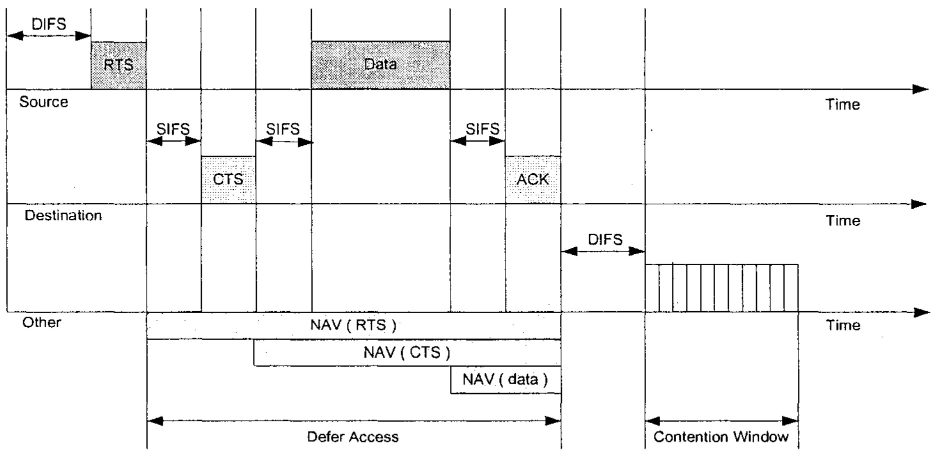


Figure 2.12: Transmission of MPDU using RTS/CTS.

be busy for the period specified in the CTS NAV. So, all the stations within the range of A as well as within the range of B remain quiet while station A proceeds with the data transmission and any potential collision involving data frame can be avoided. After receiving correct Clear To Send (CTS) frame from B, station A begins transmitting data frames. If the data frame is received without error, station B sends an ACKnowledgement (ACK) frame. If any collision occurs during the transmission of RTS, the transmitting station must execute backoff algorithm to retransmit the packet. Note that the collision of RTS frame is preferable to the collision of data frame, because RTS frame is much shorter than data frame. For example, RTS is 20 bytes the CTS is 14 bytes long while the data frame can be as long as 2300 bytes. However, RTS/CTS mechanism is inefficient for short data frames. Because, the over head provided by the RTS and CTS frames cannot be ignored when the data frames are short. Stations can choose to never use RTS/CTS, use RTS/CTS whenever the MSDU exceeds the value of RTS_Threshold (manageable parameter), or always use RTS/CTS [21].

2.6.5.2. Point Coordination Function (PCF)

The PCF is an optional capability that can be used to provide connection-oriented, connection-free services by enabling polled stations to transmit without contending for the channel [9][20][22]. The Point Coordinator (PC) in the AP performs PCF function within a BSS. Stations who operate during Contention Free Period (CFP) are also known as CFP-aware stations. AP polls stations one by one for data transmission. The method by which polling tables are maintained and the polling sequence is determined is left to the

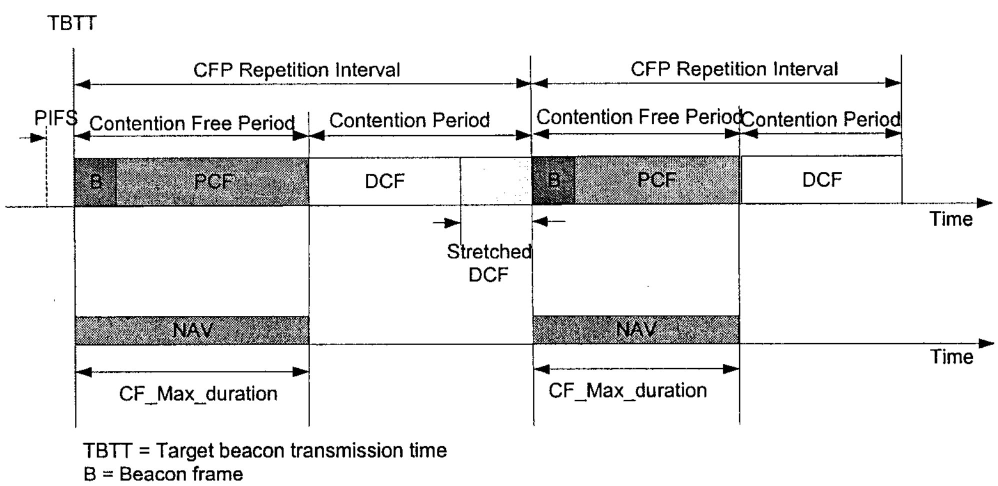


Figure 2.13: Coexistence of CFP and CP.

implementer [9][22]. The PCF is required to coexist with DCF (Figure 2.13) and logically sits on the top of the DCF. The CFP repetition interval determines the frequency at which the PCF will operate. The repetition interval which is also called a superframe, is divided into Contention Free Period (CFP) and Contention Period (CP). Figure 2.14 shows frame transfer under CFP. AP initiates the CFP repetition

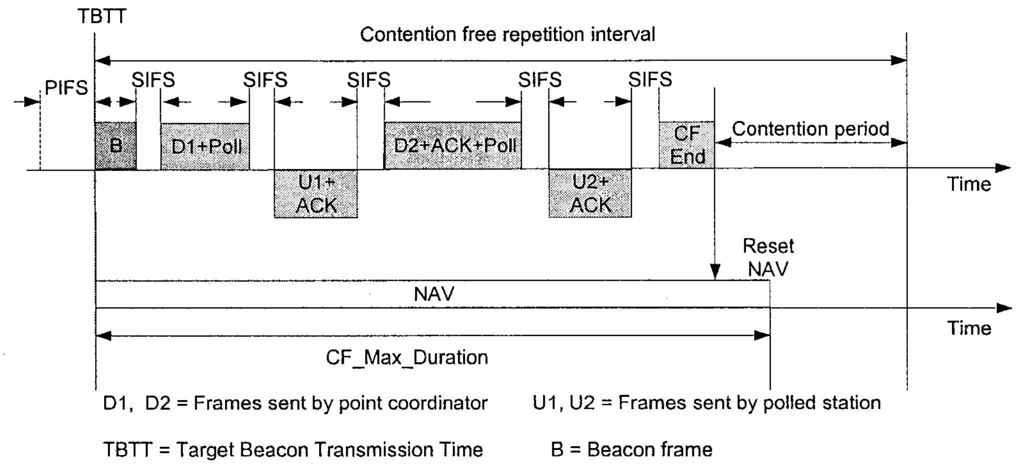


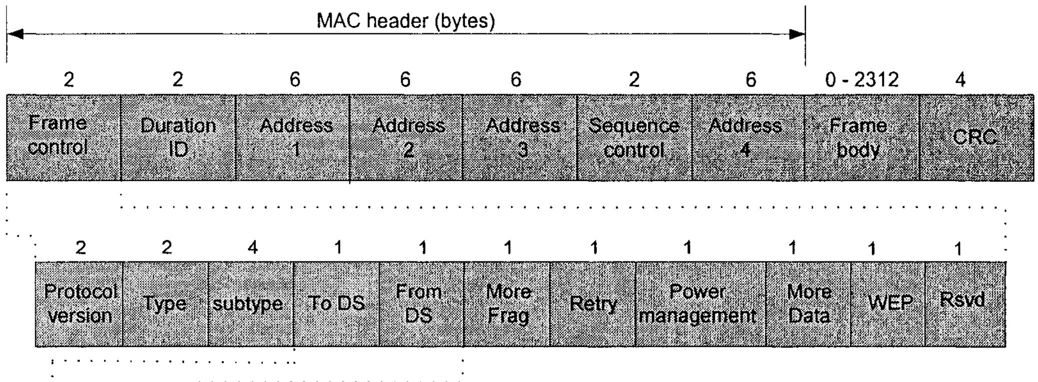
Figure 2.14: Frame transfer during CFP.

interval by transmitting a *beacon frame.* One of AP's primary functions during CFP is synchronization and timing. The duration of the CFP repetition interval is a manageable parameter and is always integral number of beacon frames. The minimum value of CFP_Max_Duration is the time required to transmit two maximum size MPDUs, including overhead, the initial beacon frame and a CF_End frame. The maximum value of the CFP_Max_Duration is determined by the CFP repetition interval minus the time required to successfully transmit a maximum-size MPDU during CP which includes the time for RTS/CTS handshaking and the ACK. Therefore, time must be allocated for at least one MPDU to be transmitted during CP. AP decides how long to operate CFP during a CFP repetition interval. If the traffic is very light, AP may shorten the CFP and the remainder period will be allocated to DCF. The CFP may also be shortened, if DCF traffic from the previous CFP repetition interval carries over to the present CFP repetition interval (stretched DCF).

For CFP mode, AP access medium after waiting a PIFS period, thus AP maintains control over transmission medium by waiting shorter time between transmissions than the stations waiting under DCF. At the nominal beginning of CFP repetition interval, so called the Target Beacon Transmission Time (TBTT), the AP senses the medium. If the medium is idle for a PIFS period, the AP transmits beacon frame that include CF Parameter Set (CPS) element. When the stations receive the beacon, they update their NAV to the CFP_Max_Duration value found in the CF Parameter Set (CPS). This value communicates the length of the contention free period to all stations and prevents stations from taking control of the medium until the end of the contention free period. During the CFP, stations may transmit only to respond to a poll from the PC or to transmit an acknowledgement one SIFS interval after receipt of an MPDU. After being polled by the AP, the station may transmit packet to any stations and can piggyback an ACK of an recently received data frame. At the end of the data transmission by all CF aware stations, AP transmits CF_End frame declaring the end of CFP period even before the time specified in CFP_Max_Duration. This action forces all stations to reset their NAV values.

2.6.5.3. MAC Frame Structure and Addressing

The IEEE 802.11 specifies three types of MAC frames: management frames, control frames and data frames. The management frames are used to establish initial communications between stations and access points. Thus management frames are used for station association and deassociation with the AP, timing and synchronization and authentication and deauthentication. The management frame sybtypes are: (1) association request frame; (2) association response frame; (3) reassociation request frame;(4) reassociation response frame; (5) probe request frame; (6) probe response frame (7)



To DS	From DS	Address 1	Address 2	Address 3	Address 4	Meaning
0	0	Destination address	Source address	BSS ID	N/A	Data frame from station to station within a BSS
0	0	Destination address	BSS ID	Source address	N/A	Data frame exiting the DS
0	0	BSS ID	Source address	Destination address	N/A	Data frame destined for the DS
0	0	Receiver address	Transmitter address	Destination address	N/A	WDS frame being distributed from AP to AP

DS = Distribution System   WDS = Wireless Distribution System   BSS = Basic Service Set
AP = Access Point   WEP = Wireless Equivalent Privacy

Figure 2.15: IEEE 802.11 MAC frame structure.

beacon frame; (8) ATM frame; (9) disassociation frame; (10) authentication frame; (11) de-authentication frame. After establishing association and authentication between stations and AP, control frames provide functionality to assist in the delivery of data frames. The control frame subtypes are (1) Request To Send (RTS); (2) Clear To Send (CTS); (3) ACKnowledgement (ACK). Data frames are used for the transmission of data. Figure 2.15 shows the format of the MAC frame that consists of a MAC header, a frame body and a CRC checksum.

2.6.6. Physical (PHY) Layer

The IEEE 802.11 wireless LAN has several physical layers defined to operate with its MAC layer. The physical layer is divided into two sublayers that correspond to two protocol functions as shown in Figure 2.16. The Physical Layer Convergence Procedure (PLCP) is the upper sublayer and it provides a convergence function to map the MAC PDU into a format suitable for transmission and reception over a given physical medium. Under the direction of PLCP, the Physical Medium Dependent (PMD) sublayer provides actual transmission and reception of physical layer entities between two stations via the physical medium. IEEE 802.11 defines three types of Physical Medium Dependent (PMD) sublayers: (i) Frequency Hoping Spread Spectrum (FHSS); (ii) Direct Sequence Spread Spectrum (DSSS); (iii) InfraRed (IR).

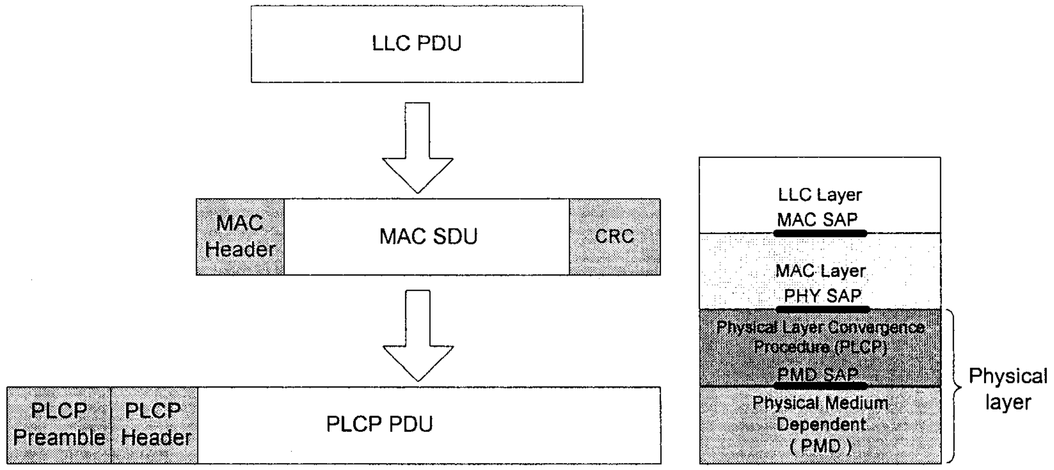


Figure 2.16: IEEE 802.11 physical layer.

Chapter 3

Scheduling of Mixed Contention/Contention Free Mode in Multi-Cluster Wireless LAN

In this chapter my thesis approach scheduling of mixed contention and contention free mode in multi-cluster wireless LAN is presented. Extended Service Set (ESS) based on infrastructure wireless LAN is a well established 802.11 standard. The great advantage of infrastructure network is its gateway to other networks. However, infrastructure network is not flexible for greater node mobility. Ad hoc wireless LAN is another well established standard defined by 802.11 which provides flexible node mobility. However, ad hoc WLAN does not have any gateway. We have proposed a hybrid infrastructure/ad hoc WLAN which not only provides greater node mobility but also keeps gateway to access other networks. We have proposed a gratuitous ESS which is composed of multiple hybrid infrastructure / ad hoc networks.

The challenge of developing an efficient yet reliable MAC has been an important research topic for over 30 years. Due to the spatial distribution of the stations, and the bursty nature of the traffic, it has been considered hard to achieve a reliable, simple, work conserving and a perfect scheduler MAC protocol [23]. We have devised a novel scheduling mechanism which keeps the basic CSMA/CA protocol as an underlying technique and uses mixed CP and CFP which can be carried out both on standard ESS and gratuitous ESS. Though the main target of this scheduling scheme is asynchronous data, its effect on time-bounded packets is also been examined.

Due to the employed random backoff algorithm and system complexity, most of the works toward system performance evaluation resort to simulation [4][24]-[26]. A generic WLAN simulation software has been designed using C++. Additionally, performance has been evaluated for two network models of uniformly and randomly distributed APs in multi-clustered wireless LANs using mixed contention and contention free mode MAC layer scheduling.

3.1. Terminology

The following terms have been used to describe the simulations and their results:

- ***Buffer :*** Buffer is a temporary data storage in the node and AP, where packets are queued before transmission or after reception. If there is a difference between packet arrival and delivery rate, the buffer temporarily holds the queue of packets to compensate the difference between packet arrival and delivery rate.

- ***Cluster :*** Every BSS is termed as a cluster. If more than one BSS form a larger network, that is termed as a multi-clustered wireless LAN. We will use the terms, cluster and BSS interchangeably.

- ***Node:*** In wireless LANs, the stations who participate in the packet transmission and reception process are called users. A node can be simply a hand held mobile set, a computer or any form of device which participates in packet transmission and reception process. The terms node and user are used interchangeably. In our simulation users are of four types:

(1) Regular Node (RN), (2) Independent node (IN), (3) Gratuitous Node (GN), and (4) Dependent Node (DN).

(1) ***Regular Node:*** When a node is a part of an infrastructure network under a BSS, that is a regular node.

(1) ***Independent Node:*** If a node does not form a part of an infrastructure network, that is an independent node.

(2) ***Gratuitous Node:*** A regular node, which helps independent users within its range, is a gratuitous node.

(3) ***Dependent Node:*** A node which does not fall under a BSS but is associated with an AP via a gratuitous node, is a dependent node.

- ***Source:*** A node, which generates a packet, and first transmits this packet toward the direction of destination.

- ***Destination:*** A node, which is the final receiver of a packet.

- ***Home AP:*** An AP, whose BSS is shared by the source node.

- ***Destination AP:*** An AP, whose BSS is shared by the destination node.

- ***Uniform AP Distribution:*** More than one BSS form a multi-clustered network which is an ESS. If APs are distributed in such a way that all the nodes are part of the infrastructure network, this distribution is termed as uniform AP distribution. We have also termed this a standard ESS.

- ***Random AP Distribution:*** AP's location is randomly chosen. So some of the nodes are part of an infra-structure network. But other nodes remain outside of that infrastructure network. Nodes outside of an infrastructure network can still communicate via a gratuitous node inside of a BSS. It is also termed as a gratuitous ESS.

3.2. Network Model and Topology

If we require greater range than the limitations of a single cell configuration, we can utilize

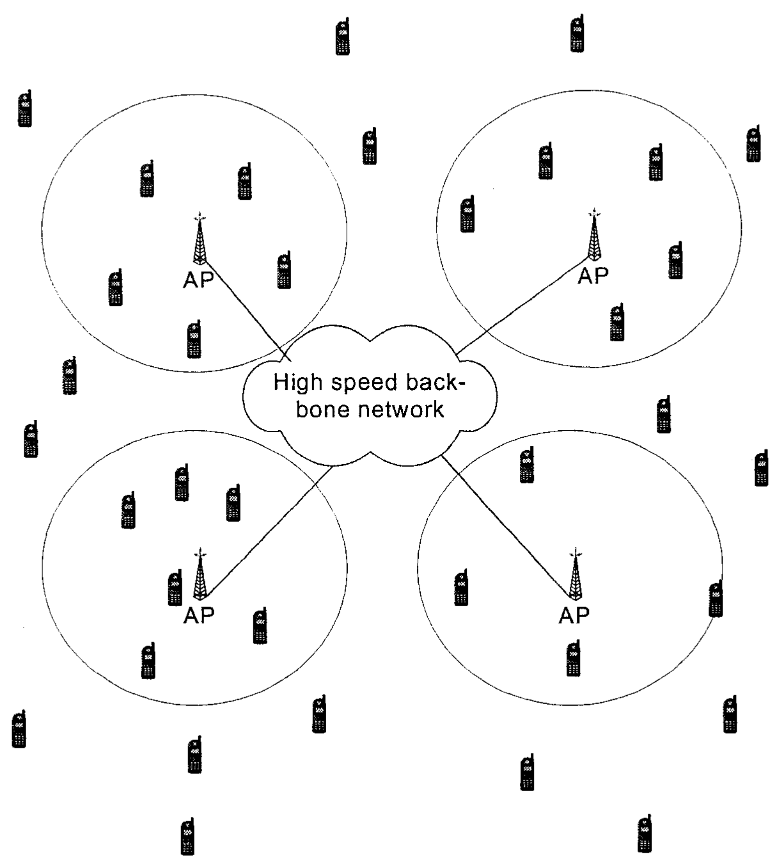


Figure 3.1: A typical distribution of APs and nodes in multi-clustered WLANs.

utilize a set of access points and a wired network backbone to create a multiple-cell configuration [16]. A typical multi-clustered wireless LAN is shown in Figure 3.1. In our thesis we have proposed a way for multi-cluster WLAN communication in both gratuitous and non-gratuitous mode. We have adopted two network models for our simulation. These are as follows:

3.2.1. Multi-Clustered WLAN with Uniform AP Distribution

This topology is shown in Figure 3.2. APs are placed uniformly to cover all the nodes under investigation. AP is placed at the centre point to cover its BSS. All the nodes within a certain area fall under the range of AP; those nodes and the AP form a BSS

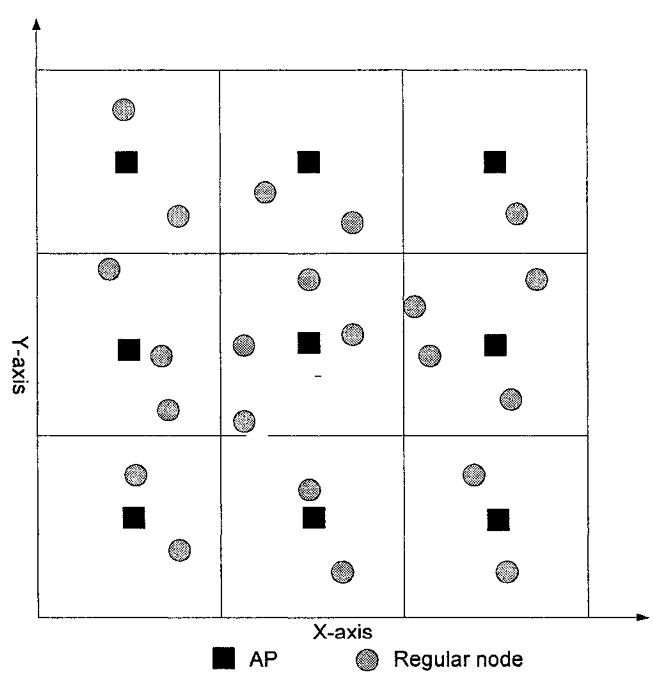


Figure 3.2 : Uniformly distributed AP topology.

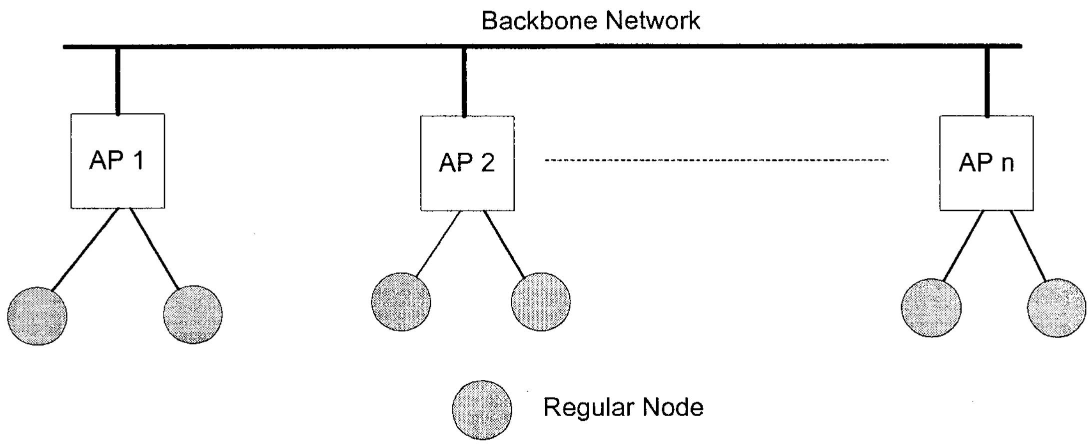


Figure 3.3 : Multi-clustered wireless LAN model with uniform AP distribution.

and hence part of an infra-structure network. The network model for uniform AP distribution is shown in Figure 3.3. All the APs are interconnected via a high speed backbone network, such as high speed optical fibre network. Several APs form a multi-clustered wireless LAN. Nodes can communicate with each other in the same BSS or in different BSS. Nodes communicate on the air interface under DCF. But some packets are destined to remote node under a different BSS. In that case, the source node first sends the packet to its own AP and then the source AP forwards the packet to the destination AP via high speed internet service. Finally, the AP at destination BSS delivers the packet to its destination node. For simplicity of the simulation, we consider square shaped clusters which will cover all the nodes within the area of investigation. In uniform AP distribution, the clusters are considered as numerous contiguous BSS which form an ESS. Random call is generated by any node to a randomly chosen destination.

3.2.2. Multi-Clustered WLAN with Random AP Distribution

Figure 3.4 shows the topology of this model. In this topology, the BSS is circular in shape and AP is located at the centre of the circle. The radius of the circle is the range of an AP. Each dependent node is associated with a nearby BSS via a nearby gratuitous node. APs are randomly located. Due to random distribution of AP, some nodes fall within the range of an AP and become regular nodes, while others are not covered by any AP and remain independent. The nodes, those are already within the coverage of an AP, are definitely the part of a BSS. However, the nodes outside of a BSS are not part of any network and cannot directly communicate with any network. We have introduced

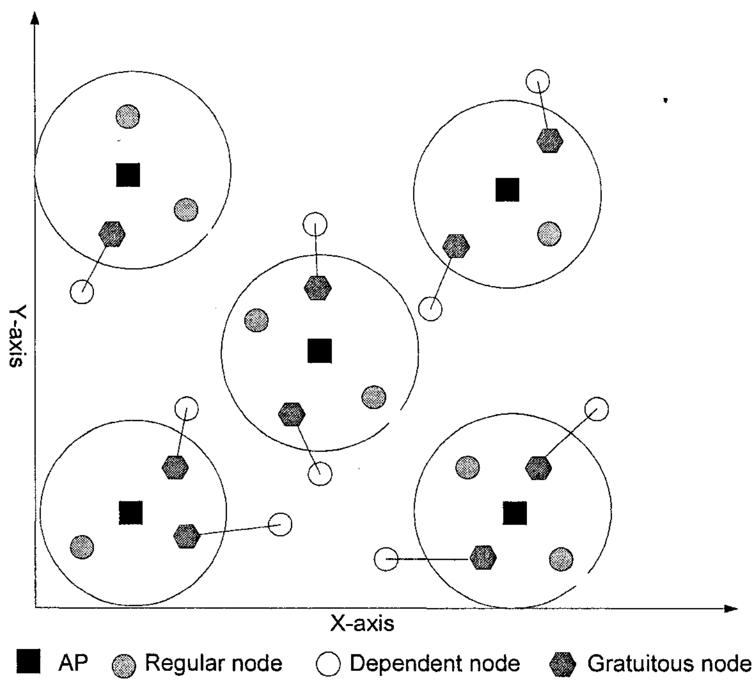


Figure 3.4 : Randomly distributed AP topology.

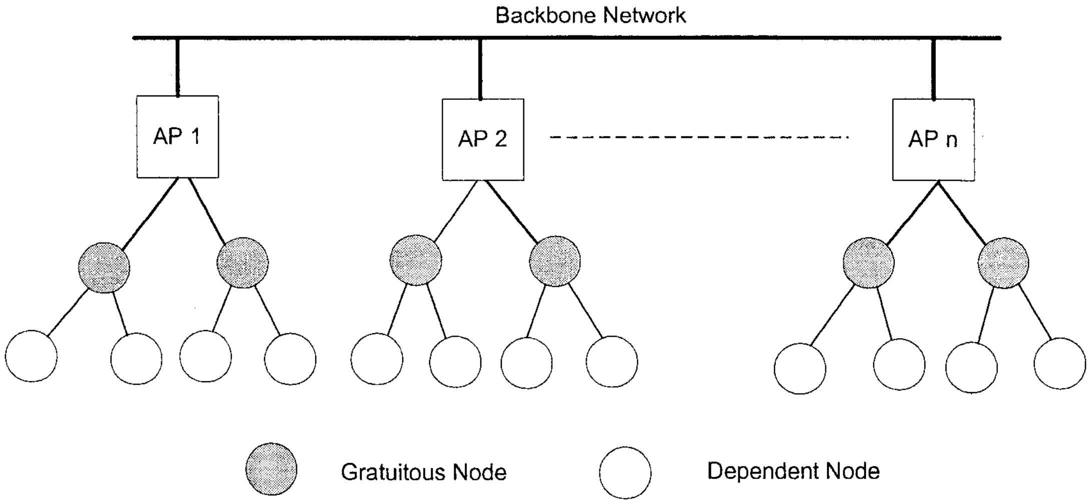


Figure 3.5: Multi-clustered wireless LAN model with random AP distribution.

gratuitous node concept to solve this problem. The gratuitous node is a regular node under a BSS but it also forms an IBSS with an independent node. In fact, it is a multi-clustered hybrid infrastructure/ad-hoc wireless LAN scenario. After initial authentication and association via a gratuitous node, the independent node becomes a dependent node of a BSS. Figure 3.5 shows the model of this gratuitous network. With the help of a gratuitous node, a dependent node can transmit and receive packets to and from BSS and hence other networks. If the destination node is just one hop away, the dependent node can directly communicate with the destination without the help of a gratuitous node.

3.2.3. Source Destination Diagram

There can be different scenarios between source and destination pair, which are shown in Figure 3.6. The arrows show the flows of packets from source to destination.

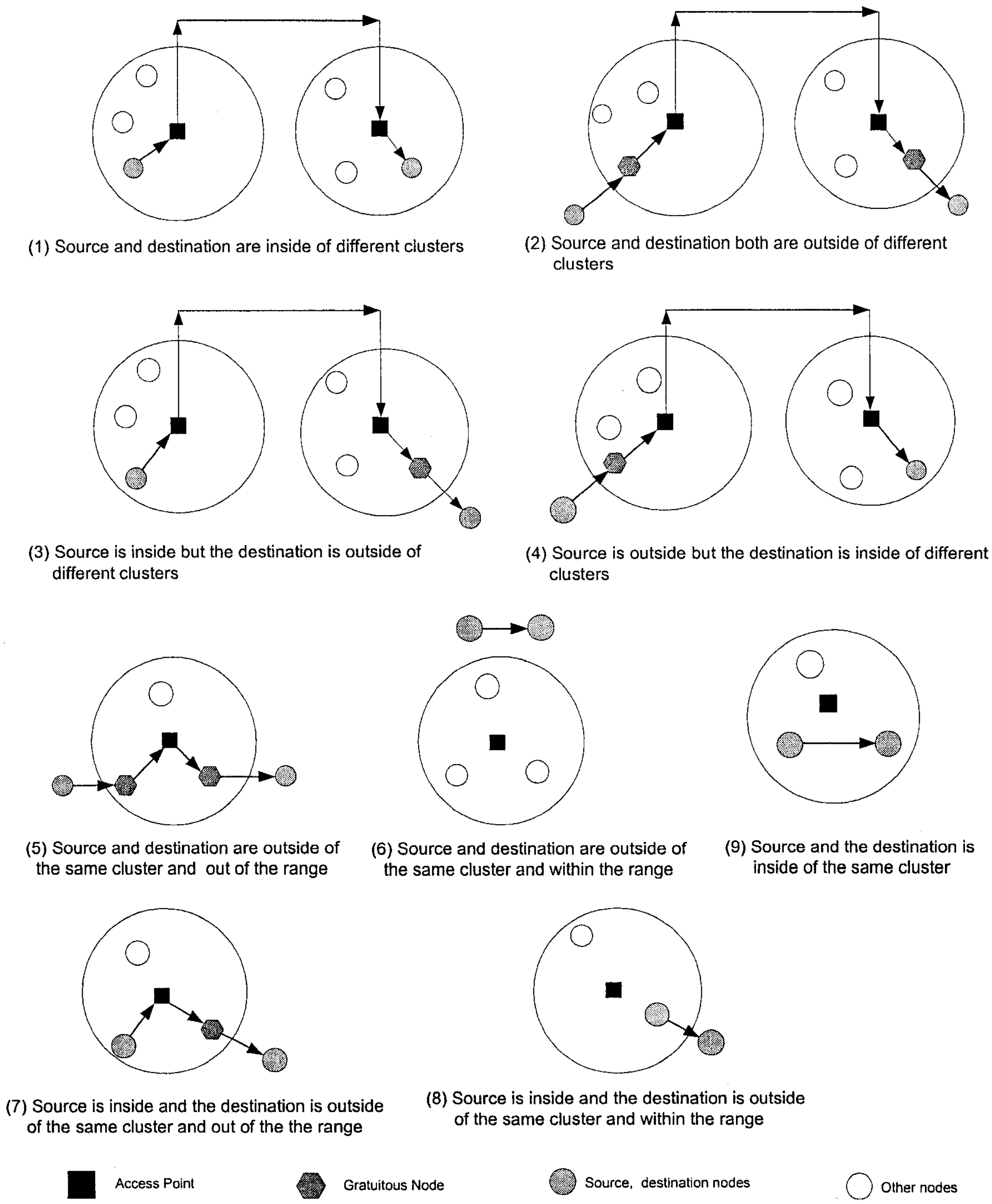


Figure 3.6 : Various possible source-destination pairs.

3.3. Mixed Contention/Contention Free Mode Transmission

If both the source and destination nodes are part of an infrastructure network, they can use standard CSMA/CA protocol to transmit and receive packets. But if one of the nodes resides outside of the infrastructure network, one of the nodes inside the cluster has to work as a gratuitous node for gratuitous communication. The dependent node outside of the cluster cannot work in the contention period, because most of the nodes including AP are outside of range of the dependent node. The dependent node can only hear the gratuitous node or some other nodes within its range. So, it cannot participate with the backoff mechanism with all nodes inside the BSS. The dependent node can transmit or receive packets when it gets clearance from the gratuitous node. AP, as a Point Coordinator (PC), can allow gratuitous transmission and reception using PCF, so that other nodes inside the BSS will remain silent during this gratuitous operation. AP can take advantage of this CFP mode by piggy backing polling and data packets which are waiting for delivery towards the destination.

The gratuitous node transmits the gratuitous packet using standard CSMA/CA protocol. If the destination is within the BSS, the node can directly transmit packets to the destination. If the destination is outside of the BSS but within the range of a node, the transmitting node can still directly transmits packets to destination. If the destination is in another AP, a node sends the packet to its home AP. The home AP then sends the packet to the destination AP using high speed back bone network. The destination AP uses the contention free period to transmit the packet to the destination node in its own cluster. If the destination is inside of the BSS the packet is accepted by the destination node. If the destination is not under the BSS but attached to it via a gratuitous node, the destination

AP allows the gratuitous node to forward the packet to the final destination during CFP. The detailed routing procedure will be discussed in the routing section.

We have extended the concept of mixed contention and contention free mode to the uniform AP distribution and measured its impact on asynchronous and synchronous data. Uniform AP distribution represents purely infra-structure network. All APs are connected via a high speed back bone network. If the destination is within the same BSS, packet can be directly transmitted to the destination using standard CSMA/CA protocol. If the packet is outside of BSS, packet can be transmitted to the destination via AP. Packet will first reach the home AP, which then sends the packet to the destination AP via backbone network. On the destination side, destination AP receives the packet from the backbone network and delivers it during CFP.

3.3.1. Implementation of CSMA/CA

CSMA/CA is the fundamental access mechanism of IEEE 802.11. We have used CSMA/CA as the basic access mechanism of our model. All the nodes in uniform AP distribution and all the regular nodes in random AP distribution use CSMA/CA. Four way handshake procedure using RTS and CTS is used with the basic CSMA/CA. RTS/CTS technique is also particularly important when the data packet size is large. In RTS/CTS technique the transmitting node reserves the channel by sending a short frame named RTS. The receiving station responds by sending back another short frame CTS. After receiving the CTS, the transmitting station transmits a packet and finally the receiving station sends an ACK frame back to the transmitter. The sender node transmits RTS using CSMA/CA algorithm. Since collision may occur

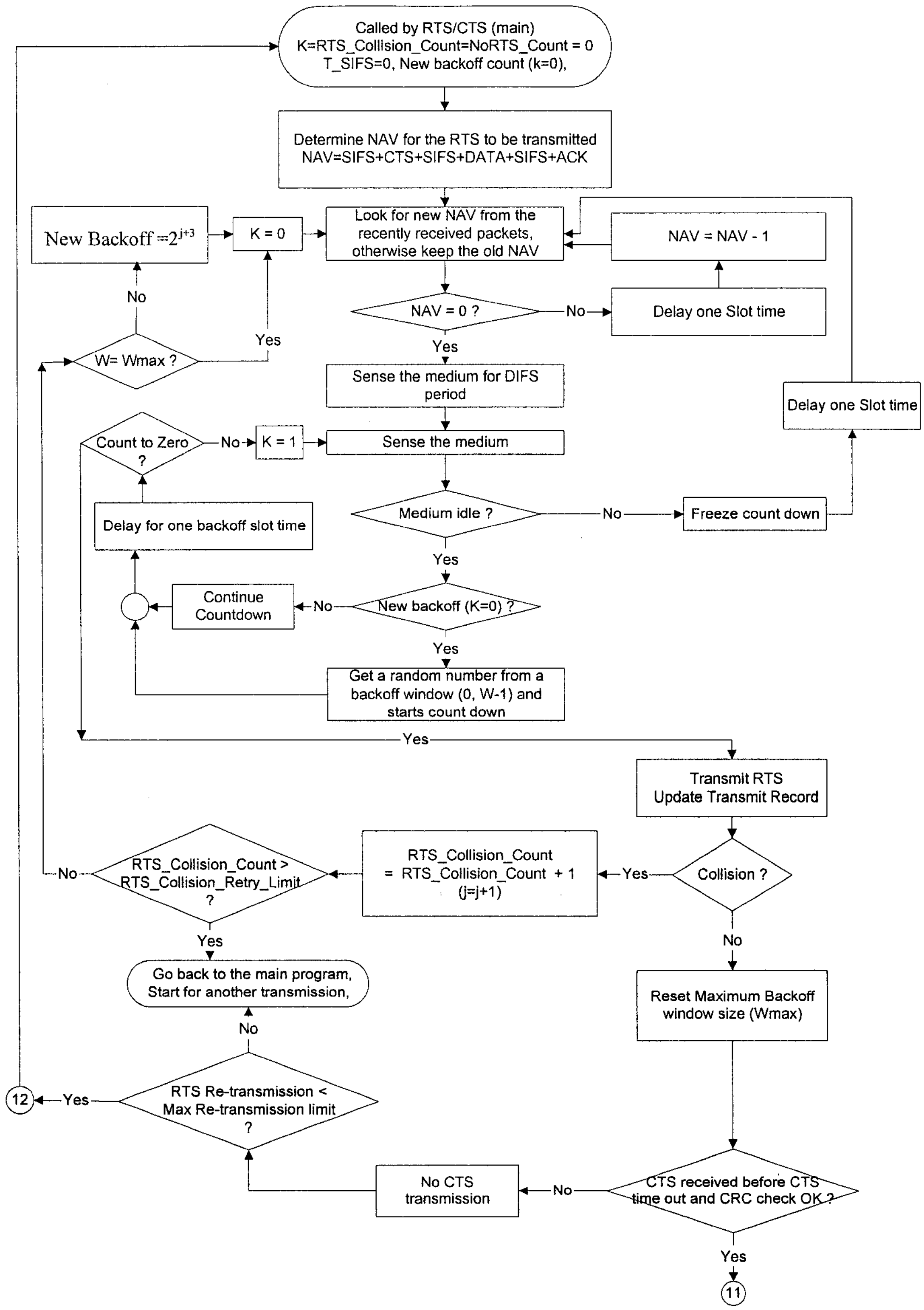


Figure 3.7(a): Implementation of RTS/CTS (part 1).

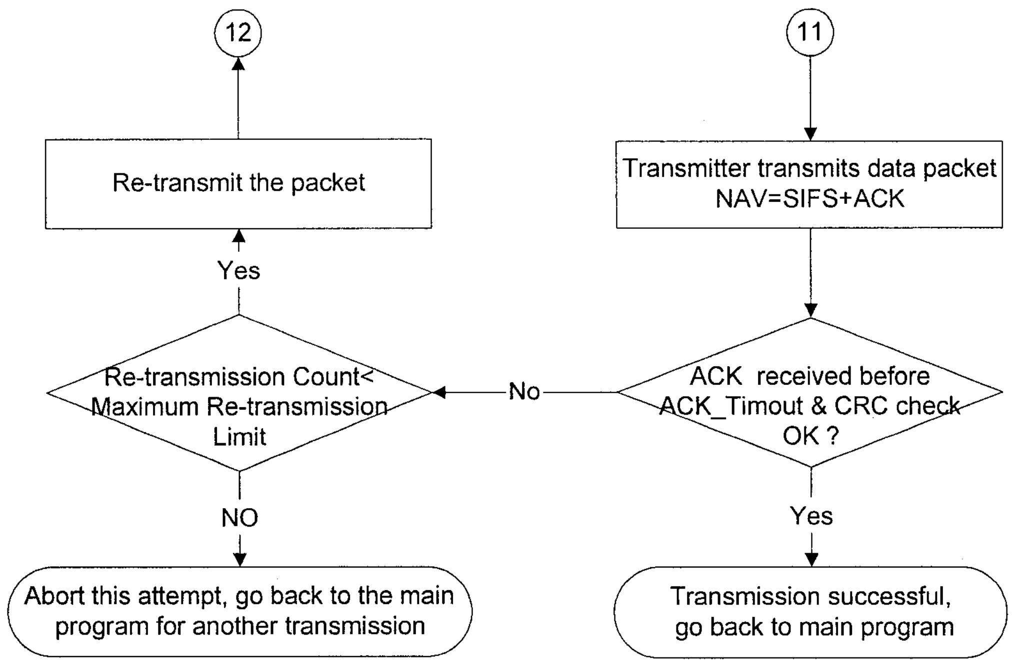


Figure 3.7(b): Implementation of RTS/CTS (part 2).

only on the RTS frame, and it is detected by the lack of CTS response, the RTS/CTS mechanism allows to increase the system performance by reducing the duration of a collision when long messages are transmitted [27]. RTS/CTS scheme also effectively combats the "hidden-terminal" problem [27] [28].

The flowchart implementing CSMA/CA using CTS/RTS is shown in Figure 3.7(a) and Figure 3.7(b). If RTS is transmitted successfully using CSMA/CA algorithm and CTS is received within CTS timeout, the node transmits the large data packet. If the ACK is received within ACK timeout the data packet transmission is successful. If the ACK is not received within ACK timeout, the sender retransmits the data packet.

3.3.2. Implementation of Contention Free Period (CFP)

In Contention Free Period (CFP) mode, the AP works as a Point Coordinator (PC). In this mode PC determines the polling sequence of the PCF. PCF can be employed by First In First Out (FIFO) and Round Robin (RR) polling schemes [29]. We have used both FIFO and RR schemes for our CFP mode. In FIFO mode, the AP transmits packets from AP to all nodes including gratuitous nodes. In RR mode, the AP polls only Gratuitous Nodes (GN), so that they would be allowed to transmit and receive with the Dependent Nodes (DN) only. However, the packet transmissions from GN to AP, follow DCF. Packet transmissions from any node to AP in a BSS also follow DCF. The super-frame containing FIFO, RR and DCF is shown in Figure 3.8.

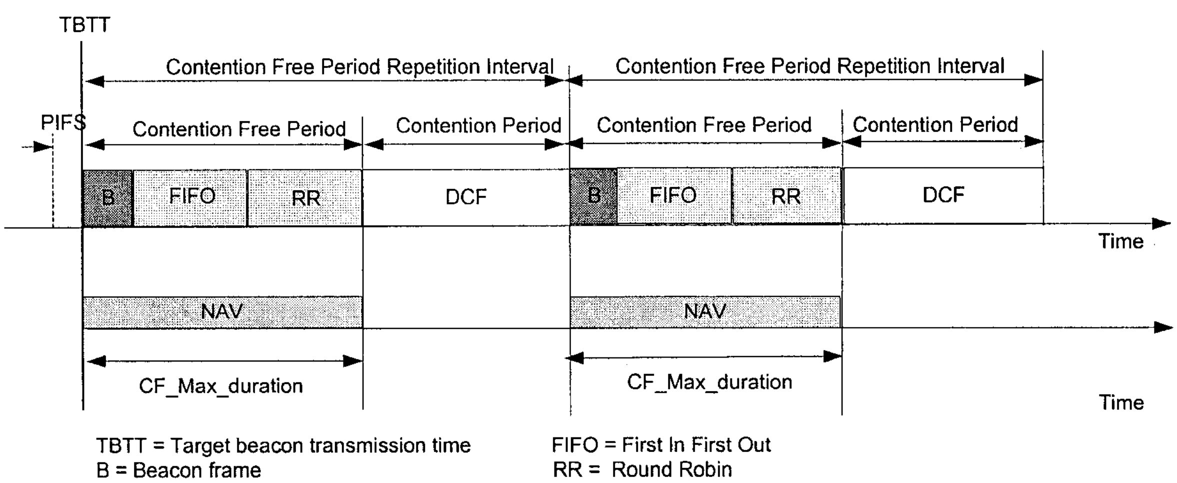


Figure 3.8: Super-frame containing FIFO, RR and DCF.

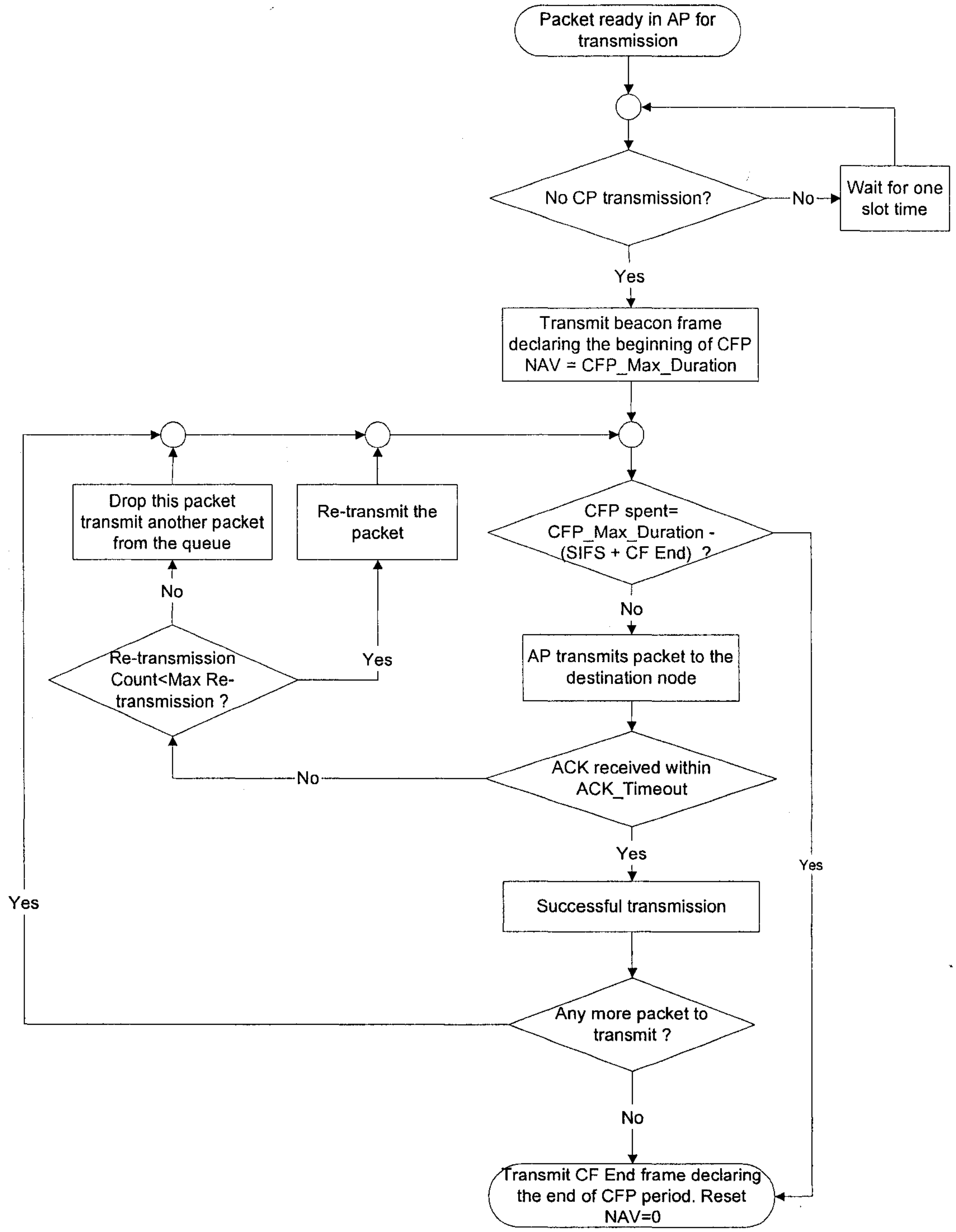


Figure 3.9 : Flowchart of FIFO polling scheme.

3.3.2.1. First in First Out (FIFO) Scheme

This scheme is shown in Figure 3.9. In this scheme, packets arrive at the AP from outside of the BSS via backbone network and are queued for transmission. AP determines the next transmitting packet and poll address on the First In First Out (FIFO) basis. For the optimum utilization of the wireless channel, the AP piggybacks the poll within the transmitting data packet. ACK is also piggybacked within the poll. If the AP does not get any acknowledgement within ACK timeout, AP assumes that the data packet was lost due to transmission error and re-transmits the packet until the re-transmission limit has been reached. AP continues transmitting packets to the nodes until the end of the queue or until the end of the CFP_Max_Duration, whichever occurs first. If all the packets in the queue have been transmitted during the CFP_Max_Duration, AP adopts Round Robin (RR) scheme for polling. During RR scheme if any packet arrives at the AP from outside of BSS, the AP again adopts FIFO scheme to transmit that packet.

3.3.2.2. Round Robin (RR) Scheme

The flow chart in Figure 3.10 shows the RR polling by AP. When the AP, as a PC takes control of the BSS during Contention Free Period (CFP), it consults its polling list. The polling list is created in ascending order of the node address. At the very beginning of RR transmission, AP starts from the lowest node address and polls the nodes in a round robin fashion. In the next CF period, the AP starts polling nodes from the polling list position where it stopped before. For optimum wireless channel utilization AP always piggybacks polling in the transmitting frame and piggy backs ACK.

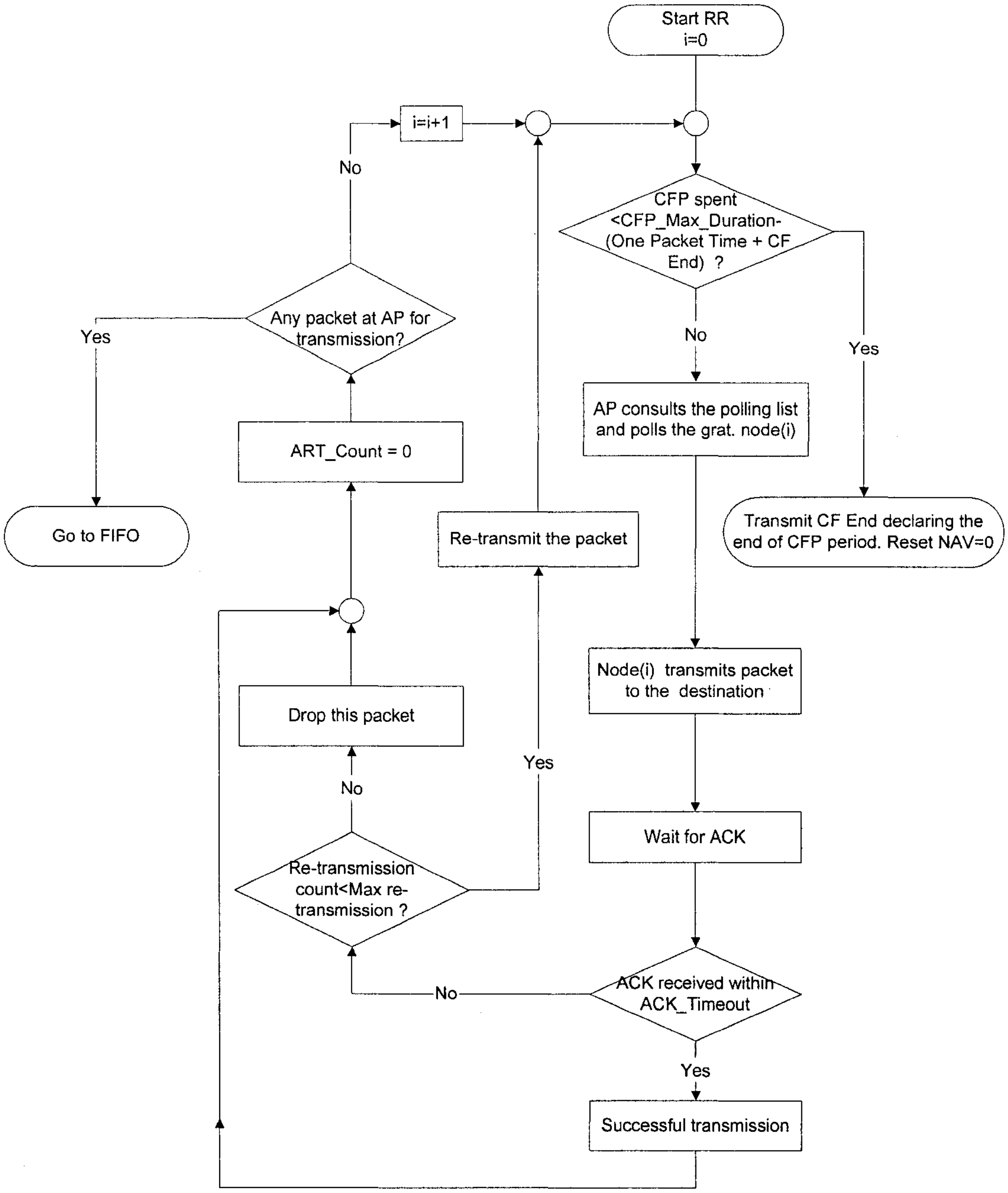


Figure 3.10: Flowchart of RR polling scheme.

3.3.2.3. Coexistence of RR and FIFO Schemes

The coexistence of gratuitous RR and FIFO polling scheme is shown in Figure 3.11. At the very beginning of CFP, the AP looks for any packet waiting for transmission in the AP. When the packet is available for transmission, the AP adopts a FIFO polling scheme. When the AP buffer becomes empty, the AP adopts RR polling scheme. The timing diagram of FIFO followed by RR is shown in Figure 3.12.

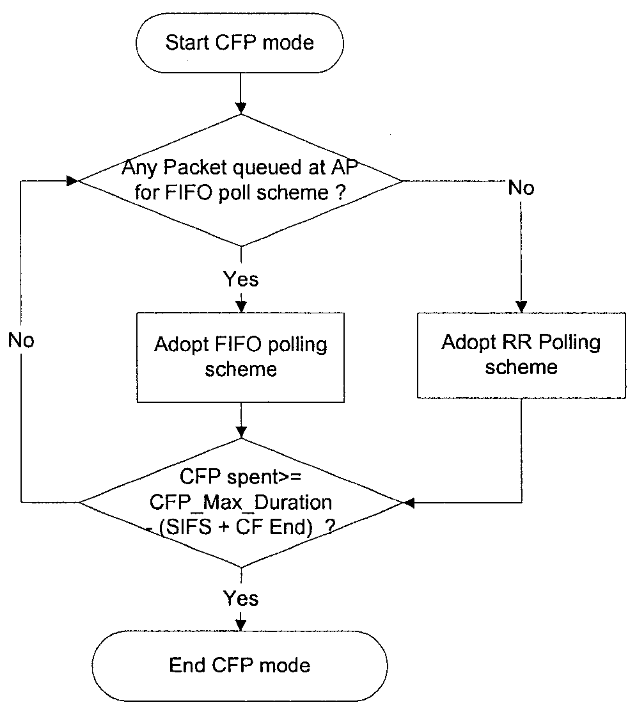


Figure 3.11: A flowchart explaining the coexistence of FIFO and RR schemes.

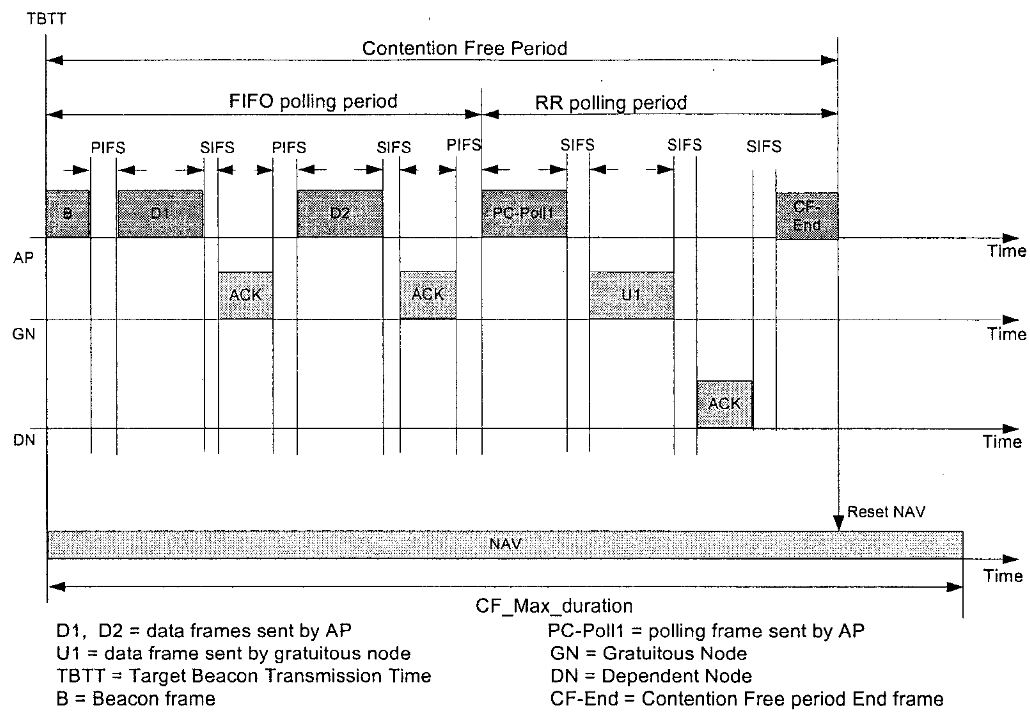


Figure 3.12: Timing diagram of FIFO followed by RR scheme.

3.3.2.4. Gratuitous Transmission between GN and DN

In gratuitous RR polling scheme, AP allows packet transmission and reception between Gratuitous Node (GN) and Dependent Node (DN). AP polls GN to poll their DNs to transmit data packets. Figure 3.13 shows the flowchart of this gratuitous polling. Round Robin polling scheme starts when AP finished transmitting packets from its own transmission buffer. AP starts polling gratuitous nodes from the one position lower in the polling list where it stopped during last RR period. As for example, AP starts transmitting gratuitous node 1 and ends RR polling after polling gratuitous node 5. Next time when the AP starts RR polling scheme, it will poll gratuitous node 6. After being polled by an AP, a GN consults its own polling list and polls DNs in a round robin fashion. We assume that during the handshaking phase between GN and DN (authentication and association),

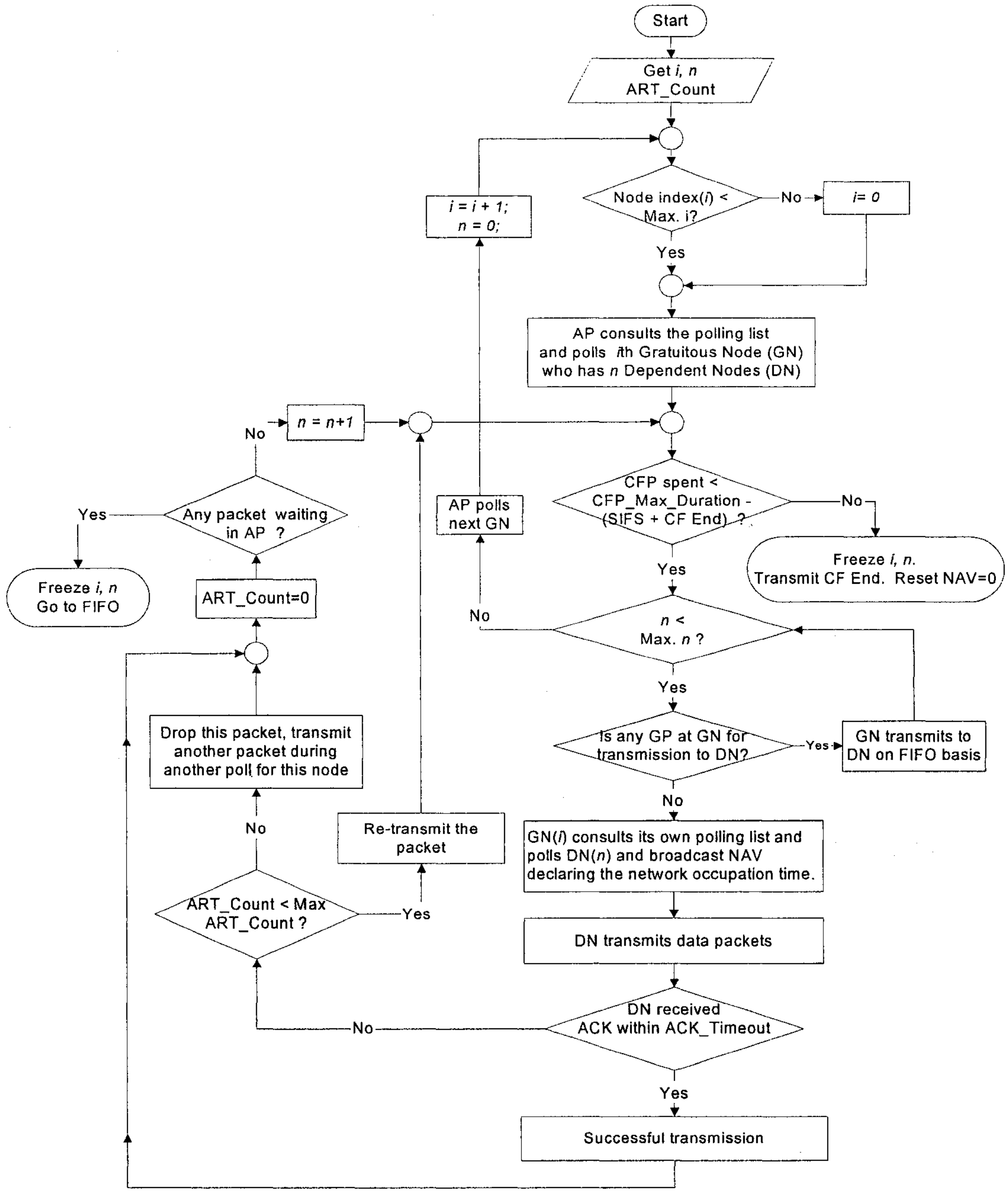


Figure 3.13: Gratuitous transmission between GN and DN.

the GN and DN would agree on a "master-slave" relationship such that the DN would act as a primary and the GN would act as secondary, i.e., the DN would transmit only if it is polled by GN.

The GN employs a FIFO scheme to transmit any gratuitous packet available in the transmission buffer to the DN. Additionally, GN employs RR scheme to allow the DN to transmit the gratuitous packets to the GN. Before each poll, GN looks for Network Allocation Vector (NAV) of AP, to see, if enough time is left for transmission. If there is enough time for transmission, the GN looks for any packet available for transmission to the DN. If there is any packet in GN's buffer, it will transmit it to the DN. The GN waits only SIFS period between two consecutive gratuitous packet transmissions. If there is no more packet in the GN for transmission, and there is enough time available for transmission under CFP, the GN polls the DN and transmits the NAV within the poll, so that the AP and the other nodes will not capture the channel during gratuitous packet transmission by DN.

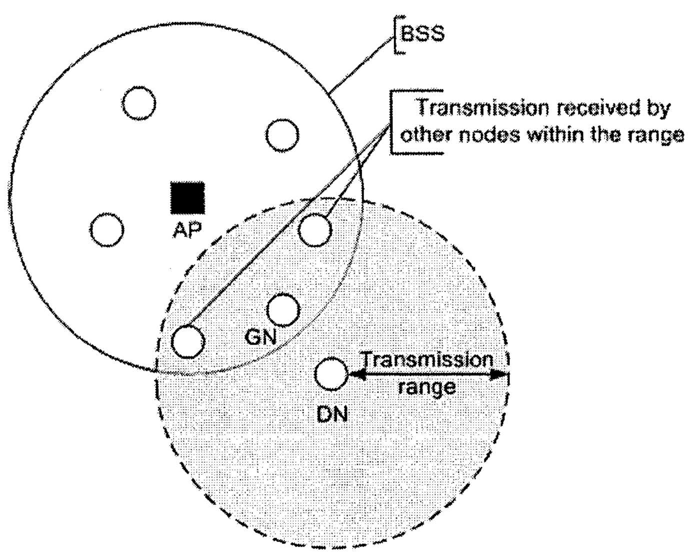


Figure 3.14: Transmission of a DN heard by more than one node in a BSS.

Polling by GN is necessary for the data packet transmission of DN. Because, when the DN transmits a packet, it can be heard by not only the GN but also other nodes within the transmission range of DN. Figure 3.14 explains this scenario. The big shaded circle is the transmission range of a DN. The big white circle is the area of a BSS. The small white circles are the nodes. The transmission of a DN is heard by not only DN but also other nodes within the transmission range of DN. When the GN polls a DN, it also transmits NAV declaring that the channel will be busy for one transmission time. After listening to the poll and corresponding NAV, other nodes including AP, will remain silent, so that no collision occurs during gratuitous packet transmission by DN.

In the RR polling scheme, AP polls GN after one PIFS period, and GN polls DN after one SIFS period. Whenever the end of CFP period comes, AP transmits CFP_End after one SIFS period. When a packet is available for transmission in the AP transmission buffer, during a RR polling period, AP waits until the end of polling and transmission of

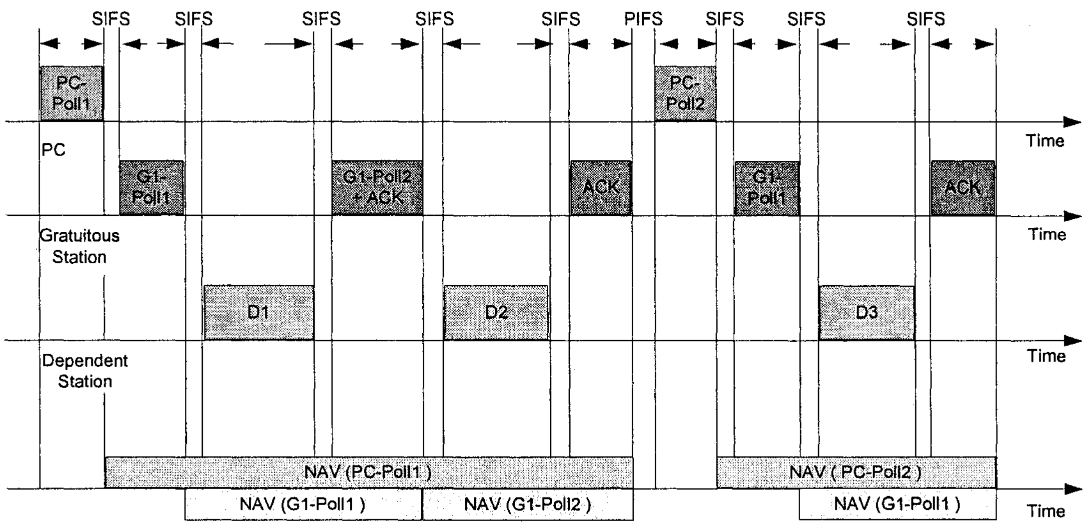


Figure 3.15: Timing diagram of RR polling.

the present gratuitous node. When there is no NAV from DN and the channel is idle, the AP takes control of the channel by transmitting packets after one PIFS period. Before FIFO polling scheme AP saves polling sequence of gratuitous nodes. Each node transmits Data and ACK after one SIFS period. The timing diagram of RR polling is shown in Figure 3.15.

3.4. Assumptions

Several assumptions have been made to reduce the complexity of our simulation. They are as follows:

- No interference is considered from nearby BSSs.
- No station operates in the "power savings" mode (PS-Mode).
- At each transmission attempt, and regardless of the number of retransmissions suffered, each packet collides with constant and independent probability.
- We consider zero propagation delay, which is a fairly realistic assumption if the maximum transmission distances are on the order of hundred meters between stations.
- We ignore high speed back bone transmission delay as the length of the test field/ESS is 2000 m.
- Zero processing delay is assumed at all nodes.
- The contract associated with a connection can not be re-negotiated during the simulation period.

- After authentication and association, a "master-slave" relationship is established between the gratuitous and the dependent node.
- All data packets are of the same size.
- The size of a buffer is expressed in terms of data packets it can store.
- Packet loss in each hop is independent of another hop and is invoked by uniform distribution function.
- Call generation probability of each node is the same.
- Packet generation probability of each node is the same.
- All the calls originate and end within the ESS.

3.5 Functions of Each Part in the Simulation

There are several parts in our simulation model. The functions of these parts are described as follows:

1) ***Source:***

- Generates packets and try to put it in the transmission buffer. If the buffer is full, there will be buffer overflow.
- Forwards the packets to the destination, gratuitous node, or AP according to the routing logic.
- If there is a transmission error, the source can retransmit the packet up to the retransmission limit.

2) ***Gratuitous Node at source BSS:***

- Receives the packet from the source and then try to put the packets in the transmission buffer. If the buffer is full there will be gratuitous packet drop.

- Transmits the gratuitous packets to the destination node or AP according to routing table.
- If there is a transmission error, the gratuitous node retransmits the packet up to the maximum transmission limit.

3) ***Home AP:***

- Receives packets from the transmitting nodes and then forward them according to routing table.
- Alternates between DCF and PCF.
- Under PCF, the AP works as a PC.
- If the packet's destination is outside of the BSS, it will forward the packet to the destination AP through the back bone network.
- If the packet's destination is inside of the BSS, it will transmit the packet in CFP mode under PCF.
- AP works as a gateway, trying to transmit immediately after receiving a packet.

4) ***Backbone Network:***

- The backbone network is a high speed wired network. Using internet protocol, it transmits data immediately to the receiving AP.
- No transmission error, and time delay in the backbone network is assumed.

5) ***Destination AP:***

- Receives packets from the backbone network and then forwards them to the destination node or gratuitous node.

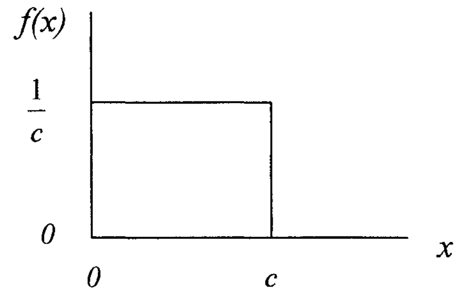
- Allows gratuitous transmission between gratuitous node and dependent node during CFP.

6) ***Gratuitous Node at Destination:***

- When AP allows gratuitous transmission during CFP, the gratuitous node does gratuitous communication with the dependent node.

3.6. Uniform Random Generator

The uniform random generator is fundamental to the whole simulation. The uniform random generator works according to uniform probability distribution function. It gives uniform probability for the value of a random number over a given interval. The probability density function of a uniform random generator is shown in Figure 3.16. Mersenne Twister (MT) [30] random number generator is well known for its good performances and availability. We have used Mersenne Twister random number generator for our simulation. We have taken a range from 0 to 1 to call the uniform random variable and define it as U(0,1).



$$f(x) = \begin{cases} \frac{1}{c} & 0 \le x \le c \\ 0 & \text{else where} \end{cases} \tag{3.1}$$

Figure 3.16: Uniform probability density function.

3.7. Functions of Node

Each node has many attributes, such as location information, traffic information, association information, routing information, buffer etc. These can be defined as follows:

- ***Node Number:***

Node numbering begins from zero. For the simplicity of our simulation node number is also used as node address.

- ***Receive/Transmit Buffer:***

The receive buffer keeps the received packets while the transmit buffer keeps the packets for transmission.

- ***Cluster Number:***

Each cluster has a unique number starting from zero. For simplicity of our simulation, the cluster number is considered as an AP address.

- ***Association Information:***

Each node keeps a record of the BSS it is associated with.

- ***Routing Table:***

Each gratuitous node as well as AP maintains a routing table.

3.7.1. Active/Idle Node State and Call Generation

Active node is that node which generates a call and is ready to generate packets. The probability of node generating calls is $\lambda < 1$. At the beginning of the simulation, each node's active/idle state is defined and remains unchanged for the rest of the time in the simulation. The call generating nodes are selected according to the algorithm shown in Figure 3.17. A node calls a uniform random generator function U(0,1) to get a random variable. If the random variable R[i], is less than the probability of call generation λ, a node becomes active and a call is generated; otherwise the node remains idle. Here i is the node number. We assume that the node which has generated a call remains active for the rest of the simulation. N is the total number of nodes.

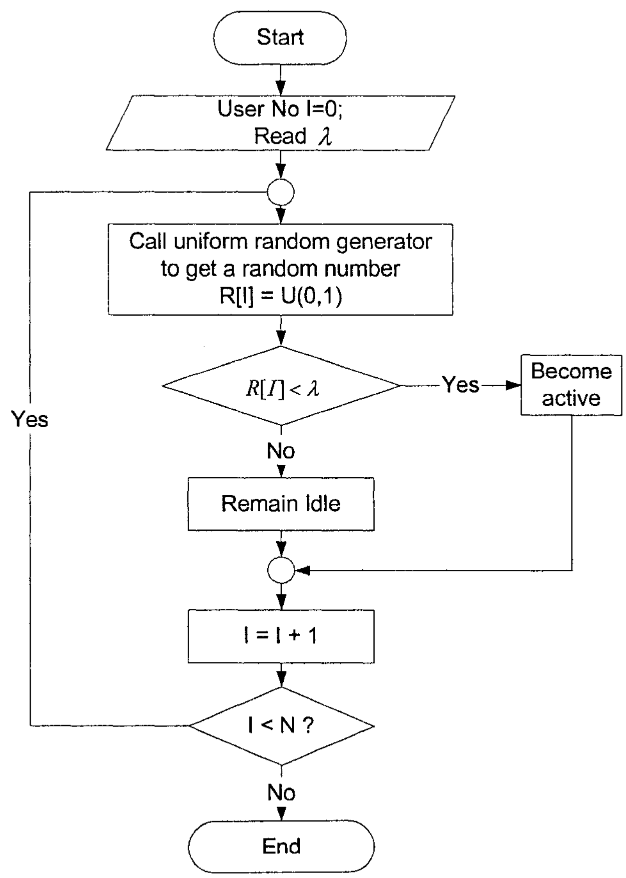


Figure 3.17: The flowchart explaining active/idle node state.

3.7.2. Input Traffic Load

When a node is active, it generates a call. Uniform random generator has been used to determine the input load at the source. At each iteration, a uniform random number generator U(0,1) is invoked to generate a random number X[i]. If the random number X[i] is less than the given load ρ, the node is allowed to generate a packet. On the other hand, if the random number X[i] is greater than the given load, no new packet is generated. For example, if the given traffic load $\rho = 0.3$ and the random number generated at a particular iteration is 0.2, a source generates a packet.

3.7.3. Initialization of Node Location

The default area of our test field is 2000x2000 square meter for both uniform and random AP distribution. For each user, we call U(0,1) two times to get two uniform random variables RanX and RanY. Thus the Cartesian coordinates of the node is (X_i = RanX*2000, Y_i = RanY*2000).

3.7.4. Selection of Destination Address

Every node has equal transmission requirements and the destination address is assigned randomly. All the nodes' index number is randomly shuffled in a destination list. Each node has been serially assigned with a destination from that shuffled list. Whenever a destination is assigned, the corresponding index number is removed from the shuffled destination list. In this way, each node has been assigned a unique destination address.

3.8. Design of a Cluster

Two types of clusters are formed. Uniform AP distribution represents standard ESS and random AP distribution represents gratuitous ESS.

3.8.1. Formation of a Random AP Cluster

Each cluster is considered as a circle of 200 meter radius inside a 2000x2000 square meter test field. The centre of the circle is randomly chosen. The distance between two circles must be greater than or equal to the diameter of the circles. AP is situated at the centre of the circle. Some of the nodes fall under a BSS and some of the nodes fall outside of BSS.

3.8.2 Formation of a Dependent Node

Figure 3.18 explains the formation of dependent node. An independent node looks for nearby gratuitous node. The independent node does the authentication and association procedure with the first available gratuitous node inside a BSS. After initial authentication and association, the independent node becomes a dependent node of a particular BSS.

3.8.3. Formation of a Uniform AP Cluster

Each cluster is considered a small square inside the 2000x2000 square meter test field. The square area is chosen so that all the nodes will fall under the infra-structure network. AP is situated at the centre of each BSS. We have chosen 400x400 square meter area for a cluster.

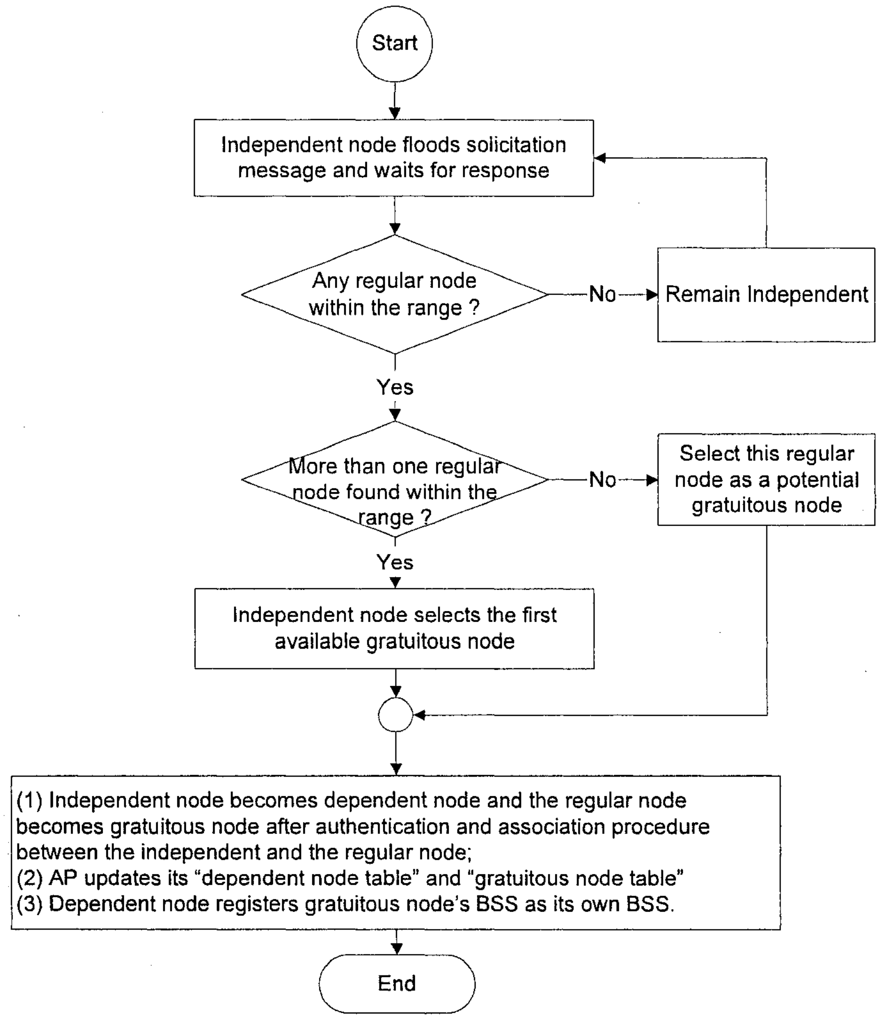


Figure 3.18: A flowchart of the joining process of a dependent node with a BSS.

3.9. Routing

Routing is required when the AP works under PCF. AP works as a gateway and forwards incoming and outgoing packets to and from BSS. The routing logic is shown in Figure 3.19.

3.9.1. Routing at AP

Each AP and gratuitous node maintains incoming and outgoing routing tables.

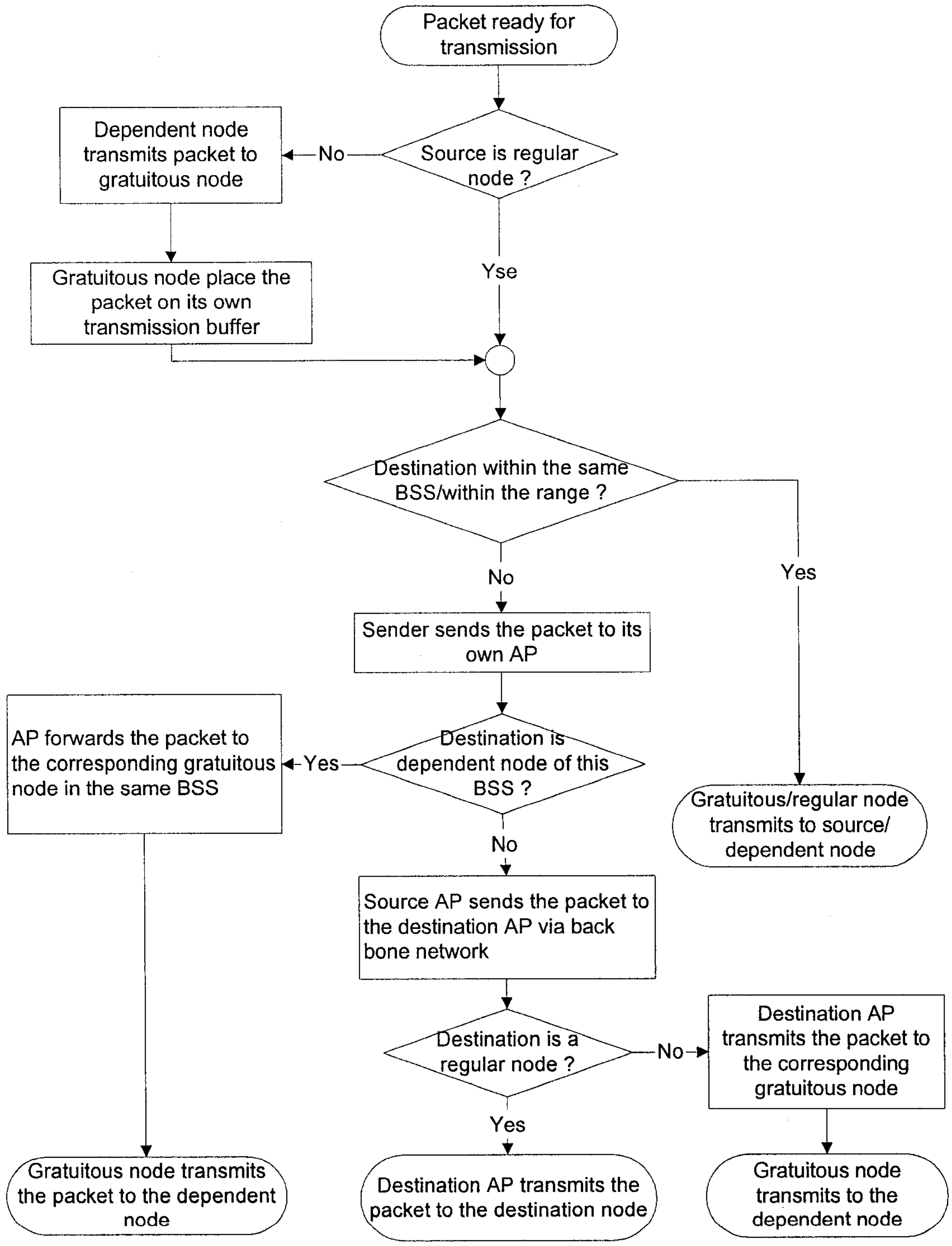


Figure 3.19: A flowchart explaining the routing logic in multi-clustered WLAN.

3.9.1.1. Outgoing Routing at AP

For outgoing packets, AP consults the routing table and decides the destination AP and sends the packet to the destination AP using the backbone network. The outgoing routing table at AP may have the format in Table 3.1.

Table 3.1: Outgoing routing table at AP.

Index	Source address	Destination address	Next AP address
1	65	19	3
2	8	85	7
3	...	...	...

3.9.1.2. Incoming Routing at AP

Whenever AP receives an incoming packet, AP consults its routing table and decides if the destination is inside the BSS or outside of the BSS. If the destination is inside the BSS, it can directly transmit the packet to the destination. If the destination is outside of the BSS it transmits the packet to the corresponding gratuitous node. The table may have the format in Table 3.2.

Table 3.2: Incoming routing table at AP.

Index	Source address	Destination address	Next node address
1	65	19	19
2	8	85	11
3	...	...	...

3.9.2. Routing at Gratuitous Node

Gratuitous node also maintains its own routing table. It maintains two routing tables.

3.9.2.1. Routing Packets from Dependent Node

When a dependent node sends a packet to the destination, the gratuitous node consults its “From DN” routing table and decides if the destination is within the BSS or outside of the BSS. If the destination is within the BSS it can directly deliver the packet to the destination. If the destination is outside of the BSS, the gratuitous node delivers the packet to the AP. The routing table may look as in Table 3.3.

Table 3.3: From DN routing table at GN.

Index	Source address	Destination address	Next node	AP
1	65	19	71	No
2	8	85	No	Yes
3	...	...	...	...

3.9.2.2. Routing Packets to Dependent Node

Whenever a DN receives a packet, it consults its "To DN" routing list and directly delivers the packet. The routing table may look as in Table 3.4.

Table 3.4: To DN routing table at GN.

Index	Source address	Destination address	Next node address
1	65	19	19
2	8	85	85
3	...	...	...

3.10. Design of Physical Layer

MAC PDU is mapped into Physical Layer Convergence Procedure (PLCP) sublayer. After that Physical Medium Dependent (PMD) sublayer deals the method of transmission on wireless medium. DSSS or FHSS transmission technique with the data data rate of 1 Mbps has been considered.

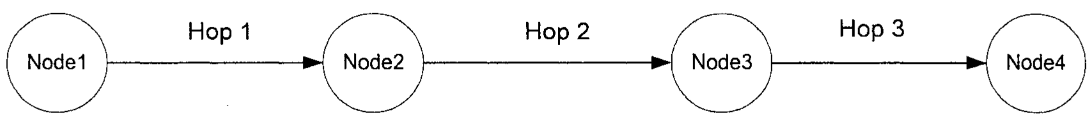
3.10.1. Shared Channel Model

All the nodes inside a cluster share the same wireless channel. A wireless channel is a radio frequency in the air interface with a particular modulation and coding scheme.

We assume a free space [31] channel so that the RF energy arriving at the receiver is a function of distance only. Whenever a node transmits a packet, it is heard by all the nodes within the same cluster. If the receiving node is within range from the transmitter, and the transmission signal strength is good enough, the receiver can receive the packet without any error. Nodes outside of a cluster do not share its channel with the nodes inside the cluster. Outside nodes only share the channel with the nodes which are within its range.

3.11. Description of Packet

When a node generates a packet, it contains source, destination derived from the call generation. It also has transmitter and receiver information fields. The source is the node which generates the packet and the destination is the final destination of a packet. The packets can travel several hops from source to destination. In one end of a hop, the transmitter sends the packet and on the other end of the hop the receiver receives the packet. The transmitter and the receiver may not be necessarily the source and the destination. In Figure 3.20, node1 is the source and the node 4 is the destination. But the packet has to go through the transmitter receiver pair in hop1, hop2 and hop3. In hop1 the source node1 is the transmitter and intermediate node2 is the receiver, similarly in hop2, intermediate node2 is the transmitter and intermediate node3 is the receiver and finally in hop3, intermediate node3 is the transmitter and the destination node4 is the receiver. Each packet starts with a timer and the timer increases with each program iteration until the packet successfully reaches destination. For simulation purpose, it is important to know the total time elapsed for end to end delivery of a packet. There is a hop count field and a retransmission count field for every packet. If the maximum hop limit or maximum retransmission limit is exceeded, the packet is discarded. There are several types of packets: (1) Data Packet; (2) RTS packet; (3) CTS packet; (4) ACK packet; (4) Poll packet; (5) Poll + Data /ACK.



Source: Node1, Destination: Node 4

Fig. 3.20: Source, destination, transmitter and receiver.

3.12. Loss Model

Buffer overflow, gratuitous packet drop and transmission error probability can contribute to packet loss. We consider these three types of losses in our simulation. Buffer overflow is dependent on the buffer condition in the source. Whenever a source generates a packet and finds that the buffer is full, there is a buffer overflow. If a gratuitous node receives packets from the other nodes and finds that its receive buffer is full, there will be gratuitous packet drop. On the other hand, loss due to transmission error depends on the loss rate of a link. The process is as similar as traffic input loss. Whenever a packet passes a link hop, we call uniform random number generator U(0,1) to get a random number Xi. If $X_i \le P_e$, where *Pe* is the priori known packet error probability, there is a packet error; otherwise, there is an error free transmission. If error occurs, the packet is retransmitted up to the maximum retransmission limit. If within the retransmission limit, no error occurs, the packet is successfully transmitted in that hop at a particular iteration.

3.13. Input Parameters

Some input parameters are varied while other input parameters are fixed to measure the performance under different situations. We have used the following input parameters for our simulation:

- **Input Traffic Load:**

We have set the minimum probability of packet generation to 0.05 and the maximum probability of packet generation to 0.5. We have carefully chosen this limit because, the packet generation probability below 0.05 contributes towards empty buffer very quickly and hence erroneous results. On the other hand, probability of packet generation above 0.5 results in too much congestion in the system and hence abnormal delaying in the packet delivery time and excessive packet loss.

- **Packet Error Probability:**

Packet error probability depends on the channel condition of a hop and the error probability of each hop is independent of the error probability of others. Throughout the simulation, it is 0.001 when not varied. While varied it ranges from 0.01 to 0.1.

• **Transmission Buffer Size:**

Transmission buffer size, while varied, varies from 2 to 6 data packet length. When fixed it is 4 data packet length.

• **Call Generation Probability:**

Call generation probability varies from 0.1 to 1. While not varied it is fixed at 1.

• **Backoff Window Size:**

Backoff window increase limit is directly related to the maximum backoff window size as per the following equation:

$$CW_{max}=2^m\, CW_{min.} \tag{3.2}$$

where CW_{min} is the minimum backoff window size and CW_{max} is the maximum backoff window size, m is the backoff window increase limit. In our simulation, we varied backoff window increase limit from 0 to 6. It means, maximum backoff window size is varied from 8 to 512. When not varied, it is fixed at 256.

• **Packet Timeout:**

This input parameter has been used for time-bounded packets. Packet timeout is varied from 5 to 50 iterations. While not varied, it is fixed at 20.

• **Retransmission Limit:**

The retransmission limit is varied from 0 to 2. When not varied, it is fixed at 2. Table 3.5 summarizes the input parameters and their values used in our simulations:

Table 3.5: All input parameters.

	Parameters	Value
1	ESS length	2000m
2	ESS width	2000m
3	WLAN radius (random AP)	200 m
4	WLAN length (uniform AP)	200m ~ 2000m
5	WLAN width(uniform AP)	200m ~2000m
6	Number of total nodes	100
7	Number of AP	1 ~100
8	Call generation probability	0.1 ~ 1.0
9	Load probability	0.05 ~ 0.50
10	Packet error probability	0 ~ 0.50
11	Buffer size	2 ~ 6 packet size
12	Maximum backoff window size	8 ~ 512
13	Maximum number of retransmissions	0 ~ 2
14	Timeout for real-time data packets	5 ~ 50 iterations
15	Number of simulation iterations	5000

3.14. Confidence Interval

Confidence interval is considered to obtain data from the simulation with a high degree of accuracy. To achieve 100% percent confidence level, we have to run the simulation for infinity number of times, which is not possible. However, we have set the number of iterations such that the error between the average of sampled data obtained and the theoretical average which correspond to infinite number of runs would not exceed 5%, therefore, the confidence interval is 95%.

3.15. Performance Criteria

The following performance parameters are used to get the performance measure of the system. During each run of the simulation program, one input parameter is varied, while others are remained constant and we obtain the output parameters. A number of nodes output values are to be averaged to get the overall performance criteria.

- **Average Buffer Overflow and its Variance:**

In each node, there is a finite buffer size. Whenever a packet is ready for transmission it is put in the transmission buffer. The packets are queued inside the buffer and are discharged on FIFO basis. However, if the packet arrival rate at the buffer is greater than packet discharge rate, the queue inside the buffer grows larger. When the queue length exceeds the buffer size, the buffer cannot accept further packets for queuing and buffer overflow occurs. We set the counter for counting the number of buffer overflows of each node during the whole run of the simulation program. The average buffer overflow(%) of a node is obtained by dividing the total number of buffer overflows of that node divided by total number of packets generated. The Average Buffer Overflow (ABO) of the network is given by:

$$ABO = \frac{\sum_{i=1}^{U}\left(\frac{b(i)}{N_i}\right)}{U} \tag{3.3}$$

Where $b(i)$ is number of buffer overflow of node i during the whole simulation. N_i is the total number of packets generated by node i during the whole simulation. U is the total number of nodes.

The Variance of Buffer Overflow (VBO) of the all the nodes can be calculated as below:

$$VBO = \frac{\sum_{i=1}^{U}\left(ABO - \left(\frac{b(i)}{N_i}\right)\right)^2}{U-1} \tag{3.4}$$

- **Average Gratuitous Packet Drop and its Variance:**

When a Dependent Node (DN) node forwards packets to the Gratuitous Node (GN), the GN receives the packet and then tries to put it in its transmission buffer for forwarding. If the GN's transmission buffer is full, it simply drops the gratuitous packet. We have set a counter in each DN to count this gratuitous packet drop. The average gratuitous packet drop of a DN is achieved by dividing the total number of gratuitous packet drops of each DN by the total number of packets generated both in the whole simulation time. The Average Gratuitous Packet Drop (AGPD) over all DNs is given by:

$$AGPD = \frac{\sum_{i=1}^{U}\left(\frac{g(i)}{N_i}\right)}{U} \tag{3.5}$$

Where $g(i)$ is number of gratuitous packet drop of node i during the whole simulation. The Variance of Gratuitous Packet Drop (VGPD) can be calculated as:

$$VGPD = \frac{\sum_{i=1}^{U}\left(AGPD - \left(\frac{g(i)}{N_i}\right)\right)^2}{U-1} \tag{3.6}$$

- **Average End-to-End Packet Delay and its Variance:**

End-to-end packet delay means the total time spent from the generation of packet in the source to its successful delivery to the final destination. It includes queuing delay, transmission delay, and the overhead of RTS, CTS, ACK, polling and transmission time. The average packet delay for each node is achieved by dividing the total transmission time of all the successful packets by the total number of successfully delivered packets. The Average End-to-end Packet Delay (AEPD) of the whole system is computed by dividing the sum of average packet delay of all the users by the number of users.

$$AEPD = \frac{\sum_{i=1}^{U} \left(\frac{\sum_{j=1}^{N_i} d(i,j)}{N_i} \right)}{U} \tag{3.7}$$

Where $d(i,j)$ is the end to end delay of the jth packet of node i. N_i is the total number of packets generated by node i during all iterations of the simulation program. U is the total number of users.

The Variance of End-to-end Packet Delay (VEPD) is calculated as follows.

$$VEPD = \frac{\sum_{i=1}^{U} \left(AEPD - \left(\frac{\sum_{j=1}^{N_i} d(i,j)}{N_i} \right) \right)^2}{U-1} \tag{3.8}$$

- **Average Throughput and its Variance**

Average throughput and variance are measured for asynchronous packets. Average throughput of a node is achieved by dividing the total number of packets successfully transmitted by the total number of packets generated by that node. To get the Average ThroughPut (ATP), we have to average this value for all the users.

$$ATP = \frac{\sum_{i=1}^{U}\left(\frac{S_i}{N_i}\right)}{U} \tag{3.9}$$

Where S_i is the total number of successful packets of user i. N_i is the total number of packets generated by users i. U is the total number of users.

Variance of average ThroughPut (VTP) is calculated as follows:

$$VTP = \frac{\sum_{i=1}^{U}\left(ATP - \left(\frac{S_i}{N_i}\right)\right)^2}{U-1} \tag{3.10}$$

- **Average Throughput of Time-Bounded Packets and its Variance:**

Average throughput of time-bounded packets of a node is achieved by dividing the total total number of packets successfully transmitted within time out by the total number of packets generated by that node. To get the Average Throughput of Time-bounded Packets (ATTP), we have to average this value for all the nodes.

$$ATTP = \frac{\sum_{i=1}^{U}\left(\frac{T_i}{N_i}\right)}{U} \tag{3.11}$$

Where T_i is the total number of successful time-bounded packets of users i. N_i is the total number of packets generated by users i during all the iterations of a simulation program. U is the total number of nodes.

Variance of average Throughput of Time-bounded Packet (VTTP) is calculated as follows:

$$VTTP = \frac{\sum_{i=1}^{U}\left(ATTP - \left(\frac{T_i}{N_i}\right)\right)^2}{U-1} \tag{3.12}$$

Chapter 4

Performance Evaluation

The simulation has been conducted to get the understanding of how mixed Contention Period (CP) / Contention Free Period (CFP) mode works in multi-clustered wireless LAN. We have used two network models in our simulation: (1) Uniform AP distribution; (2) Random AP distribution. While uniform AP distribution represents pure infrastructure networks, Random AP distribution represents hybrid infrastructure / ad hoc wireless LAN. The performance results for uniform AP distribution enable us to get an understanding of how our proposed MAC layer scheduling scheme behaves in infrastructure networks. The simulation results for random AP distribution, enable us to get an understanding of how gratuitous mode works under the CP/CFP scheduling scheme. We make a comparison between the performance criteria of uniform and random AP distribution scheme. The purpose of the comparison is to get a idea of how the performance results in gratuitous mode vary from these of standard infrastructure multi-clustered wireless LANs.

We have executed the following simulations in both uniform and random AP distribution simulating different scenarios:

1. ***Input Load Simulations:*** We vary the input load (packet generation probability) for both uniform and random AP distribution to get the performances of these two schemes.

2. ***Channel Quality Simulations:*** Packet error probability is varied to get the performances at different channel conditions on the two schemes.
3. ***AP Population Simulations:*** We vary the number of APs for a fixed number of users in both schemes.
4. ***Maximum Backoff Window Size Simulations:*** Maximum backoff window size was set at different levels to see the effect of these on two schemes.
5. ***Timeout Simulations:*** This check is particularly important for time bounded packets and we set different time out values to see the performances of time bounded packets.
6. ***Call Generation Simulations:*** We vary call generation probability for both schemes and obtain their performances. Call generation probability in random AP distribution does not give a consistent picture, because, each randomly selected node falls randomly inside and outside of the BSS. We get more consistent graphs on uniform AP distribution. At last, we compare the results of these two schemes.

The simulation has been carried out on Pentium 4 processor at 2 GHz, with 256 MB RAM with Microsoft Windows XP Professional 2002 operating system.

4.1. Performance Evaluation under Varying Load

We have varied the input load in random AP distribution to see the performances in throughput, end-to-end packet delay, buffer overflow, gratuitous packet drop, throughput of time bounded packets. The simulation has been run to see how CP/CFP mode performs in ESS. We have also run the input load simulation in the gratuitous

ESS and compared the performances in the standard and gratuitous ESS. The comparison is particularly important as we have introduced the gratuitous mode. It is important to see, how the performance criteria of gratuitous ESS vary from that of standard ESS, where every node is inside of a BSS. So far, we have seen the performance results of a single BSS or IBSS. But we want to see a comprehensive view of performances in a network with multiple BSS, using mixed CP/CFP mode. The simulation for standard ESS with the uniform AP distribution is particularly important in this aspect. Table 4.1 shows the values of input parameters used.

Table 4.1: Input parameters used for varying load simulation.

Parameters	Value
Test area	2000m X 2000m
WLAN radius (random AP)	200m
WLAN length (uniform AP)	400m
WLAN width(Uniform AP)	400m
Number of total nodes	100
Number of regular node	56 (from the simulation)
Number of dependent node	44 (from the simulation)
Call generation probability	1
Load probability	0.05 ~ 0.50
Packet error probability	0.001
Buffer Size	4 packet length
Maximum back off window size	256
Maximum number of re-transmissions	2
Time out for real time data packets	20 iterations
Number of iterations	5000

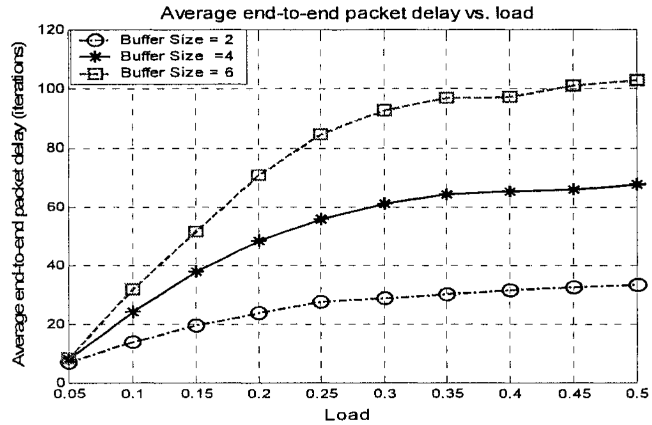


Figure 4.1: Average end-to-end packet delay vs. load in random AP

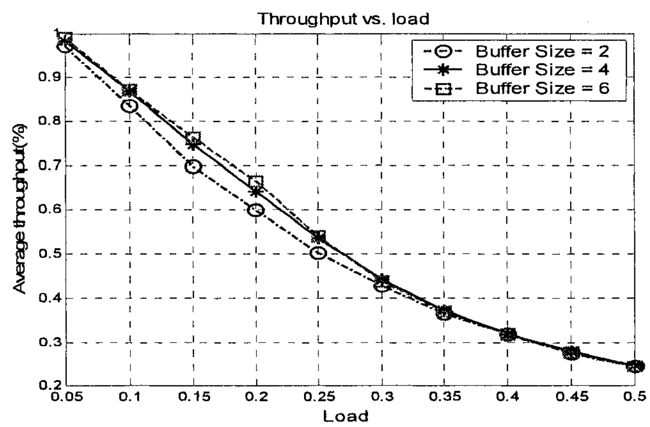


Figure 4.2: Average throughput vs. load in random AP

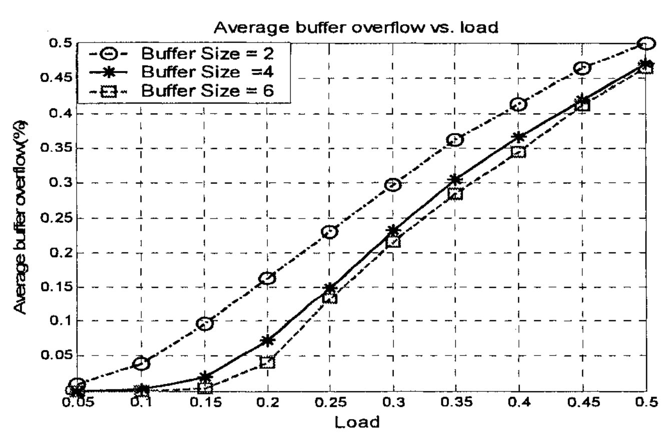


Figure 4.3: Average buffer overflow vs. load in random AP

Figures 4.1 through 4.8 show the performance criteria in gratuitous ESS with varying input load. Figure 4.1 shows that with the increase of input load, average end to end delay increases. The reason is clear, with the increase of input load, more packets are queued at the buffer. All the packets in a BSS are queued and wait until a successful transmission attempt after backoff. But the story does not end here; if more packets are injected in the system, more stations try to transmit packets simultaneously and hence collision occurs. Though the backoff mechanism is designed to avoid collision, it is more likely to occur a collision with the higher number of packets. Though polling mechanism works for dependent node and packet delivery from AP, but polling appears to be a slower process comparing to packet arrival rate at each node and AP. So with the increase in load, it is inevitable that there is an increasing end to end delay. We can also see that with the increase of buffer size, average end to end delay becomes larger. The reason is, when buffer size increases, the buffer can accommodate more packets and hence less buffer overflow. Figure 4.3 shows this aspect. However, each packet is placed in a longer queue and consequently longer queuing delay before any transmission takes place. Figure 4.2 shows that with the increase of load, the average throughput of the network decreases. Buffer size has little to do with this. As we have described before, with the increase of load, the system cannot handle more packets and there is more buffer overflow and more gratuitous packet drop. As a result the overall throughput decreases.

Figure 4.3 shows that with the increase in load, the average buffer overflow increases. However, the situation can be made better using larger buffer size. The reason is quite understandable, with the increasing load the node cannot quickly deliver

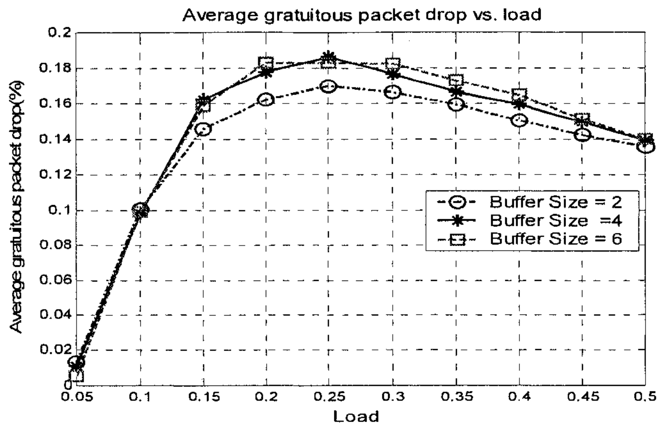


Figure 4.4: Average gratuitous packet drop vs. load in random AP

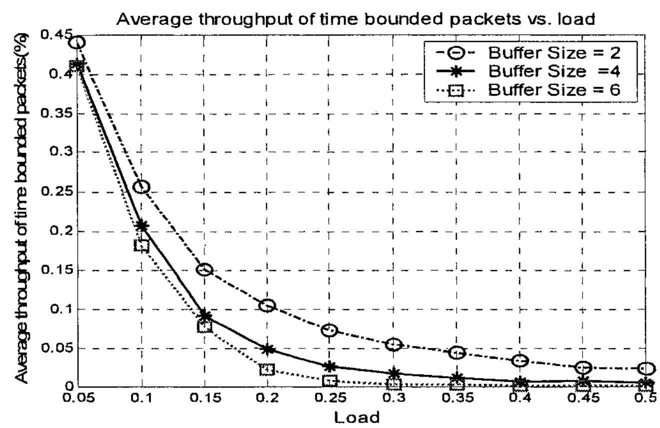


Figure 4.5: Average throughput of time-bounded packet vs. load in random AP.

the queued packet at its transmission buffer and packet delivery rate becomes lower than the packet arrival rate. And hence, the buffer becomes full very quickly. So, the additional arriving packets cannot get a place inside the buffer and buffer overflow occurs. With the increasing buffer size, more packets are queued leading to less buffer overflow.

Figure 4.4 describes the effect of increasing the load on the gratuitous packet drop. With the increasing load, the percentage of gratuitous packet drop initially increases but further increase in load ultimately decreases the percentage gratuitous packet drop. We know from Figure 4.3 that with the increase in load, the buffer overflow increases. With the increasing load, more packets are dropped at the source due to buffer overflow. The dependent node tries to send more packets to the gratuitous node, but the number of gratuitous packets reaches near saturation with a given polling frequency. In this scenario, most of the gratuitous packets are dropped at the source due to buffer overflow. The rest of the gratuitous packets are dropped at the gratuitous node. Under heavy load, the gratuitous node's transmission buffer is already full due to its own packets waiting for transmission, so the gratuitous node refuses any additional gratuitous packets from the dependent node. It is to be mentioned that this is the percentage value, the absolute number of gratuitous packet drop continuously increases with the increasing load, however, the percentage of gratuitous packet drop with respect to the total generated packet decreases.

Figure 4.5 shows the throughput of time-bounded packets with a given timeout value. The average throughput(%) of time-bounded packets decreases under increasing load. The throughput decreases in both asynchronous and synchronous packet transmission. However, in the case of time-bounded packet, the throughput decreases more quickly. Under high load, each packet faces additional delay which is serious for time sensitive packets and hence throughput of time-bounded packets rapidly declines.

Figure 4.6 shows that with the increasing load, the end-to-end packet delay variance increases. It is easily seen that with the increasing load, there are more packet collisions and longer delay for larger backoff window size. Each packet faces more queuing delay, and the delay of one packet compared to another is highly variable.

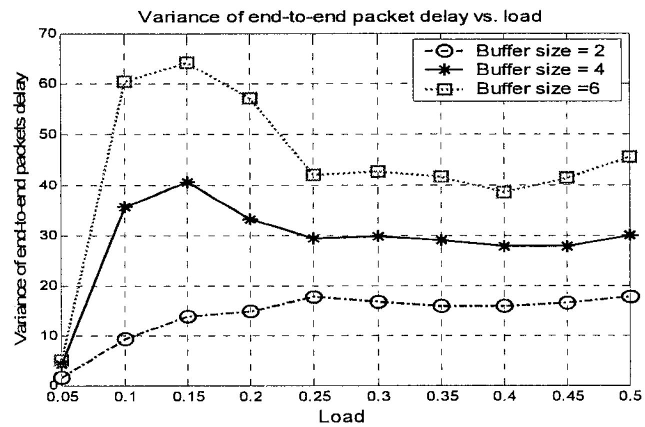


Figure 4.6: Variance of end-to-end packet delay vs. load in random AP

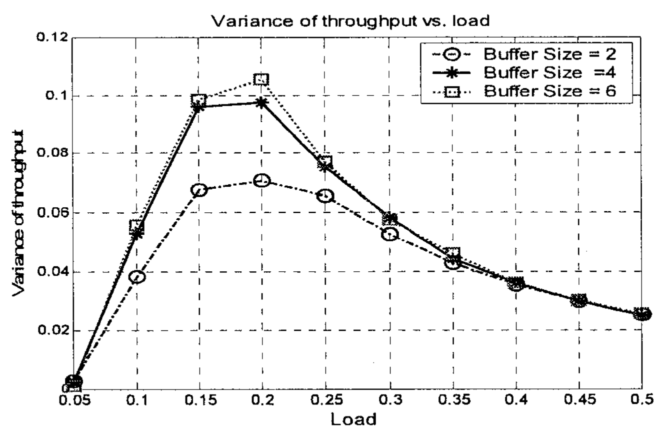


Figure 4.7: Variance of throughput vs. load in random AP

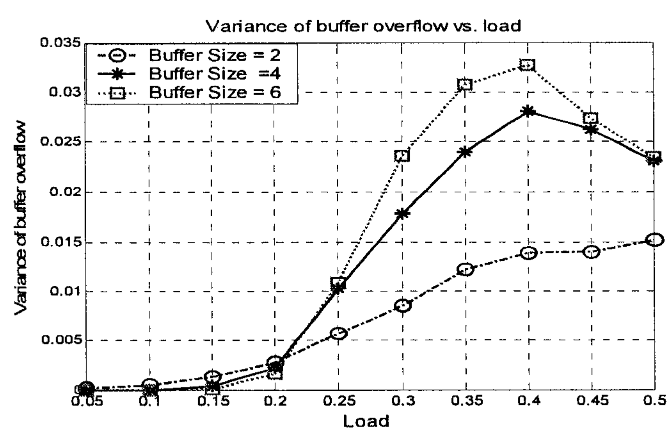


Figure 4.8: Variance of buffer overflow vs. load in random AP

It is interesting to see that the lower buffer size yields better delay variance performance. This happens at the expense of throughput. Figure 4.7 shows that the throughput variance initially increases with the increase in load, but the further increase in load decreases the throughput variance. During light load, the throughput performances of all nodes are similar. However, with the increasing load, the throughput variance increases. Further, increase load results in the lowering of throughput and corresponding variance. Figure 4.8 shows that during light load the buffer overflow variance continuously increases; however, during heavy load, the variance decreases. Very high buffer overflow almost on every node causes the variance to go down.

Figures 4.9 through Figure 4.13 describe the performance comparison between standard and gratuitous ESS with varying load. All these Figures show that the performance of randomly distributed AP is slightly worse than that of uniform AP distribution. This is the cost of gratuitous service. Figure 4.10 shows that under light load, the end-to-end packet delay performance of a standard ESS is better than that of a gratuitous ESS. But during heavy load, the scenario is reversed. The reason is, during heavy load, the overall throughput of gratuitous ESS becomes extremely low (Figure 4.2), but still then some dependent nodes can transmit packets to the neighbouring destinations which are just one hop away. These dependent nodes do not share channels with the nodes inside the BSS and hence does not contend for the channels. The end-to-end packet delay of the packets transmitted by these nodes is very small, because the destination is just one hop away. In Figure 4.14 dependent nodes A, C, E and G transmits packets during gratuitous polling to the destination which are just one hop away.

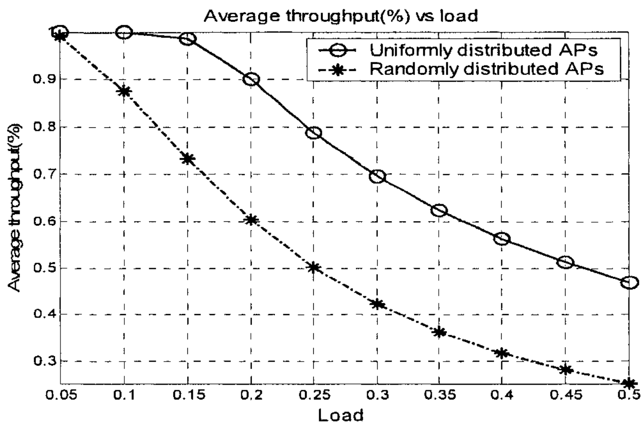


Figure 4.9: Average throughput (%) vs. load in uniform and random AP

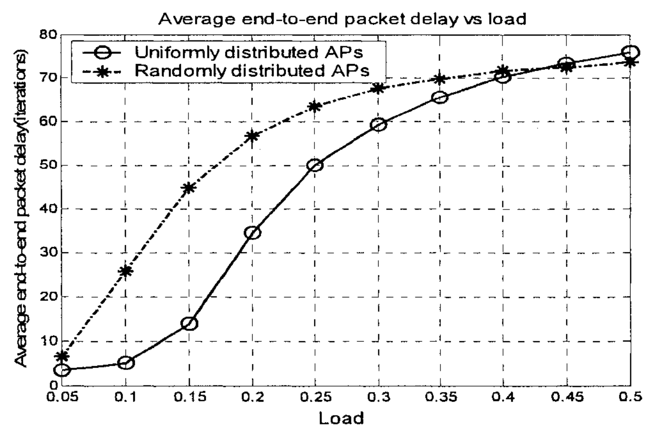


Figure 4.10: Average end-to-end packet delay vs. load probability in uniform and random AP.

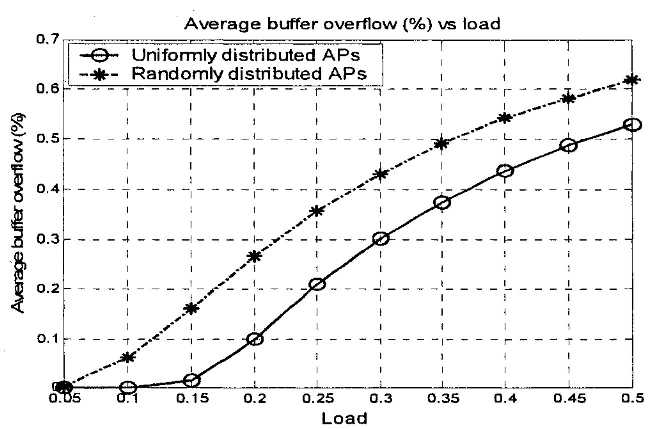


Figure 4.11: Average buffer overflow (%) vs. load in uniform and random AP.

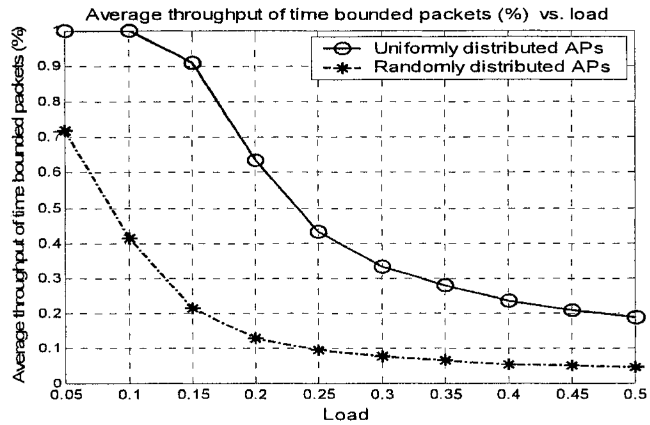


Figure 4.12: Average throughput of time-bounded packet vs. load in uniform and random AP.

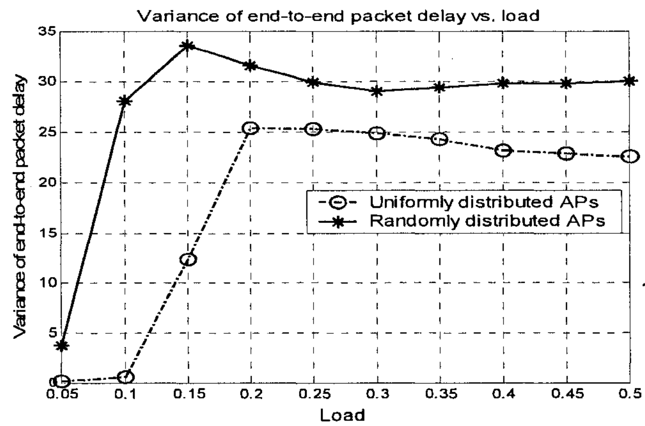


Figure 4.13: Variance of end to end packet delay vs. load in uniform and random AP.

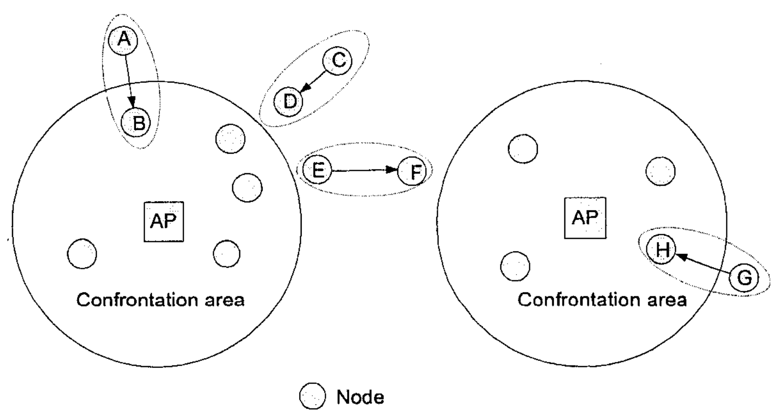


Figure 4.14: One hop transmission of dependent nodes during polling period.

4.2. Performance Evaluation under Varying Packet Error Probability

We change the packet error probability at different re-transmission limit to examine the error performance of the two networks. The input parameters used are shown in Table 4.2.

Table 4.2: Input parameter for varying packet error probability simulation:

Parameters	Value
Test area	2000m X 2000m
WLAN radius (random AP)	200m
WLAN length (uniform AP)	400m
WLAN width(Uniform AP)	400m
Number of total nodes	100
Load probability	0.10
Call generation probability	1
Packet error probability	$0 \sim 0.5$
Buffer Size	4 packet length
Maximum back off window size	256
Maximum number of re-transmissions	$0 \sim 2$
Time out for real time data packets	20 iterations
Number of iterations	5000

Figures 4.15 through 4.19 show the error performance of uniform randomly distributed AP network (standard ESS). Figures 4.20 through 4.24 show the error performance comparison between standard ESS and the gratuitous ESS. We can see from Figure 4.15 that with the increase in packet error probability, the average end-to-end packet delay increases. This is quite clear as more packets are lost with the increasing transmission error and hence more re-transmissions are needed. All these factors lead to lower throughput (Figure 4.16) and higher queuing delay at the transmitter. However, zero re-transmission contributes to low end-to-end packet delay at the cost of throughput.

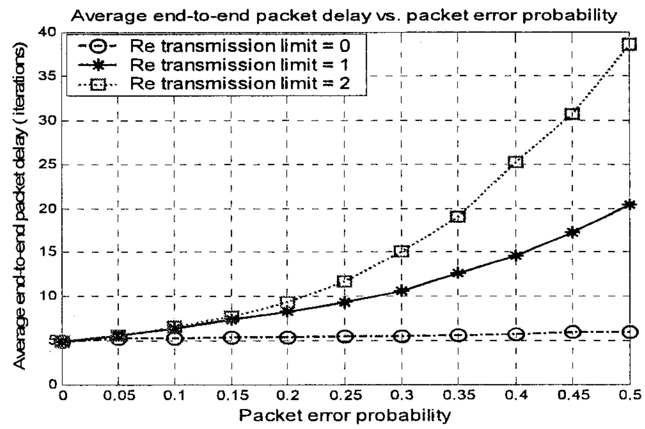


Figure 4.15: Average end-to-end packet delay vs. packet error probability in uniform AP.

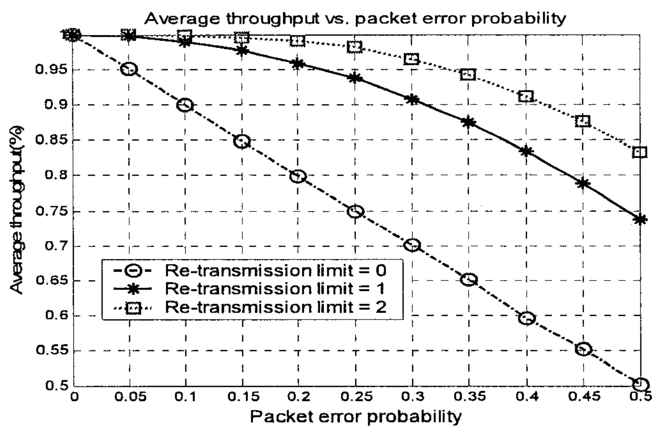


Figure 4.16: Average throughput(%) vs. packet error probability in uniform AP.

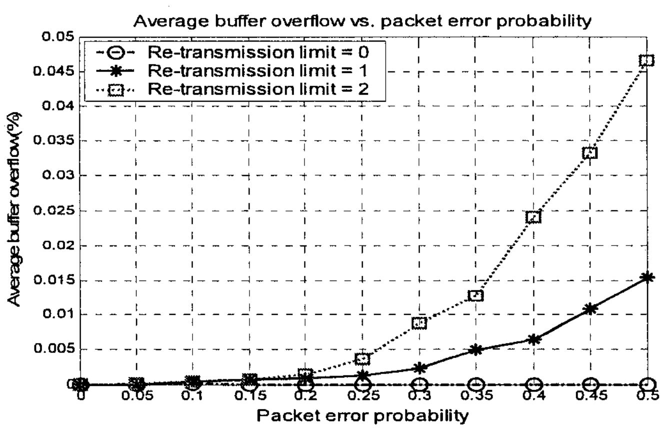


Figure 4.17: Average buffer overflow(%) vs. packet error probability in uniform AP.

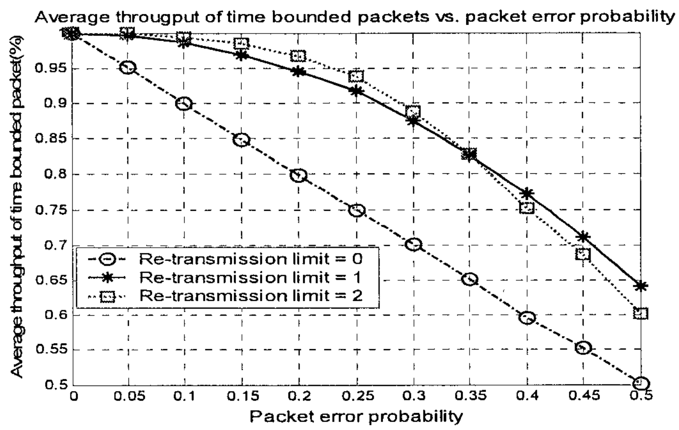


Figure 4.18: Average throughput of time bounded packets(%) vs. packet error probability in uniform AP.

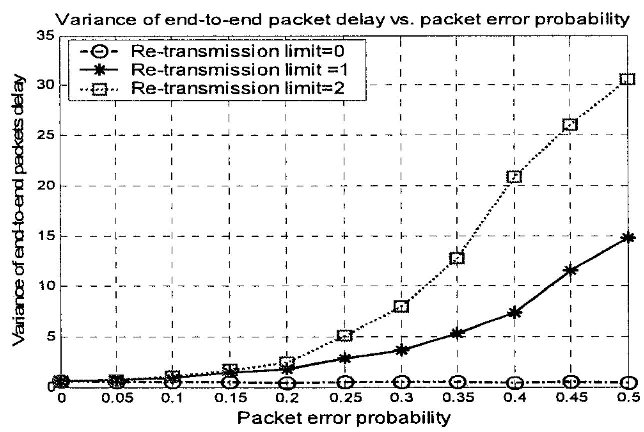


Figure 4.19: Variance of end-to-end delay vs. packet error probability in uniform AP.

Figure 4.16 shows that more retransmissions yield better throughput performance. Figure 4.17 shows that with the increasing transmission error, buffer overflow increases. The situation becomes worse with the higher retransmission limit. As each additional transmission attempt causes larger queuing length at the buffer, there are more buffer overflows. Figure 4.18 shows an interesting picture. With the increasing transmission error, the throughput of time-bounded packets decreases. The interesting observation is that under low transmission error conditions, higher retransmission limit seems to be helpful for the throughput of real time packet. However, under heavy channel error conditions, the higher retransmission limit causes degradation of real time packet throughput performance. The reason is clear, under low transmission error, very few packets gets lost, re-transmission helps to recover them, the network works faster. But under heavy channel error, more packets get corrupted and each additional re-transmission causes additional delay which results in crossing the time out limit for the real time packet. Figure 4.19 shows the variance of the end-to-end packet delay. Reasonably, the variance increases with the higher transmission error. The variance becomes also larger with the higher retransmission limit.

Figures 4.20 through 4.24 show the performance comparison between standard ESS and gratuitous ESS. It is easily seen that the error performance of standard ESS is better than that of the gratuitous ESS. Out of 100 nodes, there are 44 dependent nodes in gratuitous ESS. The 56 nodes inside the BSSs take burden of these

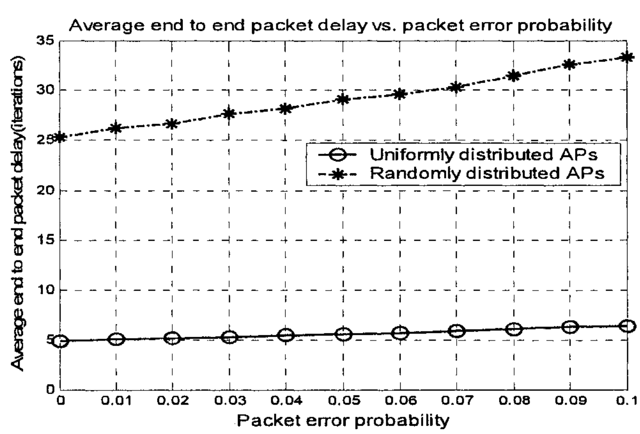


Figure 4.20: Average end-to-end delay vs. packet error probability in uniform and random AP.

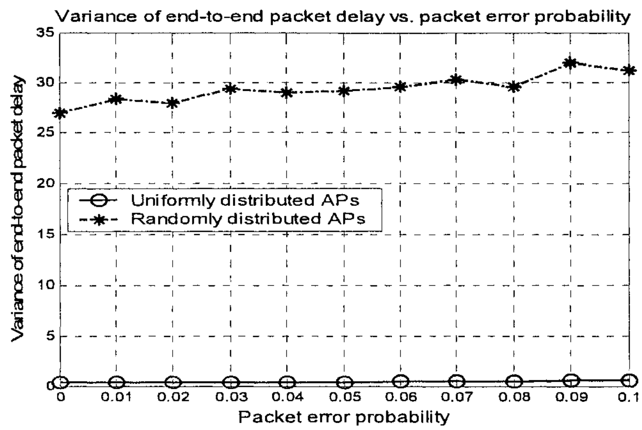


Figure 4.21: Variance of end-to-end delay vs. packet error probability in uniform and random AP.

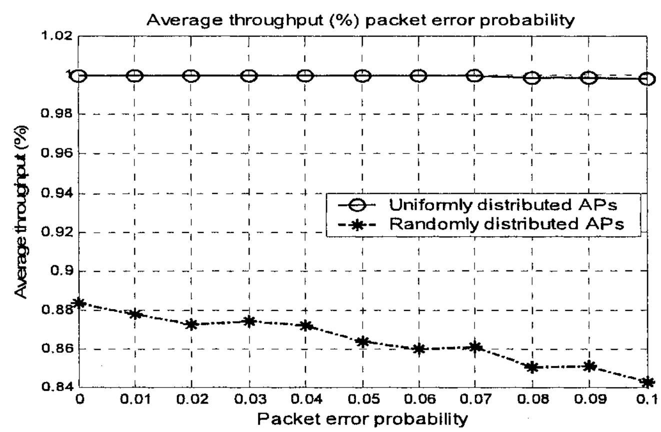


Figure 4.22: Average throughput (%) vs. packet error probability in uniform and random AP.

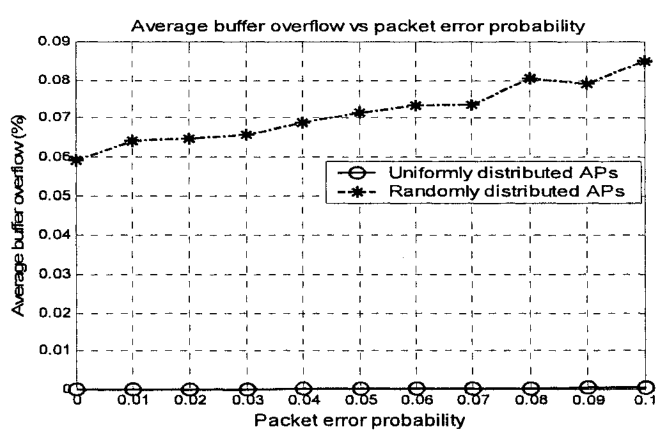


Figure 4.23: Average buffer overflow (%) vs. packet error probability in uniform and random AP.

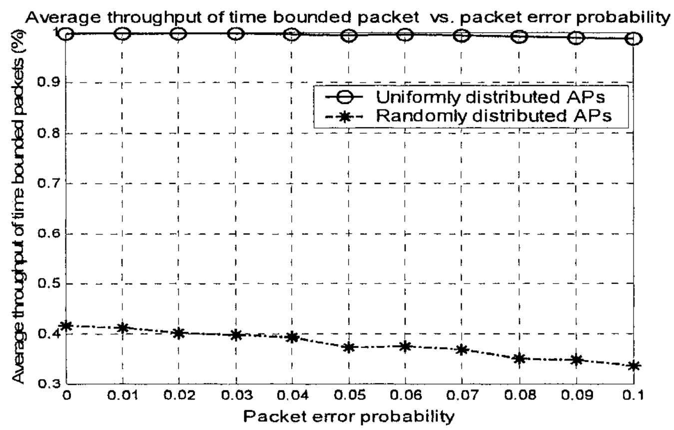


Figure 4.24: Average throughput of time bounded packet(%) vs. packet error probability in uniform and random AP.

44 dependent nodes. On the other hand gratuitous ESS has 17 APs and the standard ESS contains 25 APs. However, the real difference is that the gratuitous node provides services to almost half of the total number of nodes which are staying outside of an AP. This service is never achieved in standard ESS. From these figures, we can find an interesting difference between the two schemes. Random AP distribution network (gratuitous ESS) is more sensitive to transmission error than that of the standard ESS. This takes place because gratuitous ESS is involved more hops than that of standard ESS.

4.3. Performance Evaluation under Varying AP Population

Number of APs for a fixed number of nodes is varied while other input parameters remain constant. Table 4.3 shows the input parameters used for this simulation:

Table 4.3: Input parameter used in AP population simulation.

Parameters	Value
Test area	2000m X 2000m
WLAN length (uniform AP)	200m ~ 2000m
WLAN width(Uniform AP)	200m ~ 2000m
Number of total nodes	100
Number of AP	1 ~ 100
Load probability	0.05 ~ 0.50
Call generation probability	1
Buffer size	4 packet size
Maximum back off window size	256
Maximum number of re-transmissions	2
Time out for real time data packets	20 iterations
Number of iterations	5000

Figure 4.25 through 4.29 shows how the AP density affects the performance of a typical ESS. In this simulation, the total number of nodes is fixed while the number of AP is varied. Figure 4.25 and 4.27 shows that with the increase of number of AP, average packet delay and buffer overflow decreases. Figure 4.26 and 4.28 shows that with the increase in the number of AP, the throughputs for both the real time and non-real time packets increases. When APs are very small in number, a

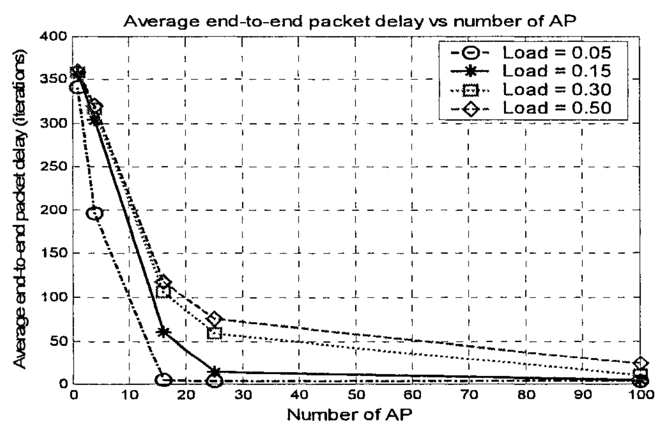


Figure 4.25: Average end-to-end packet delay (iterations) vs. number of APs in uniform AP.

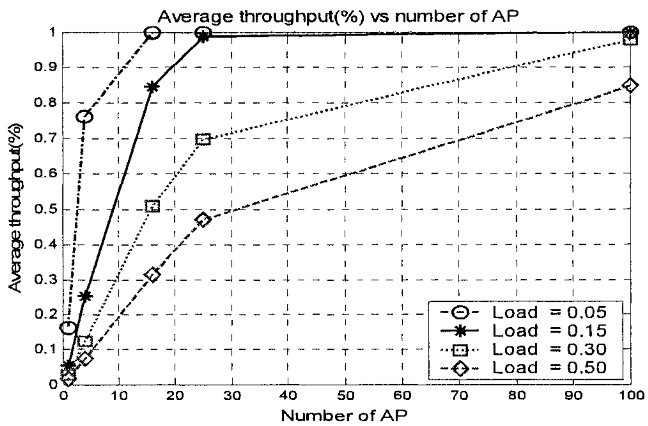


Figure 4.26: Average throughput (%) vs. number of AP in uniform AP.

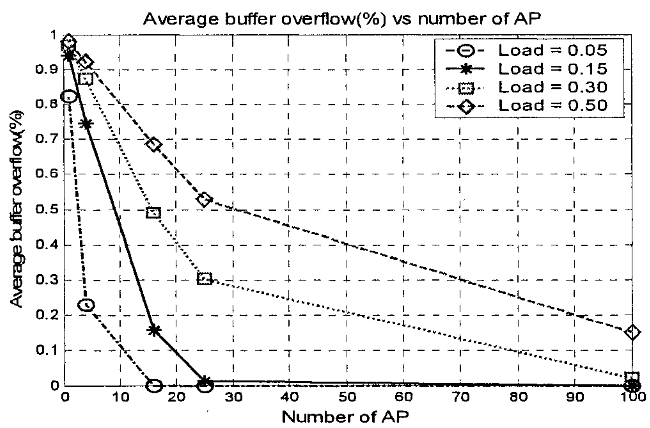


Figure 4.27: Average buffer overflow (%) vs. number of AP in uniform AP.

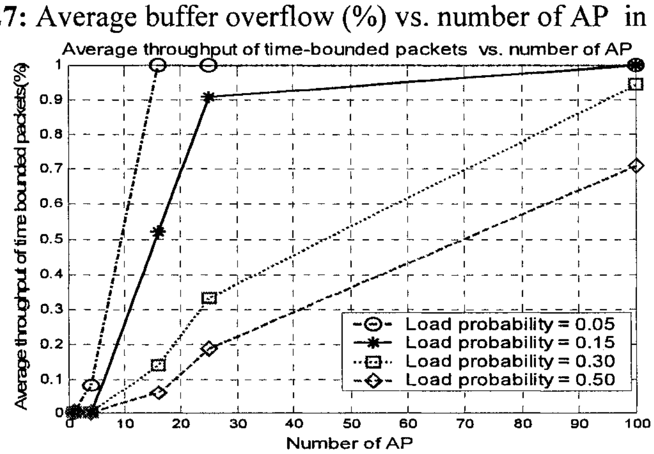


Figure 4.28: Average throughput of time-bounded packets (%) vs. number of AP in uniform AP.

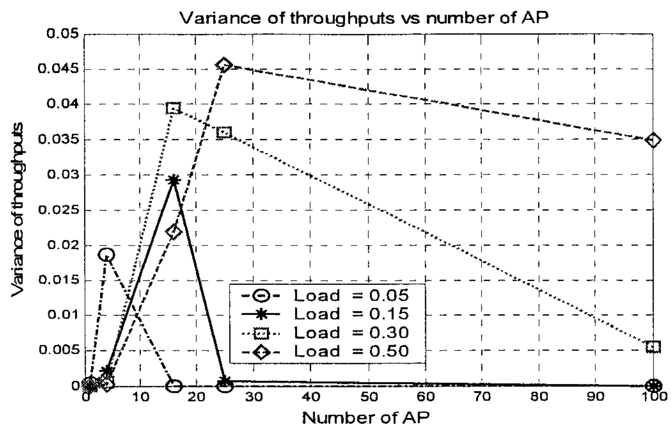


Figure 4.29: Variance of throughput vs. number of AP in uniform AP.

large number of nodes contend for the channel in each BSS, as a result throughput decreases, end-to-end packet delay increases, and buffer overflow increases.

4.4. Performance Evaluation under Varying Maximum Backoff Window

In this simulation, we vary the maximum backoff window size at different load probabilities for both uniform and randomly distributed APs. The parameters we have used are described in Table 4.4.

Figure 4.30 and 4.31 shows the output performances corresponding to uniform AP distribution with varying Maximum Backoff Window (MBW). Figure 4.30 shows the end-to-end packet delay performance with the varying Maximum Backoff Window (MBW) in uniform AP distribution. It is clear that delay is not sensitive to the MBW under higher AP population. However, under lower AP population, end-to-end packet delay slightly decreases with the increasing MBW. Figure 4.31 shows that the throughput does not change at all with the increasing MBW. Though, the increase in

Table 4.4: Input parameter used in maximum back off window size simulation.

Parameters	Value
Test area	2000m X 2000m
WLAN radius (random AP)	200m
WLAN length (uniform AP)	400m
WLAN width(Uniform AP)	400m
Number of total nodes	100
Number of uniformly distributed APs	4, 16, 25
Number of randomly distributed APs	17
Load probability	0.3
Call generation probability	1
Buffer size	4 packet size
Back off window size increase limit	0 ~ 6
Maximum number of re-transmissions	2
Time out for real time data packets	20 packet times
Number of iterations	5000

AP population shows a great improvement on delay and throughput, we can see that the delay is mainly affected by lower AP population. At higher AP density, each transmitting node faces less contention, and most of the packets can be transmitted without any collision. So any change in MBW does not affect the network. However, at lower AP density, each node faces more contention before any transmission. More

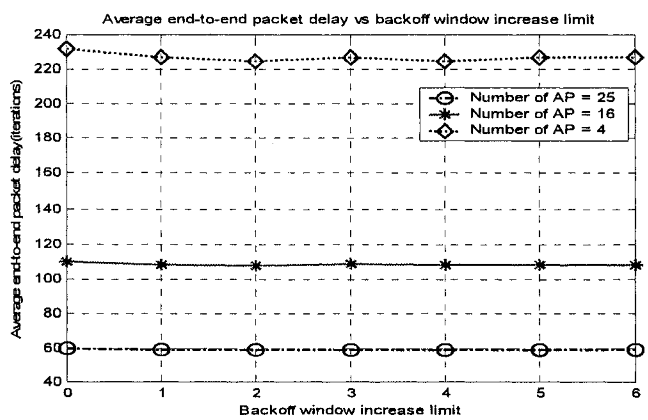


Figure 4.30: Average end-to-end delay (iterations) vs. backoff window increase limit in uniform AP.

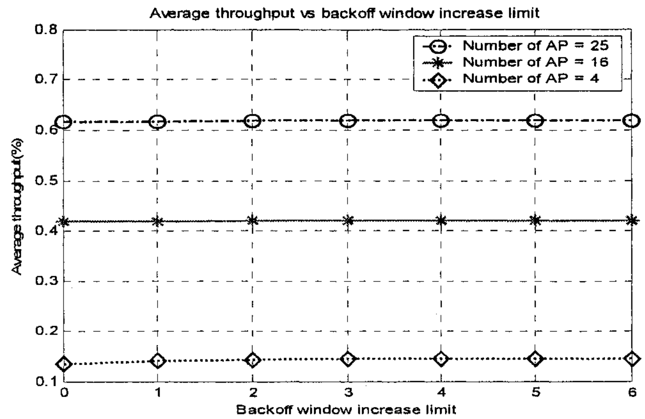


Figure 4.31: Average throughput (%) vs. backoff window increase limit in uniform AP.

contentions mean more collisions, and hence more losses in transmission time. More transmission losses result in more retransmissions which make longer queuing delay. One interesting thing is to note that the throughput is not affected; ultimately packets get their way to the destination.

Figure 4.32 through 4.41 shows the performance criteria of randomly distributed APs while varying MBW under different loads. Figures 4.32 through 4.36 show the end-to-end packet delay, throughput and buffer overflow, gratuitous packet

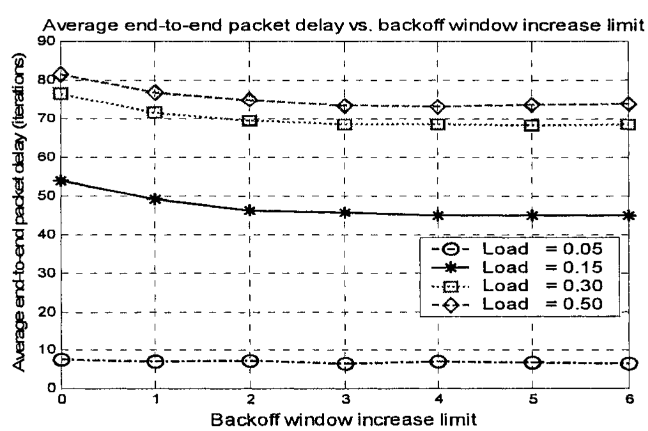


Figure 4.32: Average end-to-end packet delay (iterations) vs. backoff window increase limit in random AP.

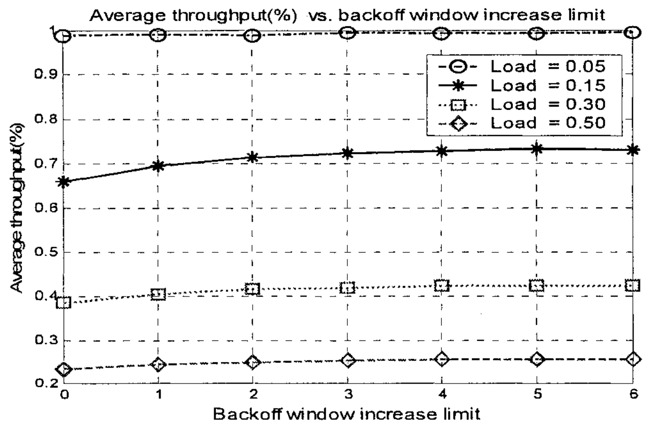


Figure 4.33: Average throughput (%) vs. backoff window increase limit in random AP.

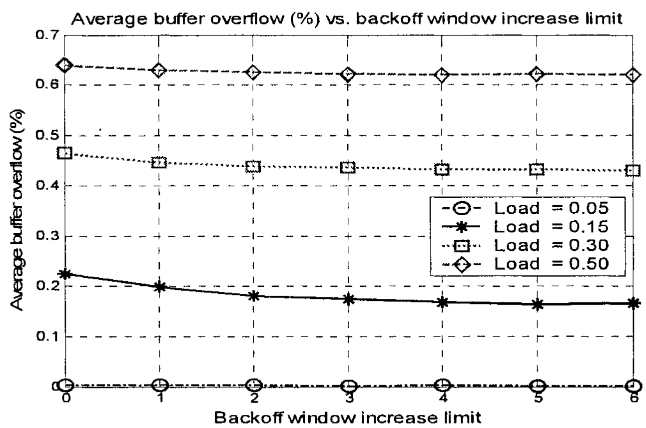


Figure 4.34: Average buffer overflow (%) vs. backoff window increase limit in random AP.

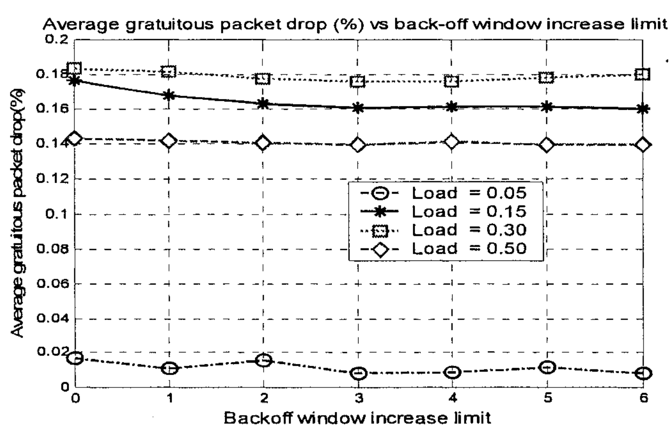


Figure 4.35: Average gratuitous packet drop (%) vs. backoff window increase limit in random AP.

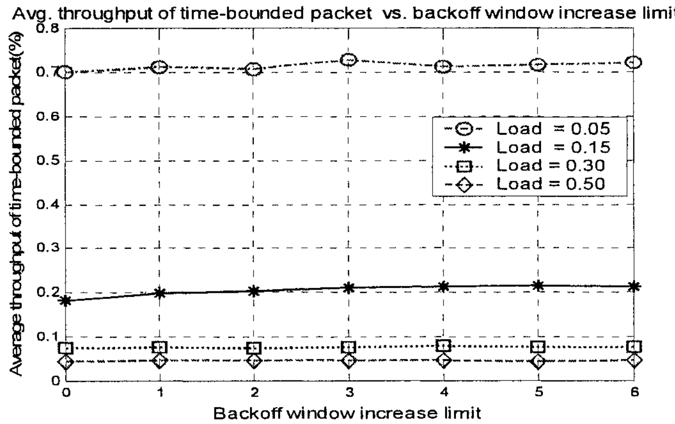


Figure 4.36: Average throughput of time-bounded packet (%) vs. backoff window increase limit in random AP.

drop and throughput for time-bounded packets, all these performance criteria shows continuous improvement with the increasing MBW, except for extremely light load conditions. It is interesting to note that in contrast with the uniform AP distribution, all the parameters of random AP distributions are sensitive to MBW. Like uniform AP distribution, most of the generated packets in random AP distribution, go through the backoff mechanism which takes place inside the BSS. However, in random AP distribution, the number of nodes inside a BSS is smaller than that of uniform AP distribution. This happens as the total number of nodes is divided between dependent and regular nodes. In random AP distribution, fewer nodes contend for the channel.

Figures 4.37 through 4.41 show the variance of the end-to-end packet delay, throughput, buffer overflow, gratuitous packet drop and the throughput of time-bounded packets. Variance performances under higher load conditions are more sensitive to the change in MBW than that of light load conditions.

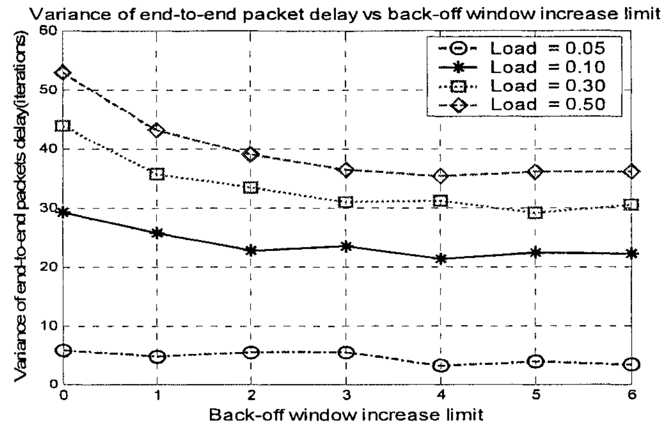


Figure 4.37: Variance of end-to-end packet delay vs. backoff window increase limit in random AP.

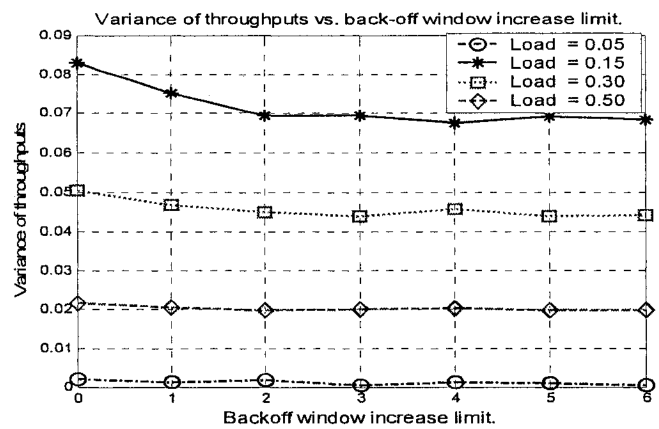


Figure 4.38: Variance of throughput vs. backoff window increase limit in random AP.

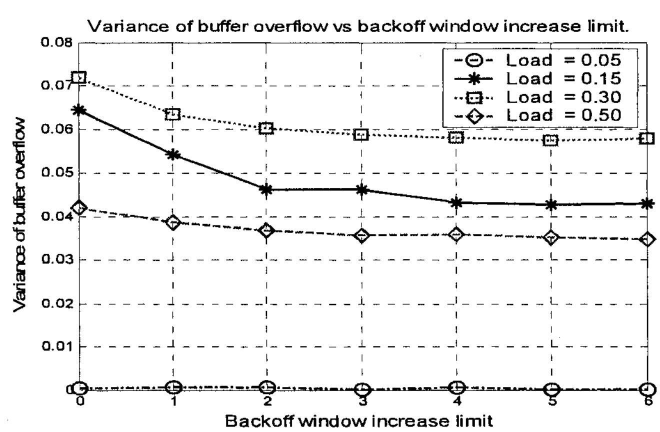


Figure 4.39: Variance of buffer overflow vs. backoff window increase limit in random AP.

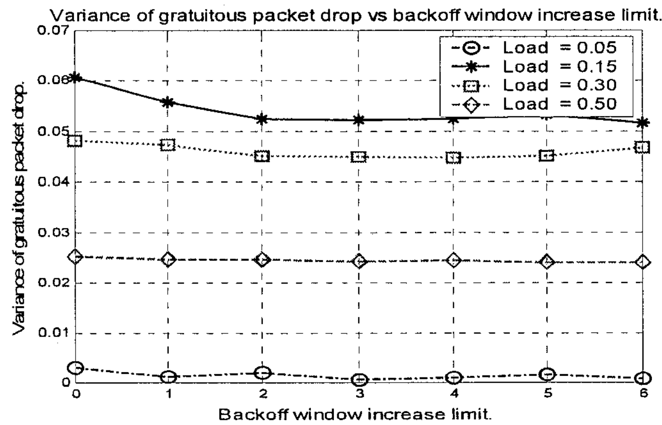


Figure 4.40: Variance of gratuitous packet drop vs. backoff window increase limit in random AP.

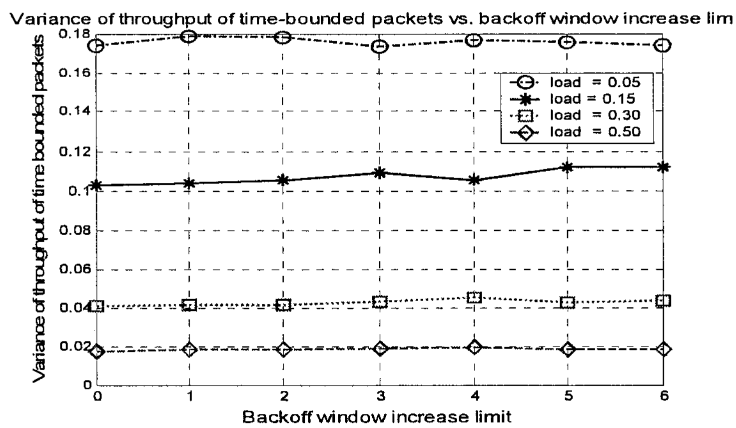


Figure 4.41: Variance of throughput of time-bounded packet vs. backoff window increase limit in random AP.

4.5. Performance Evaluation under Varying Timeout Values for Time-Bounded Packets

We have varied the timeout limit for uniform and random AP distribution to see the throughput. The parameter used are shown in Table 4.5.

Table 4.5: Input parameters used for time out simulation.

Parameters	Value
Test area	2000m X 2000m
WLAN radius (random AP)	200m
WLAN length (uniform AP)	400m
WLAN width(Uniform AP)	400m
Number of total nodes	100
Time out for real time data packets	5 ~ 50 iterations
Load probability	0.05
Call generation probability	1
Buffer size	4 data packet
Maximum number of re-transmissions	2
Simulation iterations	5000

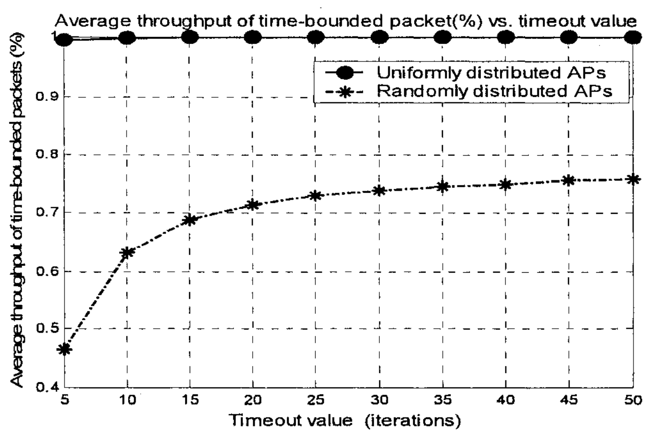


Figure 4.42: Average throughput of time-bounded packets(%) vs. timeout value in uniform and random AP.

Figure 4.42 compares the average throughput of time-bounded packets in uniform and random AP distribution under varying timeout value. While the throughput of time-bounded packets in uniform AP does not react to the changing timeout value, we observe an increase in throughput for random AP distribution. After a certain timeout value, the throughput of time-bounded packet gets saturated. Figure 4.43 compares the variances of throughputs of time-bounded packets in uniform and random AP distribution. In uniform AP distribution, under low load conditions, all the packets reaches destination within timeout value. However, in random AP distribution, each packet faces more hops before reaching the final destination. So, timeout value for real-time packets in random AP distribution becomes a more crucial issue than that of uniform AP distribution.

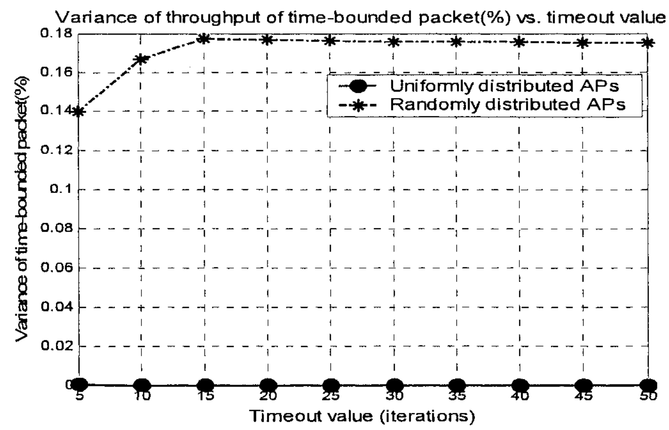


Figure 4.43: Variance of throughput of time-bounded packet(%) vs. timeout value in uniform and random AP.

4.6. Performance Evaluation under Varying Call Generation Probability

In this simulation, we vary the call generation probability of uniform AP distribution network along with packet generation probability. The parameters used for this simulation are shown in Table 4.6.

Table 4.6: Input parameter used for call generation probability simulation.

	Value
Test area	2000m X 2000m
WLAN radius (random AP)	200m
WLAN length (uniform AP)	400m
WLAN width(Uniform AP)	400m
Number of total nodes	100
Call generation probability	0.1 ~ 1
Load probability	0.05 ~ 0.50
Packet error probability	0.001
Buffer size	4 data packets
Maximum back off window size	256
Maximum number of re-transmissions	2
Timeout for real time data packets	20 iterations
Simulation iterations	5000

Figures 4.44 through 4.49 show the performance criteria correspond to varying call generation probability simulation. In Figure 4.44 the average end-to-end packet delay increases with the increase in probability of call generation. End-to-end packet delay performance becomes worse with the higher load. Figure 4.45 shows a lower throughput performance with the increasing probability of call generation. Again, lower load probability yields better throughput performance. Figure 4.47 shows a similar performance of time-bounded packet. In Figure 4.46, we can easily see that, higher call generation leads to higher buffer overflow. The reason is clear, with the increase in call generation probability, more nodes generate calls and become ready for packet transmission. More packets mean more collisions, larger backoff windows and longer queuing delays. With the other parameters constant, only an increase in probability of call generation results in greater end-to-end packet delay, lower probability of call generation results in greater end-to-end packet delay, lower throughput and greater throughput and greater buffer overflow. Time-bounded packets are also not an exception.

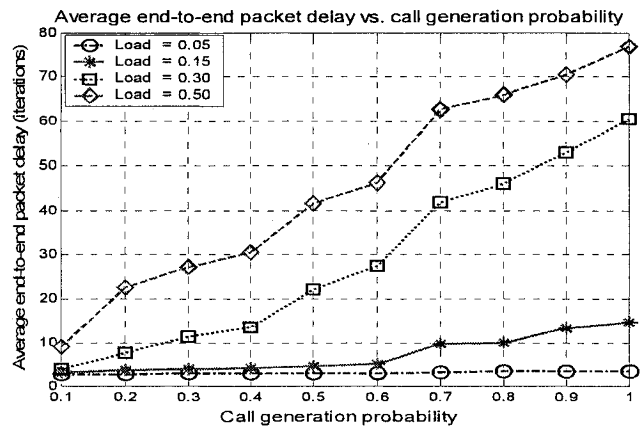


Figure 4.44: Average end-to-end packet delay(iterations) vs. call generation probability in uniform AP.

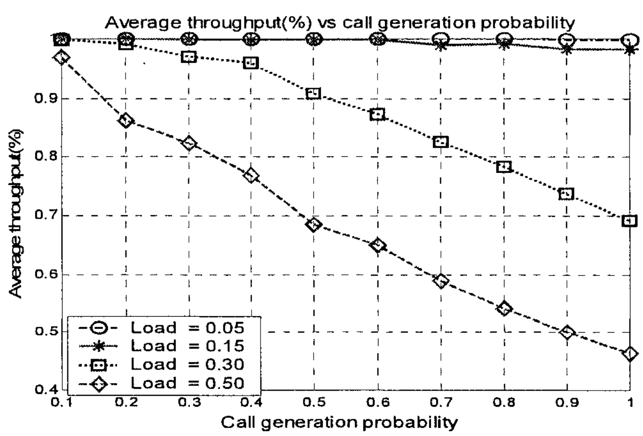


Figure 4.45: Average throughput(%) vs. call generation probability in uniform AP.

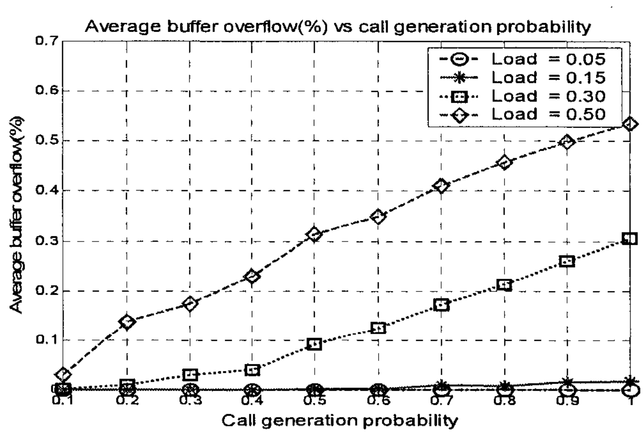


Figure 4.46: Average buffer overflow(%) vs. call generation probability in uniform AP.

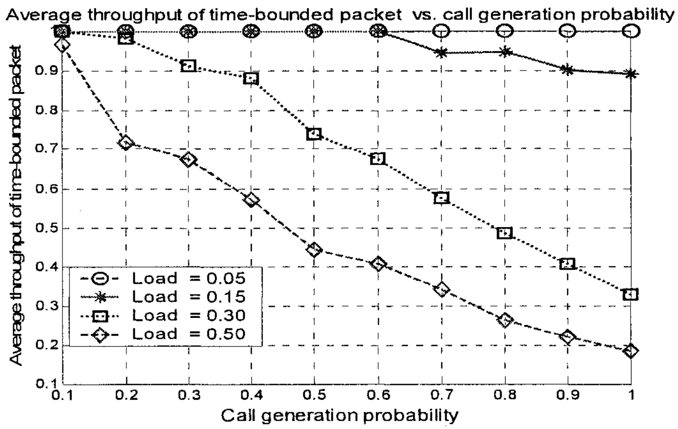


Figure 4.47: Average throughput of time-bounded packet(%) vs. call generation probability in uniform AP.

Figure 4.48 and Figure 4.49 show the variance of throughput of synchronous and asynchronous packets respectively. We can see from Figure 4.48 that with the increase of probability of call generation, the variance of throughput increases. Variance also becomes higher with higher load conditions. It seems that higher number of active nodes cause higher traffic volume in the network. These large number of packets cause larger queuing delays in the buffers. Different packets face different backoff window and hence large end-to-end packet delay variance. Also packets from different nodes have to travel different hops to reach the destinations. Figure 4.49 shows an important distinction from Figure 4.48. Under very low load conditions, when the call generation probability is varied, the variances of the throughput of time-bounded packets remain the same. However, with the increasing load, the variance of throughput of time-bounded packets tends to reach a saturation point. During heavy load, the network rapidly reaches the saturation point and then turns around. It is particularly noticeable at packet generation probability 0.50. At this value of load, the system's variance of throughput goes to the peak very rapidly and then turns back. The reason is higher call generation probability causes higher end-to-end packet delay. During heavy load conditions, almost all of the successful time-bounded packets spent the whole timeout period to reach the destination. This results in very low throughput and corresponding variance.

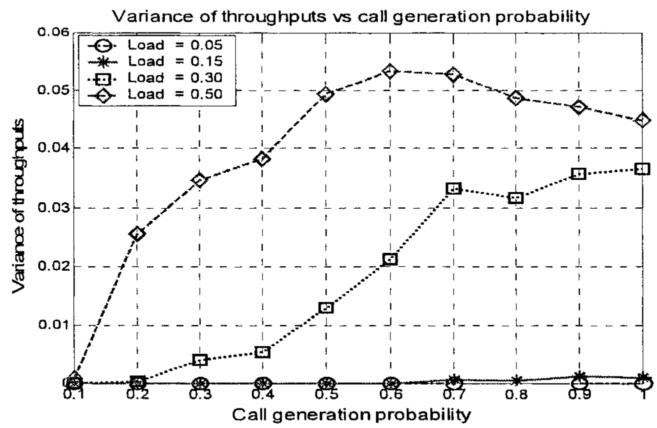


Figure 4.48: Variance of throughput vs. call generation probability in uniform AP.

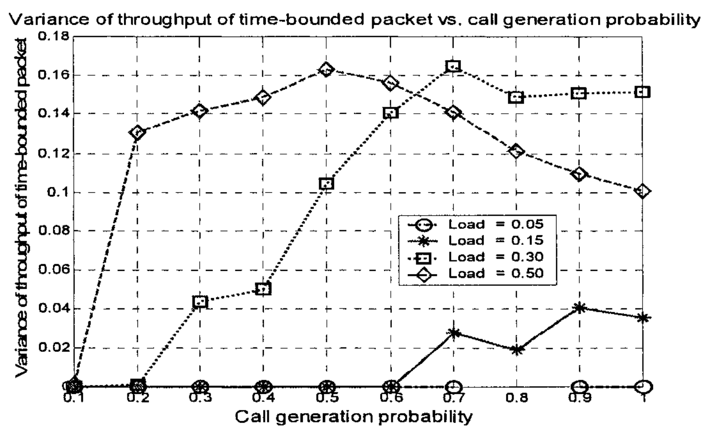


Figure 4.49: Variance of throughput of time-bounded packet vs. call generation probability in uniform AP.

Chapter 5

Conclusions and Future Works

5.1. Conclusions and Contributions

In this thesis, we intended to design a large-scale wireless LAN so that continuous network support can be provided to every mobile node in a specific geographical area. To achieve this goal, we have designed two multi-cluster network models.

We have designed a uniformly distributed AP network, namely regular ESS with uniform coverage to all the nodes under a specific area. An ESS is composed of multiple infrastructure wireless LANs namely BSSs. However, in reality, fixed ESS architecture may not provide continuous coverage to all roaming stations at all times.

We have proposed a randomly distributed AP network, namely gratuitous ESS. Each BSS in a randomly distributed AP networks provides a bridge between an infrastructure and an ad hoc wireless LAN. In this scheme, while a BSS keeps a gateway connection to the wired network, it supports out of range roaming nodes via a gratuitous node. Thus a gratuitous ESS can provide better flexibility for roaming stations.

An appropriate MAC layer implementation mechanism must be devised which will not only support a gratuitous mode in a BSS, but also work efficiently when gratuitous mode is absent. We have proposed a mixed contention and contention free

MAC layer implementation. While we keep DCF as a basic access mechanism, we introduced a combined FIFO and RR polling scheme during contention free period. Our proposed MAC layer implementation can efficiently work in both gratuitous and regular ESS.

Other relevant models have also been devised such as formation of gratuitous and regular BSS, formation of a regular and a gratuitous ESS, and the design of a routing mechanism for gratuitous ESS.

We have run the simulation programs to see the performance results of both regular and gratuitous ESS under MAC layer scheduling scheme. We have varied several input parameters such as load, call generation, AP population, maximum backoff window, buffer size, retransmission limit, timeout value to get the performance criteria of these two models. We have observed the average value and the variance of several performance measures such as end to end packet delay, buffer overflow, gratuitous packet drop, throughput of asynchronous and time bounded packets.

The performances of multi-cluster wireless LANs show very high consistency and not exceptions from what is expected. Generally, the network performs better under light load condition. However, with the increasing load the performances degrade and reach near a saturation point and become less responsive to changing load. Similar comment is applicable to increasing call generation probability, channel error and maximum backoff window size. On the other hand, the network works better under low AP populations, however increasing AP population dramatically improves the performances of the network. We have also tested our model for time-bounded packets. Time-bounded packets operate well under light load condition. However, time-bounded service during contention period can be ensured by fine tuning the existing DCF protocol [4], [32]-[34].

In general, the uniformly distributed AP network shows slightly better performances than that of randomly distributed AP network. It happens because, our designed MAC layer implementation is not only suitable for gratuitous operation but also efficient in regular multi-cluster operation. There is no RR scheme in regular ESS and hence there is no additional polling time, which is a necessity in random AP distribution. In fact, packets from the backbone networks do not have to go through backoff mechanism, which saves some time. Hence, our mixed contention and contention free MAC layer implementation is better than pure DCF in multi-cluster networks. Furthermore, the random AP distribution provides gratuitous service which is never present in regular ESS. By providing gratuitous service, a node can have greater flexibility in terms of mobility; moreover, extra cost and hassle of installation of additional APs can be avoided.

5.1.1. Major Contributions

The major contributions of this thesis are as follows:

- Design of a infrastructure multi-clustered wireless LAN with gratuitous capability.
- Setting up rules for gratuitous communication.
- Scheduling of MAC layer for multi-cluster communication via access points.
- Performance study of infrastructure multi-clustered wireless LAN.

- Performance study of infrastructure multi-cluster wireless LAN with gratuitous capability.

5.1.2. Comparison with Other Works

Very few similar articles have been found which studied multi-cluster wireless LAN performance in detailed. We have searched for similar articles to make a good comparison. However, in most cases, the simulation environments and the output parameters are different. Nevertheless, some articles are found which are somewhat similar to our works. The thesis titled "Performance Simulation of Priority Based CSMA/CA and Pseudo-Access Point Routing Protocol"[38], describes the performance of multi-hop communication using a priority based CSMA/CA protocol and a special routing protocol. In this thesis, pseudo access point is also considered. One article [39], describes a way of handling MAC layer to improve the performance of infrastructure wireless LANs. This article shows the throughput and the mean delay performances with the increasing load in the network. Another article [40] describes the performance of cellular multi-hop ad hoc network. Another article [41] describes a model to enhance the performances cellular networks of 3G and beyond. The study of these articles together with our thesis will help in better understanding of our position relative to other works.

5.2. Suggestions for Future Works

We suggest the following points for future research works:

1. For the simplification of our model, we only consider packet error probability. However, the detail study can be done in the future on the factors underlying this channel error, such as fading, interference, noise etc.

2. We have simplified the AP to AP communication with zero transmission and propagation delay. But in reality, actual effect of the wired network can not be ignored. A complete networking model including the detailed wired network should be studied in future time.

3. The MAC layer implementation can also be modified to investigate pure DCF and pure PCF communication among various clusters. It will be also interesting to study the performance of different service classes in our proposed network models.

4. Though we studied the performance of time-bounded packets, our research is mainly aimed at transmission of asynchronous packets under MAC layer. We suggest a future work that concentrates on time-bounded services.

5. It is imperative to study our network model together with other cellular networks, because a ubiquitous network will be a reality and will be composed of both WLAN and cellular networks [35]-[37].

References

[1] Angela Doufexi, Eustace Tameh, Andrew Nix, and Simon Armour "Hotspot Wireless LANs to Enhance the Performance of 3G and Beyond Cellular Networks," *IEEE Communications Magazine*, July 2003.

[2] Amre El-Hoiydi, "Implementation Options for the Distribution System in the 802.11 Wireless LAN Infrastructure Network," *in Proceedings of IEEE International Conference on Communications, 18-22 June 2000, (ICC 2000)*, vol.1, pp.164 – 169.

[3] Anders Lindgren, Olov Schelén, "Infrastructured ad hoc networks", *in Proceedings of International Conference on parallel processing workshop,* pp.64-70, August 2002.

[4] Farshad Eshghi, Ahmed K. Elhakeem, "Performance Analysis of Ad Hoc Wireless LANs for Real-Time Traffic" *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 2, February 2003.

[5] Oran Sharon and Eitan Altman, "An Efficient Polling MAC for Wireless LANs," *IEEE/ACM Transactions on Networking*, vol. 9, no.4, August 2001.

[6] Toh, C.-K.; Delwar, M.; Allen, D., "Evaluating the communication performance of an ad hoc wireless network," *IEEE Transactions on Wireless Communications*, vol. 1, issue: 3 , pp. 402 – 414, July 2002.

[7] Kin K. Leung, Bruce McNair, Leonard J. Cimini, Jr., and Jack H. Winters, "Outdoor IEEE 802.11 Cellular Networks: MAC Protocol Design and Performance," *IEEE International Conference on Communications, 2002, (ICC 2002)*, vol.1, pp.512-516, 28 April-2 May 2002.

[8] Francesca Cuomo, Andrea Baiocchi, and Roberto Cautelier, "A MAC Protocol for a Wireless LAN Based on OFDM-CDMA," *IEEE Communications Magazine,* September 2000, pp.152-159.

[9] 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."

[10] HiperLAN/2 Global Forum (web page). URL:http://www.hiperlan2.com/web/

[11] Negus, K.J.; Stephens, A.P.; Lansford, J., "HomeRF: Wireless Networking for the Connected Home," *IEEE Personal Communications*, vol. 7 , issue: 1 , February 2000, pp. 20 – 27.

[12] Anders Lindgren, Andreas Almquist, Olov Schelen, "Evaluation of Quality of Service Schemes for IEEE 802.11 Wireless LANs," *in Proceedings of the 26th Annual IEEE Conference on Local Computer Networks 2001 (LCN 2001),* pp. 348-351.

[13] Tom M. Thomas, "Network Security First-Step" Cisco Press, 2004.

[14] C.-K. Toh and Donald Allen, "Evaluating the Communication Performance of an Ad Hoc Wireless Network", *IEEE Transactions on Wireless Communications,* vol. 1, no. 3, July 2002.

[15] Hung-Yun Hsieh and Raghupathy Sivakumar, "IEEE 802.11 over Multi-hop Wireless Networks: Problems and New Perspectives," *in Proceedings of IEEE Vehicular Technology Conference,* 24-28 September, 2002.

[16] Jim Geier, "Wireless LANs:Implementing Interoperable Networks," Macmillan Technical Publishing, 1999.

[17] Pickholtz, R.L., Schilling, D.L., and Milstein, L.B., "Theory of Spread-Spectrum Communications – A Tutorial," *IEEE Trans. Commun.*, vol. COM30, no. 5, May 1982, pp.855-884.

[18] A.K. Elhakeem, H.M. Hafez and S.A. Mahmoud, "Spread Spectrum Access to mixed voice data local area network," *IEEE Journal on Selected Areas in Communications*, vol. SAC -1, pp.1054-1069, Dec. 1983.

[19] Alberto Leon-Garcia, Indra Widjaja, "Communication Networks Fundamental Concepts and Key Architectures," McGraw-Hill, 2000.

[20] Brian P. Crow, Indra Widjaja, Jeong Geun Kim, Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks", *IEEE Communications Magazine*, September 1997.

[21] B.P. Crow, I. Widjaja, J.G. Kim, and P. Sakai, "Investigation of the IEEE 802.11 Medium Access Control (MAC) Sublayer Functions", *Proceedings of the Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '97),* vol. 1, 7-11 April 1997, pages:126 – 133.

[22] Neeli Prasad, Anand Prasad, "WLAN Systems and Wireless IP for Next Generation Communications," Artech House 2002.

[23] Chuan Heng Foh, Moshe Zukerman, "CSMA with Reservations by Interruptions (CSMA/RI): A Novel Approach to Reduce Collision in CSMA/CD," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 9, September 2000.

[24] K.C. Chen, "Medium access control of wireless LANs for mobile computing," *IEEE Network*, vol. 8, pp. 50-63, Oct. 1994.

[25] B.Bing, "Measured performance of the IEEE 802.11 wireless LAN," *in Proceedings of LCN'99*, October 1999, pp. 34-42.

[26] S.Khurana, A. Kahol, and A.P. Jayasumana, "Effect of Hidden Terminals on the Performance of IEEE 802.11 MAC protocol," *in Proceedings of LCN'98*, October 1998, pp. 12-20.

[27] Giuseppe Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, March 2000.

[28] L. IKleinrock and F. Tobagi, "Packet Switching in Radio Channels, Part II-The hidden terminal problem in carrier sense multiple access and the busy tone solution," IEEE Transactions on Communications, vol. COM-23, no. 12, pp. 1417-1433, December 1975.

[29] Jing-Yuan Yeh and Chienhua Chen, "Support of Multimedia Services with the IEEE 802.11 MAC Protocol," *IEEE International Conference on Communications, 2002 (ICC 2002)*, vol.1 , 28 April-2 May 2002, Pages:600 – 604.

[30] Mersenne Twister Home Page, URL: http://www.math.sci.hiroshima-u.ac.jp/%7Em-mat/MT/emt.html.

[31] Bernard Sklar, "Digital Communications Fundamentals and Applications," 2nd edition, Prentice Hall, New Jersey, 2001.

[32] Joao L. Sobrinho and A.S. Krishnakumar, "Real-Time Traffic over the IEEE 802.11 Medium Access Control Layer," *Bell Labs Technical Journal*, Autumn 1996.

[33] Qui Qiang, Lillykutty Jacob, R. Radhakrisna Pillai, and B. Prabhakaran, "MAC protocol enhancements for QoS guarantee and fairness over the IEEE 802.11 wireless LANs," *in Proceedings of the Eleventh International Conference on Computer Communications and Networks, 2002,* 14-16 Oct. 2002, pp.628 – 633.

[34] M. Benveniste, G. Chesson, M. Hoeben, A. Singla, H. Teunissen, and M. Wentink. EDCF proposed draft text. IEEE working document 802.11-01/131r1, March 2001.

[35] Helal, S.; Choonhwa Lee; Yongguang Zhang; Richard, G.G., III, "An Architecture for Wireless LAN/WAN Integration," *IEEE Wireless Communications and Networking Conference, 2000, (WCNC 2000)* ,Volume: 3 , 23-28 Sept. 2000, pp.1035 – 1041.

[36] Salkintzis, A.K.; Fors, C.; Pazhyannur, R., "WLAN-GPRS Integration for Next-Generation Mobile Data Networks," *IEEE Wireless Communications*, Volume: 9, Issue: 5, Oct. 2002, pp.112 – 124.

[37] Ahmavaara, K.; Haverinen, H.; Pichna, R., "Interworking Architecture between 3GPP and WLAN Systems," *IEEE Communications Magazine*, Volume: 41 , Issue: 11, Nov. 2003, pp.74 – 81.

[38] Moyu Yang, "Performance Simulation of Priority Based CSMA/CA and Pseudo-Access Point Routing Protocol" *an M.A.Sc. thesis in the Department of Electrical and Computer Engineering, Concordia University, 2004.*

[39] Dong, X.J.; Ergen, M.; Varaiya, P.; Puri, A.; "Improving the Aggregate Throughput of Access Points in IEEE 802.11 Wireless LANs," *In Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks, 2003 (LCN '03),* 20-24 October 2003, pp.682 – 690.

[40] Bangnan Xu, Sven Hischke, Bernhard Walke, "The Role of Ad Hoc Networking in Future Wireless Communications," *in Proceedings of International Conference on Communication Technology Proceedings, 2003 (ICCT 2003)*, vol. 2, April 2003, pp. 1353 – 1358.

[41] Doufexi, A.; Tameh, E.; Nix, A.; Armour, S.; Molina, A., "Hotspot Wireless LANs to Enhance The Performance of 3G and Beyond Cellular Networks" *IEEE Communications Magazine,* vol. 41, issue: 7, July 2003, pp. 58- 65.