Hybrid GSM/WLAN Loose/Tight Coupled System

Weiwen Qin

A Thesis

In

The Department

Of

Electrical and Computer Engineering

Presented in Partail Fulfillment of the Requirements

for the Degree of Master of Applied Science at

Concordia University

Montreal, Quebec

July 2004

Your file Votre référence
ISBN: 0-612-94796-3
Our file Notre référence
ISBN: 0-612-94796-3

ABSTRACT

General Packet Radio Service (GPRS) is marked as the 2.5G generation of wireless servcice and it can provide data communication with low data rate and wide area coverage. Wireless Lan (WLAN) is recently spreadly used another wireless technology with very high datarate and small area coverage; normally just exist in "HOTSPOT". In this thesis we investigate the co-existence of Wireless LAN (802.11) and GPRS system. Based on the network coupling structure between the two access technologies, i.e. wireless LAN and GSM, the concept of joint radio network built on the reference structure is briefly introduced. Mobile IP is used to achieve the seamless roaming between the coupled networks.

This research uses C++ based simulation to design and to test the performance of the coupling networks. Two main network scenarios are considered, such as increasing the AP existence probability with fixed tight and loose coupling ratio and increasing tight/loose coupling ratio with fixed AP existence probability. By combining these two main network scenarios with different traffic load, we can get different performance results. The results show that the wireless LAN can be very effective in complementing GSM cellular system.

Acknowledgements

I would like to acknowledge helps from others, especially from Dr. A.E.Elhakeem whose teaching, coaching, mentoring really helped me to set the target and narrow down the problem. And also I would like to thank to my wife Xinyue for all the sides supports.

Table of Contents

Chapter 1 Introduction 1
1.1 Backgrounds and Motivation 2
1.2 Methodology Overview 3
1.3 Significant Results 4
Chapter 2 Wireless LAN Network 6
2.1 WLAN System 7
2.2 WLAN Protocol 9
2.3 Inter-frame Space 12
2.4 Distributed Coordination Function 13
2.5 Point Coordination Function 15
2.6 WLAN Frame Structure 17
Chapter 3 GSM/GPRS network 18
3.1 GSM Network 19
3.1.1 GSM System Architecture 19
3.1.2 GSM Addresses/Identifiers 22
3.1.3 GSM Radio Link 23
3.2 GPRS Network 23
3.2.1 GPRS System Architecture 23
3.2.2 GPRS Protocol Architecture 27
3.2.3 Services 32
3.2.4 Session Management, Mobility Management, and Routing 35
3.2.5 Air Interface -- Physical Layer 40
Chapter 4 Mobile IP and Interworking 45
4.1 Mobile IP 45
4.1.1 Protocol Overview 46
4.1.2 IP Mobility 51
4.2 WLAN-GPRS Inter-working 55
4.2.1 Interworking Scenarios 55
4.2.2 Inter-working Architectures 60
Chapter 5 Hybrid Tight/Loose Network Simulation 68
5.1 Simulation System Architecture 68
5.2 Simulation Description 71
5.2.1 Simulation Coverage 72
5.2.2 Network Simulation 74
5.2.3 Simulation of Users Info 76
5.2.4 Handoff and Traffic Pofile Consideration 80
5.3 Simulation Flow Chart and Initial Input Data 81
5.4 Simulation Results 90
5.5 Reseach summary and Future Work 117
References 118

List of Figures

Figure 2.1 Ad-hoc network 8
Figure 2.2 Infrastructure network 9
Figure 2.3 Protocol reference model for the 802.11 standard 10
Figure 2.4 Medium Access and Inter-frame Spacing 12
Figure 2.5 Medium Reference model 15
Figure 2.6 PCF Data transfer with 4 Stations 16
Figure 2.7 IEEE 802.11 Frame Structure 17
Figure 3.1 GSM System Architecture and components 19
Figure 3.2 GPRS System Architecture and components 24
Figure 3.3 Inter/Intra-PLMN connection topology 26
Figure 3.4 GPRS transmission plane protocol 27
Figure 3.5 PDP context Activation 37
Figure 3.6 GPRS Location management 38
Figure 4.1 Registration process in Mobile IP 49
Figure 4.2 Tunneling operation in Mobile IP 51
Figure 4.3 Protocol Reference Model for Mobile IP User Data 53
Figure 4.4 GPRS-WLAN simplied Reference Model 56
Figure 4.5 Loose Coupling Architecture 61
Figure 4.6 GPRS and Mobile IP in the Loose Coupling Network 62
Figure 4.7 PDP context activation with MIP registration 63
Figure 4.8 Dual protocol stacks in MS 65
Figure 4.9 WLAN-GPRS integration with tight coupling 66
Figure 4.10 Tight coupling system Gb interface reference diagram 67
Figure 5.1 Hybrid tight/loose coupling network 70
Figure 5.2 MS user data dual IP stack for the BTS and AP 70
Figure 5.3 Flowchart for the Main Program 82
Figure 5.4 Continuance for the main program 83
Figure 5.5 Packet reachability and loss perentage with Plt:0.5, Pbts:0.9
Pdatageneration:0.1 and light traffic load 93
Figure 5.6 Packet reachability and loss variance with Plt:0.5, Pbts:0.9,
Pdatageneration:0.1 and light traffic load 93
Figure 5.7 Packet reachability and loss perentage with Plt:0.5, Pbts:0.9
Pdatageneration:0.5 and medium traffic load 94
Figure 5.8 Packet reachability and loss variance with Plt:0.5, Pbts:0.9,
Pdatageneration:0.5 and medium traffic load 94
Figure 5.9 Packet reachability and loss perentage with Plt:0.5, Pbts:0.9
Pdatageneration:0.5 and heavy traffic load 95
Figure 5.10 Packet reachability and loss variance with Plt:0.5, Pbts:0.9,
Pdatageneration:0.5 and heavy traffic load 95
Figure 5.11 Packet reachability and loss perentage with Plt:0.9, Pbts:0.9
Pdatageneration:0.5 and medium traffic load 97
Figure 5.12 Packet reachability and loss variance with Plt:0.5, Pbts:0.9,
Pdatageneration:0.5 and medium traffic load 98

Figure 5.13 End-to-End Packet Latency Average for whole Simulation with Pap increasing 99
Figure 5.14 End-to-End Packet Latency Variance for the whole Simulation with Pap increasing 99
Figure 5.16 Number of End-to-End Packet received and throughput with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 light traffic 101
Figure 5.17 Number of End-to-End Packet received and throughput variances with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 light traffic 101
Figure 5.18 Number of End-to-End Packet received and throughput with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic 102
Figure 5.19 Number of End-to-End Packet received and throughput variances with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic 102
Figure 5.20 Number of End-to-End Packet received and throughput with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 heavy traffic 103
Figure 5. 21 Number of End-to-End Packet received and throughput variances with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 heavy traffic 103
Figure 5.22 Number of End-to-End Packet received and throughput with Plt:0.9, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic 104
Figure 5.24 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 300 users light traffic 106
Figure 5.25 Buffer variance with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 300 users light traffic 106
Figure 5.26 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users medium traffic 107
Figure 5.27 Buffer variance with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users medium traffic 107
Figure 5.28 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users heavy traffic 108
Figure 5.29 Buffer variance with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users heavy traffic 108
Figure 5.30 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users medium traffic 109
Figure 5.31 Buffer variance with Plt: 0.5, Pbts: 0.9, Pdatagenerate: 0.5, Pair: 0.2 300 users medium traffic 109
Figure 5.32 Packet reachability and loss with Pap:0.5, Pbts:1.0, Pdatageneration:0.1 and light traffic load 110
Figure 5.33 Packet reachability and loss variance with Pap:0.5, Pbts:1.0, Pdatageneration:0.1 and light traffic load 111
Figure 5.34 Packet reachability and loss with Pap:0.5, Pbts:1.0, Pdatageneration:0.1 and medium traffic load 111
Figure 5.35 Packet reachability and loss variance with Pap:0.8, Pbts:1.0, Pdatageneration:0.1 and medium traffic load 112
Figure 5.36 Number of End-to-End Packet received and throughput with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.1, Pair:0.2 light traffic 113
Figure 5.37 Number of End-to-End Packet received and throughput variances with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.1, Pair:0.2 light traffic 113

Figure 5.38 Number of End-to-End Packet received and throughput with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.5, Pair:0.2 light traffic 114
Figure 5.39 Number of End-to-End Packet received and throughput variances with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.5, Pair:0.2 medium traffic 114
Figure 5.40 End-to-End Packet Latency Average for whole Simulation with Plt increasing 115
Figure 5.41 End-to-End Packet Latency variance for whole Simulation with Plt increasing 115

List of Tables

Table 3.1 GPRS CS-1 to CS-4 coding Character List 44
Table 4.1 Mobility binding table 47
Table 4.2 Characteristic of WLAN and GPRS 55
Table 4.3 3GPP Scenarios for interworking WLAN 59
Table 5.1 Initial Input Data Table 81

Abbreviations

2G	Second Generation (Cellular System)
3G	Third Generation (Cellular System)
3GPP	Third Generation Project Partner
AAA	Authentication, Authorization and Accounting
AAAH	Home AAA
AAAL	Local AAA
ACK	Acknowledgment
AP	Access Poin
AUC	Authentication
BCCH	Broadcast Control Channel
BSC	Base Station Controll
BSS	Basic Service Set
BSSAP+	Base Station System Application Part
BSSGP	Base Station System GPRS Protocol
BTS	Base transceiver station
CCA	Clear Channel Assessment
CCCH	Common Control Channel
CDPD	Cellular Digital Packet Data
CG	Charging Gateway
CFP	Contention-Free Period
CFU	Call Forwarding Unconditional
CFNRc	Call Forwarding on mobile subscriber Not Reachable
CI	Cell Identifier
CN	Correspondent Node
COA	Care-of address
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear-to-Send
CUG	Closed User Group
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DS	Distribution System
EDGE	Enhanced Data for Global Evolution
EIR	Equiment Identity Register
ESS	Extended Service Set
ETSI	European Telecommunication Standards Institute
FA	Foreign Agent
GGSN	Gateway GPRS Support Node
GIF	GPRS Interworking Function
GTP	GPRS Tunneling Protocol
GMSC	Gateway Mobile Switching Centre
GPRS	Global Packet Radio Services
GRE	Generic Routing Encapsulation

GSN	GPRS support nodes
HA	Home Agent
HLR	Home Location Register
IETF	Instiute of Electrical and Electronic Engineers
IFS	Inter-frame Spaces
IMEI	Iternational Mobile Station Equipment Identity
LA	Lcation Aea
MAC	Medium Access Control
MAP	Mobile Application Part
MIP	Mobile IP
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber Number
NAV	Network Allocation Vector
NS	Network Service
P-TMSI	Packet Temporary Mobile Subscriber Identity
PACCH	Packet Associated Control Channel
PAGCH	Packet Access Grant Channel
PBCCH	Packet Broadcast Control Channel
PCCCH	Packet Common Control Channel
PCF	Point Coordination Function
PDCH	Packet Data Channel
PDN	Packet Data Networks
PDP	Packet Data Protocol
PDSN	Packet Data Serving Node
PDTCH	Packet Data Traffic Channel
PNCH	Packet Notification Channel
PPCH	Packet-Paging Channel
PRACH	Packet Random Access Channel
PTCCH	Packet Timing Advance Control Channel
PTP	Point-to-Point
PTM	Point-to-Multipoint
PIFS	PCF Interframe Space
PLMN	Public Lan Mobile Netowork
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
QoS	Quality of Service
RA	Routing Areas
RAI	Routing Area Identity
RAN	Radio Area Network
RADIUS	Remote Authentication Dial In User Service
RLC	Radio Link Control
RRP	Mobile IP Registation Reply
RRQ	Mobile IP Registation Request
SCCP	Signaling Connection Control Part
SGSN	Serving GPRS Support Node

SIFS	Short Interframe Space
SIM	Subscriber Identity Module
SNDCP	Subnetwork Dependent Convergence Protocol
SMS	Short Message Services
TCAP	Transaction Capabilities Application Part
TMSI	Temporary Mobile Subscriber Identity
USF	Uplink State Flag
VLR	Vistor Location Register

Chapter 1 Introduction

Two technological advances in the recent years have radically altered the nature of the telecommunication industry. These advances are the exponential growth of the Internet and cell telephone networks. In its beginnings as the Arpanet of the 1970s, the Internet was primarily limited to academic and scientific institutions. In the same way, the usage of cell telephones was restricted by high costs and limited coverage.

Today, the widespread use of the Internet for communications, file transfer and World-Wide-Web connectivity is commonplace for most business and home users. Just as there has been an unstoppable growth in the Internet, the number of cell telephones has similarly advanced at an amazing pace.

As the subscribers grow very rapidly in both areas, the need for the mobile data communication will be great. From Short Message Services (SMS) [1], Cell Digital Packet Data (CDPD) [2] to Global Packet Radio Services (GPRS) [3] and Packet Data Service Node (PDSN) [4], the market attracts all kinds of technologies and tries to combine them in Cellular network. These attempts to integrate data services into cellular networks have brought the limitations of both the Internet and the cellular network into sharp focus. The Internet's best effort model is limited in its ability to support the real time constraints of a voice conversation. While, the cell telephone network's low data rate is not sufficient for web-browsing or large file transfers. Ongoing research is aimed at improving Quality of Service (QoS) for the Internet, and increasing data rates on cellular networks.

This research effort focuses on supporting data traffic in "hotspots," by interworking the Wireless Local Area Network (WLAN) technologies into the existing second Generation (2G) cellular networks, the GSM network.

1.1 Backgrounds and Motivation

The cell telephone industry was originally focused on providing voice communications to the outdoors, traveling user. Technological advances have increased the coverage and the quality of that service, but are still quite limited in their ability to provide quality coverage inside buildings. The ability to provide quality coverage in "hotspots" (indoor locations with high concentrations of potential customers, e.g., office building and airports) would increase the potential for mobile systems to compete directly with infrastructure-based communications systems.

The term "3GPP (Third Generation Partnership Project) specification" covers all GSM (including GPRS and EDGE [5]) and W-CDMA specifications. It is one of the primary standards bodies developing the standards for Third Generation (3G) mobile cellular systems. Much of their work focuses on addressing the convergence of voice and data communications.

WLAN technologies are complementary to the cellular data network. There are several advantages over the cellular networks, including higher speed and low operating and equipment costs. However their coverage is limited to the corporate building, residences and certain public hotspots. This capacity can be leveraged to both support a high concentration of users and allow the potentially limited cell capacity to be reserved for voice traffic. For these reasons, the 3GPP group SA1 (Services and System Aspects) has

published a feasibility study and began development of proposed standards supporting the interworking of 3GPP systems with WLAN systems [12]. The study identifies six scenarios with the potential to integrate the two systems. These scenarios are presented in Section 4.2.1. This research addresses the 3GPP proposed Scenario 2 supporting authentication and access control functions for a client capable of using WLAN to gain high capacity network access.

There are a lot of studies on the integrating WLAN solution with WCDMA by using Opnet to investigate the network performance. Mobile IP is not proposed to get the intermediate solution.

In this thesis, the migration period from 2G to 3G, the interworking between WLAN and 2G(GSM) is studied and mobile IP is introduced as the intermediate solution. The interworking proposal from 3GPP is also applicable to WLAN and 2G systems.

To combine the existing technologies, which are WLAN, GPRS and Mobile IP, we can achieve seamless roaming in this coupled network. In this thesis, the block diagram of this coupled system is first introduced and protocol stack is shown based on this architecture.

1.2 Methodology Overview

The simulation herein was developed using C++ and no existing protocol code is used in this thesis. First the site topology was randomly generated according to the input, such as WLAN Access Point (AP) and GPRS Base Transceiver Station (BTS) coverage, connections of AP/BTS to the SGSNs, the connections of SGSNs to GGSNs, and the tight/loose connection of the AP to the core GPRS network. The IP forwarding traffic is

generated from each user according to the probability defined in the input file and sent to the destination user, which is randomly assigned. All the users are moving in the range of random speed in the defined area. The Wireless Lan connection is preferred when the Mobile Node is under both the AP and BTS coverage as it has higher bandwidth and cheaper price, which is the case for the Mobile IP client in reality.

The performance data of the system was evaluated based upon IP packets reachability, latency from all the users, etc. The simulation parameters were selected to accurately model an interworked WLAN-GSM system supporting a "hot spot". The factors that were varied in the simulation include the AP/BTS existence probability, tight/loose probability.

1.3 Significant Results

The results of this research indicate that Wireless LAN is a useful enhancement to the GSM network. Specifically, they demonstrate that integrating WLAN into the GSM system would allow a service provider to reserve the limited channels for the revenue producing voice calls, by shifting data service users to the WLAN access network. The users who are shifted to the WLAN access network also experience significantly reduced application delays and improved the IP reachability.

The results also demonstrate that the WLAN access network, when tightly coupled with GPRS network, reduces delays signficently as compared to loosely coupled system.

Also the results prove that the WLAN offers high bandwidth in the "hotspot" area and improves the throughput.

Chapter 2 Wireless LAN Network

Wireless Local Area Networks (WLANs) are becoming increasingly present in corporate and residential indoor environments. WLAN is not a single radio technology, several different technologies fall into the category called WLAN. In general, the IEEE802.11 series standard are called WLAN standard [10].

WLANs provide high capacity connectivity to the wired infrastructure providing IP-based services within "hotspot" area. Section 2.1 provides an introduction to the WLAN technology and concludes with a discussion of components of the IEEE 802.11 architecture. Section 2.2 provides an introduction to the WLAN MAC architecture, which includes an introduction to the three basic access mechanisms. Section 2.3 discusses the inter-frame spacing mechanisms for controlling access to the wireless medium. Section 2.4 presents a detailed description of the Distributed Coordination Function (DCF), specifically covering the basic medium access mechanism, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Section 2.6 covers the time-bounded data service provided by the Point Coordination Function (PCF). Finally, Section 2.6 presents the WLAN Frame structures.

Whenever a packet is to be transmitted, the transmitting node first sends out a short ready-to-send (RTS) packet containing information on the length of the packet. If the receiving node hears the RTS, it responds with a short clear-to-send (CTS) packet. After this exchange, the transmitting node sends its packet. When the packet is received successfully, as determined by a cyclic redundancy check (CRC), the receiving node transmits an acknowledgment (ACK) packet. This back-and-forth exchange is necessary to avoid the "hidden node" problem. For instance, Node A can communicate with node

B, and node B can communicate with node C. However, node A cannot communicate node C. Thus, for instance, although node A may sense the channel to be clear, node C may in fact be transmitting to node B. The protocol described above alerts node A that node B is busy, and hence it must wait before transmitting its packet.

2.1 WLAN System

The WLAN protocol discussed in this research effort is based on the IEEE 802.11 standard

[10]. The standard defines a medium access control (MAC) sub-layer and three physical (PHY) layers. Despite the different radio technologies, all WLAN systems are commonly transpent to IP datagrams, which means the WLAN specification affect the Physical and Datalink layer refered to the 7 layered structure. The goal of the IEEE 802.11 standard is to describe a WLAN that delivers services commonly found in wired networks.

The IEEE 802.11 architecture consists of several components that work together to provide a Wireless LAN (WLAN) connectivity and that is transparent to the upper layers. The Basic Service Set (BSS) is the basic building block of an 802.11 WLAN. A station is the component that connects to the wireless medium. The station may be mobile, portable, or stationary. A station provides the following WLAN services: authentication, privacy, and delivery of the data (MAC service data unit). The BSS is a set of stations that communicate with one another. In IEEE's proposed standard for wireless LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure.

In the ad-hoc network, stations are brought together to form a network "on the fly". As shown in Figure 2.1[9], there is no structure in the network; there are no fixed points; and usually every node is able to communicate with the other nodes. A good example of this is the meeting where employees bring laptop computers together to communicate and share design or test information. Although it seems that order would be difficult to maintain in this type of network, election among the PCs were done and one of the PC has been designed to be as the base station (master) of the network with the others being slaves. Another way in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish links.

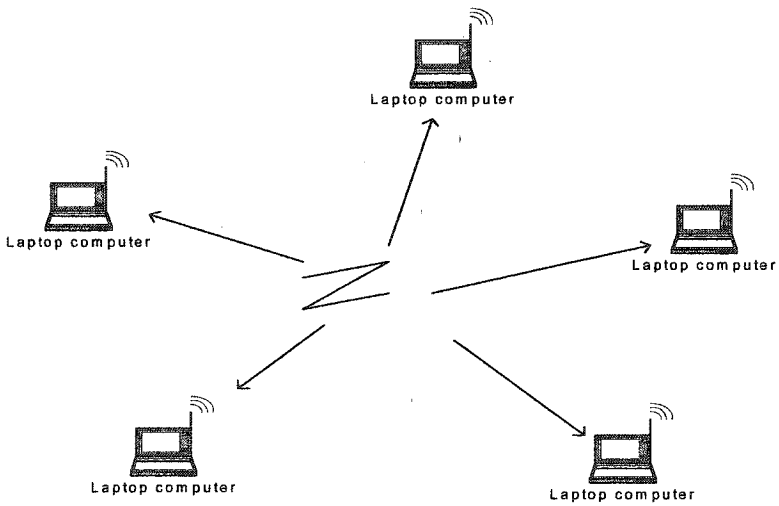

Figure 2.1 Ad-hoc network

In the infrastructure network, fixed network access points with which mobile nodes can communicate are used. These network access points are sometime connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. This structure is very similar to the present day cellular network, see the Figure 2.2[9].

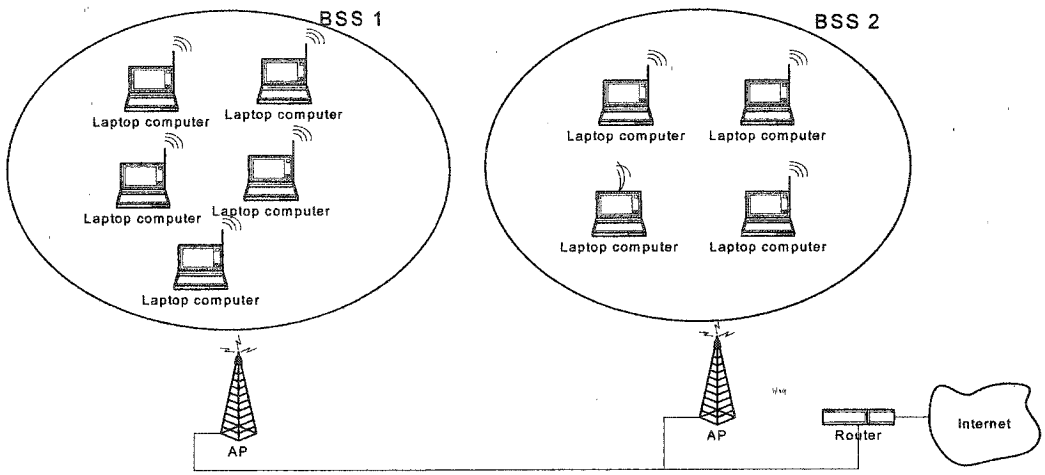

Figure 2.2 Infrastructure network

In this case, the BSS includes an access point (AP), the BSS is no longer independent—it is called an infrastructure BSS or simply a BSS. The stations in a BSS communicate with the AP only. The AP provides relay function within the BSS as well as provides the connectivity to networks outside the BSS.

An Extended Service Set (ESS) is a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another. The APs perform this communication via a distribution system (DS). A DS is the backbone of the WLAN and maybe constructed of either wired or wireless networks. Figure 2.2 is an example of an ESS with two infrastructure BSSs connected via a DS. The DS also is connected to an IP backbone through a gateway router.

2.2 WLAN Protocol

The IEEE 802.11 fits well into other 802.x standards (802.3 Ethernet standard for instance) for wired LANs. Applications should not notice any difference apart from a lower bandwidth and possibly a higher access time from the WLAN. Therefore, the higher layers (application, TCP/IP, etc) in a wireless node look the same as the wired

node. The IEEE 802.11 standard only covers the medium access (MAC) and physical (PHY) layers like the other 802.x LAN standards. Figure 2.3 is the basic reference protocol reference model from [10].

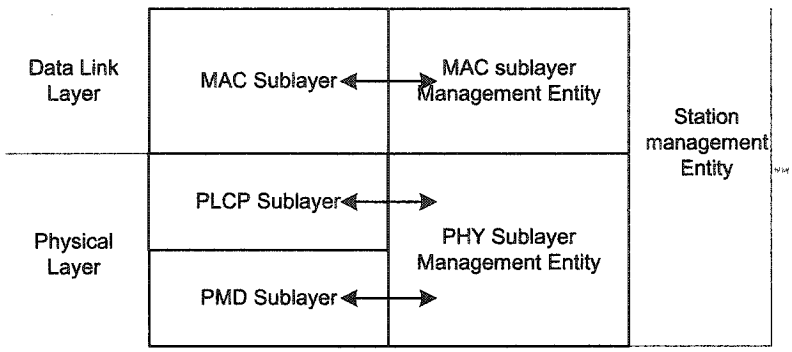

Figure 2.3 Protocol reference model for the 802.11 standard

The IEEE 802.11 standard places specifications on the parameters of both the physical (PHY) and medium access control (MAC) layers of the network.

The PHY layer, which actually handles the transmission of data between nodes, can use either direct sequence spread spectrum, frequency-hopping spread spectrum, or infrared (IR) pulse position modulation. IEEE 802.11 makes provisions for data rates of either 1 MBPS or 2 MBPS, and calls for operation in the 2.4 - 2.4835 GHz frequency band (in the case of spread-spectrum transmission), which is an unlicensed band for industrial, scientific, and medical (ISM) applications, and 300 - 428,000 GHz for infrared transmission. Infrared is generally considered to be more secure to eavesdropping, because Infrared transmissions require absolute line-of-sight links (no transmission is possible outside any simply connected space or around corners), as opposed to radio frequency transmissions, which can penetrate walls and be intercepted by third parties unknowingly. However, infrared transmissions can be adversely affected by sunlight, and

the spread-spectrum protocol of 802.11 does provide some basic security for typical data transfers.

The physical layer can be subdivided into a physical layer convergence protocol (PLCP) and the physical medium dependent (PMD) sub-layers. The PLCP sub-layer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY interface for the MAC that is independent of the transmission technology. The PMD sub-layer handles modulation and encoding/decoding of signals.

The basic tasks of the MAC layer are medium access, fragmentation of user data, and encryption. The primary responsibility of the WLAN MAC is to control medium access, but it can also provide optional support for roaming, authentication, and power conservation. The basic services provided by the MAC layer are the mandatory asynchronous data service and an optional time-bounded service. The standard specifies that 802.11 only offer the asynchronous service in the ad-hoc network mode, while both services work together in an infrastructure based network with an access point coordinating medium access. The 802.11 standard defines the following three basic access mechanisms: the mandatory basic method based on a version of carrier sense multiple access with collision avoidance (CSMA/CA), an optional method avoiding the hidden terminal problem, and a contention-free polling method for time-bounded service. The first two methods are termed the distribution coordination function (DCF), and the third is the point coordination function (PCF). Figure 2.4 [10] shows the interaction of the waiting time between frames, termed inter-frame spaces (IFS), used for controlling the waiting time before accessing the medium.

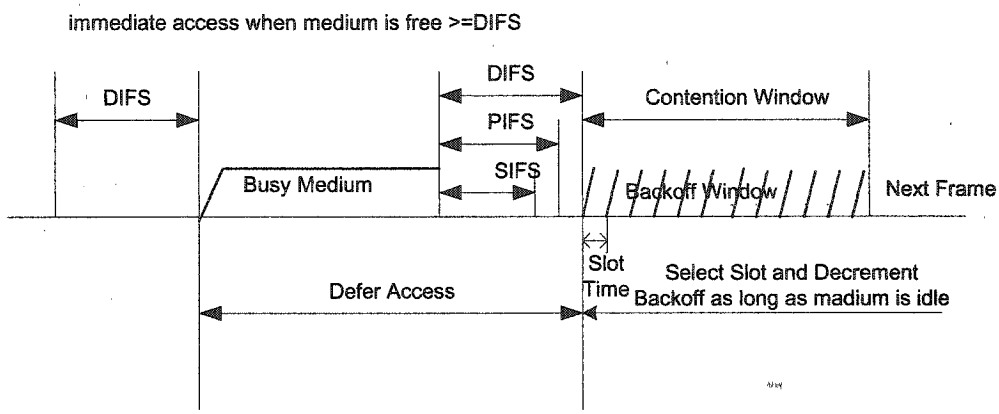

Figure 2.4 Medium Access and Inter-frame Spacing

2.3 Inter-frame Space

The time interval between frames is called the IFS. A station will determine that the medium is idle through the carrier sense mechanism, specifically the CCA in the PLCP sublayer. Four different IFSs are specified in [10] to provide priority levels of access to the wireless media; the main three that are relevant to this research are listed below.

A station must wait an IFS after sensing an idle medium before it can attempt to access the medium.

Short Interframe Space (SIFS)

SIFS is the shortest waiting time for medium access and thus the highest priority for medium access. It is defined for short control messages, such as acknowledgements for data packets or polling responses. SIFS is covered in greater detail in Sections 2.4 and 2.5.

DCF Interframe Space (DIFS)

DIFS is the longest waiting time (and thus the lowest priority). This IFS is defined for the asynchronous data service within a contention period used in the DCF. Both DCF and DIFS are covered in greater detail in Section 2.4.

PCF Interframe Space (PIFS)

PIFS is the waiting time between DIFS and SIFS (and thus medium priority). It is defined for the time-bounded service used in PCF. An access point only has to wait PIFS after sensing an idle medium in order to access. Both PCF and PIFS are covered in greater detail in Section 2.5.

2.4 Distributed Coordination Function

WLAN Media Access Control specification [10] defines the basic medium access protocol as the distributed coordination function (DCF). It allows stations in the same BSS to share the medium using CSMA/CA and a random backoff time following a busy medium. It also specifies that a receiving station will respond with an immediate positive acknowledgement (ACK frame) following successful receipt of a frame, while the sender schedules immediate retransmission if the ACK is not received.

In this CSMA/CA protocol, when a node receives a packet to be transmitted, it first listens to the medium to ensure no other node is transmitting. If the channel is clear, it then transmits the packet. Otherwise, it chooses a random "backoff factor" which determines the amount of time the node must wait until it is allowed to transmit its packet. During periods in which the channel is clear, the transmitting node decrements its backoff counter. (When the channel is busy it does not decrement its backoff counter.) When the backoff counter reaches zero, the node transmits the packet. Since the probability that two nodes will choose the same backoff factor is small, collisions between packets are minimized. Collision detection, as is employed in Ethernet, cannot

be used for the radio frequency transmissions of IEEE 802.11. The reason for this is that when a node is transmitting it cannot hear any other node in the system that may be transmitting, since its own signal will drown out any others arriving at the node.

CSMA/CA with binary exponential backoff is the basic access mechanism specified by the

DCF. Using the physical carrier sense mechanism provided by the CCA, a station will listen to the medium before beginning a transmission. If the medium is already carrying a transmission, the station will not begin its own transmission. This is the CSMA portion of the access mechanism. If two or more stations sense an idle medium and begin their transmission at the same time then there will be a collision, which may result in one or more frames being corrupted.

The IEEE 802.11 MAC uses collision avoidance rather than collision detection in IEEE802.3 in order to transmit and receive simultaneously. For this reason, the IEEE 802.11 MAC implements a virtual sensing mechanism termed the network allocation vector (NAV). The NAV is a value that indicates to a station the amount of time that remains before the medium will become available. The NAV is kept current through duration values that are transmitted in all frames.

By combining this virtual sensing mechanism (using the NAV) with the physical sensing mechanism (using the CCA), the MAC implements the collision avoidance portion of the CSMA/CA access mechanism.

DCF and DIFS

The DCF uses the physical and virtual carrier sense mechanisms to determine if the medium is idle. If both mechanisms indicate that the medium in not in use for an interval of DIFS then the station will begin to transmit the frame. However, if the medium is busy

then the backoff algorithm is applied. The transmission is considered to be unsuccessful if an ACK is not received, resulting in the retransmission of the frame.

2.5 Point Coordination Function

The DCF cannot guarantee a maximum access delay or minimum transmission bandwith. To provide a time-bounded service, [10] specifies the PCF on top of the basic DCF access mechanism (see Figure 2.5). Using PCF requires an AP that controls medium access by polling individual stations. The polling mechanism in the AP is termed the point coordinator (PC). The PC splits the access time into super-frame periods shown in Figure 2.5 [10]. A super-frame comprises a contention-free period (CFP) and a contention period. The contention period is used for stations that are not accessing the AP and are using the DCF access mechanism.

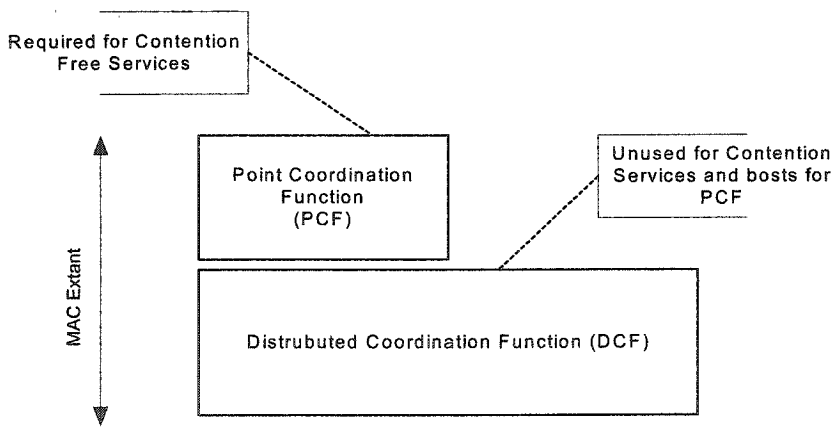

Figure 2.5 Medium Reference model

PCF operates by requiring stations to request that the PC register them on a polling list. Once a station is registered with the PC, it becomes contention-free pollable (CF-Pollable).

During the CFP, the PC polls and delivers traffic to the CF-Pollable stations at regular intervals. Figure 2.6 is an example of PCF data transfer with four stations.

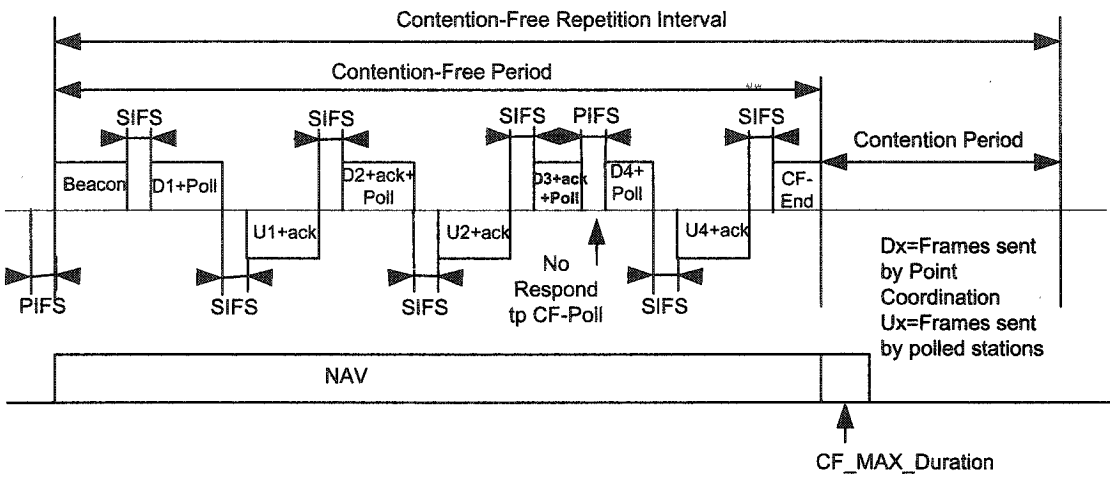

Figure 2.6 PCF Data transfer with 4 Stations

In this example, there are four CF-Pollable stations. The AP has data to send to all four stations, but only stations 1, 2, and 4 have data to send to the AP. The PC transmits a Beacon to mark the beginning of the CFP. The PC will transmit data to, respond with an ACK, and/or poll a CF-pollable station using the SIFS as is the cases when it sends data to stations 1, 2, and 3. Stations 1 and 2 wait a SIFS period before responding to the AP with an ACK and subsequent data transmission. The data exchange attempt with station 3 highlights what happens when a CF-Pollable station does not respond to its poll. The PC expects station 3 to respond with an ACK and transmit any data it might have after waiting a SIFS. When a SIFS period elapses without the receipt of the expected transmission, the PC may send its next pending transmission as soon as one PIFS after

the end of its last transmission. This permits the PC to retain control of the medium in the presence of an overlapping BSS. The PC ends the CFP with a CF-End Beacon.

2.6 WLAN Frame Structure

WLAN Media Access Control specification [10] specifies the basic frame structure shown in Figure 2.7. Each frame consists of the following basic components:

a) A MAC header, which comprises frame control, duration, address, and sequence control information;

b) A variable length frame body, which contains information specific to the frame type;

c) A frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

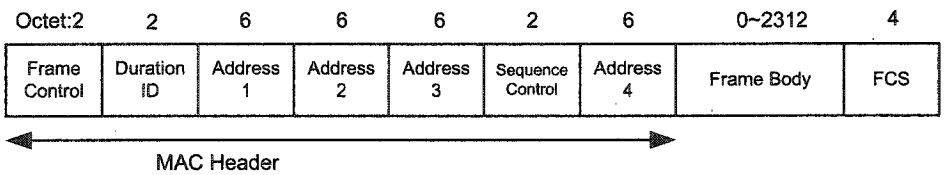

Figure 2.7 IEEE 802.11 Frame Structure

Chapter 3 GSM/GPRS network

GSM was introduced in Europe in 1990. The goal of GSM was to replace the various European 1G analog systems with a single digital system. GSM operates in the 890-960 MHz frequency band, and a PCS version termed Digital Cellular System (DCS) 1800 operates in the 1.8-2.0 GHz band. GSM uses slow frequency hopping, and a 200 kHz carrier bandwidth. Its frame structure supports eight users per carrier. GSM is the most widely used 2G standard, accounting for about 66 percent of the world market by the end of year 2003.

Standards have been developed to provide both data and voiced service, and increase the data rate in GSM networks. General Packet Radio Service (GPRS) is a packet overlay network designed to provide data services in a GSM network. GPRS utilizes the same frame structure as GSM, and supports a maximum data rate of 21.4 kbps per timeslot and it can reachs 171kbps per 200kHZ radio channel. The GPRS infrastructure adds two new nodes to the GSM network, the Gateway GPRS Support Node (GGSN) and the Serving GPRS Support Node (SGSN). The GGSN serves as a gateway to external data networks and tunnels data traffic to the appropriate SGSN. The SGSN is responsible for delivering data packets to the mobile user. The GPRS architecture is discussed later in Section 3.2.1. Enhanced Data rates for GSM Evolution (EDGE) is an ongoing effort to increase the data rate of GSM. EDGE will provide data rates up to 384 kbps over the basic GSM 200 kHz channel by using higher order modulation schemes. Both GPRS and EDGE bring the capabilities of GSM closer to the goals of 3G, and they are often referred to as 2.5G standards.

3.1 GSM Network

3.1.1 GSM System Architecture

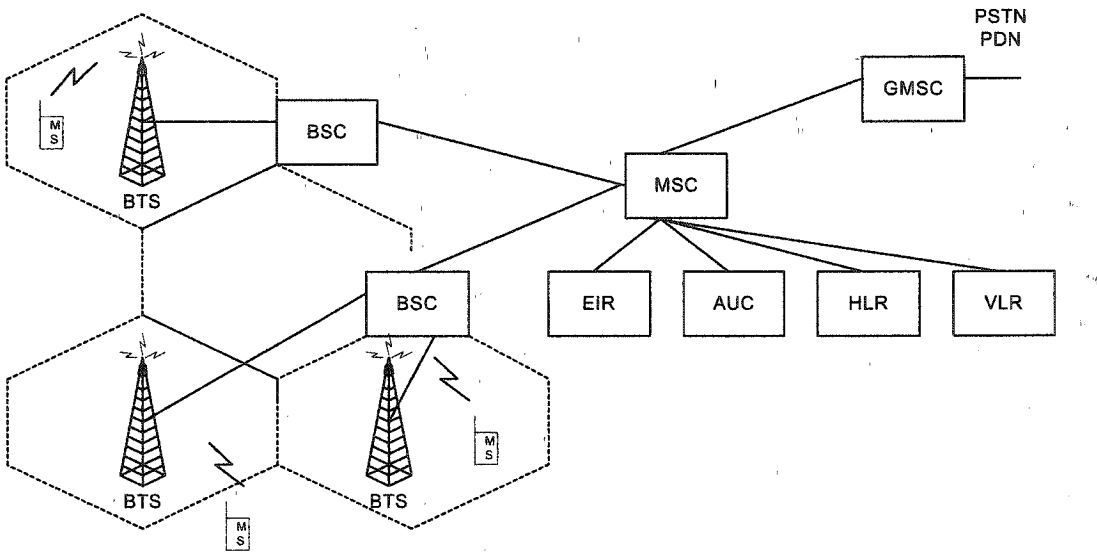

Figure 3.1 GSM System Architecture and components

Figure3.1 shows the system architecture of a GSM public land mobile network (PLMN) with essential components [13]. The components are defined as follows:

- *Mobile station*

  The GSM mobile station (or mobile phone) communicates with other parts of the system through the base-station system.

- GSM Base station system (BSS)

- *Base transceiver station (BTS)*

  The base transceiver station (BTS) handles the radio interface to the mobile station. The base transceiver station is the radio equipment (transceivers and antennas)

- *Base station controller (BSC)*

  The BSC provides the control functions and physical links between the MSC and BTS. It provides functions such as handover, cell configuration data and control of

RF power levels in base transceiver stations. A number of BSCs are served by a MSC.

- *Mobile services switching center (MSC)*

  The MSC performs the telephony switching functions of the system. It also performs such functions as toll ticketing, network interfacing, common channel signalling, and others.

- *Home location register (HLR)*

  The HLR database is used for storage and management of subscriptions. The home location register stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status.

- *Visitor location register (VLR)*

  The VLR database contains temporary information about subscribers that is needed by the mobile services switching center (MSC) in order to service visiting subscribers. When a mobile station roams into a new mobile services switching center (MSC) area, the visitor location register (VLR) connected to that MSC will request subscriber data about the mobile station from the HLR, reducing the need for interrogation of the home location register (HLR).

- *Authentication center (AUC)*

  The AUC provides authentication and encryption parameters that verify the user's Identity and ensure the confidentiality of each call. The authentication center (AUC) also protects network operators from fraud.

- *Equipment identity register (EIR)*

The EIR database contains information on the identity of mobile equipment to prevent calls from stolen, unauthorized or defective mobile stations.

- *Gateway mobile services switching center (GMSC)*

  Gateway mobile services switching center (GMSC) is a node used to interconnect two networks.

In general, a GSM cell is formed by the radio area coverage of a base transceiver station (BTS). Several BTSs together are controlled by one base station controller (BSC). The BTS and BSC together form the base station subsystem (BSS). The combined traffic of the mobile stations in their respective cells is routed through a switch, the mobile switching center (MSC). Connections originating from or terminating in the fixed network are handled by a dedicated gateway mobile switching center (GMSC). GSM networks are structured hierarchically. They consist of at least one administrative region, which is assigned to a MSC. Each administrative region is made up of at least one location area (LA). A location area consists of several cell groups. Each cell group is assigned to a BSC.

Several databases are available for call control and network management: the home location register (HLR), the visited location register (VLR), the authentication center (AUC), and the equipment identity register (EIR).

For all users registered with a network operator, permanent data (such as the user's profile) as well as temporary data (such as the user's current location) are stored in the HLR. In case of a call to a user, the HLR is always first queried, to determine the user's current location. A VLR is responsible for a group of location areas and stores the data of

those users who are currently in its area of responsibility. This includes parts of the permanent user data that have been transmitted from the HLR to the VLR for faster access. But the VLR may also assign and store local data such as a temporary identification. The AUC generates and stores security-related data such as keys used for authentication and encryption, whereas the EIR registers equipment data rather than subscriber data.

3.1.2 GSM Addresses/Identifiers

GSM distinguishes explicitly between user and equipment and deals with them separately. Besides phone numbers, subscriber and equipment identifiers, several other identifiers have been defined; they are needed for the management of subscriber mobility and for addressing of all the remaining network elements [13]. The international mobile station equipment identity (IMEI) uniquely identifies a mobile station internationally. It is a kind of serial number. The IMEI is allocated by the equipment manufacturer and registered by the network operator who stores it in the EIR. Each registered user is uniquely identified by its IMSI. It is stored in the subscriber identity module (SIM). A mobile station can only be operational if a SIM with a valid IMSI is inserted into equipment with a valid IMEI. The "real telephone number" of a mobile station is the mobile subscriber number (MSISDN). It is assigned to the subscriber (his or her SIM, respectively), such that a mobile station can have several MSISDNs depending on the SIM. The VLR, which is responsible for the current location of a subscriber, can assign a temporary mobile subscriber identity (TMSI) which has only local significance in the area handled by the VLR. It is stored on the network side only in the VLR and is not passed to the HLR.

3.1.3 GSM Radio Link

On the physical layer, GSM uses a combination of FDMA and TDMA for multiple accesses. Two frequency bands 45 MHz apart have been reserved for GSM operation: 890 - 915 MHz for transmission from the mobile station, i.e., uplink, and 935 - 960 MHz for transmission from the BTS, i.e., downlink. Each of these bands of 25 MHz widths is divided into 124 single carrier channels of 200 kHz widths. A certain number of these frequency channels, the so-called cell allocation, are allocated to a BTS, i.e., to a cell. Within a carrier, 8 way TDMA is used to define 8 slots within a frame. Each slot lasts 0.577 ms. On top of this, TDMA structure is defined a multiframe structure; a multiframe consists of 26 time frames spanning a total of 120 ms. The multiframe is used to define a complex array of control channels and traffic channels. SACCHs and FACCHs (slow and fast associated control channels) are associated with a traffic channel (TCH) and carry link control information between the mobile and the BSSs. A number of different bitrate TCHs are defined in the standard. A second multiframe structure (51 frames long) is also defined to derive dedicated control setup, broadcast, synchronization, frequency control, paging, random access, and access granting control channels.

3.2 GPRS Network

3.2.1 GPRS System Architecture

In order to integrate GPRS into the existing GSM architecture, a new class of network nodes, called GPRS support nodes (GSN), has been introduced [15]. GSNs are responsible for the delivery and routing of data packets between the mobile stations and

the external packet data networks (PDN). Figure 3.2 illustrates the system architecture [13].

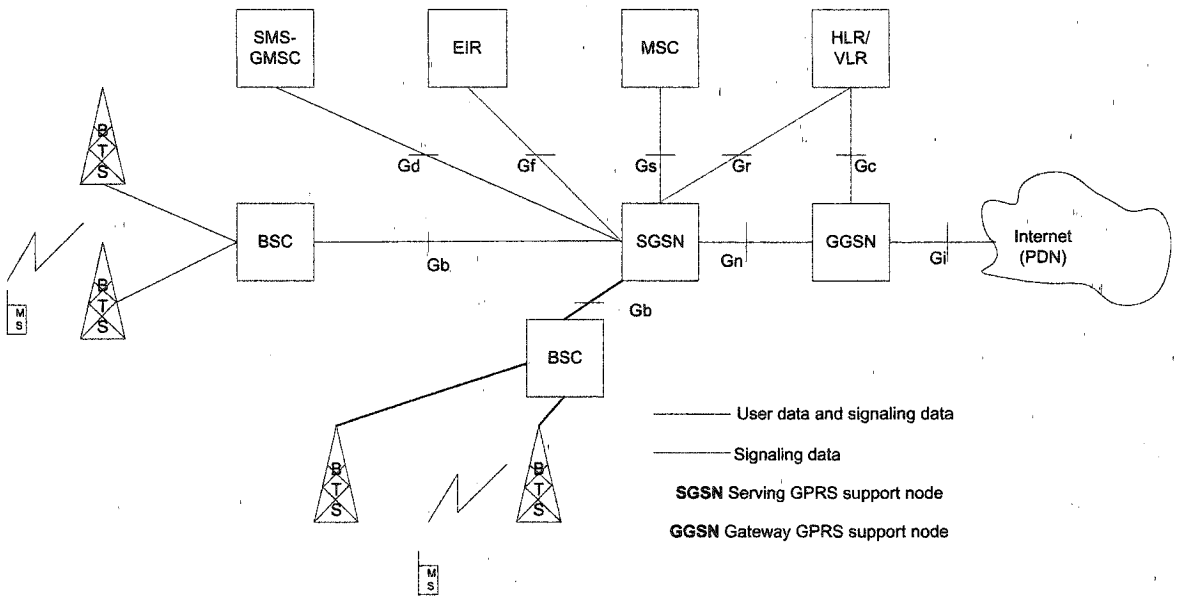

Figure 3.2 GPRS System Architecture and components

A serving GPRS support node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address (es) used in the packet data network) of all GPRS users registered with this SGSN.

A gateway GPRS support node (GGSN) acts as an interface between the GPRS backbone network and the external packet data networks. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format (e.g., IP) and sends them out on the corresponding packet data network. In the other direction, PDP addresses of incoming data packets are converted to the GSM address of the destination

user. The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN also performs authentication and charging functions. In general, there is a many-to-many relationship between the SGSNs and the GGSNs: A GGSN is the interface to external packet data networks for several SGSNs; an SGSN may route its packets over different GGSNs to reach different packet data networks. Figure 3.2 also shows the interfaces between the new network nodes and the GSM network as defined by ETSI in [14]. The Gb interface connects the BSC with the SGSN. Via the Gn and the Gp interfaces, user data and signaling data are transmitted between the GSNs. The Gn interface will be used if SGSN and GGSN are located in the same PLMN, whereas the Gp interface will be used if they are in different PLMNs. All GSNs are connected via an IP-based GPRS backbone network. Within this backbone, the GSNs encapsulate the PDN packets and tunnel them using the GPRS Tunneling Protocol GTP. There are two kinds of GPRS backbones:

- Intra-PLMN backbone networks connect GSNs of the same PLMN and are therefore private IP-based networks of the GPRS network provider.
- Inter-PLMN backbone networks connect GSNs of different PLMNs. A roaming agreement between two GPRS network providers is necessary to install such a backbone.

Figure 3.3 shows two intra-PLMN backbone networks of different PLMNs connected with an inter-PLMN backbone. The gateways between the PLMNs and the external inter-PLMN backbone are called border gateways. Among other things, they perform security

functions to protect the private intra-PLMN backbones against unauthorized users and attacks.

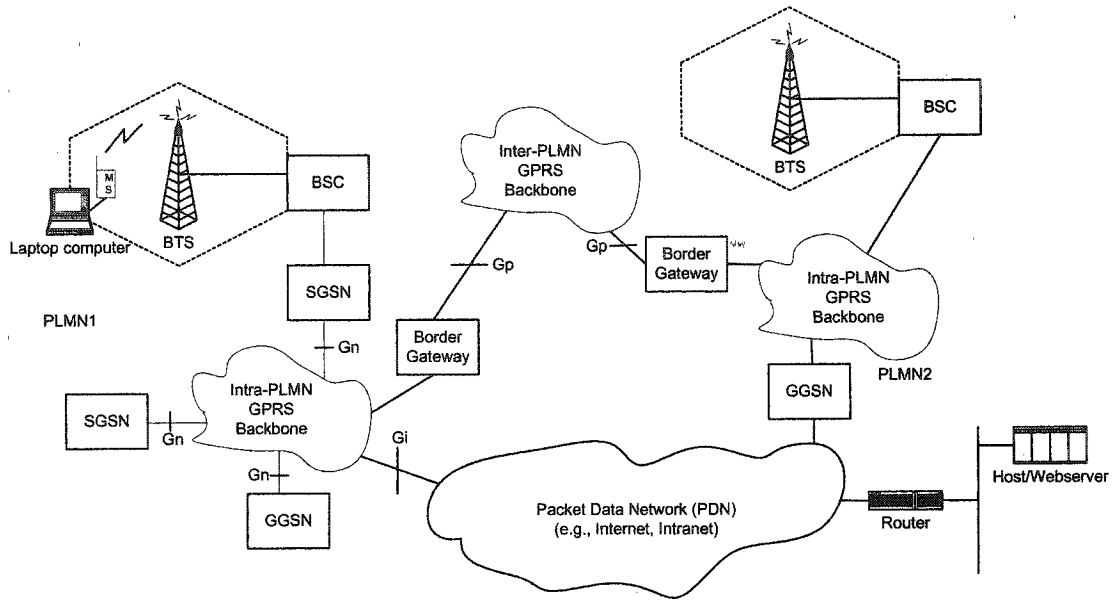

Figure 3.3 Inter/Intra-PLMN connection topology

The Gn and Gp interfaces are also defined between two SGSNs. This allows the SGSNs to exchange user profiles when a mobile station moves from one SGSN area to another. Across the Gf interface, the SGSN may query the IMEI of a mobile station trying to register with the network.

The Gi interface connects the PLMN with external public or private PDNs, such as the Internet or corporate intranets. Interfaces to IP (IPv4 and IPv6) and X.25 networks are supported. The HLR stores the user profile, the current SGSN address, and the PDP address for each GPRS user in the PLMN. The Gr interface is used to exchange this information between HLR and SGSN. For example, the SGSN informs the HLR about the current location of the MS. When the MS registers with a new SGSN, the HLR will send the user profile to the new SGSN. The signaling path between GGSN and HLR (Gc

interface) may be used by the GGSN to query a user's location and profile in order to update its location register.

In addition, the MSC/VLR is extended with functions and register entries that allow efficient coordination between packet switched (GPRS) and circuit switched (conventional GSM) services. Examples of this are combined GPRS and non-GPRS location updates and combined attachment procedures. Moreover, paging requests of circuit switched GSM calls can be performed via the SGSN. For this purpose, the Gs interface connects the databases of SGSN and MSC/VLR.

To exchange messages of the short message service (SMS) via GPRS, the Gd interface is defined. It interconnects the SMS gateway MSC (SMS-GMSC) with the SGSN.

3.2.2 GPRS Protocol Architecture

The GPRS transmission plane consists of a layered protocol structure providing user information transfer, along with associated information transfer control procedures such as flow control, error detection, error correction and error recovery.

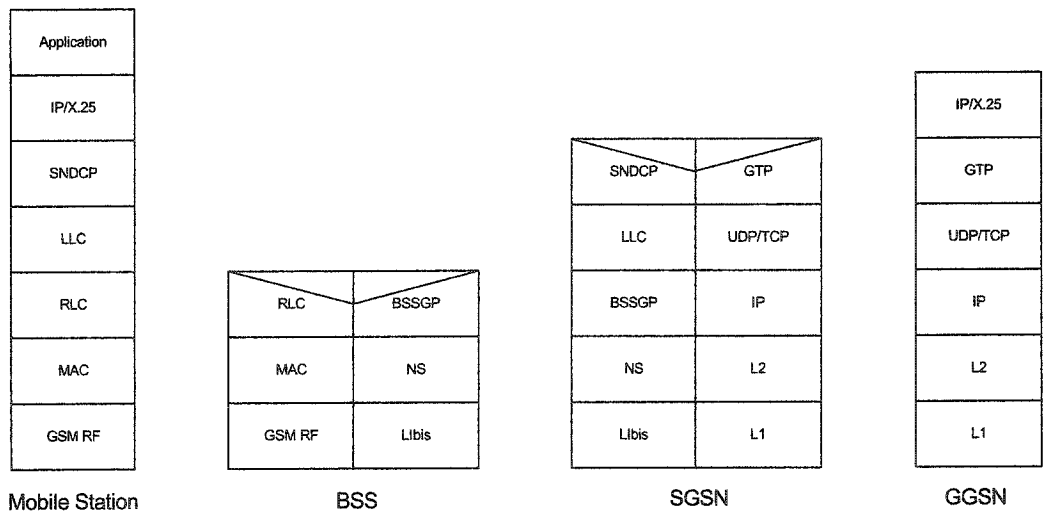

Figure 3.4 GPRS transmission plane protocol

Figure 3.4 [14] shows the layered protocols used along the GPRS network, which includes the following:

- **GPRS Tunneling Protocol (GTP):** This protocol tunnels user data and signaling between GPRS Support Nodes in the GPRS backbone network.
- **TCP:** carries GTP PDUs in the GPRS backbone network for protocols that need a reliable data link, and UDP carries GTP PDUs for protocols that do not need a reliable data link. TCP provides flow control and protection against lost and corrupted GTP PDUs. UDP provides protection against corrupted GTP PDUs.
- **IP**: This is the GPRS backbone network protocol used for routing user data and control signaling.
- **Logical Link Control (LLC)**: This layer provides a highly reliable ciphered logical link. LLC is independent of the underlying radio interface protocols in order to allow introduction of alternative GPRS radio solutions.
- **Base Station System GPRS Protocol (BSSGP):** This layer conveys routing- and QoS-related information between BSS and SGSN.
- **Network Service (NS)**: This layer transports BSSGP PDUs. NS is based on a Frame Relay connection between BSS and SGSN.
- **RLC/MAC**: This layer contains two functions: The Radio Link Control function provides a radio-solution dependent reliable link. The Medium Access Control function controls the access signaling (request and grant) procedures for the radio channel, and the mapping of LLC frames onto the physical channel.

GPRS Backbone: SGSN - GGSN -- As mentioned earlier, user data packets are encapsulated within the GPRS backbone network. The GPRS Tunneling Protocol (GTP)

[9] tunnels the user data packets and related signaling information between the GPRS support nodes (GSNs). The protocol is defined both between GSNs within one PLMN (Gn interface) and between GSNs of different PLMNs (Gp interface). In the transmission plane, GTP employs a tunnel mechanism to transfer user data packets. In the signaling plane, GTP specifies a tunnel control and management protocol. The signaling is used to create, modify, and delete tunnels.

GTP packets carry the user's IP or X.25 packets. Below GTP, the standard protocols TCP or UDP are employed to transport the GTP packets within the backbone network. X.25 expects a reliable data link, thus TCP is used. UDP is used for access to IP-based packet data networks, which do not expect reliability in the network layer or below. IP is employed in the network layer to route packets through the backbone. Ethernet, ISDN, or ATM-based protocols may be used below IP.

To summarize, in the GPRS backbone we have an IP/X.25-over-GTP-over-UDP/TCP-over-IP transport architecture.

Subnetwork Dependent Convergence Protocol -- The Subnetwork Dependent Convergence Protocol (SNDCP) is used to transfer data packets between SGSN and MS. Its functionality includes:

- Multiplexing of several connections of the network layer onto one virtual logical connection of the underlying LLC layer.
- Compression and decompression of user data and redundant header information.

Air Interface -- In the following, we consider the data link layer and the physical layer at the air interface Um.

Data Link Layer: The data link layer between the MS and the network is divided into two sublayers: the LLC layer (between MS-SGSN) and the RLC/MAC layer (between MS-BSS).

The logical link control (LLC) layer [15] provides a highly reliable logical link between an MS and its assigned SGSN. Its functionality is based on the well-known HDLC protocol and includes sequence control, in-order delivery, flow control, detection of transmission errors, and retransmission (automatic repeat request (ARQ)). The data confidentiality is ensured by ciphering functions. Variable frame lengths are possible. Both acknowledged and unacknowledged data transmission modes are supported. The protocol is mainly an adapted version of the LAPDm protocol used in GSM.

The RLC/MAC layer [15] at the air interface includes two functions. The main purpose of the radio link control (RLC) layer is to establish a reliable link between the MS and the BSS. This includes the segmentation and reassemble of LLC frames into RLC data blocks and ARQ of uncorrectable codewords. The medium access control (MAC) layer controls the access attempts of an MS on the radio channel shared by several MSs. It employs algorithms for contention resolution, multiuser multiplexing on a PDTCH, and scheduling and prioritizing based on the negotiated QoS. The GPRS MAC protocol is based on the principle of slotted Aloha. In the RLC/MAC layer, both the acknowledged and unacknowledged modes of operation are supported.

Physical Layer: The physical layer between MS and BSS is divided into the two sublayers: the physical link layer (PLL) and the physical RF Layer (RFL). The PLL provides a physical channel between the MS and the BSS. Its tasks include channel coding (detection of transmission errors, forward error correction (FEC),

indication of uncorrectable codewords), interleaving, and detection of physical link congestion.

The RFL operates below the PLL. Among other things, it includes modulation and demodulation.

BSS - SGSN Interface -- The BSS GPRS Application Protocol (BSSGP) delivers routing and QoS-related information between BSS and SGSN. The underlying Network Service (NS) protocol is based on the Frame Relay protocol.

Signaling Plane

The protocol architecture of the signaling plane comprises protocols for control and support of the functions of the transmission plane, e.g., GPRS attach and detach, PDP context activation, control of routing paths, and allocation of network resources. Between MS and SGSN, the GPRS Mobility Management and Session Management (GMM/SM) protocol supports mobility and session management when performing functions such as GPRS attach/detach, security functions, PDP context activation, and routing area updates.

The signaling architecture between SGSN and the registers HLR, VLR, and uses the same protocols as conventional GSM and extends them with GPRS-specific functionality. Between SGSN and HLR as well as between SGSN and EIR, an enhanced Mobile Application Part (MAP) is employed. The MAP is a mobile network-specific extension of the Signaling System SS#7. It transports the signaling information related to location updates, routing information, user profiles, and handovers. The exchange of MAP messages is accomplished over the transaction capabilities application part (TCAP) and the signaling connection control part (SCCP). The base station system application

part (BSSAP+) includes functions of GSM's BSSAP. It is applied to transfer signaling information between the SGSN and the VLR (Gs interface). This includes signaling of the mobility management when coordination of GPRS and conventional GSM functions is necessary (e.g., combined GPRS and non-GPRS location update, combined GPRS/IMSI attach, or paging of an MS via GPRS for an incoming GSM call).

Interworking with IP Networks

The Gi interface is the inter-working point with IP networks. From outside, i.e., from an external IP network's point of view, the GPRS network looks like any other IP subnetwork, and the GGSN looks like a usual IP router.

3.2.3 Services

Bearer Services and Supplementary Services

The bearer services of GPRS offer end-to-end packet switched data transfer. There are two different kinds: The point-to-point (PTP) service and the point-to-multipoint (PTM) service. In the current release of GPRS just the PTP is supported. The PTP service offers transfer of data packets between two users. It is offered in both connectionless mode (PTP connectionless network service (PTP-CLNS), e.g., for IP) and connection-oriented mode (PTP connection-oriented network service (PTP-CONS), e.g., for X.25).

The PTM service offers transfer of data packets from one user to multiple users. There exist two kinds of PTM services:

- Using the multicast service PTM-M, data packets are broadcast in a certain geographical area. A group identifier indicates whether the packets are intended for all users or for a group of users.

- Using the group call service PTM-G, data packets are addressed to a group of users (PTM group) and are sent out in geographical areas where the group members are currently located.

It is also possible to send SMS messages over GPRS. In addition, it is planned to implement supplementary services, such as call forwarding unconditional (CFU), call forwarding on mobile subscriber not reachable (CFNRc), and closed user group (CUG). Moreover, a GPRS service provider may offer additional non-standardized services, such as access to databases, messaging services, and tele-action services (e.g., credit card validations, lottery transactions, and electronic monitoring and surveillance systems).

Quality of Service

The Quality of Service QoS requirements of typical mobile packet data applications are very diverse (e.g., consider real-time multimedia, Web browsing, and e-mail transfer). Support of different QoS classes, which can be specified for each individual session, is therefore an important feature. GPRS allows defining QoS profiles using the parameters service precedence, reliability, delay, and throughput.

- The service precedence is the priority of a service in relation to another service. There exist three levels of priority: high, normal, and low.
- The reliability indicates the transmission characteristics required by an application. Three reliability classes are defined, which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption (an undetected error) of packets.
- The delay parameters define maximum values for the mean delay and the 95-percentile delay. The latter is the maximum delay guaranteed in 95 percent of all

transfers. The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the Gi interface to an external packet data network. This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network. Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account.

- The throughput specifies the maximum/peak bit rate and the mean bit rate.

Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the current available resources. The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

Simultaneous Usage of Packet Switched and Circuit Switched Services

In a GSM/GPRS network, conventional circuit switched services (speech, data, and SMS) and GPRS services can be used in parallel. Three classes of mobile stations are defined:

- A class A mobile station supports simultaneous operation of GPRS and conventional GSM services.
- A class B mobile station is able to register with the network for both GPRS and conventional GSM services simultaneously. In contrast to an MS of class A, it can only use one of the two services at a given time.
- A class C mobile station can attach for either GPRS or conventional GSM services. Simultaneous registration (and usage) is not possible. An exception is SMS messages, which can be received and sent at any time.

3.2.4 Session Management, Mobility Management, and Routing

In order to send and receive packets, the MS need to attach to the network and also the network need to keep track of the current location of the user.

Attachment and Detachment Procedure

Before a mobile station can use GPRS services, it must register with an SGSN of the GPRS network. The network checks if the user is authorized, copies the user profile from the HLR to the SGSN, and assigns a packet temporary mobile subscriber identity (P-TMSI) to the user. This is called GPRS attach. For mobile stations using both circuit switched and packet switched services it is possible to perform combined GPRS/IMSI attach procedures. The disconnection from the GPRS network is called GPRS detach. It can be initiated by the mobile station or by the network (SGSN or HLR).

Session Management, PDP Context

To exchange data packets with external PDNs after a successful GPRS attach, a mobile station must apply for one or more addresses used in the PDN, e.g., for an IP address in case the PDN is an IP network. This address is called PDP address (Packet Data Protocol address). For each session, a so-called PDP context is created, which describes the characteristics of the session. It contains the PDP type (e.g., IPv4), the PDP address assigned to the mobile station (e.g., IP address), the requested QoS, and the address of a GGSN that serves as the access point to the PDN. This context is stored in the MS, the SGSN, and the GGSN. With an active PDP context, the mobile station is "visible" for the external PDN and is able to send and receive data packets. The mapping between the two addresses, PDP and IMSI, enables the GGSN to transfer data packets between PDN and MS. A user may have several simultaneous PDP contexts active at a given time.

The allocation of the PDP address can be static or dynamic. In the first case, the network operator of the user's home-PLMN permanently assigns a PDP address to the user. In the second case, a PDP address is assigned to the user upon activation of a PDP context. The PDP address can be assigned by the operator of the user's home-PLMN (dynamic home-PLMN PDP address) or by the operator of the visited network (dynamic visited-PLMN PDP address). The home network operator decides which of the possible alternatives may be used. In case of dynamic PDP address assignment, the GGSN is responsible for the allocation and the activation/ deactivation of the PDP addresses. Figure 3.5[13] shows the PDP context activation procedure. Using the message "activate PDP context request," the MS informs the SGSN about the requested PDP context. If dynamic PDP address assignment is requested, the parameter PDP address will be left empty. Afterward, usual security functions (e.g., authentication of the user) are performed. If access is granted, the SGSN will send a "create PDP context request" message to the affected GGSN. The latter creates a new entry in its PDP context table, which enables the GGSN to route data packets between the SGSN and the external PDN. Afterward, the GGSN returns a confirmation message "create PDP context response" to the SGSN, which contains the PDP address in case dynamic PDP address allocation was requested. The SGSN updates its PDP context tables and confirms the activation of the new PDP context to the MS ("activate PDP context accept").

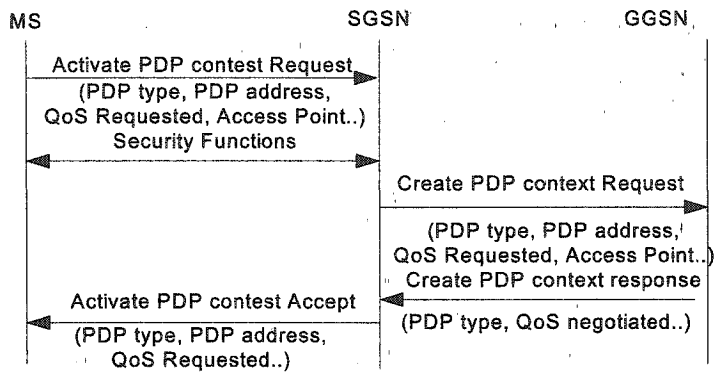

Figure 3.5 PDP context Activation

GPRS also supports anonymous PDP context activation. In this case, security functions as shown in Figure 3.5 are skipped, and thus, the user (i.e., the IMSI) using the PDP context remains unknown to the network. Anonymous context activation may be employed for pre-paid services, where the user does not want to be identified. Only dynamic address allocation is possible in this case.

Routing

We assume that a GPRS mobile station located in PLMN1 sends IP packets to a host connected to the IP network, e.g., to a Web server connected to the Internet. The SGSN that the mobile station is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context, and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates the packets and sends them out on the IP network, where IP routing mechanisms are used to transfer the packets to the access router of the destination network. The latter delivers the IP packets to the host.

Let us assume the home-PLMN of the mobile station is PLMN2. An IP address has been assigned to the mobile by the GGSN of PLMN2. Thus, the MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2. The correspondent host is now

sending IP packets to the MS. The packets are sent out onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1. It encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1. The SGSN decapsulates the packets and delivers them to the MS.

Location Management

The main task of location management is to keep track of the user's current location, so those incoming packets can be routed to the right MS. For this purpose, the MS frequently sends location update messages to its current SGSN. If the MS sends updates its location (e.g., its current cell) less frequently and paging is necessary for each downlink packet, resulting in a significant delivery delay. On the other hand, if location updates happen very often, the MS's location is well known to the network, and the data packets can be delivered without any additional paging delay. However, quite a lot of uplink radio capacity and battery power is consumed for mobility management in this case. Thus, a good location management strategy must be a compromise between these two extreme methods.

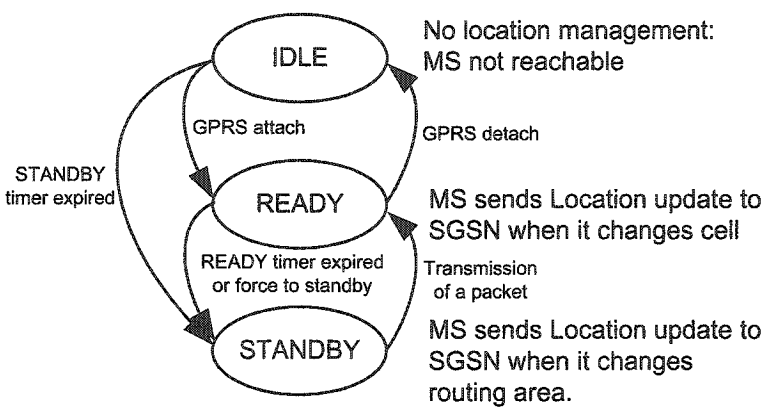

Figure 3.6 GPRS Location management

For this reason, a state model Figure 3.6 [13] has been defined for location management in GPRS. A MS can be in one of three states depending on its current traffic amount; the location update frequency is dependent on the state of the MS.

In IDLE state the MS is not reachable. Performing a GPRS attach, the MS gets into READY state. With a GPRS detach it may disconnect from the network and fall back to IDLE state. All PDP contexts will be deleted. The STANDBY state will be reached when an MS does not send any packets for a longer period of time, and therefore the READY timer (which was started at GPRS attach) expires.

In IDLE state, no location updating is performed, i.e., the current location of the MS is unknown to the network. An MS in READY state informs its SGSN of every movement to a new cell. For the location management of an MS in STANDBY state, a GSM location area (LA) is divided into several routing areas (RA). In general, an RA consists of several cells. The SGSN will only be informed when an MS moves to a new RA; cell changes will not be disclosed. To find out the current cell of an MS in STANDBY state, paging of the MS within a certain RA must be performed (see Figure 3.6). For MSs in READY state, no paging is necessary.

Whenever an MS moves to a new RA, it sends a "routing area update request" to its assigned SGSN. The message contains the routing area identity (RAI) of its old RA. The base station subsystem (BSS) adds the cell identifier (CI) of the new cell, from which the SGSN can derive the new RAI. Two different scenarios are possible:

- Intra-SGSN routing area update: The MS has moved to an RA that is assigned to the same SGSN as the old RA. In this case, the SGSN has already stored the

necessary user profile and can assign a new packet temporary mobile subscriber identity (P-TMSI) to the user ("routing area update accept"). Since the routing context does not change, there is no need to inform other network elements, such as GGSN or HLR.

- Inter-SGSN routing area update: The new RA is administered by a different SGSN than the old RA. The new SGSN realizes that the MS has changed to its area and requests the old SGSN to send the PDP contexts of the user. Afterward, the new SGSN informs the involved GGSNs about the user's new routing context. In addition, the HLR and (if needed) the MSC/VLR are informed about the user's new SGSN.

There also exist combined RA/LA updates. These occur when an MS using GPRS as well as conventional GSM moves to a new LA. The MS sends a "routing area update request" to the SGSN. The parameter "update type" is used to indicate that an LA update is needed. The message is then forwarded to the VLR, which performs the LA update. To sum up, GPRS mobility management consists of two levels: Micro mobility management tracks the current routing area or cell of the mobile station. It is performed by the SGSN. Macro mobility management keeps track of the mobile station's current SGSN and stores it in the HLR, VLR, and GGSN.

3.2.5 Air Interface -- Physical Layer

Multiple Access and Radio Resource Management Principles

The channel allocation in GPRS is different from the original GSM. GPRS allows a single mobile station to transmit on multiple time slots of the same TDMA frame (multislot operation). This results in a very flexible channel allocation: one to eight time

slots per TDMA frame can be allocated for one mobile station. Moreover, uplink and downlink are allocated separately, which efficiently supports asymmetric data traffic (e.g., Web browsing).

In GPRS, the channels are only allocated when data packets are sent or received, and they are released after the transmission. For burst traffic this results in a much more efficient usage of the scarce radio resources. With this principle, multiple users can share one physical channel.

A cell supporting GPRS may allocate physical channels for GPRS traffic. Such a physical channel is denoted as packet data channel (PDCH). The PDCHs are taken from the common pool of all channels available in the cell. Thus, the radio resources of a cell are shared by all GPRS and non-GPRS mobile stations located in this cell. The mapping of physical channels to either packet switched (GPRS) or circuit switched (conventional GSM) services can be performed dynamically, depending on the current traffic load, the priority of the service, and the multislot class. A load supervision procedure monitors the load of the PDCHs in the cell. According to the current demand, the number of channels allocated for GPRS (i.e., the number of PDCHs) can be changed. Physical channels not currently in use by conventional GSM can be allocated as PDCHs to increase the quality of service for GPRS. When there is a resource demand for services with higher priority, PDCHs can be de-allocated.

Logical Channels in GPRS

On top of the physical channels, a series of logical channels are defined to perform a multiplicity of functions, e.g., signaling, broadcast of general system information, synchronization, channel assignment, paging, or payload transport.

The GPRS channels can be divided into two categories: traffic channels and signaling (control) channels as conventional GSM.

- Packet data traffic channel (PDTCH): is employed for the transfer of user data. It is assigned to one mobile station (or in the case of PTM to multiple mobile stations). One mobile station can use several PDTCHs simultaneously.
- Packet broadcast control channel (PBCCH): is a unidirectional point-to-multipoint signaling channel from the base station subsystem (BSS) to the mobile stations. It is used by the BSS to broadcast specific information about the organization of the GPRS radio network to all GPRS mobile stations of a cell. Besides system information about GPRS, the PBCCH should also broadcast important system information about circuit switched services, so that a GSM/GPRS mobile station does not need to listen to the broadcast control channel (BCCH).
- The packet common control channel (PCCCH) is a bidirectional point-to-multipoint signaling channel that transports signaling information for network access management, e.g., for allocation of radio resources and paging. It consists of four sub-channels:
    - The packet random access channel (PRACH) is used by the mobile to request one or more PDTCH.
    - The packet access grant channel (PAGCH) is used to allocate one or more PDTCH to a mobile station.
    - The packet-paging channel (PPCH) is used by the BSS to find out the location of a mobile station (paging) prior to downlink packet transmission.

- The packet notification channel (PNCH) is used to inform a mobile station of incoming PTM messages (multicast or group call).
- The dedicated control channel is a bidirectional point-to-point signaling channel. It contains the channels PACCH and PTCCH:
- The packet associated control channel (PACCH) is always allocated in combination with one or more PDTCH that are assigned to one mobile station. It transports signaling information related to one specific mobile station (e.g., power control information).
- The packet timing advance control channel (PTCCH) is used for adaptive frame synchronization.

The coordination between circuit switched and packet switched logical channels is important. If the PCCCH is not available in a cell, a mobile station can use the common control channel (CCCH) of conventional GSM to initiate the packet transfer. Moreover, if the PBCCH is not available, it will listen to the broadcast control channel (BCCH) to get informed about the radio network.

A mobile station requests radio resources for uplink transfer by sending a "packet channel request" on the PRACH or RACH. The network answers on the PAGCH or AGCH, respectively. It tells the mobile station which PDCHs it may use. A so-called uplink state flag (USF) is transmitted in the downlink to tell the mobile station whether or not the uplink channel is free.

Channel Coding

Channel coding is used to protect the transmitted data packets against errors. The channel coding technique in GPRS is quite similar to the one employed in conventional GSM. An

outer block coding, an inner convolutional coding, and an interleaving scheme is used. Four different coding schemes are defined in 3GPP specification. Their parameters are listed in Table 3.1

Scheme	Code Rate	USF	Pre-coded USF	**Radio Block excl. USF and BCS**	BCS	Tail	Coded Bite	Punctured bits	Date Rate kb/s
CS-1	½	3	3	181	40	4	456	0	9.05
CS-2	2/3	3	6	268	16	4	588	132	13.4
CS-3	¾	3	6	312	16	4	676	220	15.6
CS-4	1	3	12	428	16	-	456	-	21.4

Table 3.1 GPRS CS-1 to CS-4 coding Character List

For the coding of the traffic channel (PDTCH), one of the four coding schemes is chosen, depending on the quality of the channel. Under very bad channel conditions, we may use CS-1 and obtain a data rate of 9.05 kbit/s per GSM time slot, but a very reliable coding. Under good channel conditions, we transmit without convolutional coding and achieve a data rate of 21.4 kbit/s per time slot. With eight time slots, we obtain a maximum data rate of 171.2 kbit/s. In practice, multiple users share the time slots, and thus, a much lower bit rate is available to the individual user.

After encoding, the codewords are input into a block interleaver of depth 4. On the receiver side, the codewords are de-interleaved. The decoding is performed using the well know Viterbi Algorithm [18].

Chapter 4 Mobile IP and Interworking

4.1 Mobile IP

The IP address of a host consists of two parts:

- The higher order bits of the address determine the network on which the host resides
- The remaining low-order bits determine the host number.

IP decides the next-hop by determining the network information from the destination IP address of the packet. On the other hand, higher-level layers like TCP maintain information about connections that are indexed by a quadruplet containing the IP addresses of both the endpoints and the port numbers. Thus, while trying to support mobility on the Internet under the existing protocol suite, we are faced with two mutually conflicting requirements:

- A mobile node has to change its IP address whenever it changes its point of attachment, so that packets destined to the node are routed correctly
- To maintain existing TCP connections, the mobile node has to keep its IP address the same. Changing the IP address will cause the connection to be disrupted and lost.

Mobile IP was suggested as a means to attain wireless networking. It focuses its attention at the Network Layer, working with the current version of the Internet Protocol (IP version 4). In this protocol, the IP address of the mobile machine does not change when it

moves from a home network to a foreign network by allowing each mobile node to have two IP addresses and by transparently maintaining the binding between the two addresses [19]. One of the IP addresses is the permanent home address that is assigned at the home network and is used to identify communication endpoints. The other is a temporary care-of address that represents the current location of the host. The main goals of Mobile IP are to make mobility transparent to the higher-level protocols and to make minimum changes to the existing Internet infrastructure. In order to maintain connections between the mobile node and the rest of the network, a forwarding routine is implemented.

When a person in the physical world moves, they let their home post office know to which remote post office their mail should be forwarded. When the person arrives at their new residence, they register with the new post office. This same operation happens in Mobile IP. When the mobile agent moves from its home network to a foreign (visited) network, the mobile agent tells a home agent on the home network to which foreign agent their packets should be forwarded. In addition, the mobile agent registers itself with that foreign agent on the foreign network. Thus, all packets intended for the mobile agent are forwarded by the home agent (HA) to the foreign agent (FA), which sends them to the mobile agent on the foreign network. When the mobile agent returns to its original network, it informs both agents (home and foreign) that the original configuration has been restored. No one on the outside networks need to know that the mobile agent moved.

4.1.1 Protocol Overview

Mobile IP supports mobility by transparently binding the home address of the mobile node with its care-of address. This mobility binding is maintained by some specialized

routers, known as mobility agents. Mobility agents are of two types - home agents and foreign agents. The home agent, a designated router in the home network of the mobile node, maintains the mobility binding in a mobility binding table where each entry is identified by the tuple <permanent home address, temporary care-of address, association lifetime>.

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
31.193.171.2	119.123.56.78	150

Table 4.1 Mobility binding table

Table 4.1 shows a mobility-binding table. The purpose of this table is to map a mobile node's home address with its care-of address and forward packets accordingly.

Foreign agents are specialized routers on the foreign network where the mobile node is currently visiting. In a typical scenario, the care-of address of a mobile node is the foreign agent's IP address. There can be another kind of care-of address, known as colocated care-of address, which is usually obtained by some external address assignment mechanism. In this reseach the collocated care-of address is used in simulation.

The basic Mobile IP protocol has four distinct stages [24]. These are:

- **Agent Discovery:** Agent Discovery consists of the following steps:

    1. Mobility agents advertise their presence by periodically broadcasting Agent Advertisement messages. An Agent Advertisement message lists one or more care-of addresses and a flag indicating whether it is a home agent or a foreign agent.

2. The mobile node receiving the Agent Advertisement message observes whether the message is from its own home agent and determines whether it is on the home network or a foreign network.

3. If a mobile node does not wish to wait for the periodic advertisement, it can send out Agent Solicitation messages that will be responded by a mobility agent.

- **Registration:** Registration consists of the following steps:

4. If a mobile node discovers that it is on the home network, it operates without any mobility services.

5. If the mobile node is on a new network, it registers with the foreign agent by sending a Registration Request message which includes the permanent IP address of the mobile host and the IP address of its home agent.

6. The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.

7. When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of address of the mobile node with its home address.

8. The home agent then sends an acknowledgement to the foreign agent.

9. The foreign agent in turn updates its visitor list by inserting the entry for the mobile node and relays the reply to the mobile node.

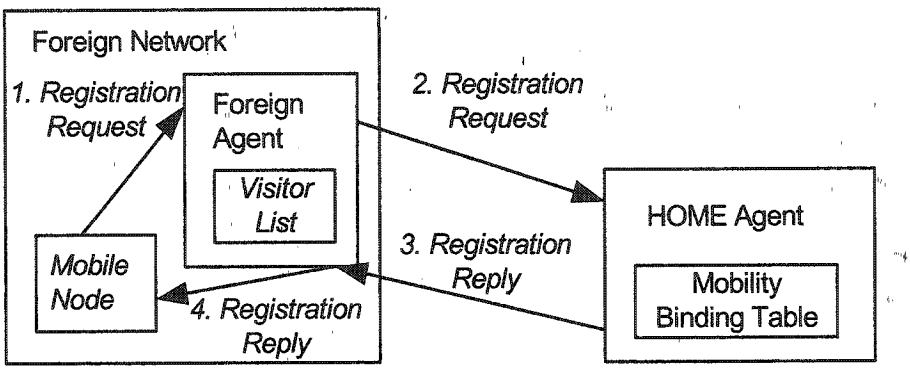

Figure 4.1 Registration process in Mobile IP

- **In Service:** This stage can be subdivided into the following steps:

10. When a correspondent node wants to communicate with the mobile node, it sends an IP packet addressed to the permanent IP address of the mobile node.

11. The home agent intercepts this packet and consults the mobility binding table to find out if the mobile node is currently visiting any other network.

12. The home agent finds out the mobile node's care-of address and constructs a new IP header that contains the mobile node's care-of address as the destination IP address. The original IP packet is put into the payload of this IP packet. It then sends the packet. This process of encapsulating one IP packet into the payload of another is known as **IP-in-IP** encapsulation [25], or **tunneling**.

13. When the encapsulated packet reaches the mobile node's current network, the foreign agent de-capsulate the packet and finds out the mobile node's home address. It then consults the visitor list to see if it has an entry for that mobile node.

14. If there is an entry for the mobile node on the visitor list, the foreign agent retrieves the corresponding media address and relays it to the mobile node.

15. When the mobile node wants to send a message to a correspondent node, it forwards the packet to the foreign agent, which in turn relays the packet to the correspondent node using normal IP routing.

16. The foreign agent continues serving the mobile node until the granted lifetime expires. If the mobile node wants to continue the service, it has to reissue the Registration.

- **Deregistration:** If a mobile node wants to drop its care-of address, it has to deregister with its home agent. It achieves this by sending a Registration Request with the lifetime set to zero. There is no need for deregistering with the foreign agent as registration automatically expires when lifetime becomes zero. However if the mobile node visits a new network, the old foreign network does not know the new care-of address of the mobile node. Thus datagrams already forwarded by the home agent to the old foreign agent of the mobile node are lost.

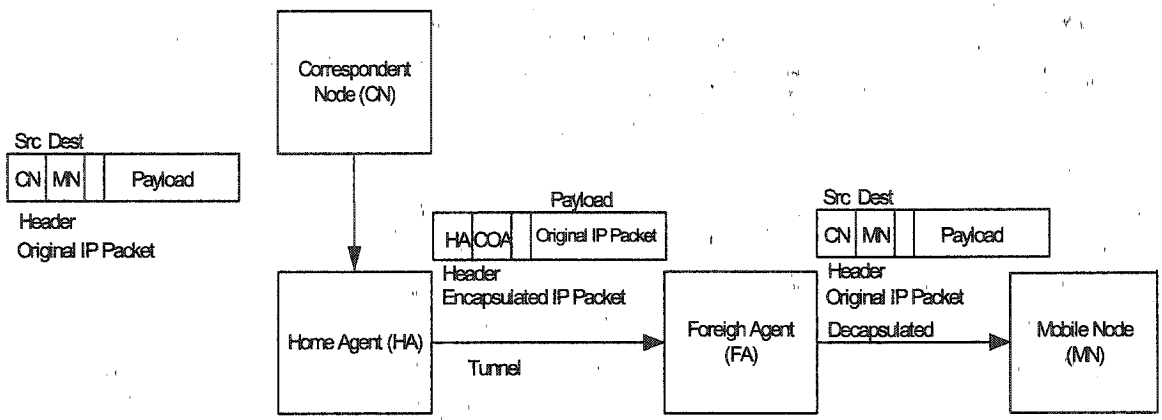

Figure 4.2 Tunneling operation in Mobile IP

4.1.2 IP Mobility

This refers to the access method based on RFC3344 [19]. The user may use either static or dynamic address belonging to its home IP network. The user will be able to maintain its IP address even when it moves throughout the networks.

IP mobility support describe the framework of procedure, messages and messages formats that enables a node to change its point of attachment to a network without requiring alternation to its IP address, which would otherwise disrupt layer 3 and higher operation. Peer nodes can respond to the sending node indicated by the IP source address of incoming packets regardless of IP prefix of the network through which the sending node obtained connectivity. To achieve this, the following things are defined in RFC 3344.

- Introduce a key distinction between the home address and the care-of address (COA).
- Defines three entities—the mobile node (MN), foreignagent (FA) and homeagent (HA).

- Delineates the exchanges between the MN, FA and HA that facilitate seamless roaming in layer 3 and above. Also argument the functionality of an existing standard, ICMP, router discovery messages, and extends it to define a mobility agent advertisement extension that enables the nodes to advertise their availability to provide the foreign agent services in a manner similar to RFC 1256 provisions for the advertisement of routers.

The home address, which is the IP address assigned to a mobile node by its controlling provider, is assigned in much the same way as some ISP give a subscriber a fixed class C address. This address, which can be assigned dynamically, is the source address value in the IP header of outgoing packets. Because the network prefix is the same as that of network assigned to the controlling provider, this address will probably be topologically incorrect when the mobile node roams into a new network. The care-of address functions as an indirect pointer to the mobile node. It represents the topologically correct and reachable IP address that corresponds to the mobile node's correct network attachment, so that the home agent can tunnel packets to it. The care-of address can be located

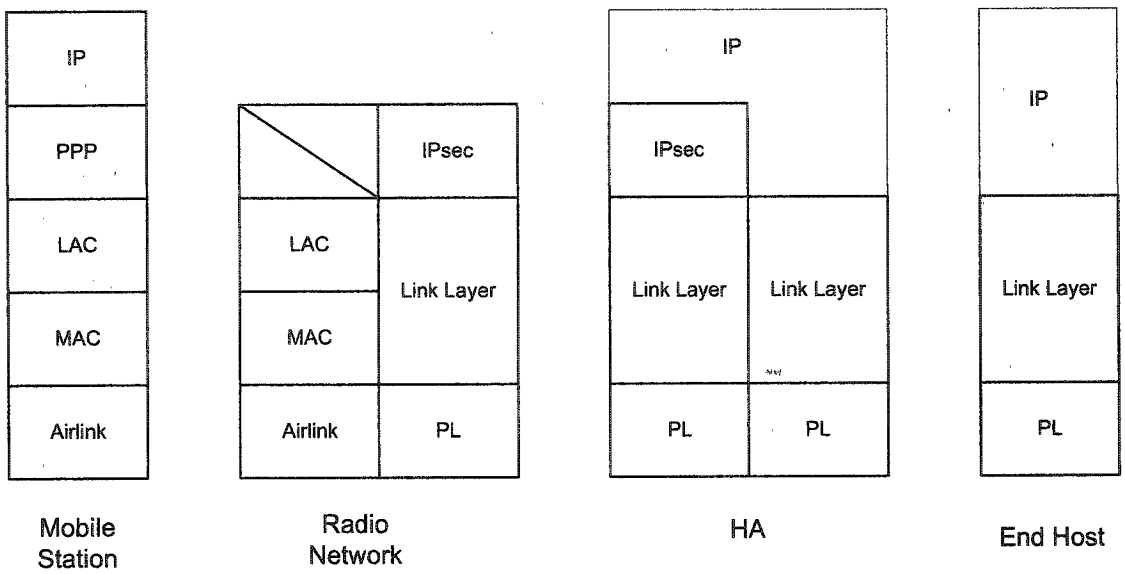

Figure 4.3 Protocol Reference Model for Mobile IP User Data

- In the foreign agent
- In mobile node itself

In Figure 4.3, the PPP layer in the mobile station stack is only for the MS in CMDA2000 network. The COA is located Radio Network of the protocol reference model. And physically it could be colocated with MS or separatedly with Radio access network. The foreign agent is the critical entity in the visited network, making the mobility service available to the roaming mobile node. It is also one endpoint of the HA-FA tunnel that is created when mobile nodes successful register with its home agent for mobile IP service. This might be IP-IP generic routing encapsulation (GRE), or minimal encapsulation tunnel. The foreign agent advertise its availability for service when mobile node roams into its network and accepts, processes and forwards a mobile node registration request to the home agent [26]. The foreign agent also accepts, processes and forwards registration replies from the home agent. The home agent, which is the other end-point of HA-FA

tunnel, is responsible for attracting traffic destined for the mobile node (based on the network prefix) and for tunneling it to the care-of address associated with a given mobile node for further delivery to the mobile node.

During the time, the local AAA find it belongs to the remote area, it will sends request to HOME AAA to check the mobility right of MN. Upon getting answer from MN's home IP network, it will forward the message whatever is accepted or rejected to HA. The message between HA and Radius may be protected by IP security. Then the connection is setup.

The position of home agent in attracting and tunneling traffic to the mobile node give rise to inefficiencies in routing of traffic. If the roaming mobile node and a peer node are geographically very close to each other, packets from the peer to mobile node must still travel through the additional hops.

4.2 WLAN-GPRS Inter-working

WLAN was originally considered to be a competitor to cellular mobile systems, but the industry has realized that the two technologies can be integrated to provide both enhanced services to the user and increased business potential for the provider. The complement happens as the characteristic of the different radio access as showed in table 4.2:

Wireless LAN	GPRS
Small coverage size (maximum 400~500m)	Large coverage (up to 20~30 km)
High speed (up to 54 Mbps raw data in 802.11a)	Low speed (up to 8*21Kpbs in GPRS)
Cheap base station	Expensive Base Station
Easy to maintain	Hard to maintain
Easy to installation	Much more difficult to install

Table 4.2 Characteristic of WLAN and GPRS

So for the indoor environment and hotspot area, the Wireless LAN access technology providers a perfect broadband complement for the existing GSM and GPRS services.

4.2.1 Interworking Scenarios

Six 3GPP - WLAN interworking scenarios are proposed by ETSI [12]. Each scenario realises an additional step in integrating WLAN in the 3GPP service offering and naturally includes the previous level of integration of the previous scenario.

3GPP -WLAN interworking scenarios may be considered with the aid of the simplified reference diagram in figure 4.4. This reference diagram illustrates the elements of the GPRS system and WLANs being interworked.

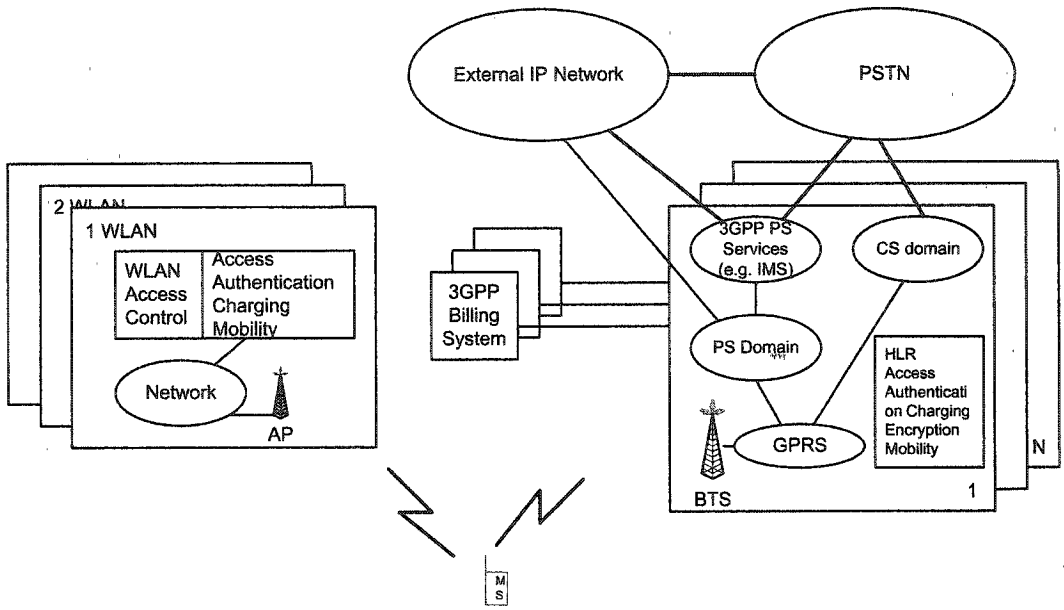

Figure 4.4 GPRS-WLAN simplied Reference Model

Scenario 1 - Common Billing and Customer Care

This is the simplest scheme of 3GPP -WLAN interworking. The connection between the WLAN and the GPRS system is that there is a single customer relationship. The customer receives one bill from the mobile operator for the usage of both 3GPP and WLAN services. Integrated Customer Care allows for a simplified service offering from both the operator and the subscriber's perspective. The security level of the two systems may be independent.

This scenario does not pose any new requirements on 3GPP specifications.

Scenario 2 – GPRS system based Access Control and Charging

This is the scenario where authentication, authorization and accounting are provided by the GPRS system. The security level of these functions applied to WLAN is in line with that of the GPRS system. This ensures that the user does not see significant difference in the way access is granted. This may also provide means for the operator to charge access

in a consistent manner over the two platforms. Reusing the GPRS system access control principles allows for additional benefits seen from a user and GPRS system operator standpoint.

First, the GPRS system operator may easily allow subscribers within his existing GPRS system customer base to access the WLAN with a minimum effort both for the subscriber and the operator.

In addition, the maintenance of the subscriber may also be simplified. No requirements are put upon the set of services to be offered in the WLAN part beyond those inherently offered by being addressable in an IP network.

Scenario 3: Access to GPRS system PS based services

The goal of this scenario is to allow the operator to extend GPRS system PS based services to the WLAN. These services may include, for example, APNs, IMS based services, location based services, instant messaging, presence based services, MBMS and any service that is built upon the combination of several of these.

Even though this scenario allows access to all services, it is an implementation question whether only a subset of the services is actually provided.

However, service continuity between the 3GPP system part and the WLAN part is not required.

Scenario 4: Service Continuity

The goal of this scenario is to allow the services supported in Scenario 3 to survive a change of access between WLAN and GPRS systems. The change of access may be noticeable to the user, but there will be no need for the user/UE to re-establish the service. There may be a change in service quality as a consequence of the transition

between systems due to the varying capabilities and characteristics of the access technologies and their associated networks. It is also possible that some services may not survive, as the continuing network may not support an equivalent service.

The criteria and decision mechanism for change of access network is under investigation.

Change in service quality may be a consequence of mobility between radio access technologies, due to varying capabilities and characteristics of radio access technologies.

Scenario 5: Seamless services

The goal of this scenario is to provide seamless service continuity, as defined in [30], between the access technologies, for the services supported in Scenario 3.

By seamless service continuity is meant minimizing aspects such as data loss and break time during the switch between access technologies.

Scenario 6: Access to GPRS CS Services

This scenario allows access to services provided by the entities of the GPRS Circuit Switched Core Network over WLAN. This scenario does not imply any circuit-switched type of characteristics to be included into WLAN.

It shall be possible to provide a technical implementation that would allow:

- Access to services provided by the 3GPP CS core network entities over WLAN interface.

- Seamless and user-transparent switching between access technologies for a connection carrying service provided by the entities of GPRS CS core network

To summarize the six interworking scenarios, see the table 4.3:

Service and Operational capacities	Scenario 1: Common Billing and Customer Care	Scenario 2: 3GPP System based Access control and Charging	Scenario 3: Access to 3GPP system PS based service	Scenario 4: Service continuity	Scenario 5: Seamless Service	Scenario 6: Access to 3GPP system CS based service
Comon Billing	x	x	x	x	x	x
Common customer care	x	x	x	x	x	x
3GPP system based Access Control		x	x	x	x	x
3GPP based Access Charge		x	x	x		x
Access to 3GPP system PS based sevice from WLAN			x	x	x	x
Service Continuity				x	x	x
Seamless Service Contimuity					x	x
Access to 3GPP system CS based sevice with seamless mobility						x

Table 4.3 3GPP Scenarios for interworking WLAN

In this research, the scenario 1 and scenario 2 are studied. The new interworking scheme is introduced to achieve the integrated authentication, integrated billing, roaming capacity, terminal mobility, and application reachability and the main effort is on the migration from scenario1 to scenario 2. To integrate those two scenarios together, especially the seamless roaming becomes a critical issue. The mobile IP [19] is the only option to keep the network layer reachability during the roaming.

4.2.2 Inter-working Architectures

Several approaches have been proposed for the inter-working between WLANs and cellular networks. The ETSI specifies in two generic approaches for inter-working – the loose coupling and tight coupling [31]. The fundamental difference is on the point of interconnection of 3GPP and WLAN system. With the loose coupling the WLAN is deployed as access network or called external PDN network complementary to the GPRS core network. In this case the WLAN utilizes the subscriber databases in GPRS network but no data interface to the GPRS core network. Considering the simplified GPRS reference diagram Figure 3.2, we could get the conclusion that the loose coupling between GPRS and WLAN is carried out at the Gi interface point. This means that with the loose coupling the WLAN by passes the GPRS network and provides direct data access to the external Packet Data Networks.

On the other hand, the tight coupling is connected to the GPRS core network, the same as GPRS Radio Area Network (RAN), which is referred to the Gb interface (Figure 3.2). In this case, WLAN traffic goes through the GPRS core network before reaching the external PDN.

Currently, the short-term is to follow the loose coupling approach and user SIM-based authentication and billing. With this approach, a subscriber can re-use his Subscriber Identity Module (SIM) card to access a set of wireless data service over WLAN. And the Operator can protect the GPRS network investment.

The above subtle difference in the point of interconnection leads to significant differences between the overall system architecture, operation and characteristics. It will be shown later that the throughput and latency will impact with the different coupled system.

Loose Coupling

When loose coupling is implemented, which is the inter-working scenario 1 and only the GPRS authentication, billing and service could be re-used as showed in Figure 4.5 [31], the session continuity is the critical issue because of IP layer's change mobility change. Also loose coupling could be the most possible scenario in the beginning of WLAN deployment, as the joint force for WLAN could be the best option to speed up the coverage and service.

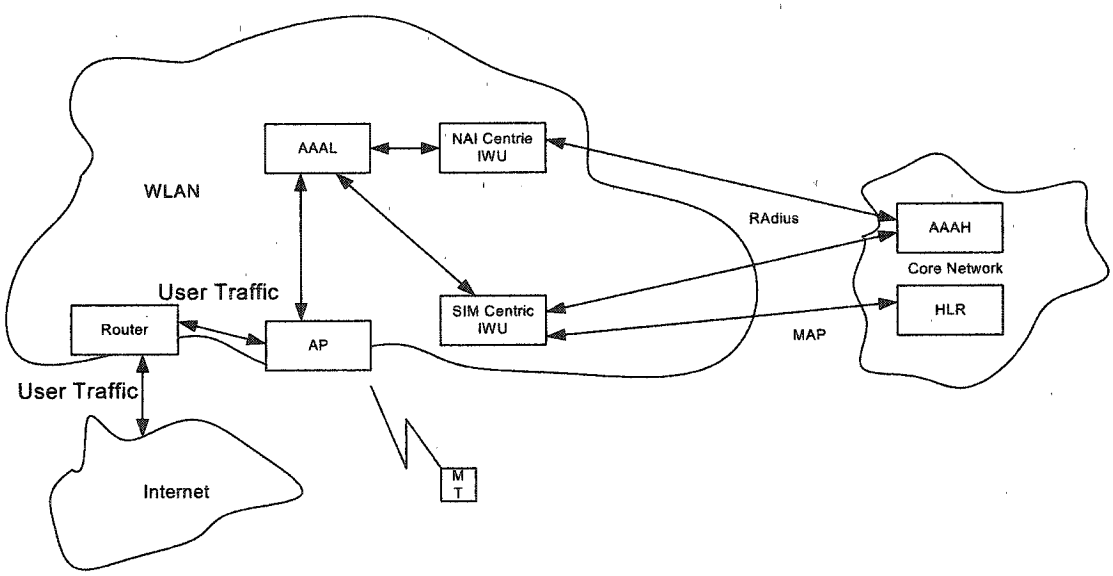

Figure 4.5 Loose Coupling Architecture

Based on this reason, 3GPP technical specification [33] determines Mobile IP can be optionally supported to provide mobility management for inter-system roaming in network layer. To enable Mobile IP service, a home agent (HA) is required so that datagram could be tunneled to the proper destination.

However, the location of HA is not defined in the specification. The HA and FA in Figure 4.6 are the logical entities. The actual HA node could be collocated physically with one of GGSN and FA could be collocated physically with the MS.

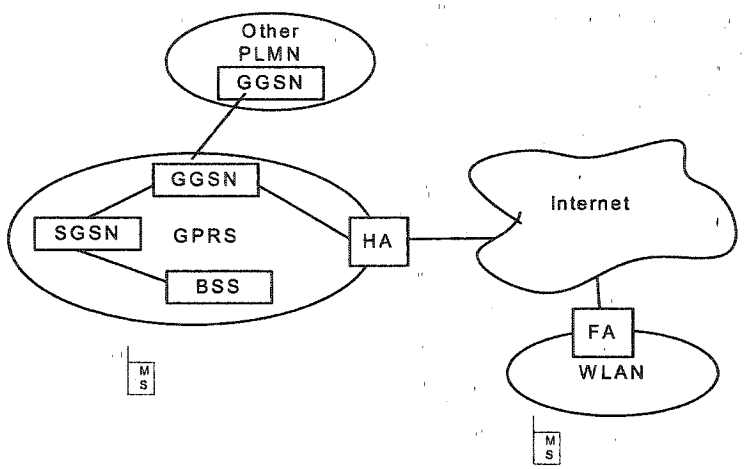

Figure 4.6 GPRS and Mobile IP in the Loose Coupling Network

As all the signalling of MIP call (registration and de-regrestration messages) and MIP traffic need to pass the HA, HA is the perfect entity to have the authentication and accounting clients inside, which means the authentication and accounting request will be generated by HA as needed. To manage the roaming mobility and to achieve the integrated authenitcation and accounting information, the HA need to work closely with the existing GPRS authenitcation and accounting system. So logically, one side of HA must be connected to the GPRS core network to deal with all authentications, accounting requests and MIP signalling and traffic from GPRS side, the other side of HA must be connected to the Internet for the MIP signalling and traffic from AP side. In GPRS network, there is no specification for the FA function available. So the MS needs to have the collocated FA function described in section 4.1 to achieve the seamless roaming. To have the consistence behaviors, we assume the MS will use collocated FA mode even it is in the AP coverage.

To identitfy the request of Mobile IP or general packet data service, the access point name is a basis to select a specific network service. Figure 4.7 displays the PDP context activation with MIP registration procedure in GPRS network. The Mobile IP registration

will be performed after the completion of the PDP context activation. The packets sent to MS's home IP address will be intercepted by HA. Since MS is in the GPRS network, the tunnel of the datagram is built between HA and FA, where is FA is collocated in the MS. HA decapsulates the packets and then GGSN will transmit datagram based on GTP tunneling to the suitable SGSN. The datagram is transmitted depending on two types of tunneling, the tunnel path from HA to FA is responsible for packet data network, and the tunnel between SGSN and GGSN operates in the GPRS core network. Mobility management is a primary task for this integration of heterogeneous networks.

When the user is in WLANs area, the MS first will get one IP address from WLAN network and uses that one as the Care-of-address to send Registration Request to HA through WLAN. After the registration is passed, the binding is created in HA where the current location (care-of-address) is linked. And the MS get assigned IP address from HA or with its static IP [19], which is unique wherever it will be in any WLAN area. In this case, any packet sent from Correspondent Node (CN) to MS will reach HA and HA will tunnel to MS through the HA-FA tunnel. When the packet send out from MS, the packets will first reach the HA through HA-FA tunnel and the HA will send out to the destination.

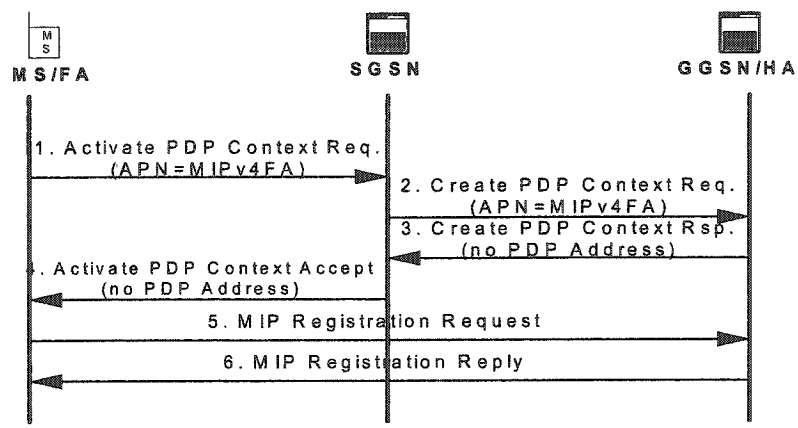

Figure 4.7 PDP context activation with MIP registration

When the user is in the GPRS area, the MS will get one IP address from GPRS network and uses that one as the Care-of –address to send the MIP Registration Request through the GTP tunnel. After the registration processed, in HA the binding is created and the care-of-address is written in the binding table. So whenever there is packet to MS, the HA will know where to send through the GTP tunnel to the Care-of-address. For the loose coupling, the MS must equip with WLAN-compatible radius interface and it needs to understand the protocol stacks of both systems as showed in the Figure 4.8. Figure 4.8(a) represents the user plant of GPRS, while the Figure 4.8(b) shows a conventional Internet protocol stack, in which Layers 1 and 2 are based on a WLAN system in MS side and IpinIP layer is typical MIP layer with reversal tunnel enabled. MS should still enable the GPRS interface such as the location update and paging even though packet transmission is through WLAN interface. SGSN thus still regards MS as reachable so that the high cost and longs latency for the reattaching when MS switches back to GPRS can be minimized. Besides, the circuit-switched network service is still available for the voice phone call. Basically they do not interfere with each other because of different radio frequency.

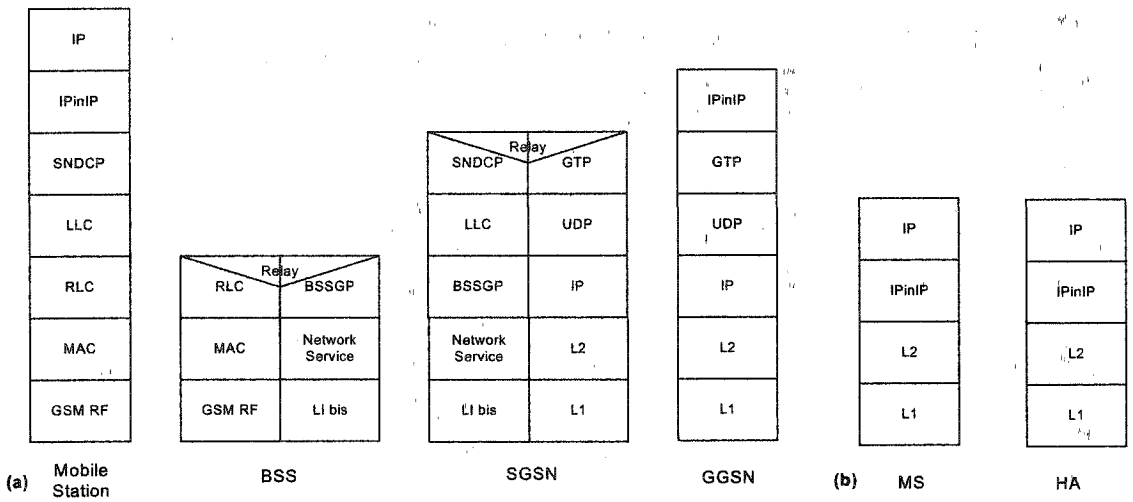

Figure 4.8 Dual protocol stacks in MS

Tight Coupling

When tight coupling is deployed, the common authentication, authorization and billing, as well as seamless service across the WLAN and GPRS network could be guaranteed. Depending on the WLAN technology, and in particular on whether the WLAN can support quality of service (QoS) equivalent to GPRS QoS specification, the proposed architecture might satisfy the requirements of scenario 5.

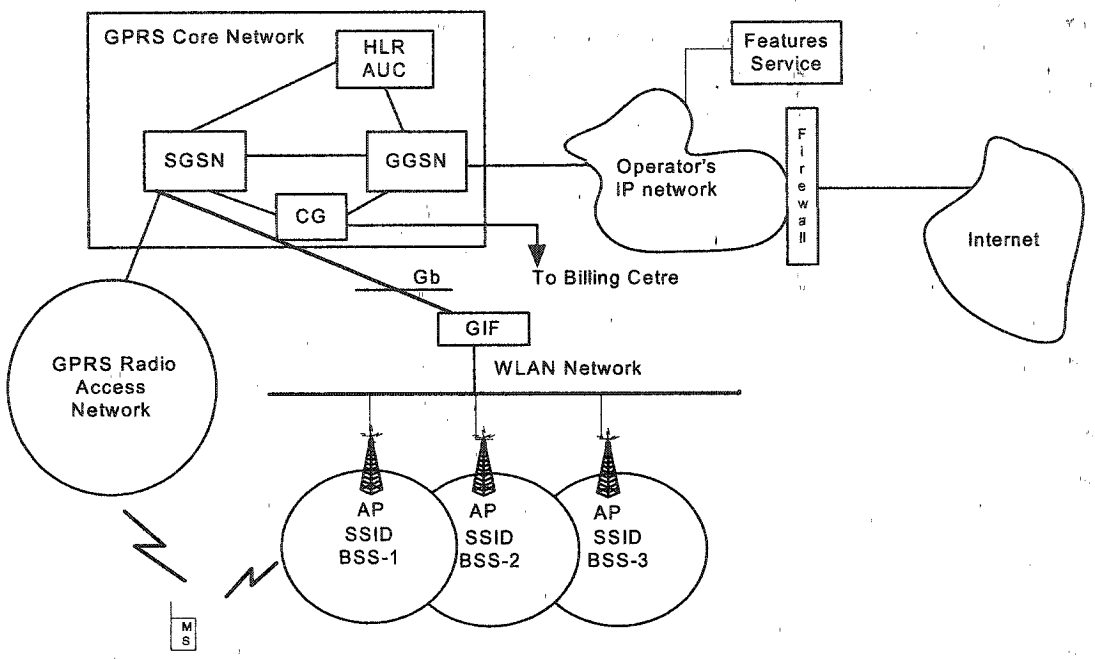

Figure 4.9 WLAN-GPRS integration with tight coupling

Figure 4.9 shows the proposed architecture of the tight coupling system. The WLAN is deployed in an infrastructure configuration, as another RAN and connects to the GPRS data network through the standard Gb interface. From the GPRS core network point of view, the WLAN is considered like any other GPRS routing area in the system. In other words, the GPRS core network does not really identify the difference between a normal routing (BSS) area and WLAN radio access.

The key aspects of tight coupling approach system are the following:

- MS is dual mode. It means the MS uses the same set of core network protocols but different radio access protocols with an additional adaptation function in the between, see Figure 4.10[31]. In the MS side, there is no change for the tight coupling and loose coupling system.

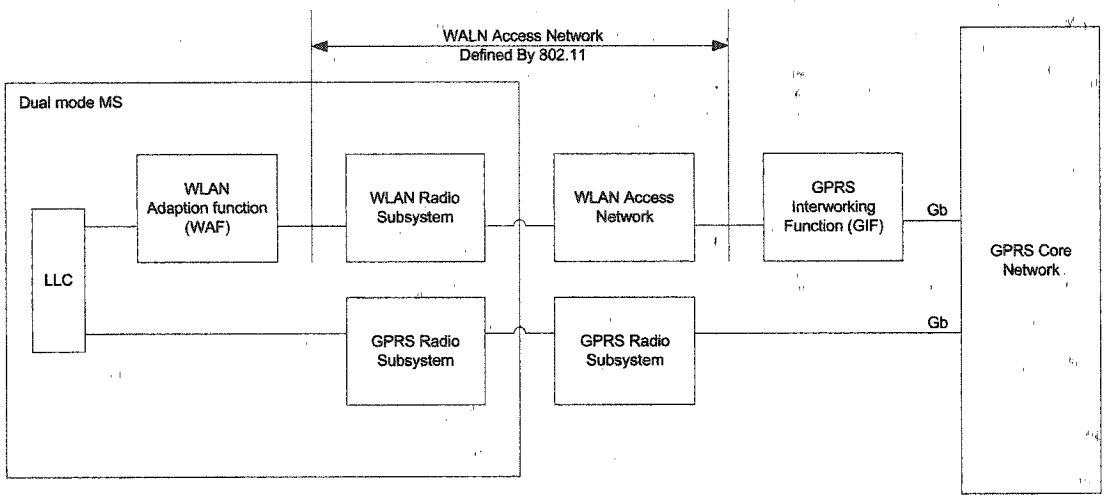

Figure 4.10 Tight coupling system Gb interface reference diagram

- The WLAN access network connects to the GPRS core network with the same interface as BSS of cellular systems. This also requires an inter-working adaptation function in the WLAN access network, GIF interface as showed in Figure 4.10 [31].
- The WLAN access network looks like a single routing area with a single cell to the GPRS packet data network. This requires that the WLAN access network is able to advertise its routing area.

As MSs are dual mode, which means they support both GPRS and WLAN access. The seamless mobility is achieved by means of RA update procedure, which is the core mobility management in GPRS. Typically, when a mobile enters a WLAN area, the RAU procedure takes place and subsequent GPRS signaling and user data transmission are carried over the WLAN interface. Similarly, when the mobile exits a WLAN area, another RAU procedure takes place and the GPRS interface is enabled and used to carry further data and signaling traffic. From the core network point of view, handover between WLAN and GPRS is considered as handover between the two individual cells.

Chapter 5 Hybrid Tight/Loose Network Simulation

This chapter presents the methodology used through this thesis and also presents the simulation results. By analyzing the results, some conclusions and issues will come out and those could be useful for other investigators for the further study of WLAN and GPRS inter-working. Also it will be similar for the study of WLAN and UMTS inter-working.

This chapter is organized in five sections. Section 5.1 introduces the simulation model and main variables of the "Hybrid Tight/Loose coupling network", which combines the tight/loose coupling and Mobile IP together to enable the seamless moving between the WLAN and GPRS network. Section 5.2 describes each part of the simulation, assumption and all the other variables in the program. Section 5.3 provides simulation flow chart, typical initial input data and explanation of the flowchart. Section 5.4 gives the typical simulation results and the condition and explanation of the results. Section 5.5 summarizes the research and issues for further work.

5.1 Simulation System Architecture

The main emphasis of this simulation is on the inter-working of WLAN and GPRS. As discussed in the Chapter 4, there are two kinds of inter-working models, loose coupling and tight coupling. To achieve seamless roaming in "Loose coupling network" between WLAN and GPRS, the Mobile IP (MIP) is mandatory where it could use the IP layer in the network level to gain seamless roaming. When the "Tight coupling" is deployed, the

seamless roaming between WLAN and GPRS is controlled by the GPRS network and WLAN need an adapter to connect to the Gb interface of GPRS core network. Of course, with the tight coupling network, the QoS could be imported as discussed in Chapter 4.2.

To be more general, the main theme of this thesis will present the "Hybrid Loose/Tight coupled network". This means some portions of WLAN are tightly coupled with GPRS network and the others are loosely coupled. In this case, to achieve seamless roaming, the Mobile IP (MIP) is needed across the whole network. The trade-off to have the MIP is more over-head (20 bytes of IP-in-IP tunnel) for the traffic when the user is in the tight coupling area than the user is having the normal GPRS data call.

Figure 5.1 shows the typical hybrid tight/loose coupling network. The AP connected to the SGSN directly is call tight coupling connection. The AP connected to GGSN/HA through the Internet is called loose coupling. In both cases, the authentication and billing system could be the same as they are proxyed to the home network, see the connection between the AAA and HLR.

The ratio "r" represents the percentage of Tight coupling WLAN in the network and then "1-r" is the percentage of loose coupling WLAN in the network. "r" could be "0", which means a whole "Loose coupled network", "r" could be "1", which means a whole "Tight Coupled network". The coverage of AP and BTS is independent with each other and it is represented by WLAN/GPRS base station existing probability representatively. So there will be overlaped area of AP and BTS coverage and none covered area by both AP and BTS depended on the probability.

Figure 5.2 shows the FA enabled dual mode terminal stack. In the tight coupling case, the MN's care-of-address will not be changed as the GPRS network keep the mobility

management. So in this case, the MIP layer is another overhead to normal GPRS packet for the user traffic. But it enables seamless hand-over between tight coupling and loose coupling network. And the user could have unchanged IP address and high speed even out of GPRS network area but maintain the common billing and authentication.

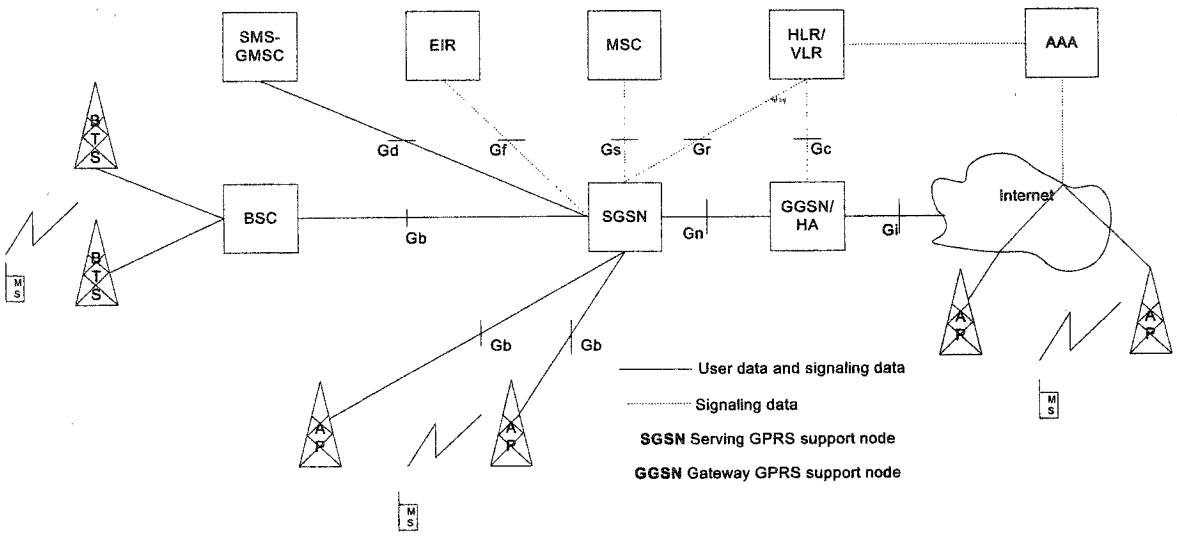

Figure 5.1 Hybrid tight/loose coupling network

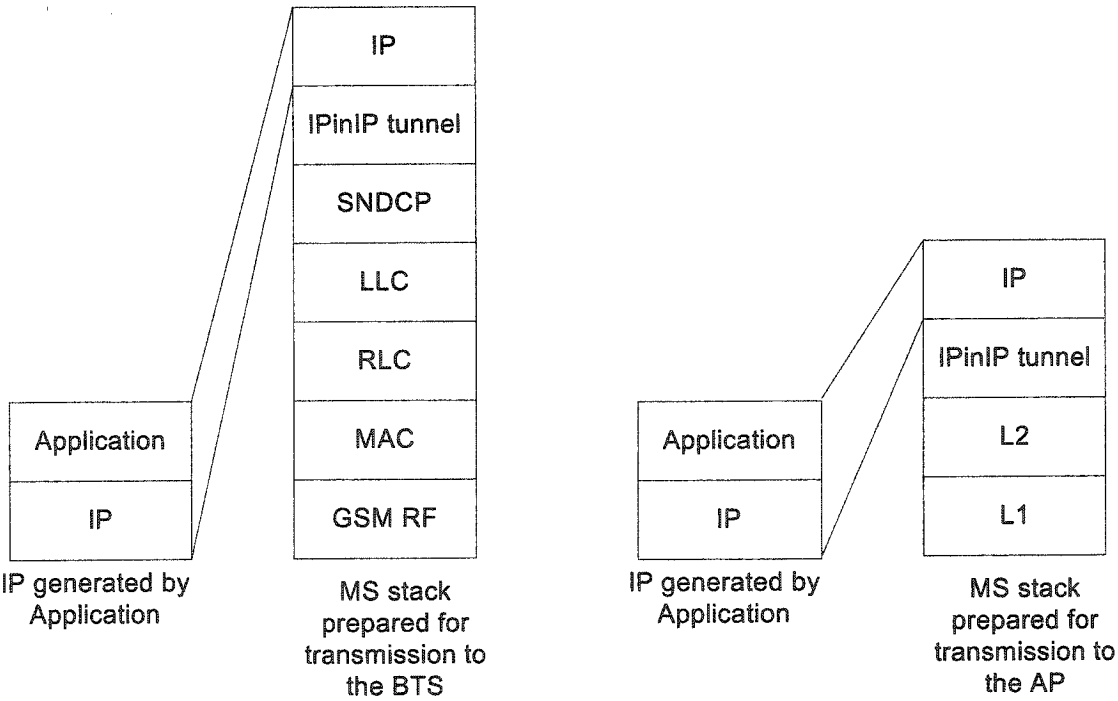

Figure 5.2 MS user data dual IP stack for the BTS and AP

5.2 Simulation Description

This system level simulation, based on the above theory discussed, gives the end-to-end system performance such as the throughput, latency. The end-to-end means from one mobile node to another mobile node, the mobile node either connects to GPRS network or to WLAN network or neither. The network in this simulation has certain size and all the simulation must be within this scope. By modeling comprehensively GPRS and WLAN network data transaction as described below, we achieve the performance results. In this simulation, the following assumptions are made:

- To simplify the performance measurement, the user either sends packet or receives packet and the user's behavior will not change during the whole simulation period.
- To remove the constant variable in the simulation, in this thesis, only IP packet is considered, the physical layer and all the other layers are not counted in the simualtion.
- The packets sent from users are considered to be the UDP packet, which means it will be one-way traffic and there is no ACK from the receiver.
- The packet size in the simulation is just considered to be the RAW size of packet including the IP/UDP and IP tunnel overhead for MIP traffic that are the parts generated by application and excluding the physical layer, link layer which are the parts for adapting the air environment.
- The session setup and authentication time are not simulated and they are ignored. As in this thesis, the performance of traffic is the main focus and the session setup and

authentication are the signal parts. So without signal parts, the results will be more clear.

- For the initial input data "delays for each hop", in this thesis the value is picked without verifying with "real world" and also not consider any difference when the node is under light traffic and the node under heavy traffic. So the latency results will show the ideal situation and in the "real world" the latency results with heavy traffic will be worse.
- For the latency, as this thesis is network level simualtion, the packet delays in the radio link is not considered. In the "real world", the radio link delay might longer than the network side. But the simulation results still make sense to the time sensitive packets like VoIP application. As any latency achievement will be greate for the quality.

5.2.1 Simulation Coverage

This simulation is limited to a certain assumed coverage area, which is covered by WLAN and GPRS network. The area is considered it as a square or rectangle. So the area could be described as: A (meter) x B (meter), where A and B are the length of input variable.

To simplify the simulation, the AP and BS coverage areas are considered to be square shaped, where the AP is basic transmitter/receiver component in WLAN and BS is the counterpart in GPRS network. The coverage area shape does not affect the simulation result for the WLAN and GPRS inter-working, also in this way the handoff is simplified.

Typical values used in the simulation are:

- Simulate area: 5000 Meter x 5000 Meter. The area will be divided automatically by the numbers of AP and BS.
- AP coverage: 400 (Meter) x 400(Meter)
- BS coverage: 800(Meter) x 800(Meter). In this simulation, always give the numbers of AP coverage.

So the whole simulation area could be divided into sub-area of AP coverage, where AP/BS may and may not have the coverage, as implied by the AP/BS probability of existence. These probabilities are obtained from the list of input parameters and these values will be fixed for one iteration. The following are some of the typical values used in the simulation:

- Pap: Probability of AP existence, 0, 0.05, 0.1, …, 0.85, 0.9, 0.95, 1
  All APs follow the U(0,1) uniform distribution.
  If X=U(0,1)<Pap, implies AP existence.
- Pbs: Probability of BS existence: 0.9, 1
  All BSs follow the U(0,1) uniform distribution.
  If X=U(0,1)<Pbs, implies BS existence

In each iteration, only one value of Pap and Pbs will be used. In the next iteration, the AP/BS existence probability might increase depending on the simulation scenario. In the thesis, two scenarioes are considered, the loose/tight coupling ratio with fixed AP/BS existence probability and the AP existence probability with fixed loose/tight coupling.

5.2.2 Network Simulation

Figure 5.1 shows the typical WLAN-GPRS inter-working network. To simulate this network, the following variables need to be identified:

- HA

  In this simulation, only one HA is expected and this HA is assumed to be associated with the first GGSN.

- GGSN and SGSN

  The number of GGSNs and SGSNs and connections need to be defined. In this simulation, the maximum possible number of SGSNs and GGSNs is 4 each. The existence probability is Pgsn = 0.5. And the existence follows the uniform distribution U(0,1).

  So the number of SGSN and GGSN in the network is determined by the following:

  SGSN: If U(0,1) < Psgsn, SGSN exists, repeat 4 times for all the SGSNs. And mark it as SGSN (N) if it exists. At least, there will be one SGSN.

  GGSN: If U(0,1) < Pggsn, GGSN existing, repeat 4 times for all the GGSNs. And mark it as GGSN(M) if it exists. At least there will be one existing. And normally N >= M.

  The link GGSN (M)—SGSN (N): If U(0,1) <= 1/N, then GGSN(M) is connected to SGSN(N). Loop N times for each M if N is not connected. Make sure the GGSN1 is always connected to one of SGSNs and all the SGSN are connected to one of GGSNs.

  Assume the GGSNs are connected to each other directly and form a mash network.

- AP and BS

The BS needs to connect the one of the SGSNs. And when AP is in the tight coupling configuration with GPRS network, it needs to connect to SGSN also.

In this simulation, the interconnection of one SGSN to each AP/BS is assumed to follow uniform distribution. If the SGSN random value U(0,1)<=1/N, then that SGSN is connected to the particular AP/BS. If not, the program goes to the next SGSN and recalculate the U(0,1) until the AP/BS is connected to one of the SGSNs. The program loops upon the number of BSs and number of tight coupling APs times to get each one of them to be connected to one of the SGSNs.

- Tight/Loose coupling

Assume the tight/loose rate is R, this initial value is obtained from the input program file and may increase by a certain step automaticly in the program, according to the simulation scenario described in 5.2.1. In this simulation, all the APs follow uniform distribution for loose/tight couple. The AP's tight/loose coupling attribute is defined as follows:

Loose coupled AP: If X = U(0,1) > R, marked it as loosely coupled AP

Tight coupled AP: If X = U(0,1) <= R, marked it as tightly coupled AP

All the tightly coupled APs and BSs are connected to the SGSNs directly. The loosely coupled APs are connected to the IP network directly.

When loose coupling is used by AP, the hops between AP to the HA will be allocated randomly to reflect the spirt and diversified nature of world wide Internet. Assume the maximum hops will be 20 (from input data) and also the numbers of hops will

follow the uniform distribution, the actual hops will be generated randomly in uniform range {1,20}.

In this simulation, the program generates a descriptor to show the status and connectivities of all the nodes, AP, BS, SGSN and GGSN. This descriptor is based on location. As described in section 5.2.1, the simulation area is divided into sub-area of AP coverage area. And each descriptor is connected to one sub-area. See the following example of descriptor:

[AP, BS, LT, SGSN, GGSN]

If AP=0, AP does not exist. Otherwise AP=1.

If BS=0, BS does not exist. Otherwise BS=1.

If LT=0, this AP is connected to the Internet. Otherwise this AP is connected to the GRPS core network, tightly coupled to the GPRS.

SGSN=N, indicates the AP/BS in this location is connected to N's SGSN.

GGSN=M, indicateds that the N's SGSN is connected to M's GGSN.

So from the set of desciptors, the initial network topology will be formed and also connections between AP/BS—SGSN—GGSN could be seen. The tight/loose ratio of AP coonection is similarly defined with the descriptor.

5.2.3 Simulation of Users Info

The user information simulation part includes simulating user moving around in the coverage area, the user sending or receiving packets, etc.

The numbers of users will stem from input file. And in this simulation, 300 users are simulated.

Initial position of all users are scattered all over the area. Assume the initial position of users will follow the uniform distribution from 0-L in length and width respectively. L is one side of the square corner area, which should be a mutiple of BS coverage length. Loop over number of users, and then get all users initial position.

The users will keep on moving as in the real mobile world. The direction is randomly selected and it will be kept until the mobile hits the border of area then the moving direction will be re-generated randomly. During all the simulation there will be no user increase and decrease in the area.

The speed range is read from input file. And we assume each user's moving speed follows the uniform distribution. Then the user's moving speed could be generated within that range. The user's moving speed will be re-generated after every NxTi. N is obtained from the input data and Ti is the snapshot interval during the simulation that is equivelent to transmit one packet time to AP.

The followings are the examples of simulation.

The user moving speed: $Vi = 10KM — 100KM$, means $Vi = 2.8m/s—28m/s$

The user moving direction: $\theta = \{0, 2\pi\}$

The user's new position: $Xi = Xi + Vi*Ti*\cos\theta$

$Yi = Yi + Vi*Ti*\sin\theta$

Ti: Time interval for every snapshot.

Because the user can have higher data rate to the AP than to the BS, the packet time, which is also called snapshot intrval, should be calculted according to the transmission speed in the AP as per the following example:

Assume that the AP supports 1Mbits/s in radio link and the packet size is 1500 bytes. Then we can get one packet time Ti and this is the snapshot time for the simulation.

For example, Ti=1500*8/1,000,000=0.012s

Every 10 snapshots, the uses will change his data rate according to a uniform distribution within the range of 0-1Mbits.

For user location, we can get the moving distance in each Ti in the speed range of 2.8m/s-28m/s:

$\Delta D = (2.8, 28) * Ti = (0.033, 0.33)$

In this simulation, each user will experience three states which are power-off, on-line, active (sending or receiving data). In Power-off state, the users are not reachable. In on-line state, the user will go in active state either actively sending or actively receiving and their state for the sending and receiving state will be kept until the end of simulation.

Initially all the users are in power-off state. As simulation goes, more and more users will be power-on and go to on-line state. The value to be on-line is either 1 or 0, which indicates the user is on-line or not. The user on-line behavior follows the uniform distribution. The on-line probability is read from input file. If the uniform random value is less than on-line probability, then the user will be on-line. Looping for all the power-off users in each Ti, all the users on-line state will be updated.

To be on-line, the user need to request to the HLR for data service. If the user has right identification, the request will get accepted. In this simulation, the users always have the right identification. There is no rejected call in this simulation. All users use SIM card based authentication in both GPRS and WLAN network. The EAP-SIM protocol is used when the user is in WLAN loose coupling area for the authentication. So it is practical to

assume all the authenitcation will be successful. And in this simulation, the authentication time is omited as it does not impact the performance of network and the call setup rate is out of this thesis scope.

The probability from on-line to active sender state is read from input file and it follows a uniform distribution. When the generated uniform random value is less than state change probability, then the user will start to send the UDP data to the receiver. The receiver is randomly selected from the on-line users so as to generate unique send/receiver pair. Assume there is no mutiple connection for one receiver. Once the selection is made, it will remain until the end of the simulation. That means the sender will always the sender and receiver will be always the receiver. Also the one-one connections will be kept until the end of simulation.

In active state, the user could be either a sender or a receiver. As a sender, it needs to see if there is data in its buffer to send. Also it needs to generate data and put to the sender's buffer. The probability of data generation is used to control if need to put data to buffer. When the uniform random value generates a value that is less than the data generation probability, the sender will be in active state. The active sender will generate a number of traffic bits, the traffic is within the uniform range read form input and it need to re-from within the range for every 10 snapshot according the uniform distribution. Sending will be held when the user buffer is full.

In this simulation, the matrix userinfo (I) (xi, yi, vi, generating call or not, send data or not, send data speed, destination user, sender buffer size used, packets sending out from the sender buffer, packets received, duration summary) is used to describe the activities of a user.

The initial user information will be read from the file and put into a userinfo matrix. Also this matrix is dynamicly changed in each Ti especailly the sending packets and receiving packets are collected and accumulated in the buffer.

5.2.4 Handoff and Traffic Pofile Consideration

As discussed above, the coverage of GPRS and WLAN will be overlapped. In this simulation, the coverage and overlap are controlled by AP and BS existing probabilities. And those are read from the input data file.

When the user is in the overlap area, as discussed in Chapter 4.2, the MN has dual stack and can sense the existence of the dual system. As normally in data communication, the Mobile Node (MN) will select automaticly the system according to the bandwidth and cost. So in case of co-existence WLAN and GPRS coverage, the MN will always connect with the WLAN for the better data rate and lower cost.

When the user is moving from one AP/BS to the other, in this simulation, the MIP is enabled and the MIP re-regestigation process time is igored. So the session could be considered seamless and the transmitter and reception could be considered continuous. The only impact considered is when the user moves from tight coupling to loose coupling or vice versa. For each packet, even it travels the same hop; the time it costs will be randomly different. In this simulation, the range of latency for each hop is obtained from the input file and such latency will follow a uniform random distribution. So the latency for each hop is randomly generated within a given range.

5.3 Simulation Flow Chart and Initial Input Data

In this simulation, all the initial data is read from file as shown in table5.1:

5000	Length of the overallsite coverage in meter	input(0)
5000	Width of the overall site coverage in meter	input(1)
400	Side of AP coverage lenth in meter	input(2)
400	Side of AP coverage width in meter	input(3)
2	BTS coverage in number of AP (in length and width)	input(4)
0	Probability of AP existence	input(5)
1	Probability of BTS existence	input(6)
0.5	Tight/loose probability for the APs	input(7)
4	Number of SGSN	input(8)
0.5	Psgsn, existing probability for each SGSN	input(9)
4	Number of GGSN	input(10)
0.5	Pggsn, existing probability for each GGSN	input(11)
3000	Maximum number of users	input(12)
2.8	Speed of 10KM/h in meter/s	input(13)
28	Speed of 100KM/h in meter/s	input(14)
1000000	Data rate in AP side B/S	input(15)
1500	Data size in AP/BTS side Bytes/packet	input(16)
0.5	Call generation Probability	input(17)
0.2	Send data probability	input(18)
1000000	Data generated rate Bits/S	input(19)
512000	Buffer size of the user sender (byte)	input(20)
0.2	Packet loss rate in the wireless link	input(21)
20	Maximum number of hops in case of loose couple	input(22)
3	Maximum delays for each hop in unit of Ti	input(23)
0.1	Data generation probability	input(24)
60000	Datarate in BTS Bits/S	input(25)
32000	Buffer size of the receiver in the AP/BTS (Byte)	input(26)
300	No of users in the network	input(27)
40	Threshold for packet loss in units of Ti	input(28)

Table 5.1 Initial Input Data Table

From the above table, we can see that the BS will have 100% coverage and there is no AP coverage at all from the initial input data. In the program, the AP existing probability will increase by step of 0.05 each iteration until it reaches the 100% of coverage. Also by simply fixing the AP existing probability and changing the tight/loose ratio every 0.05 step, we can get another set of simulation results.

The program flowchart is shown in Figures:

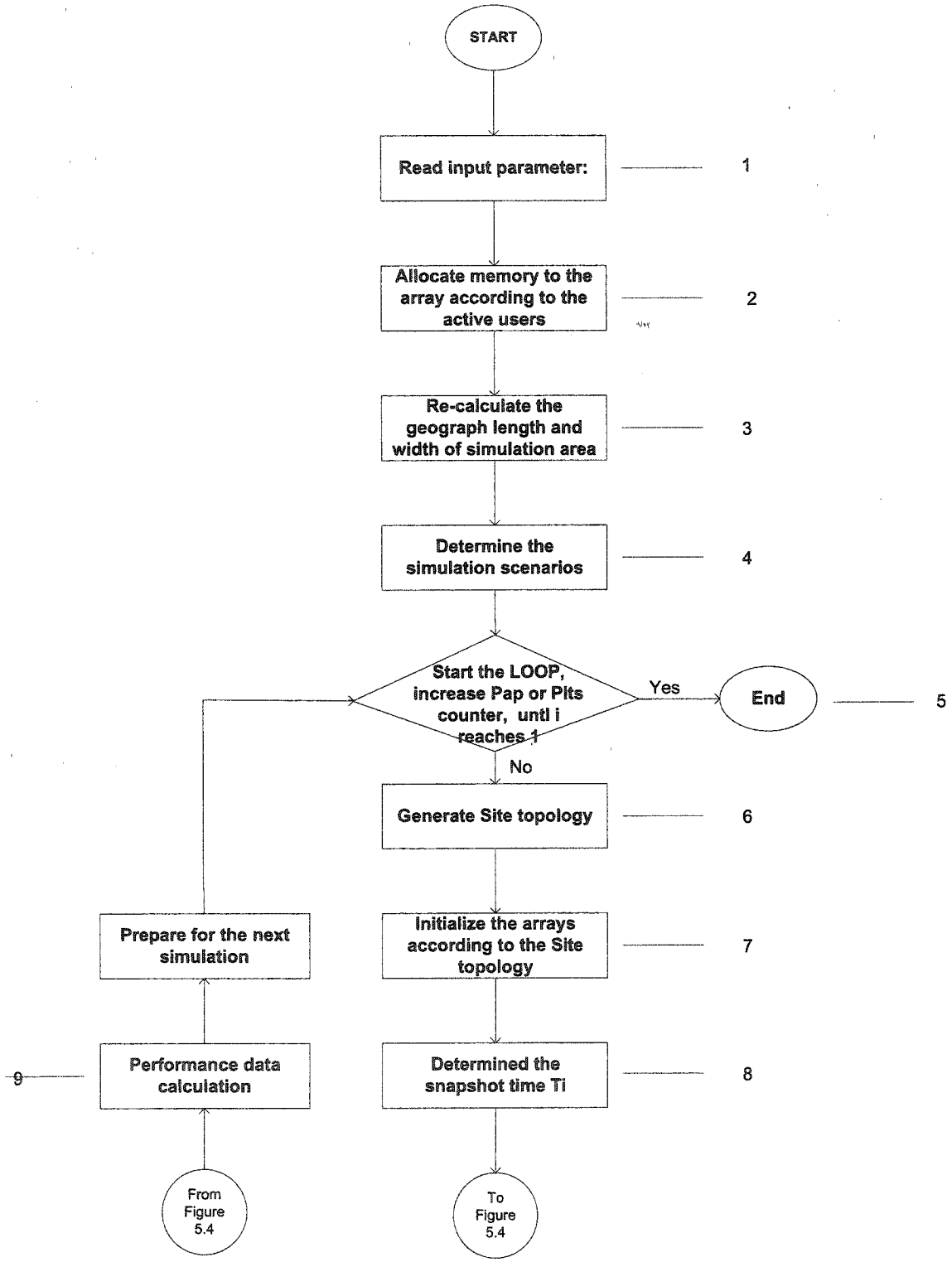

Figure 5.3 Flowchart for the Main Program

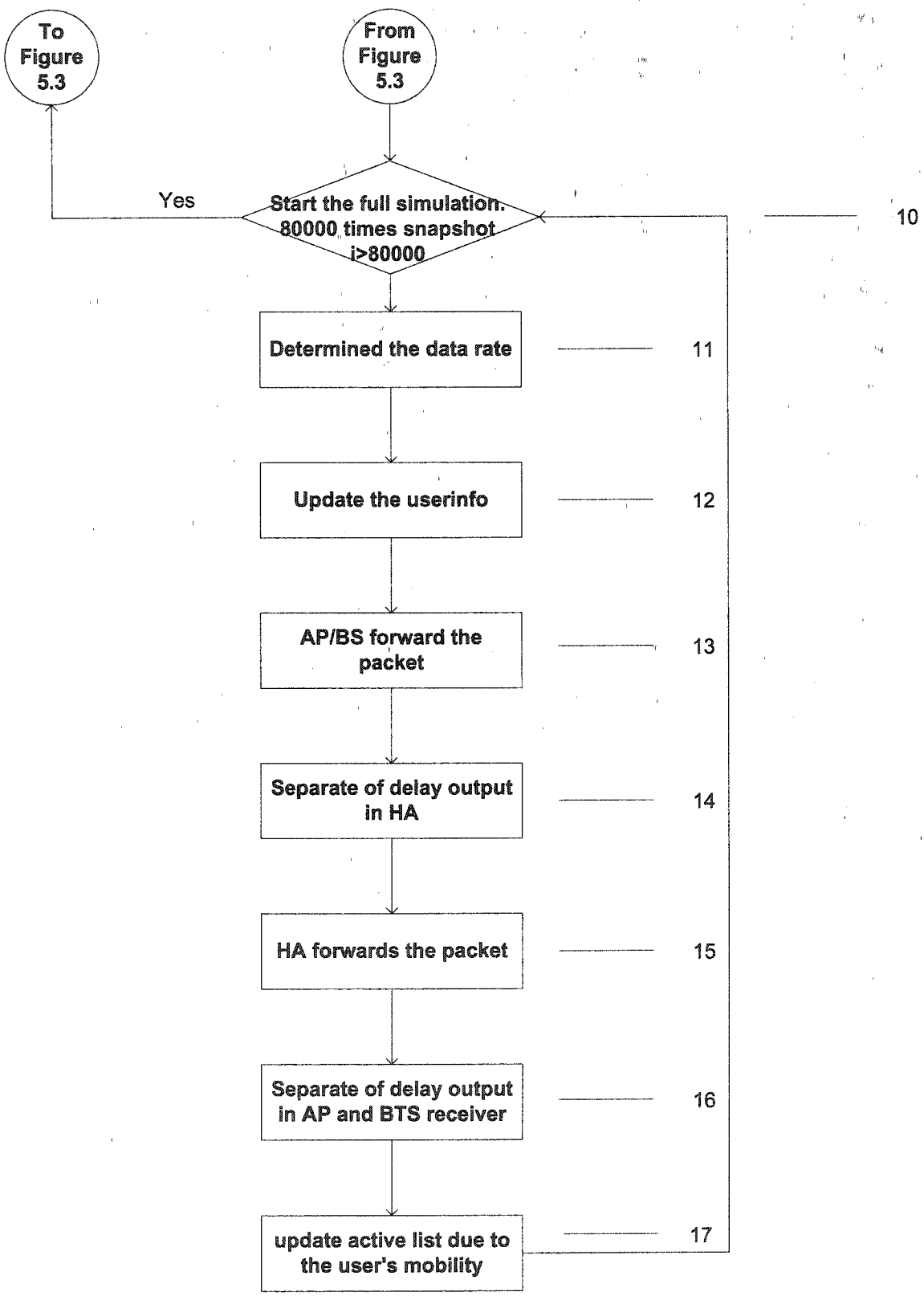

Figure 5.4 Continuance for the main program

The following for details of each blocks of the general flowchart in Figure 5.3, 5.4:

1. Read input parameter:

   Get Site size (AP, BS, Simulation area), probability of Loose/tight couple, AP existence Probability, BS existence Probability, number of subscribers, etc. All information listed in Table5.1 for example will be read in the beginning of program.

2. Allocate memory to the array according to the active users:

   Initialize part of array HA[i]; userinfo[i], packet[i] according to i, i is the number of users in the simulation, read from initial input

3. Re-calculate the geograph length and width of the simulation area:

   Adjust the simulation gepgraph area size to the integer times of the AP coverage lengh and width.

4. Determine the simulation senarios:

   Read from the initial Input file and determine if this simulation is for the fixed AP existence probability and increasing tight/loose ratio or fixed tight/loose ratio and increasing AP existence probability.

5. Start the LOOP, increase Pap or Plt counter, until it reaches 1:

   Start the simulation with the initial Pap or Plts value from step 4. And increasely 0.05 after one iteration until the Pap or Plt reaches 1.

6. Generate Site topology:

   Call the function SiteMatrix to generate the size topology which defines the nodes (AP/BS) coverage, loose/tight connection, and connectivities between all the

nodes (AP, BS, SGSN, GGSN). For more details see section 5.2.2 Network Simulation.

7. Initialize the arrays according to the Site topology:

   Initialize the arrays, such as APbuffer[ap]; BTSbuffer[bts]; HA[i]; AP[ap]; BTS[bts]; APreceiver[ap]; BTSreceiver[bts]; userinfo[i] according to the number of APs and BSs.

   APbuffer[ap] is the array to store each AP receiver buffer size.

   BTSbuffer[bts] is the array to store each BTS receiver buffer size.

   AP[ap] is the array to keep the waiting list for sending.

   BTS[bts] is the array to keep the waiting list for sending.

   APreceiver[ap] is the array to store message ids received from internet/SGSN.

   BTSreceiver[bts] is the array to store message ids received from SGSN.

   HA[i] is the array to keep the subscriber binding in the HA

8. Determined the snapshot time Ti:

   As the simulation is done by snapshoting for each packet, the one packet time Ti is calculated here according to the initial input. For more details on the Ti see the section 5.2.3.

9. Performance calculation:

   According to the all the collected data, the packet loss, packet latency, packet reachibility, etc, are calculated here.

10. Start the simulation.

In this simulation, a full iteration consists of 80000 snapshots. During the simulation, we have also tried 40,000, 80,000, 120,000 and the results show 80,000 yields satisfied results.

11. Determined the data rate.

    To simulate the real world, the data rate will be changed randomly every 10 snapshots.

12. Update the userinfo:

    Call the function userinfo. As users move around in the simulation area, the user's speed, position, status (power off, on-line, active) and the sender buffer size are pdated for each snapshoot.

13. AP/BS forwards the packet:

    Call the function SENDerTOHAANDRECEIVER. The AP/BTS will check its list and forward one packet to the HA or the receiver by polling mechanism. The packet loss probability (Ploss) is applied in wireless air environment when sending packet from user to AP/BTS or conversely. The packet loss in air follows a uniform distribution and the counter in userinfo array will increase if the generated random value is less than or equal to Ploss. The duration for each hop will be applied and the value that follows a uniform distribution is generated randomly from the range defined in the input file. The hops from AP/BS to HA will be calculated accordingly regarding the Loose/tight coupling. In case of loose coupling, hops following a uniform distribution are generated from a range defined in the input file.

14. Separation of delay output in HA:

In the program, after packet leaves the AP/BTS, it will reach HA in no time. And in real world, it will take a few Ti to reach HA. So in HA function, the queue called array HA[I] is setup to store the duration in unit of Ti for each packet from leaving AP/BTS to reaching HA. After each snapshoot, "1" will be reduced from the duration in the queue. When the duration reaches "0", the packet will send to next function in step 15.

15. HA forwards the packet:

    Call the function SENDerTOAPBTS. The HA maintains the list of packets from different receivers with different duration. When the duration reaches the 0, this function will lookup the destination user and delivery the packet to the proper AP/BTS according to the result in this snapshot. Hops to AP/BTS will be calculted according to the Loose/Tight couple and duration for each packet to AP/BTS will be maintained.

16. Separation of delay output in AP and BTS receiver:

    Same as step 14, queue is setup in AP/BTS to store the duration for each packet from HA to AP/BTS. And after each snapshop, "1" will be reduced from duration. When the duration reaches "0", the packet will send to the next function in step 17.

17. Update the active list due to the user mobility:

    When the AP and BTS receiver arrays's duration value for each packet reach "0", add a indicator "@recv" to the AP/BTS list to indicate that there is packet in the AP/BTS receiving buffer and waiting for the polling to the destination users.

From the above program flowchart, it is clear that there are two loops. The outer one is the loop to get the step increase of AP existing probability or tight/loose ratio until it reaches 1. The inner loop is to finish a full simulation around 80,000 snapshots. And in the simulation, the flow follows the way the packet travels, i.e sender→AP/BS→HA (SGSN, GGSN, IP network will be presented in delays of packets)→AP/BS→receiver.

Users send packets to AP/BTS using a polling mechanism to share the channel. The AP/BTS itself shares the channel like other users so as to send packet to the receiver if there are packets in its queue. In the program, the delay is calculated based on the random hops and random delay for each hop. The random delay is given per hop and the range of delay for each hop is read from the initial input file.

All packets have to pass to HA and then forward to different AP/BS, which supposes the receiver's current position and the proper AP/BS is lookuped by HA whenever the packet duration in HA reaches "0" as described in step 14, see Figure 5.1. In case of no coverage for the receiver, the packet loss will be applied. So in the HA, the queue is setup based on users and duration (from AP/BTS to HA). The duration will reduce 1 after each snapshoot and the packet will be sent to AP/BTS or packet will be lost if the receiver is not in the coverage when the duration reaches "0".

After the packet leaves the HA, it will go to the proper AP/BTS then to the receiver. As the HA already knows where to send the packet, so in the program the packet will arrive at the desired AP/BTS and mark the duration from HA to AP/BTS in receiver side. In the AP/BTS, the receiver queue is setup for decreasing the duration. When the duration reaches "0", which means the packet is reaching the AP/BTS, the AP/BTS will get noticed from its receiver queue and wait its turn to send the packet to the end receiver.

In this program, three different packet loss informations are collected, which are the packet loss in air, packet loss in moving and packet loss in overflow. The packet loss in air is due to the air interference, etc, and the probability is given from the input file. It is calculated for each packet during the sending and receiving where the probability of success applied on each packet. The packet loss in moving is due to the user's mobility, such that when the packet is reaching the HA the user is in AP1 and when the packet reaches the AP1 the user is in AP2. The only way to reduce this type of loss is to reduce the number of hops between HA and AP/BTS and the queue in the AP/BTS. The packet loss in overflow is due to the heavy traffic or in other word, the narrow bandwidth.

5.4 Simulation Results

In this simulation, the results are presented in several sets. And analysis of the results is given after each set. The followings are presented in the results:

- Packets Reachability:

  Percentage for received packets out of total sent packets.

- Packets Loss percentage In Air:

  Packets loss during the simulation while it is in air. The loss probability is fixed during all simulation. In this simulation, the value Ploss is always 0.2, i.e. it is an input value to the program.

- Packet Loss Percentage In Moving:

  Packets loss during the simulation because of the receiver's moving. This information is collected for each iteration, i.e. it is an output of the program.

- Packet Loss Percentage in Overflow:

  Packets loss during the simulation because of the overflow happened. This information is collected for each iteration, i.e. it is an output of the program.

- Packet Latency:

  Duration from the packet leaving the sender until it reaches the receiver, in this simulatin, it is measured by numbers of Ti (snapshot interval), i.e. it is an output of the program.

- Throughput:

  Packets received during each iteration under defined threldhold. The packet received after the theldhold will be considered lost, i.e. it is an output of the

program. In this simulation, the threldhold is given 40Ti always. And it could be changed in initial input data.

- Received packet average:

  Packets received during one simulation without defining any threldhold, i.e. it is an output of the program.

- User average packet in buffer:

  Numbers of packets in user's buffer waiting for the transmittion, , i.e. it is an output of the program.

- AP average packets in buffer:

  Numbers of packets in AP's network interface receiver's buffer, i.e. it is an output of the program.

- BTS average packets in buffer:

  Numbers of packets in BTS's network interface receiver's buffer, i.e. it is an output of the program.

- Variances for all above variables, all are output of the program.

- Capacity used percentage

  In the simulation area, the total capacity is the APs capacity plus BTSs capacity. AP capacity is calculated by AP radio bandwidth multipled by the numbers of APs. The same applies to the BTS capacity. The capacity used is calculated by all the packets sent out during the simulation divided by simulation time duration, i.e number of Ti.

Also the parameter shown in figures are:

- Plt:

Loss/tight probability. For instance, Plt=0.6 means there is a probability 60% of APs using tight connection and 40% are using loose connection to the GPRS network.

- Pap:

  AP's existence probability in each area. The site is split according to the AP and BTS coverage. See section 5.1 site simulation. In each split area the AP probability is applied and AP may or may not exist.

- Pbts:

  BTS existence probability in each BTS area.

- Pair:

  Probability of packet loss in the air

- Pdatageneration:

  The sender's probability of generating data

Figure 5.5 ~ 5.10 shows the simulation results for the packet reachability and loss percentage versus Pap.

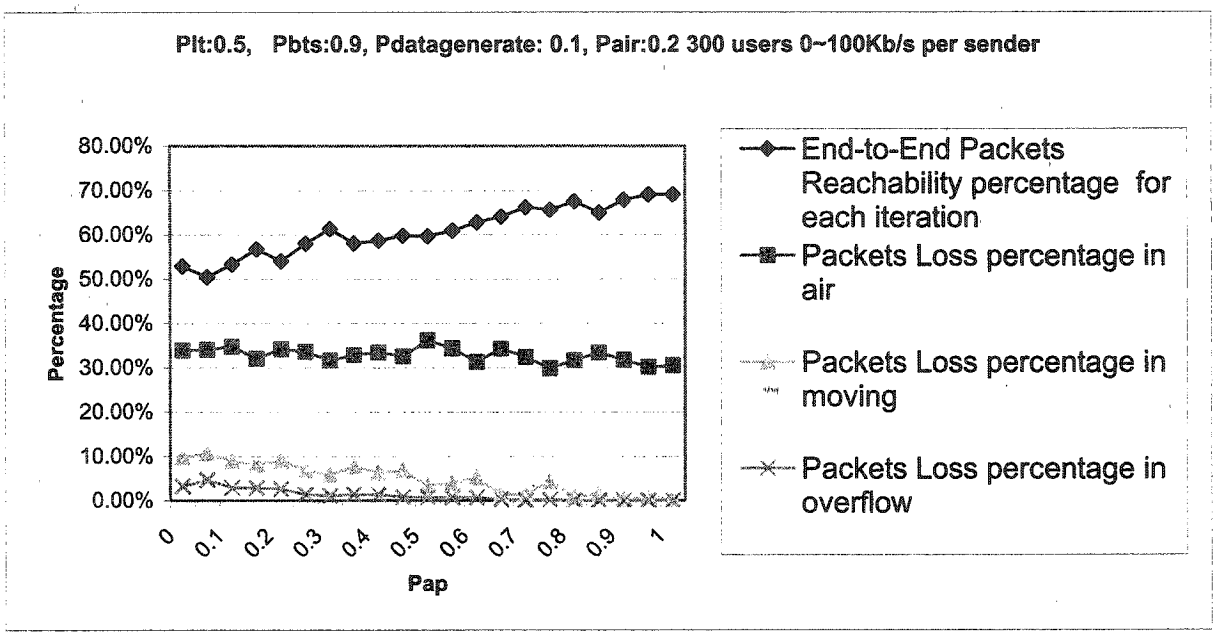

Figure 5.5 Packet reachability and loss perentage with Plt:0.5, Pbts:0.9 Pdatageneration:0.1 and light traffic load

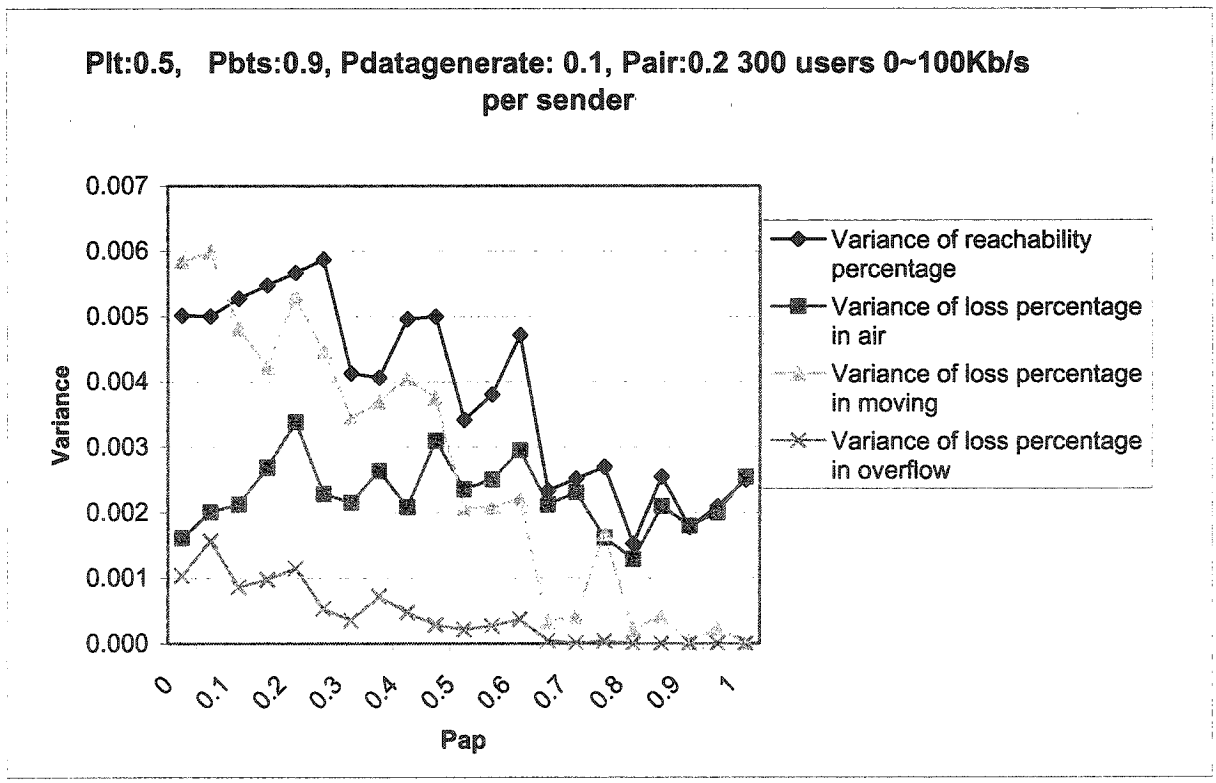

Figure 5.6 Packet reachability and loss variance with Plt:0.5, Pbts:0.9, Pdatageneration:0.1 and light traffic load

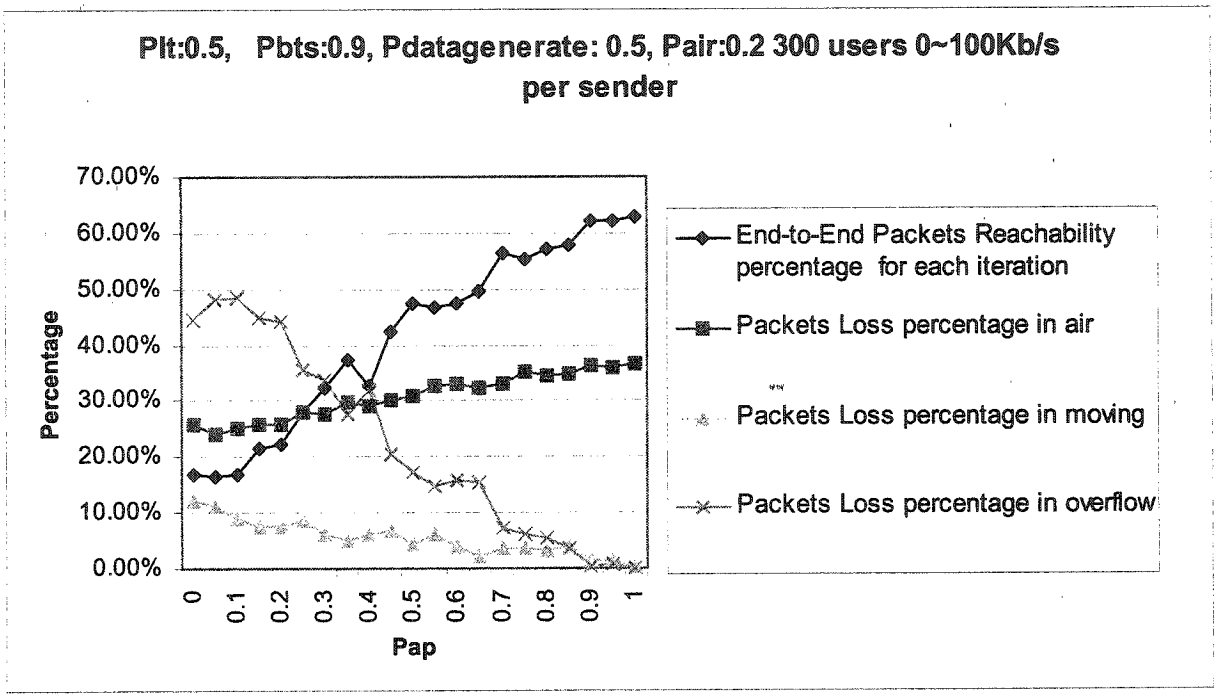

Figure 5.7 Packet reachability and loss perentage with Plt:0.5, Pbts:0.9 Pdatageneration:0.5 and medium traffic load

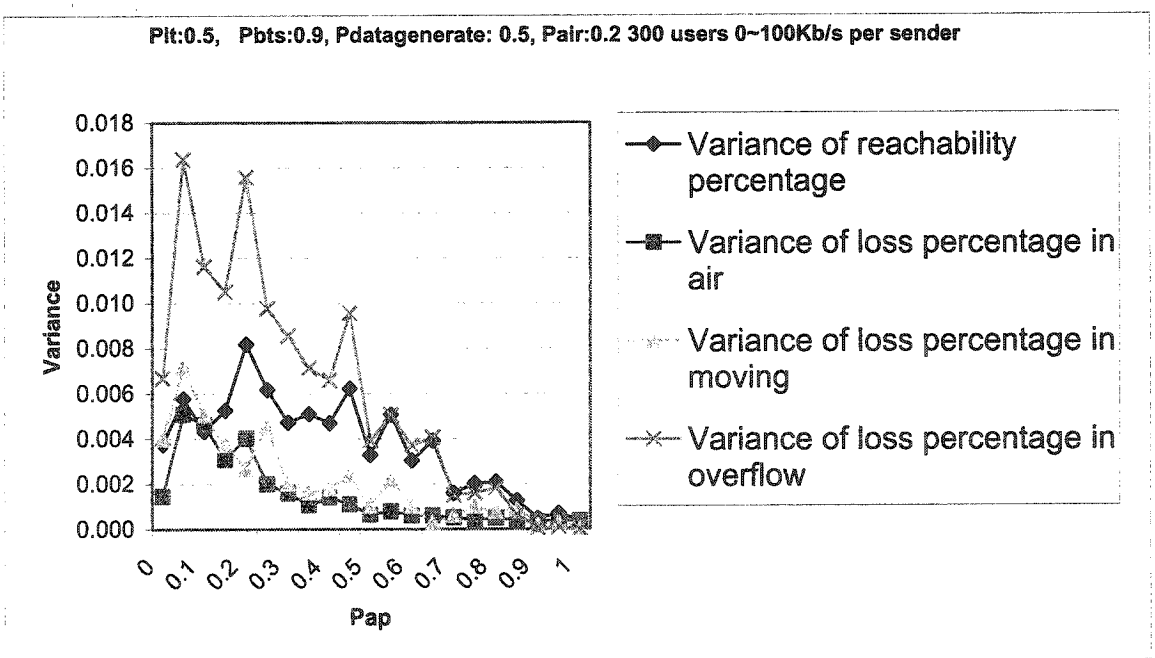

Figure 5.8 Packet reachability and loss variance with Plt:0.5, Pbts:0.9, Pdatageneration:0.5 and medium traffic load

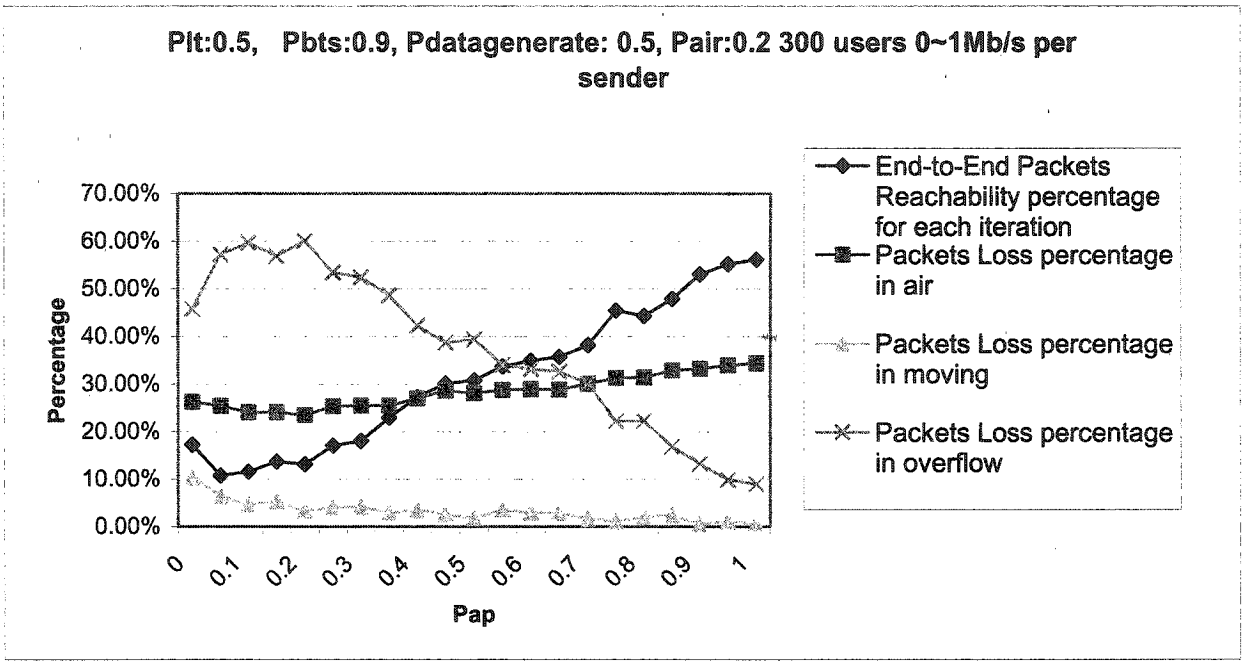

Figure 5.9 Packet reachability and loss perentage with Plt:0.5, Pbts:0.9 Pdatageneration:0.5 and heavy traffic load

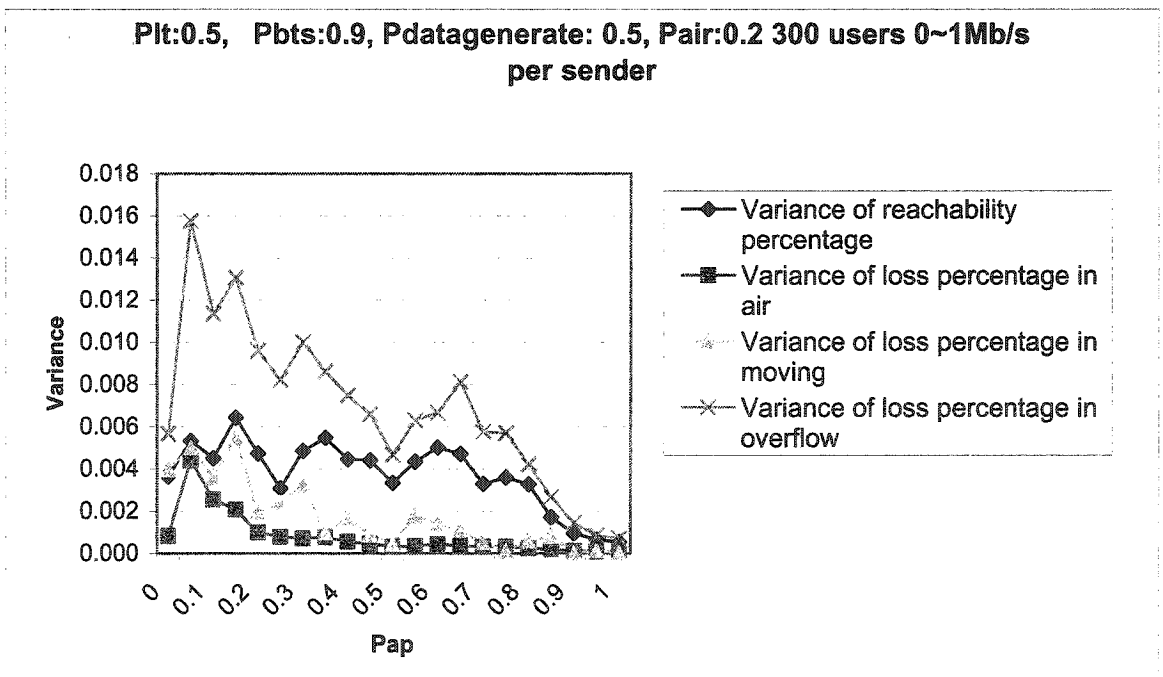

Figure 5.10 Packet reachability and loss variance with Plt:0.5, Pbts:0.9, Pdatageneration:0.5 and heavy traffic load

From Figure 5.5 ~ 5.10, the followings are clearly shown in chart:

- With Pap increasing, in general the packet reachability percentage increases and the packets loss in moving and overflow are reduced. And it is also noticed that when Pap increases in the range 0-->0.3 for heavy traffic and 0-->0.15 for the medium traffic, the packet reachability goes down a bit and the packet loss in overflow is increased. Actually it is easy to understand that with the Pap increasing, at the beginning especially for Pap in the range of 0~0.3 the wireless network is mixed and the slow radio links such as BTS dominates. This is because packets get dropped in the slow link. As shown the packet loss in overflow increases a bit when Pap increases from 0 to 0.15 for medium traffic and 0 to 0.3 for heavy traffic. Also the variance of packet reachability and loss in overflow grow with Pap in its lower range.
- Packet loss in air percent has almost no change in case of light traffic. In case of medium and heavy traffic, the packet loss in air percentage increases a little bit. The reason is that the sending traffic is considered to be constant while the packet loss in overflow and packet loss in moving decrease in general when Pap increases, which causes more packets in the air environment and then the packets lost in air could increase. Of course the percentage of packets loss in air will increase.
- The user buffer and BTS buffer go down with the Pap increasing; also their variances go down.
- It is noticed that the packet loss probability in air is defined by 20% while the results show the variable and seem to reach 36% at maximum. The reason is the

air loss probability is applied on each packet travel from MN1→AP/BTS and then AP/BTS→MN2. So if there is no other packet loss and 20% air loss is applied, then the overall packet loss in air will be at 36%, which is the best case. And there will be packet loss in moving and packet loss in overflow as shown in the result diagrams.

- The variance of the results is moving within a big range. The reason is that in this simulation the network diagram will re-generate for every simulation (80,000 snapshoot). So in this way there is more room for the variable result.

Figures 5.11 ~ 5.12 show results for the packet reachability and loss percentage under different loose/tight ratio.

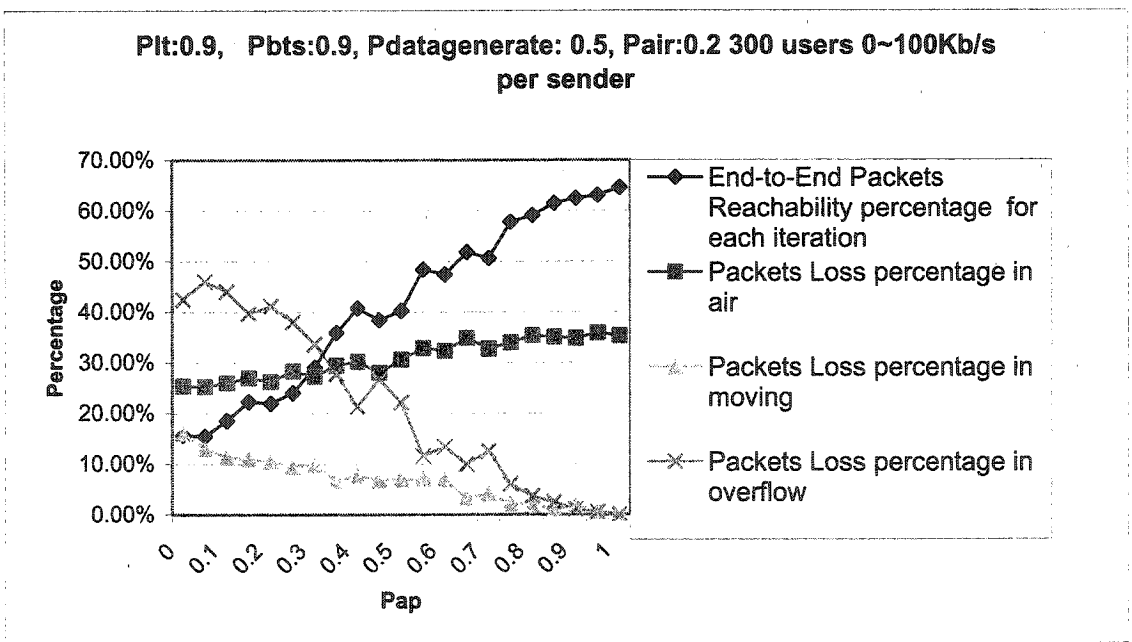

Figure 5.11 Packet reachability and loss perentage with Plt:0.9, Pbts:0.9 Pdatageneration:0.5 and medium traffic load

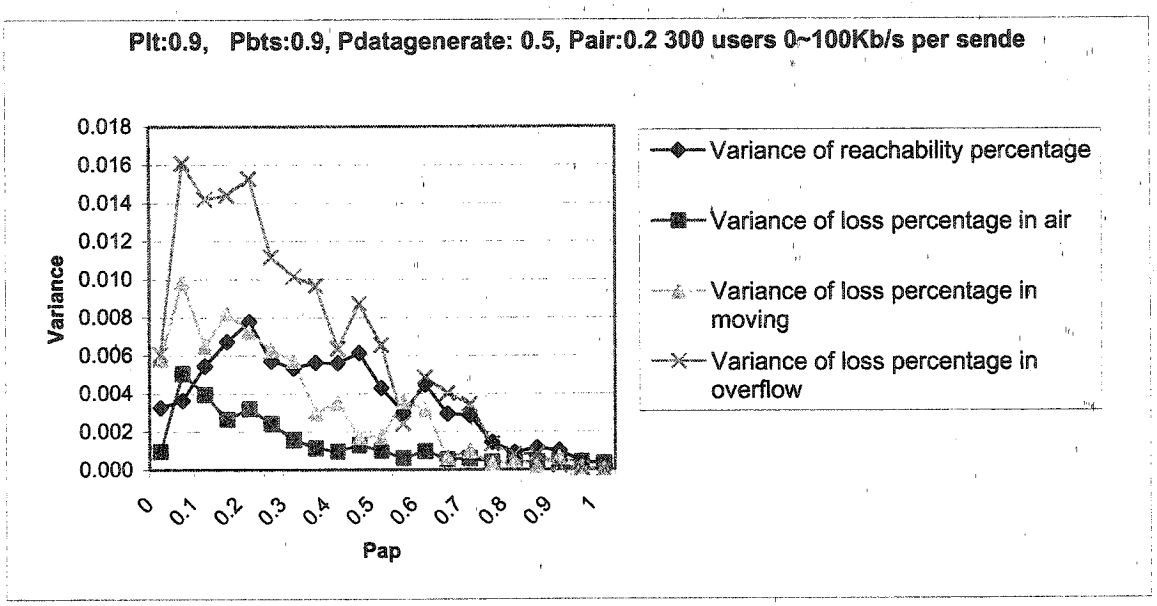

Figure 5.12 Packet reachability and loss variance with Plt:0.9, Pbts:0.9, Pdatageneration:0.5 and medium traffic load

From Figures 5.11-5.12, we can see that the Plt does not change with the percentage of packet reachability and packet loss. By comparing those two figures with Figure 5.7-5.8, there is no difference in packet reachability and packet loss.

Figures 5.13 ~ 5.14 show the results of end-to-end packet latency.

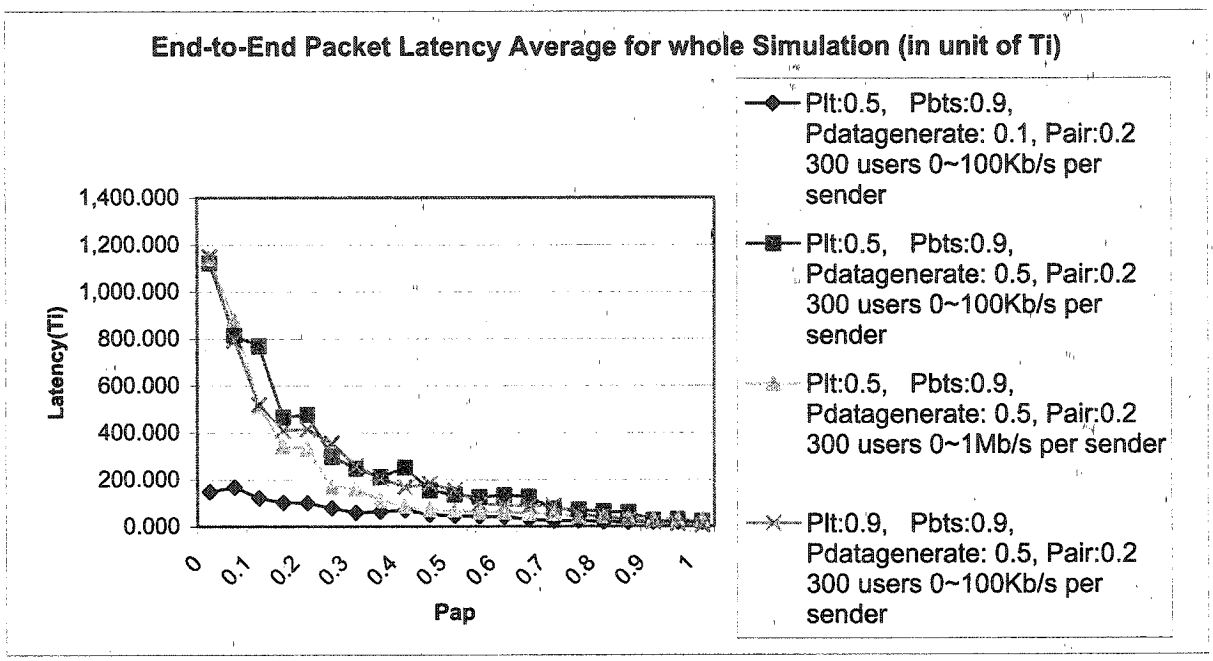

Figure 5.13 End-to-End Packet Latency Average for whole Simulation with Pap increasing

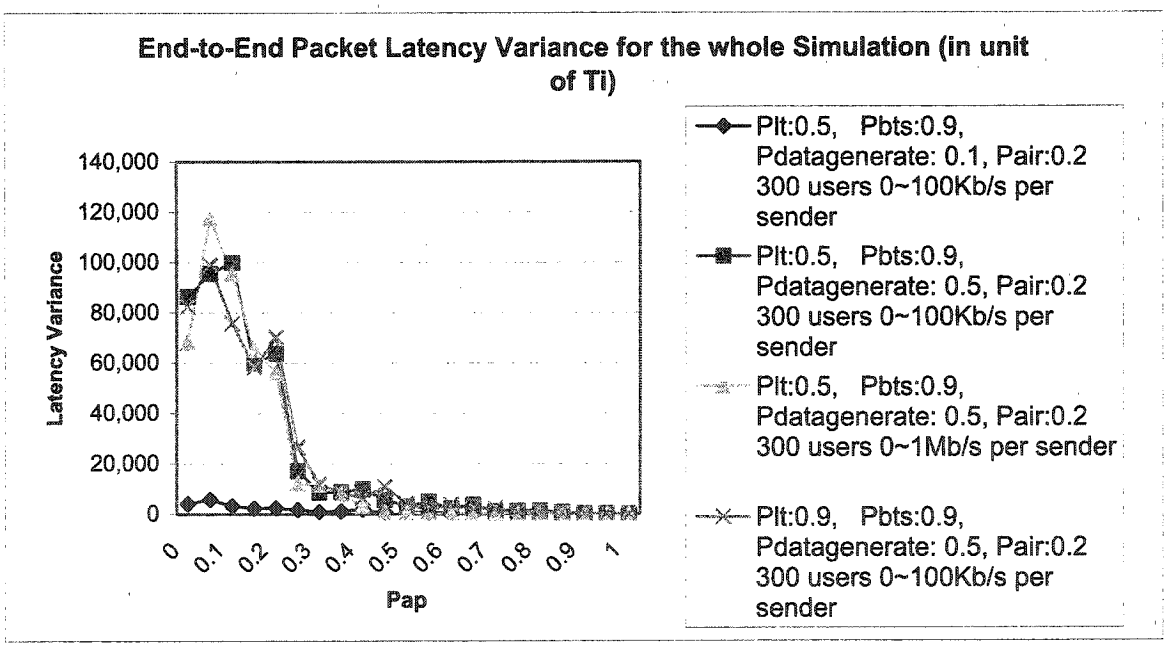

Figure 5.14 End-to-End Packet Latency Variance for the whole Simulation with Pap increasing

From Figure 5.13 ~ 5.14, it is clear to see that:

- With Pap increasing, the end-to-end packet latency decreases. Especially in medium and heavy traffic, the latency decreases 85% when Pap moves from 0 to 0.45.
- With Pap increasing, the latency variance decreases in general. And with Pap increasing from 0 → 0.1, the variance actually increases. The reason is during the time the BTSs dominate the simulation area and just a few APs exist. Thus the latency varies a lot. With higher Plt, the variance starts to decrease earlier than the others.

Figure 5.15 ~ 5.23 show the received packets and throughput results under different conditions.

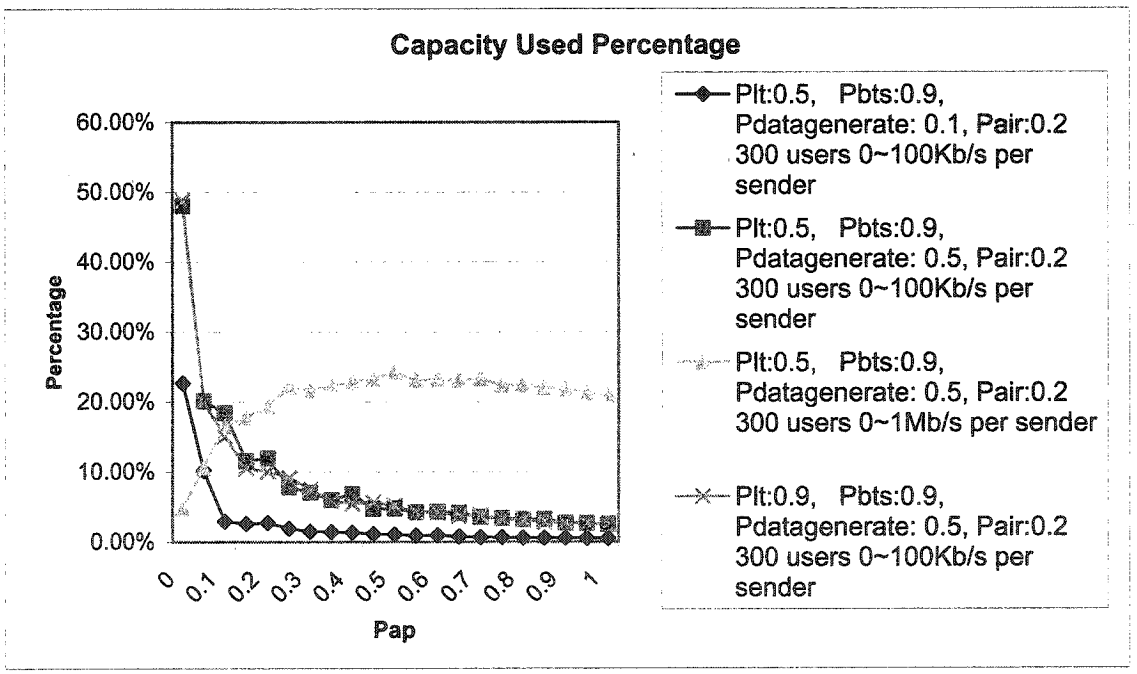

Figure 5.15 Capacity Used Percentage with Pap increasing

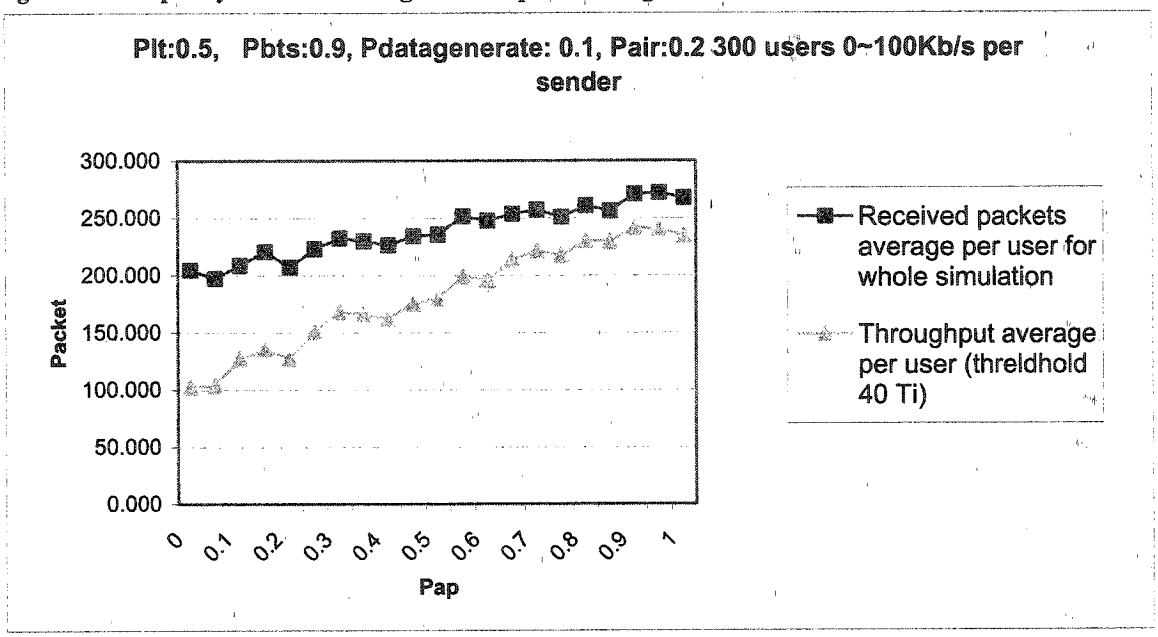

Figure 5.16 Number of End-to-End Packet received and throughput with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 light traffic

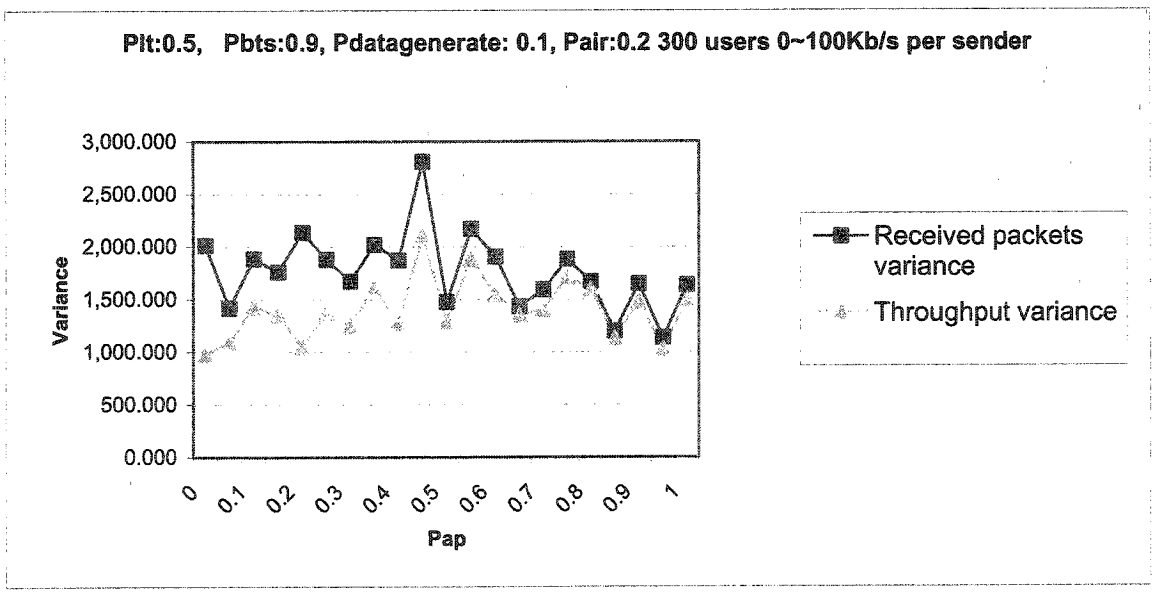

Figure 5.17 Number of End-to-End Packet received and throughput variances with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 light traffic

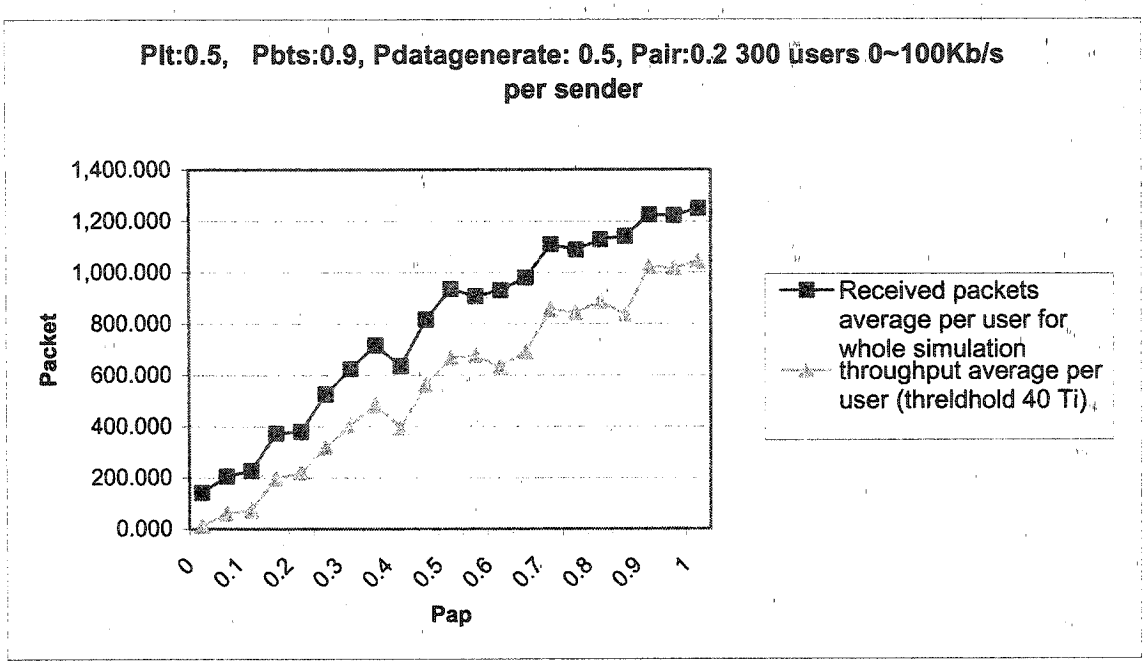

Figure 5.18 Number of End-to-End Packet received and throughput with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic

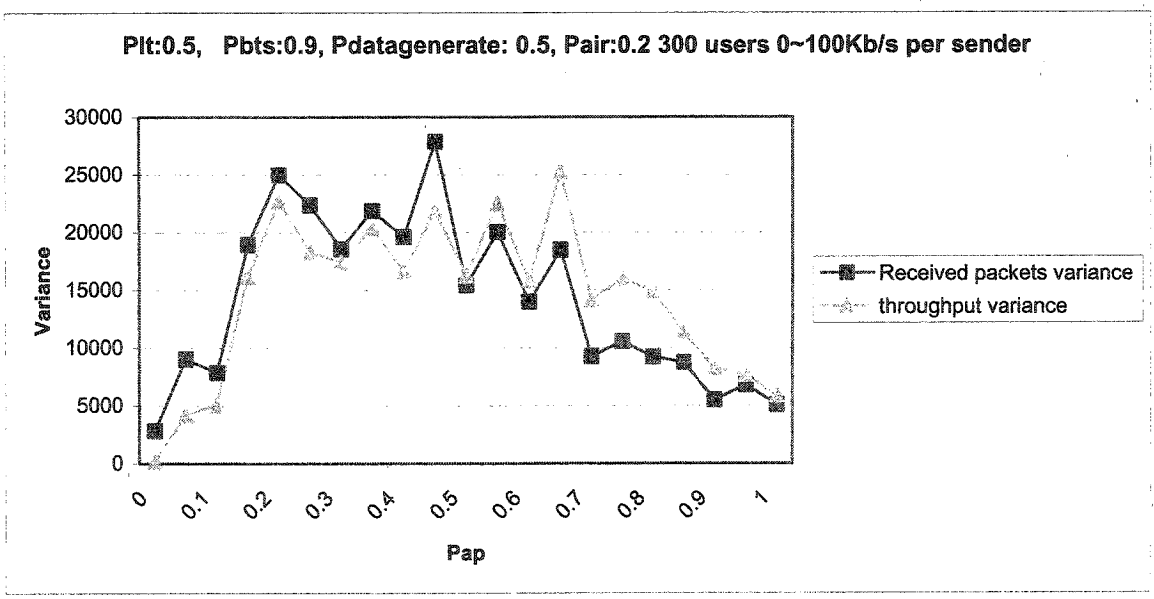

Figure 5.19 Number of End-to-End Packet received and throughput variances with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic

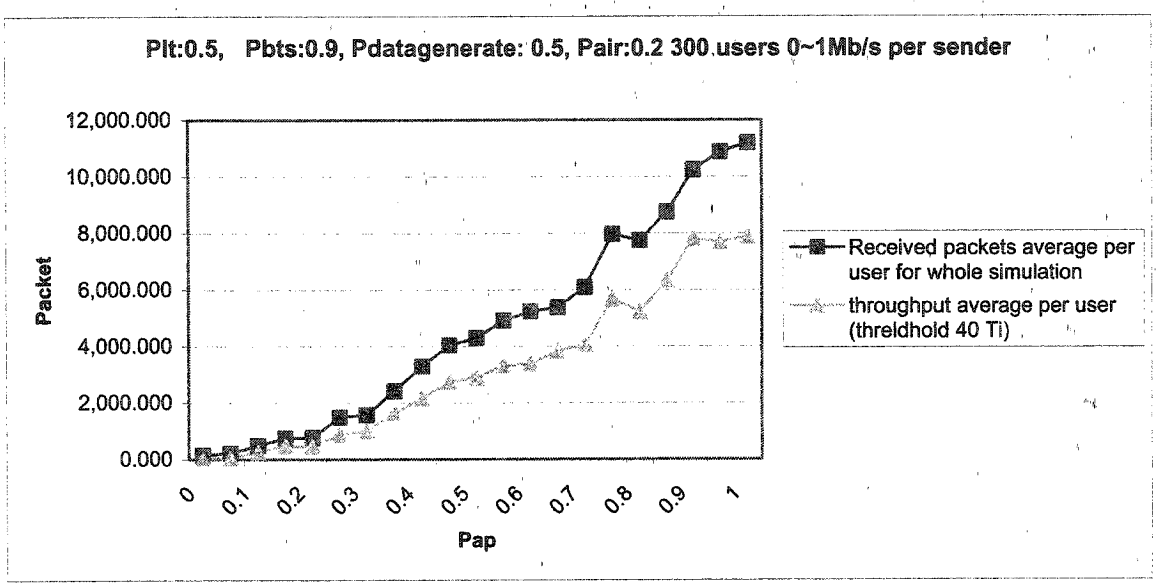

Figure 5.20 Number of End-to-End Packet received and throughput with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 heavy traffic

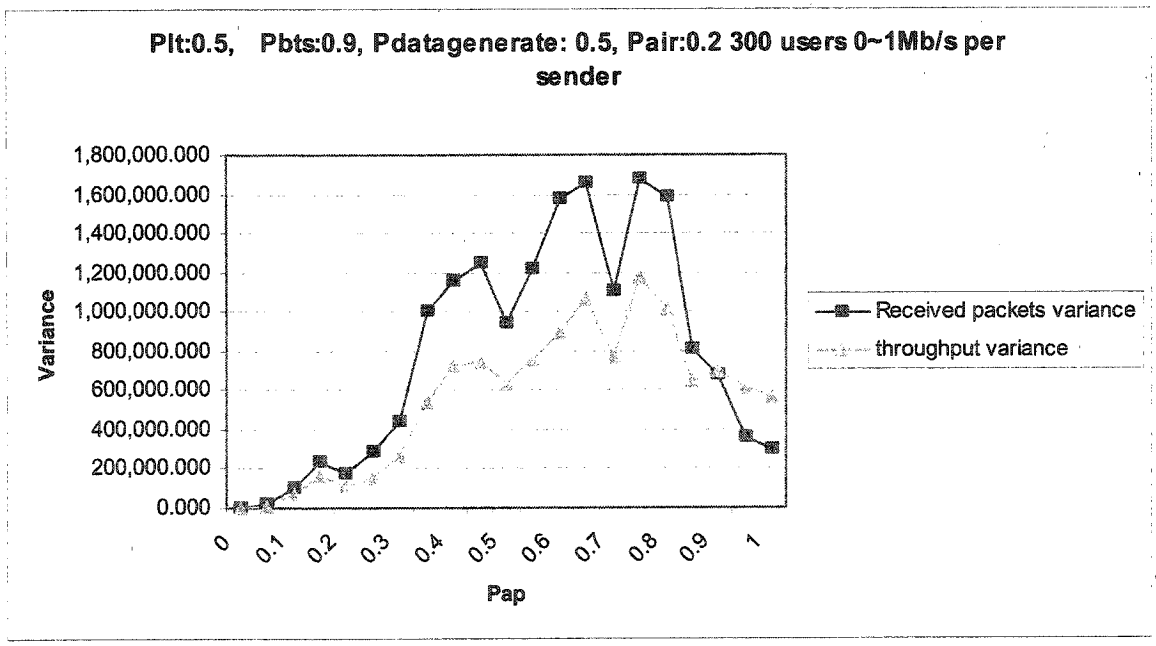

Figure 5. 21 Number of End-to-End Packet received and throughput variances with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 heavy traffic

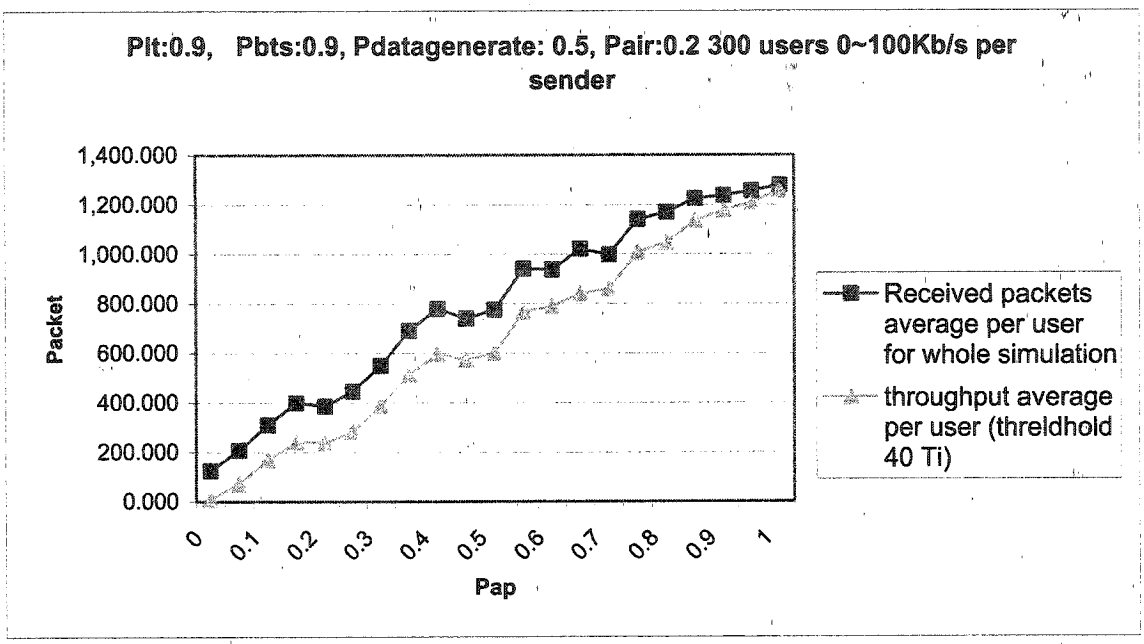

Figure 5.22 Number of End-to-End Packet received and throughput with Plt:0.9, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic

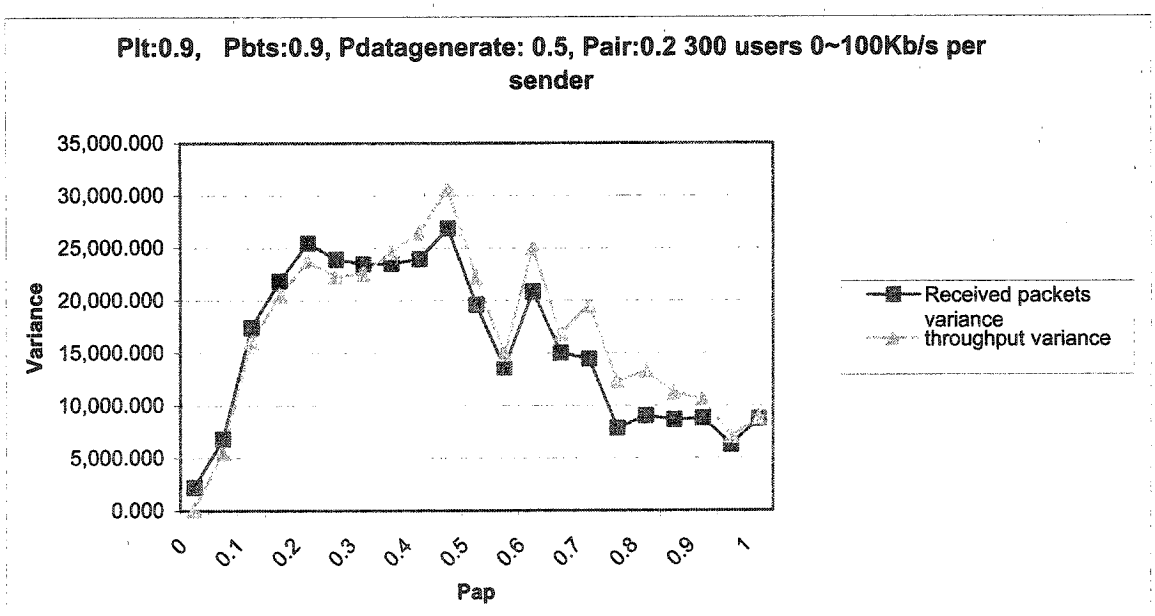

Figure 5.23 Number of End-to-End Packet received and throughput variances with Plt:0.9, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 medium traffic

From Figures 5.15 ~ 5.23, we can see clearly:

- With the Pap increasing, the received packets and throughput increase simultaneously.
- With the Pap increasing, the capacity of the whole simulation area increases. Capacity used percentage goes down very fast when Pap is in the range 0-0.3 and is stable after that.
- The curve movement of variance for the received packets and throughput is increasing with Pap increasing and then keeps in the high level then goes down with Pap. Also it is noticed that with different traffic loads, the peak of variance is reached with different Pap. With medium traffic, the peak is reached when Pap is 0.25 and with heavy traffic, the peak is delayed until Pap is 0.6.
- With medium and heavy traffic, and when Pap is zero, the throughput is close to zero. That means the latency is very high.

Figures 5.24 ~ 5.31 show the user sending buffer content, AP buffer and BTS buffer usage.

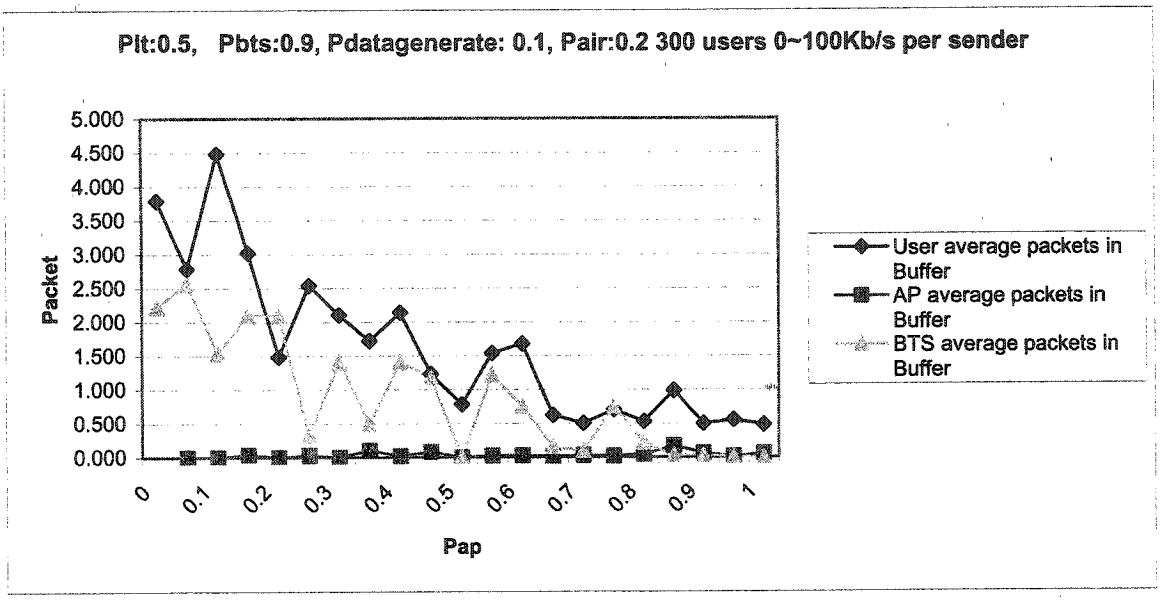

Figure 5.24 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 300 users light traffic

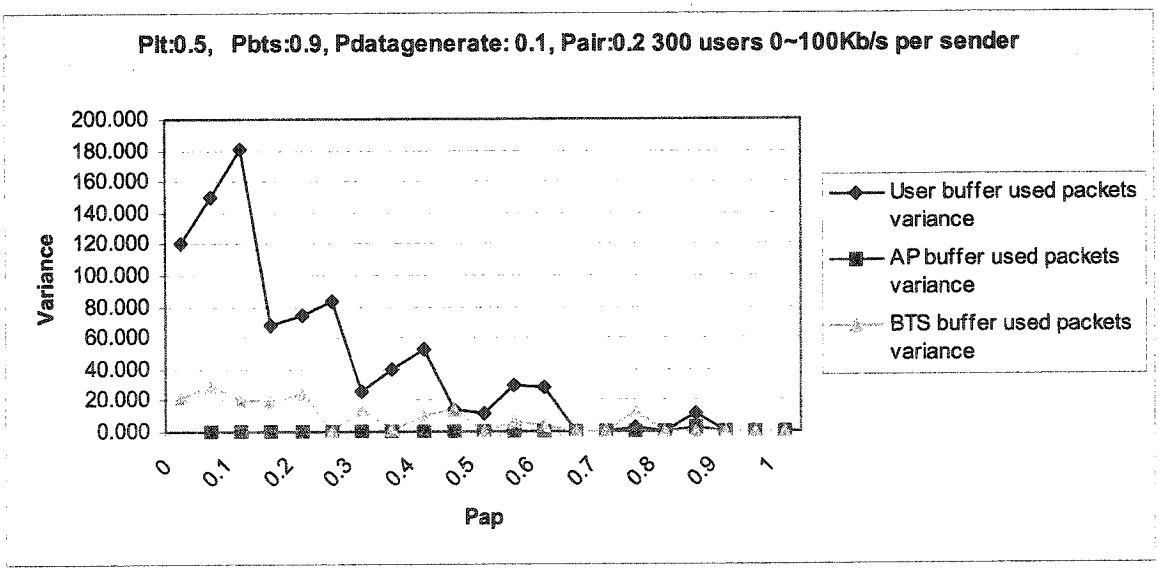

Figure 5.25 Buffer variance with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.1, Pair:0.2 300 users light traffic

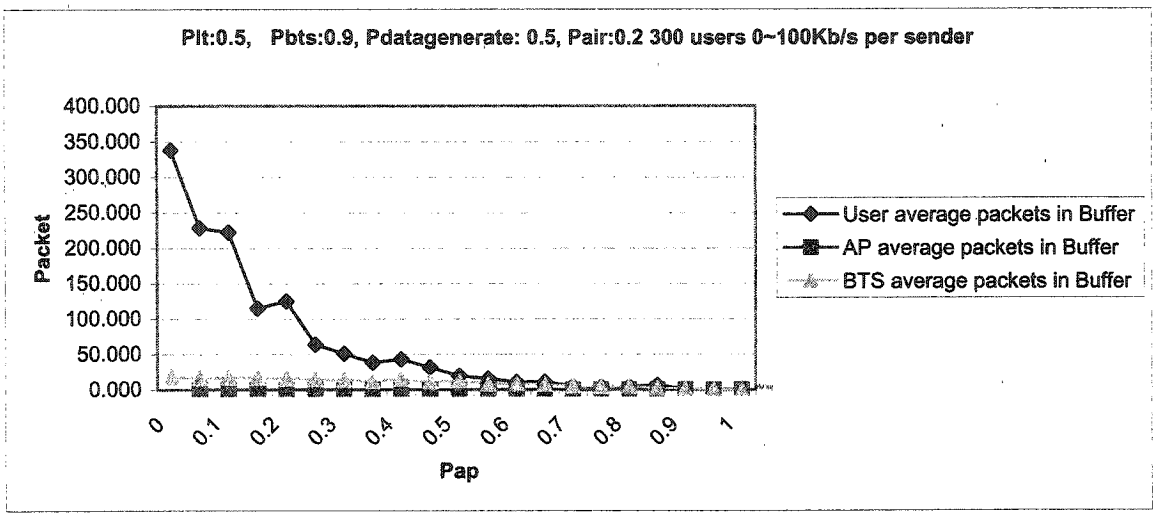

Figure 5.26 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users medium traffic

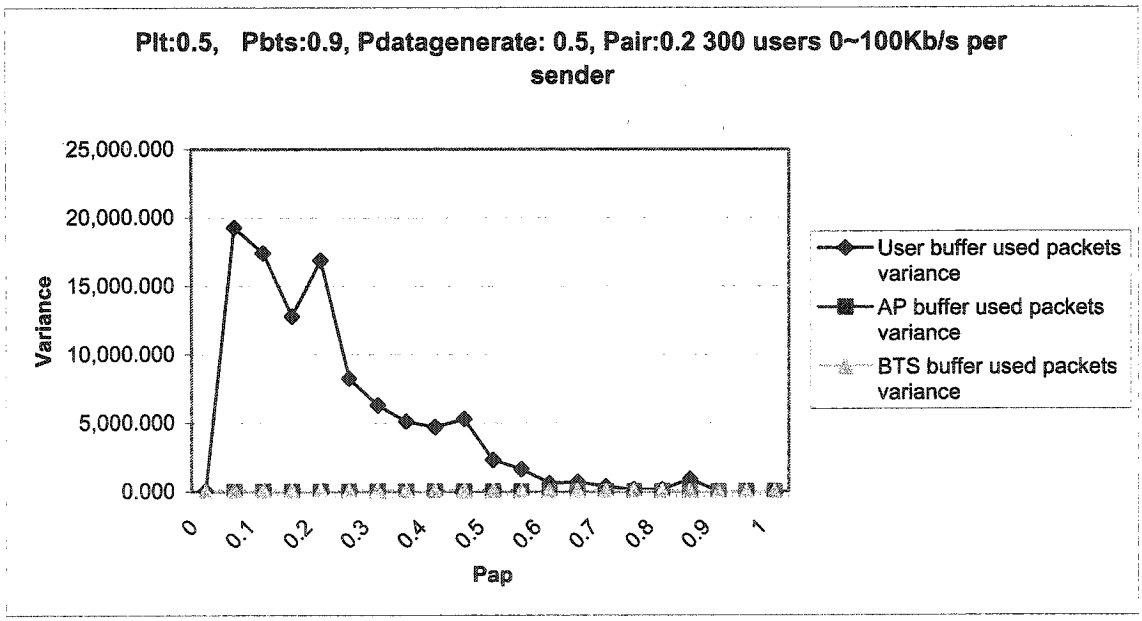

Figure 5.27 Buffer variance with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users medium traffic

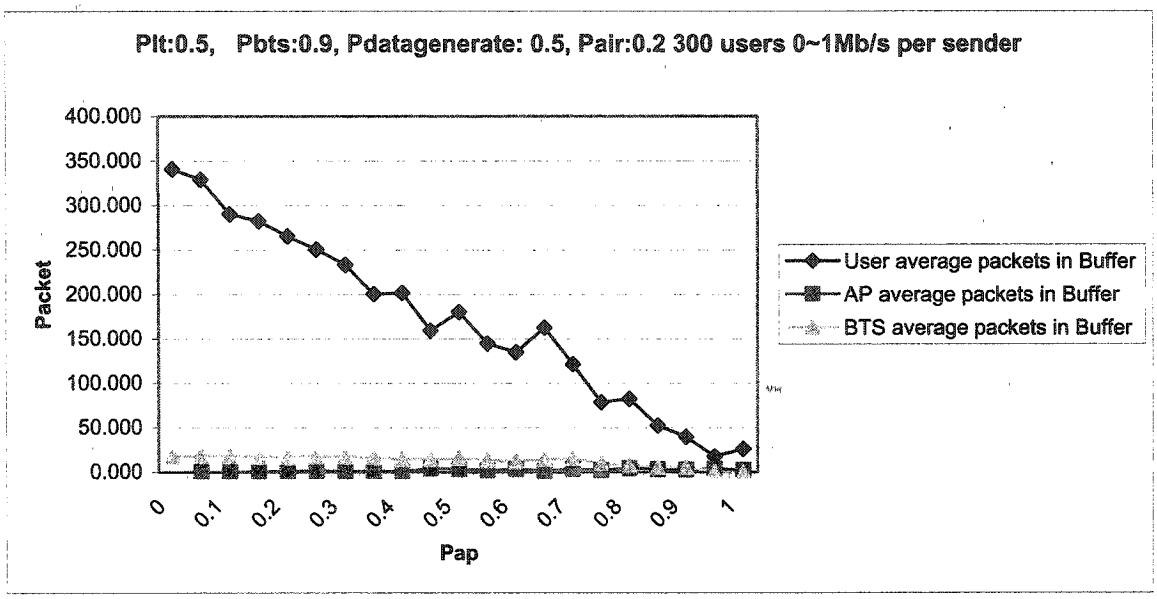

Figure 5.28 Buffer content with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users heavy traffic

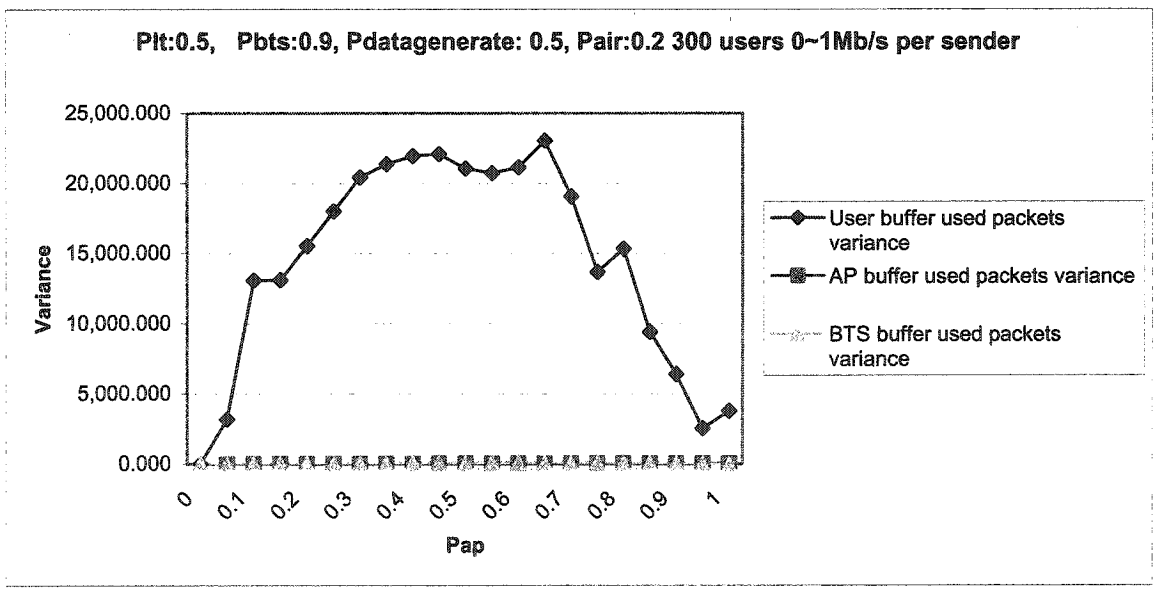

Figure 5.29 Buffer variance with Plt:0.5, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users heavy traffic

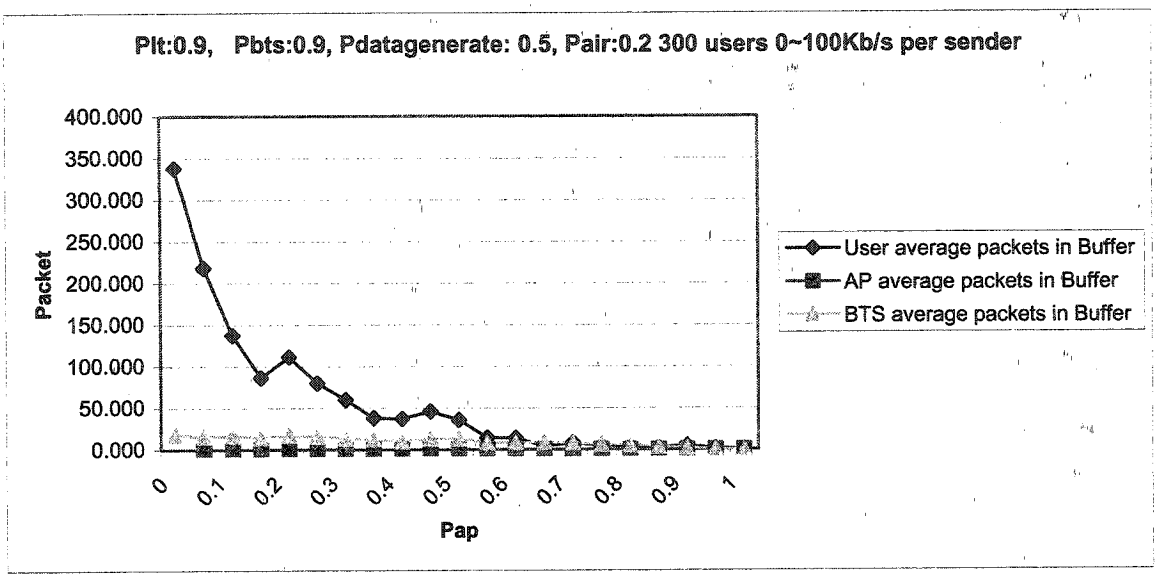

Figure 5.30 Buffer content with Plt:0.9, Pbts:0.9, Pdatagenerate: 0.5, Pair:0.2 300 users medium traffic

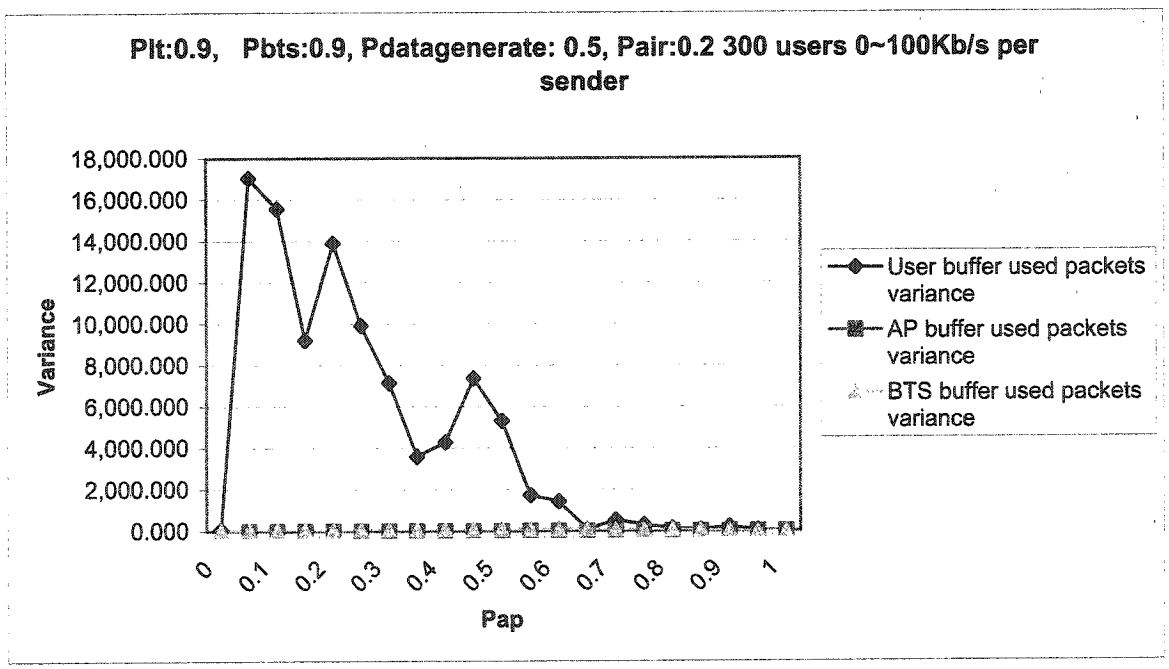

Figure 5.31 Buffer variance with Plt: 0.9, Pbts: 0.9, Pdatagenerate: 0.5, Pair: 0.2 300 users medium traffic

From Figures 5.24 ~ 5.31, we can observe the following:

- With the Pap increasing, the user used buffer decreases especially with the medium and heavy traffic. As the packet can be sent out much fast when the Pap increases.
- With the Pap increasing, the BTS used buffer decreases. The reason is the AP offloads the traffic in the network.
- With the Pap increasing, the variance of user used buffer increases first then starts to decrease.

Figures 5.32 ~ 5.35 show the packet reachability and loss when Pap is fixed and Plt is increased from 0 to 1.

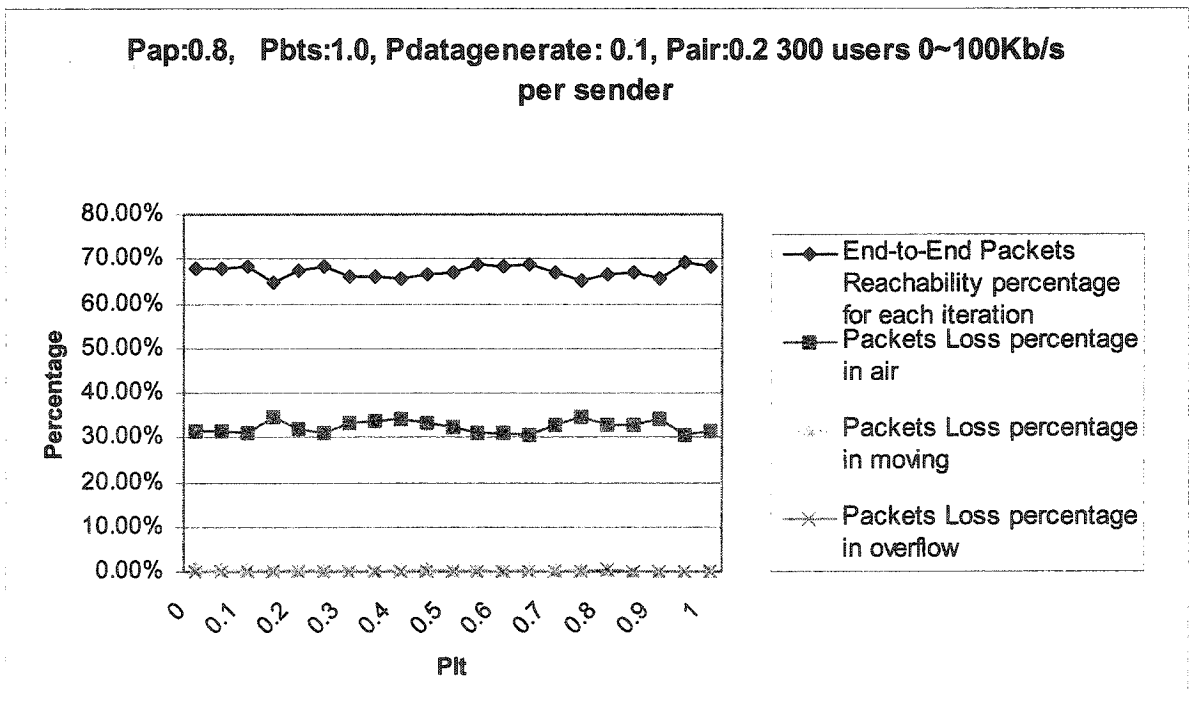

Figure 5.32 Packet reachability and loss with Pap:0.5, Pbts:1.0, Pdatageneration:0.1 and light traffic load

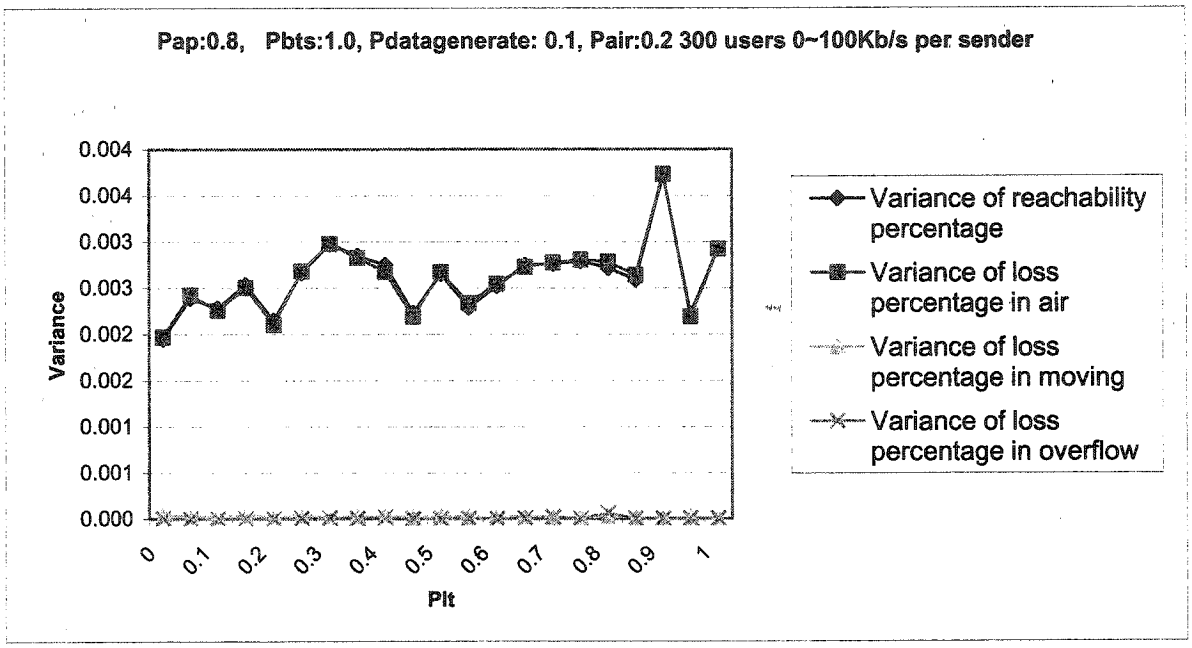

Figure 5.33 Packet reachability and loss variance with Pap:0.5, Pbts:1.0, Pdatageneration:0.1 and light traffic load

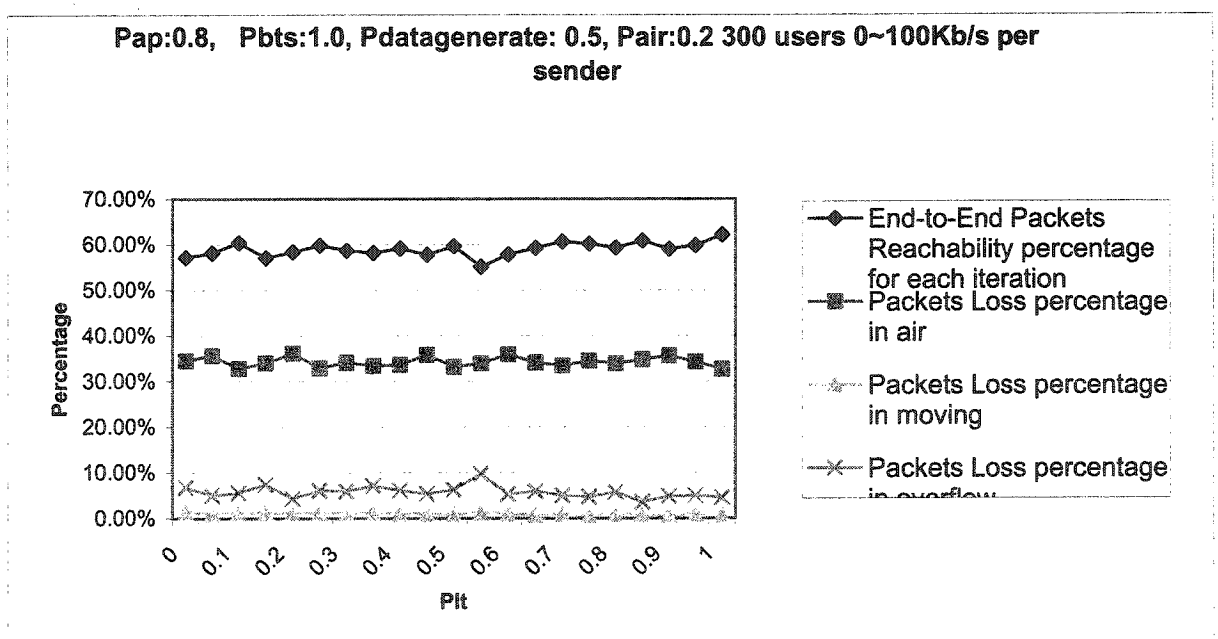

Figure 5.34 Packet reachability and loss with Pap:0.5, Pbts:1.0, Pdatageneration:0.1 and medium traffic load

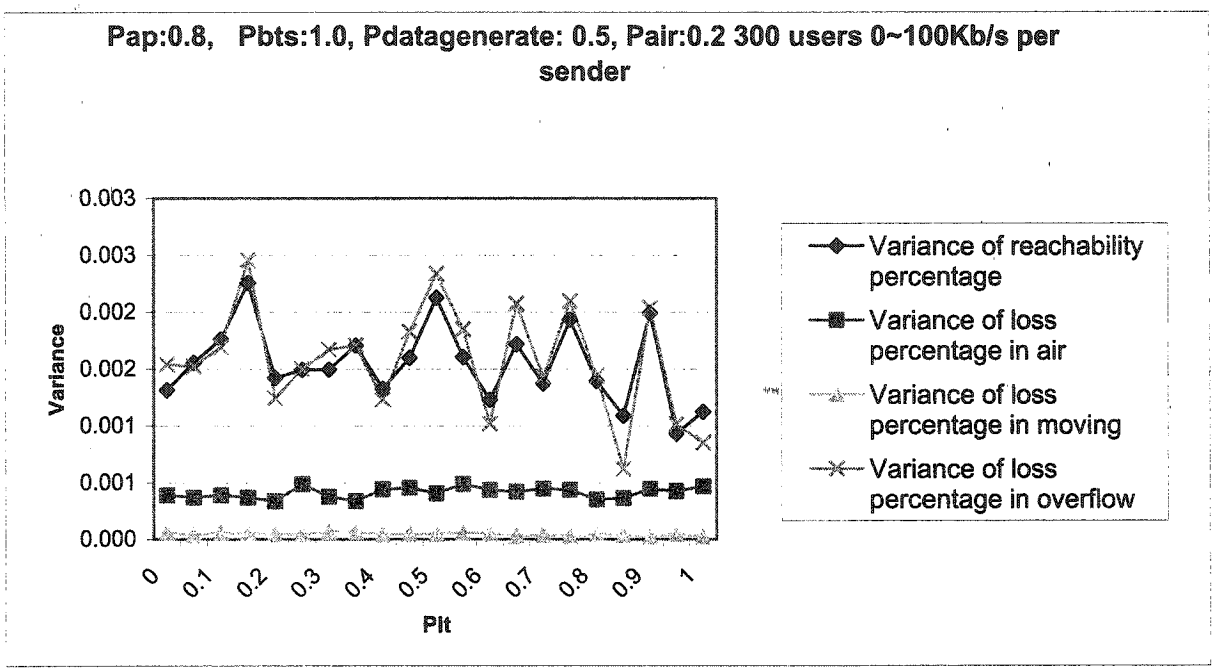

Figure 5.35 Packet reachability and loss variance with Pap:0.8, Pbts:1.0, Pdatageneration:0.1 and medium traffic load

From Figures 5.32 ~ 5.35, we can seethat:

- With the Plt increasing, there is no impact on the packet reachability and packet loss.

Figures 5.36 ~ 5.41 show the received packet, throughput and latency.

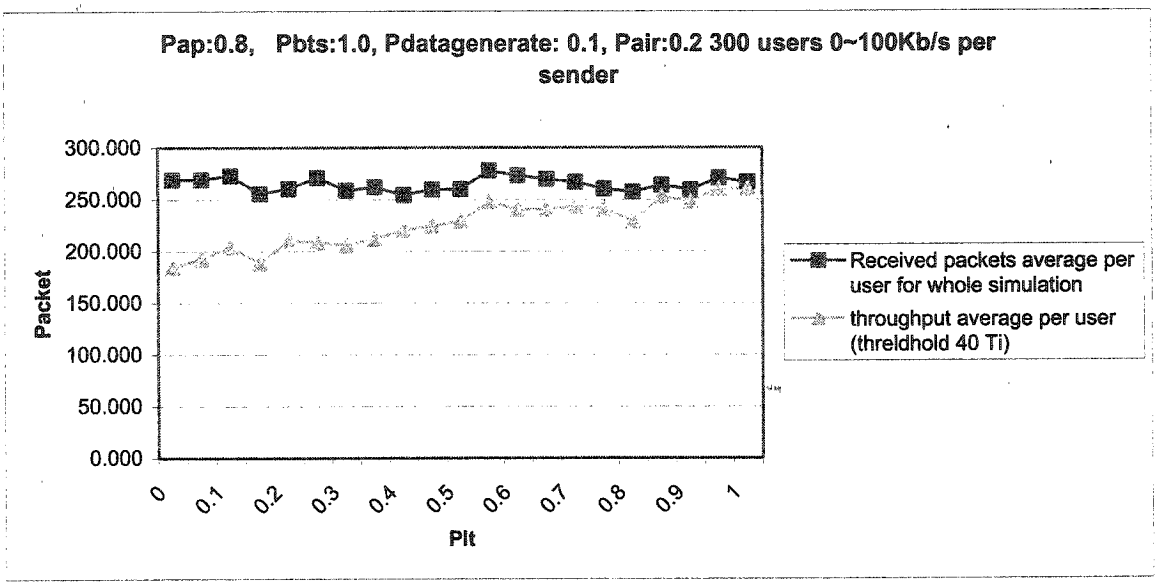

Figure 5.36 Number of End-to-End Packet received and throughput with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.1, Pair:0.2 light traffic

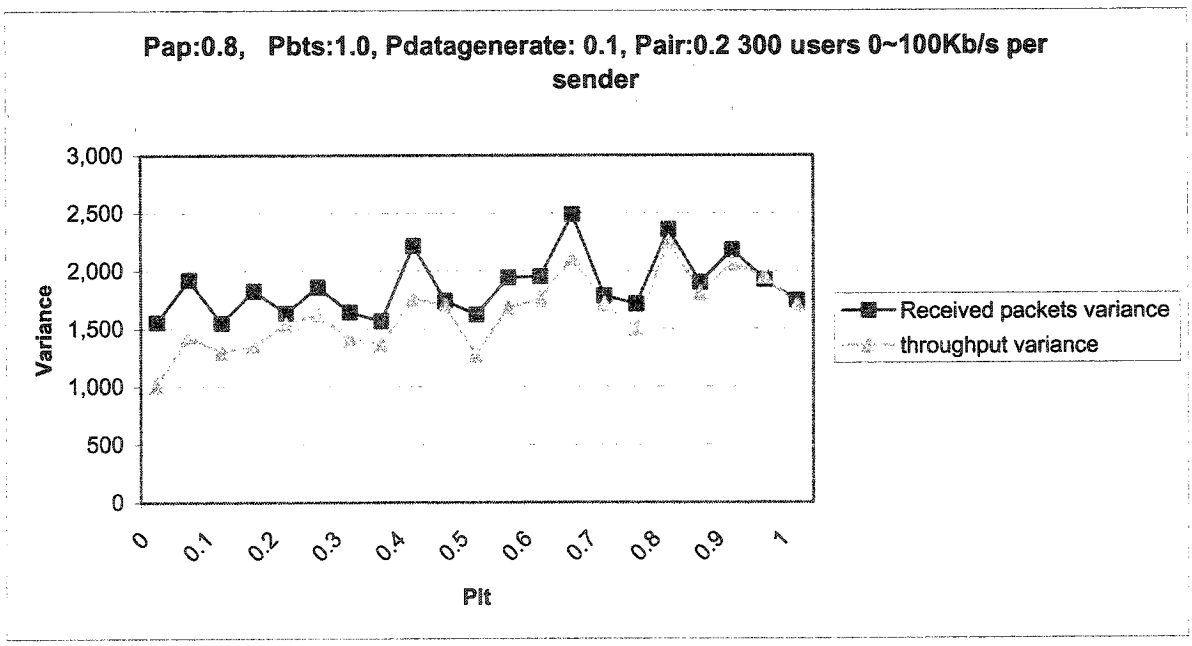

Figure 5.37 Number of End-to-End Packet received and throughput variances with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.1, Pair:0.2 light traffic

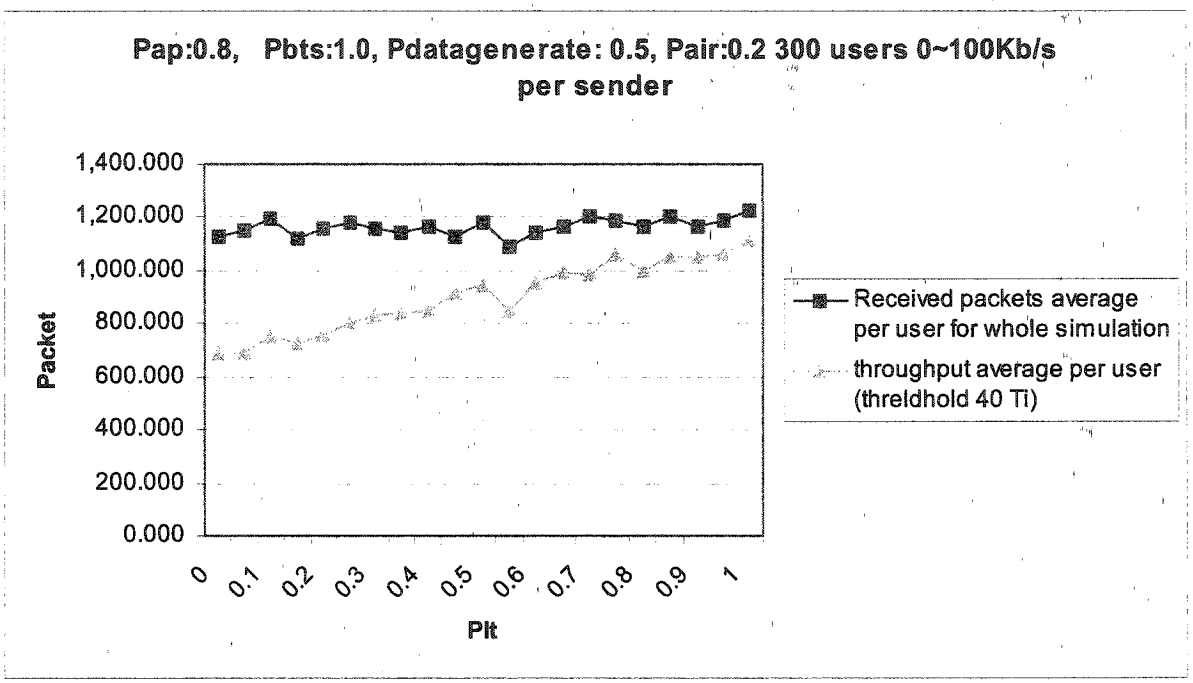

Figure 5.38 Number of End-to-End Packet received and throughput with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.5, Pair:0.2 medium traffic

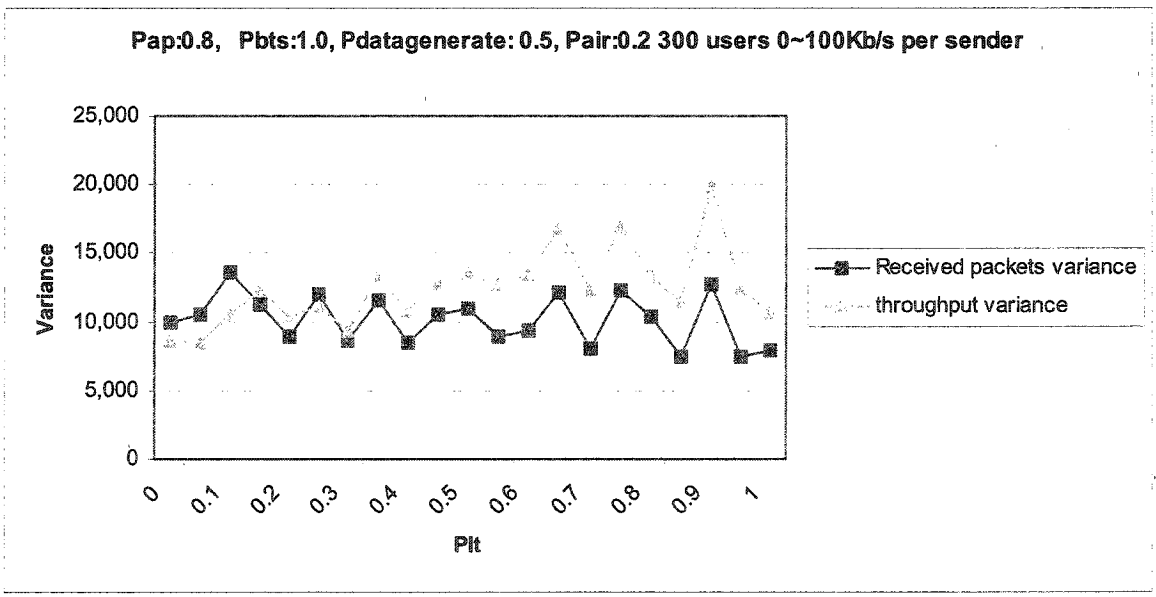

Figure 5.39 Number of End-to-End Packet received and throughput variances with Pap:0.8, Pbts:1.0, Pdatagenerate: 0.5, Pair:0.2 medium traffic

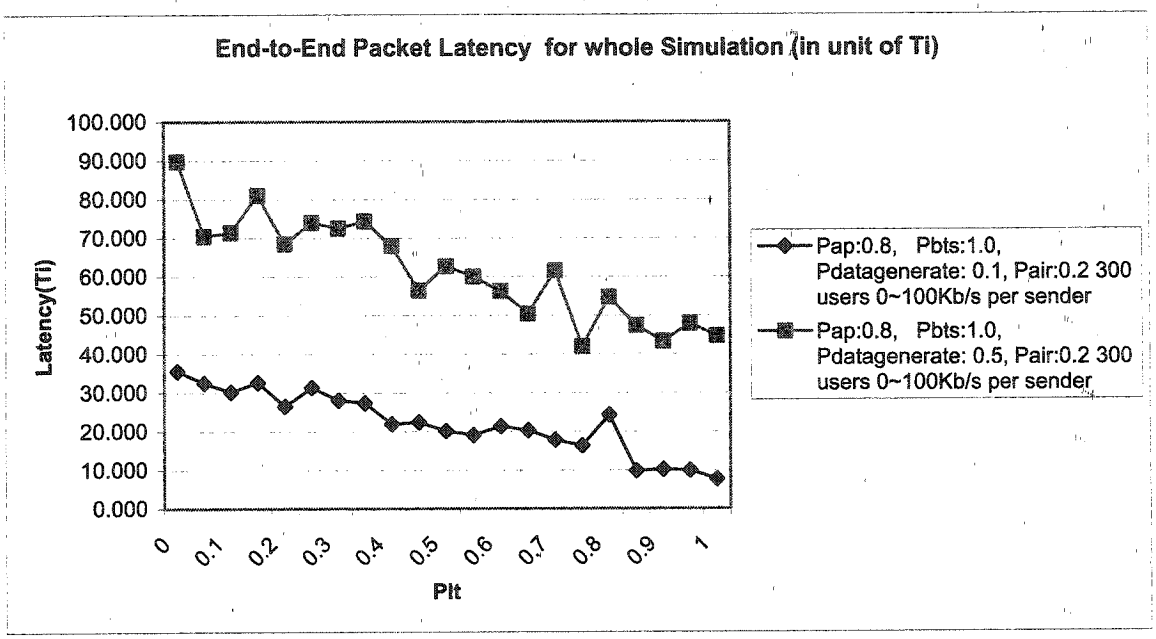

Figure 5.40 End-to-End Packet Latency Average for whole Simulation with Plt increasing

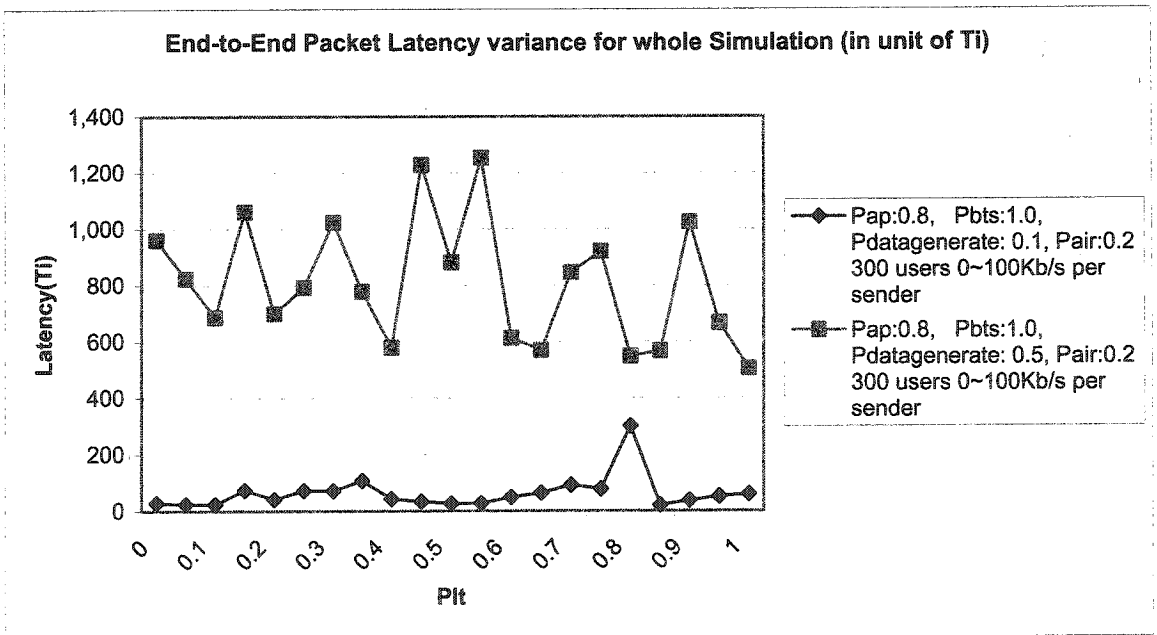

Figure 5.41 End-to-End Packet Latency variance for whole Simulation with Plt increasing

From Figures 5.36 ~ 5.41, the following is observed:

- With Plt increasing, the throughput increases and latency decreases.
- With Plt increasing, the number of received packets does not change much.

5.5 Reseach summary and Future Work

This chapter has presented conclusions based on the WLAN and GPRS inter-working model. The goal of this reseach was to design, implement and test the netowrk level simulation to investigate the issues and tradeoff for the interworking. From the results presented in section 5.4, we conclude that the implementation of AP in the GPRS network is a complement to the whole network from the performance prospective, especially during the heavy traffic. Also there are two ways to have the AP connected to GPRS network, tight coupling and loose coupling. From the simulation results, we can see that tight coupling reduces the packet latency, which means it will be suitable for the voice over IP applications. Also the hybrid tight/loose coupling APs connected the network is not that complicated. From the results, we can also see that the operators of GPRS networks can bring the WLAN solution into the core network gradually either in loose coupling or tight coupling or in both. And the performance improvement is tremendous. In this way, it is easy to control the investment and get the revenue from extra high-speed services. Also we can see from the results, with the whole tight coupling system, the network is better structured and the APs will be easy to manage as those are connected directly to SGSNs. More than that, the Mobile IP is not necessary for the roaming function in that case and we even have the QoS guaranteed all over the whole network.

In this simulation, the IP overhead and QoS are not considered. There are left for the future research.

References

[1] SMS Forum "SMPP v3.4 Protocol Implementation guidance for GSM/UMTS" Version 1.0

[2] M.Sreetharath and Rajiv Kumar "Cellular Digital Packet Data" Artech House, June, 1996

[3] GSM 09.60: - "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface", ETSI.

[4] 3GPP2 X.P0011-001-C v.01, "CDMA2000 Wireless IP Network Standard"

[5] A.Furuskar et al., "EDGE: Enhance Data rates for the GSM and TDMA/136 Envolution", IEEE Personnal Xommunication, June 1999, Vol.6, No.3

[6] 3G TR 22.934:"Feasbility study on 3GPP system to Wireless Local Area Network (WLAN) interworking" Release 6, version 1.0.0 February 2002

[7] ESTI TR 101 957:"Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular systems" V1.1.1 (2001-08)

[8] Jijun Luo, Rahul Mukerjee, Markus Dillinger, Eiman Mohyeldin, and Egon Schulz, SIEMENS AG "Investigation of Radio Resource Scheduling in WLANs Coupled with 3G Cellular Network" IEEE Communication magazine, June 2003

[9] http://www.computer.org/students/looking/summer97/ieee802.htm

[10] ANSI/IEEE Std 802.11, "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999 Edition.

[11] http://www.it.iitb.ac.in/~satyajit/seminar

[12] Universal Mobile Telecommunications System (UMTS);Feasibility study on 3GPP system to Wireles Local Area Network (WLAN) interworking (3GPP TR 22.934 version 6.2.0 Release 6)

[13] Prof. Dr. Jorg Eberspacher, Technische university Munchen, "GSM Switching, Services and protocol"

[14] 3GPP, "BSS GPRS protocol," 3GPP TS 08.18 V8.10.0

[15] General Packet Radio Service (GPRS), Radio Link Control/Medium Access Control (RLC/MAC) protocol, 3GPP TS 44.060 version 4.9.0 Release 4

[16] GSM 03.03: - "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification", ETSI.

[17] TS 22.060 General Packet Radio Service (GPRS); Service description; Stage 1

[18] TS 44.064 Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification

[19] C.Perkins, "IP Mobility Support IPV4", RFC3344, January 2002

[20] C. Perkins and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions", RFC3012, Nov. 2000

[21] C. Rigney, Livingston, "Radius Accounting V2", RFC2866, June 2000

[22] Behet Sarikaya, "Packet Mode in Wireless Network: Overview of Transition to Third Generation", IEEE Communications, September 2000 Vol.38 No.9, PP164-172

[23] Antoine Stephane, Andrej Mihailovic and A.Hamid Aghvami, "Mechanism and Hierarchical Topology for Fast Handover in Wireless IP network", IEEE Communications, November 2000 Vol.38 No.11, PP112-115

[24] Chen Yi-an. *A Survey Paper on Mobile IP.* http://www.cis.ohio-state.edu/~jain/cis788-95/mobile_ip

[25] RFC 2003 - IP Encapsulation within IP. http://www.ietf.org/rfc/rfc2003.txt. October 1996.

[26] G. Montenegro, "Reverse Tunneling for Mobile IP", RFC2344, May 1998

[27] Johan Bergkwist, Hohan Engren, Ola Eriksson,"WLAN as a Complement to UMTS" in May23, 2002 commissioned by Ericsson

[28] Apostolis K. Salkintzis, "Interworking Between WLANs and third Generation Cellular Data Networks" in 2003 IEEE 0-7803-7757-5/03, P1802~P1806

[29] Ala-Laurila Juha, Mikkonen Jouni, Rinnemaa Jyri, "Wireless LAN Access Network Architecture for Mobile Operators" in IEEE Communication Magazine Nov. 01.

[30] 3GPP TS 22.129: "Handover Requirements between UTRAN and GERAN or other Radio Systems"

[31] Apostolis K. Salkintzis, 0-7803-7757-5/03, 2003, IEEE, "Interworking Between WLAN and Third Generation Cellular Networks".

[32] 3GPP TS 29.061, "Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Network (PDN)," 2002.

[33] ETSI TR 101 957 v1.1.1 (2001-08) Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Requirements and Architecture for the Interworking Between HIPERLAN/2 and 3rd Generation Cellular systems

[34] RFC 2486 (1999) "The Network Access identifier".

[35] Apostolis K. Salkintzis, "Interworking Techniques and Architectures for WLAN/3G Integration Towards 4G Mobile Data Networks".

[36] Swapuinil K.Raktale, Ashok Kumur, Hugher Siftware System "WLAN-3GPP Intergation Architectures for Packet Based Data Service".

[37] Gabriel Cristache, Klaus David, Matthias Hildebrand in 3rd Scandinavian Worshop on Wireless Ad-hoc Network, "Aspect for the integration of Ad-hoc and cellular Networks".

[38] XinGang Wang, John Mellor and Khalid Al-Begain, "Towards Providing QoS for the Integarted Cellular And WLAN Networks" in ISBN:1-9025-6009-4@2003 PGNET

[39] Muhammad Jaseemuddin, "An Architecture for Integrating UMTS and 802.11 WLAN Networks" in preceedings of IEEE Symposium on Computers and Communications, Antalya, PP.716-723, 2003

[40] Ye Min-hua, Liu Yu, Zhang Hui-min, "The Mobile IP Handoff Between Hybrid Networks"in 0-7803-7589-0@2002 IEEE.

[41] Stefan Aust, Daniel Proetel, Andreas Konsgen, Cornel Pampu, Carmelita Gorg, "Design Issue of Mobile IP Handoffs between General Packet Radio Service (GPRS) Networks and Wireless LAN (WLAN) System" in IEEE Wireless Personal Multimedia Communication, P27-30 Oct, 2002.

[42] M.Ylianttila, M.Pande, J.Makela, P.Mahonen, "Optimization Scheme for Mobile User Performance Vertical Handoffs between IEEE 802.11 and GPRS/EDGE networks" in IEEE Global Telecommunications Cerference, Page 25-29 Nov, 2001.

[43] Hui Luo, Zhimei Jiang, Byoung-Jo Kim, N.K.Shankaranarayanan and Paul Henry, "Integrating Wireless LAN and Cellular Data for the Enterprise" in IEEE Internet Computing, March, 2003.

[44] Angela Doufexi, Eustace Tameh, Andrew Nix and Simon Armour, "Hotspot Wireless LANs to Enhance the Perfirmance of 3G and Beyond Cellular Networks" In IEEE Communication Magazine, July 2003.

[45] Hong-Yon Lach, Christophe Janneteau and Alexandru Petrescu, "Netowrk Mobility in Beyond-3G Systems" in IEEE Communication magazine, July 2003.

[46] Fabio M.Chiussi, Denis A.Khotimsky and Santosh krishnan, "Mobility Management in Third-Generation All-IP Networks" in IEEE Communications Magazine, Sep 2002.