

PROTOCOL DEVELOPMENT AND PERFORMANCE
ANALYSIS OF WIP AND WMPLS WIRELESS
NETWORKING TECHNOLOGIES

By

KANNAN SRINIVASAN

Bachelor of Engineering

University of Madras

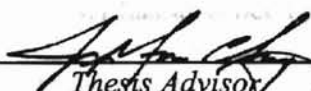
Chennai, India

2000

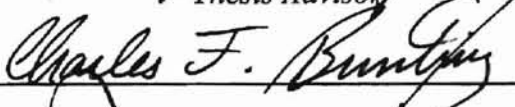
Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
August, 2002

PROTOCOL DEVELOPMENT AND PERFORMANCE
ANALYSIS OF WIP AND WMPLS WIRELESS
NETWORKING TECHNOLOGIES

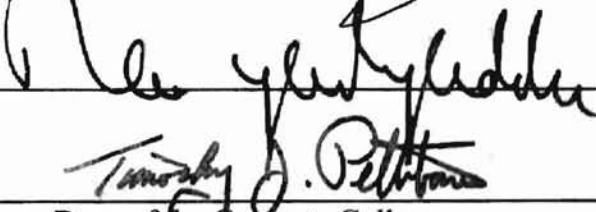
Thesis Approved:



Thesis Advisor



Charles F. Buntz



Timothy J. Petterson

Dean of the Graduate College

PREFACE

This thesis is based on two new wireless protocols that can support soft handoff over the wireless network. In this thesis, a network layer protocol called Wireless Internetworking Protocol (WIP) and novel data layer protocol called Wireless Multiprotocol Label Switching (WMPLS) protocol have been introduced. The performance analysis of WMPLS compared to an existing wireless network access layer protocol called wireless ATM (WATM) has also been given in detail to demonstrate the advantages of WMPLS over WATM.

Traditional IP assumes fixed IP assignment to the hosts for the entire duration of a connection. Hence, IP does not support soft handoff over wireless networks. WIP is a new protocol that has been proposed as an extension to IP in the networking layer, to make soft handoff possible with IP. WIP technology enables the wireless hosts to be mobile while establishing soft handoffs in support of high quality of service (QoS) for real-time data traffic over mobile wireless environments. WIP technology solves some of the fundamental problems of mobile IP (MIP), such as the triangle routing problem and the requirement of redundant buffering, comparing and transferring of stacks of data between the foreign agents and the mobile host (MH). WIP enables make-before-brake soft handoff procedures, which enables end-to-end reliability through transport control

protocol (TCP) connections to provide full connectivity during handoff procedures thereby reducing the number of undetectable lost packets during the handoff instants.

WMPLS has been designed to be a homogeneous protocol to multiprotocol label switching (MPLS), generalized MPLS (GMPLS), and MPLambdaS, which are the strongest candidates for next generation wide area networking (WAN) technologies. The protocol format of WMPLS closely resembles the original MPLS protocol architecture with wireless communication link reliability enhancements. Integrated & differentiated services can be provided in broadband mobile communications through the classification, queuing, and scheduling (CQS) mechanism of WMPLS systems. This paper provides the framework of WMPLS and its signaling protocols to establish connection-oriented and connectionless label switched paths (LSPs). Due to various inefficiencies with WATM such as fixed cell size, no support for differentiated services, poor support for dynamic multicasting and poor performance with ad hoc mobile networking, WMPLS has been strongly suggested as future wireless networking protocol. Performance analysis of WMPLS carried out for this thesis proves some of the advantages of WMPLS over WATM.

ACKNOWLEDGMENTS

I wish to express my deep and sincere thanks and gratitude to my advisor Dr. Jong-Moon Chung for his supervision, support, critical suggestions, and inspiration without whom this thesis would not have been possible. My appreciation and thanks are also due to my committee members, Dr. R. K. Yarlagadda and Dr. Charles Bunting for their invaluable support, assistance, encouragement and guidance throughout my Master's program here at the Oklahoma State University.

I would like to thank the Advanced Communication Systems Engineering Laboratories (ACSEL) at the Oklahoma State University for supporting resources. I would like to thank my group members for their contribution. I would also like to thank other members of the ACSEL laboratories for their recommendations and support and my friends who made my thesis work an enjoyable and pleasant one.

I would like to thank my parents, my sister and my brother for their support and encouragement. Finally, I would like to thank and dedicate this work to my fiancée Ms. Kadambari Kaluri without whom completion of this work would have been impossible.

TABLE OF CONTENTS		39
Chapter		Page
I. INTRODUCTION.....		10
II. LITERATURE REVIEW.....		4
2.1 Mobile IP (MIP).....		4
2.1.1 Handover in MIP.....		6
2.2 Brief Introduction to HAWAII.....		7
2.2.1 HAWAII Path Setup Schemes.....		8
2.2.1.1 Multi-Stream Forwarding (MSF) and Single Stream Forwarding (SSF).....		9
III. WIRELESS INTERNETWORKING PROTOCOL.....		13
3.1 A brief overview of WIP.....		13
3.2 Wireless IP Packet Format.....		14
3.3 Wireless IP Operations & Architecture.....		17
3.4 Fetching an IP address for the next possible subnet.....		20
3.5 Preparing for Handoff.....		21
3.6 Packet Re-encapsulation during Handoff.....		23
3.7 Handoff Completion.....		24
3.8 Enquiry and Registration Procedures.....		26
IV. TCP FOR WIP.....		27
4.1 TCP Over WIP.....		27
V. WIP Over Bluetooth.....		31
5.1 WIP Over Bluetooth.....		31
5.2 Selection of a next possible Base Station (BS).....		32
5.3 Master-to-Slave Switching.....		33
VI. WIP OVER IMT-2000.....		35
6.1 IMT-2000.....		35
6.2 Inter-Cell Soft Handoff.....		35
6.3 WIP Over IMT-2000.....		36

VII. Wireless Multiprotocol Label Switching (WMPLS).....	39
7.1 Wireless ATM (WATM).....	40
7.1.1 WATM Limitations and Challenges.....	42
7.2 WMPLS Networking.....	46
7.3 Extensions to RSVP-TE for WMPLS.....	50
7.4 Extensions to CR-LDP for WMPLS.....	52
7.5 Handover in WMPLS Mobile Communication Networks.....	53
7.5.1 The Proposed Network Topology.....	54
7.5.1.1 Initial Path Setup.....	55
7.5.1.2 Path Establishment during Handover.....	58
7.5.2 WMPLS over IMT-2000.....	61
VIII. WMPLS Performance Analysis.....	66
8.1 WMPLS Performance Analysis Based on GoBackN Technique.....	66
8.2 WMPLS Performance Analysis Based on SREJ Technique.....	72
IX. Conclusion.....	77
REFERENCES.....	79

LIST OF FIGURES

Figure	Page
1 Triangle Routing Problem with MIP	5
2 Domain Hierarchy in HAWAII	8
3 Typical HAWAII Network Domain	9
4 Forwarding Schemes	11
5 Non-Forwarding Schemes	12
6 Protocol layer stack of WIP and relevant networking protocols	14
7 WIP, MIP and ROMIP Packets	14
8 WIP Packet Format	15
9 WIP Packet Types.....	16
10 Fetching an IP for the next possible subnet.....	21
11 Client IP notification for WIP handoff procedures.....	22
12 Packet Re-encapsulation for data forwarding over WIP Networks	24
13 Src/Dstn routing table information update process.....	25
14 TCP operations with a WIP translator interoperating between the WIP non-supportive network and the WIP network.....	30
15 WIP handoff operations in support of Bluetooth system connectivity.....	32
16 Flow chart of WIP handoff procedures in support of Bluetooth system connectivity.....	34
17 WIP handoff operations in support of IMT-2000 mobile communications services.....	36

Figure	Page
18	Flow chart of WIP handoff procedures in support of IMT-2000.....38
19	Functional diagram of the LSR CQS operation.....47
20	MPLS protocol structure.....48
21	Format of the RSVP-TE..... 52
22	Format of the CR-LDP..... 53
23	The proposed WMPLS networking topology..... 55
24	Initial Path Setup..... 58
25	Path Establishment during Handover..... 59
26	Message and Data Flow during and after Handover..... 61
27	WMPLS Over IMT-2000..... 63
28	Error Control Algorithm..... 67
29	WMPLS Performance with GoBackN for BER = 10^{-4}69
30	WMPLS Performance with GoBackN for BER = 10^{-6}71
31	Optimal WMPLS Packet Size..... 74
32	WMPLS Performance with SREJ ARQ.....75

CHAPTER I

INTRODUCTION

LIST OF TABLES

Table		Page
1	WMPLS header Flag bits	48
2	WMPLS header flow control and error control acknowledgement control bits.....	50

CHAPTER I

INTRODUCTION

The popularity of wireless mobile communication systems has significantly increased during the past decade where now nearly half of the telephone lines of the world are supporting wireless communication devices. Standard IP assumes fixed IP addressing to hosts till the end of communication. But the mobile hosts (MHs) that keep changing their point of attachment and thus change their IP addresses during the connection phase cannot be supported by the standard IP protocol. Mobile IP (MIP) was developed to provide a solution to this problem. Research on MIP has been done for years and MIP has been considered to be a future mobile communications protocol.

The focus of this thesis is to address some of the basic problems that MIP faces and to provide a viable solution to those problems. As a solution to those fundamental problems, in this thesis, a novel IP layer protocol called wireless internetworking protocol (WIP) has been developed. WIP has been designed to enable reliable data communication services in the IP layer over various novel wireless communication architectures.

The basic assumption of WIP is that the underlying wireless communication systems (e.g., cellular phones, Bluetooth [19, 31], International Mobile Telecommunications (IMT-2000) [29], etc.) will allow the MHs to participate in more than one network, simultaneously during handoff procedures. This assumption of WIP enables a make-before-break type soft handoff to be possible for the real-time traffic over the wireless environment. WIP has been developed to enable IP layer soft handoff operation and to enhance the overall.

WIP also assumes availability of two active IP addresses for a mobile device during handoff. WIP also provides a way to keep the same TCP connection alive during and after handoff, thus enabling efficient and continuous data flow throughout. WIP informs the node that is communicating with the MH, called as the correspondent node about the MH's handoff to a different subnet. This has been already suggested for route optimized mobile IP (ROMIP). In addition, minimal encapsulation of the headers has been suggested as well. The difference here is that the correspondent node does not need to do encapsulation of packets to the MH.

Another major objective of this thesis is to investigate the network access layer protocols for the support of mobile data communications. Wireless ATM is considered an effective and favorable network access layer protocol for mobile data communications. The reason for this is that ATM has been the most prominent wide area network (WAN) topology and that WATM is homogeneous with ATM. Since advanced protocols with differentiated services support and other traffic engineering (TE) parameters support, like multiprotocol label switching (MPLS), generalized MPLS (GMPLS) and MPLambdaS have been proposed and are potential future WAN protocols, there is a need for the wireless version of these future protocols. In this thesis, wireless MPLS (WMPLS) has been proposed to be a homogeneous protocol with MPLS, GMPLS, and MPLambdaS networking. WMPLS has been developed to provide differentiated services (DS) over the wireless network along with other traffic engineering (TE) features. Through the use of signaling protocols like label distribution protocol (LDP) and resource reservation protocol with traffic engineering extensions (RSVP-TE), WMPLS is also capable of providing effective and efficient mobile ad hoc networking and dynamic multicasting. It

has also been shown through performance analysis that WMPLS has better throughput efficiency than WATM under varying channel conditions, applying GoBackN and SREJ ARQ packet/cell error recovery.

CHAPTER II

LITERATURE REVIEW

2.1 Mobile IP (MIP)

In this subsection, a brief introduction to mobile IP (MIP) has been given. In MIP, every MH is uniquely identified with an IP address called home address. This is the address that a MH is assigned in its home network, where it actually belongs. As the MH moves, it enters different subnets and may need to get a new IP address for that subnet. This new IP address is called its collocated care-of address. This new network is called a foreign network. The router in this foreign network is called a foreign agent. The MHs know that they are entering a new foreign network because of agent advertisements they receive from an agent. For this reason, all the agents are required to advertise themselves frequently on their local links. Whenever a MH moves to a network other than its home network, it has to register the care-of address with a router in its home network, called as home agent. This care-of address can either be a collocated care-of address, which is the MH's IP address in the foreign agent or can be a foreign agent care-of address, which is the IP address of the foreign agent itself.

When a MH is away from its home network, all the packets destined for the MH will be intercepted by its home agent and will be tunneled to MH's care-of address. If the care-of address is the collocated care-of address then the MH is the end point of the tunnel. But if the care of address were the foreign agent care-of address, then the foreign agent will be the end point of the tunnel and the foreign agent will have to decapsulate all the packets for MH and forward them to MH. But if the MH has to send anything, it will

send the packets using standard IP routing directly to its correspondent node. As it is obvious, there is a virtual triangle route between the correspondent node, home agent and MH as shown in Fig. 1. Since, MIP requires all the packets to be first intercepted by a home agent and then tunnel packets to MH; this will lead to a sub-optimal route between the home agent and MH when actually the correspondent node could have sent them directly to MH in an optimized route. This is called triangle routing problem (Refer Fig. 1). Because of this, there will be additional delay experienced by packets received at MH if MH is far away from its home network. Also, tunneling of packets includes more header to a packet and since every packet has to be tunneled to MH, there will be a tremendous wastage of network capacity over time, even if minimal header encapsulation is adopted.

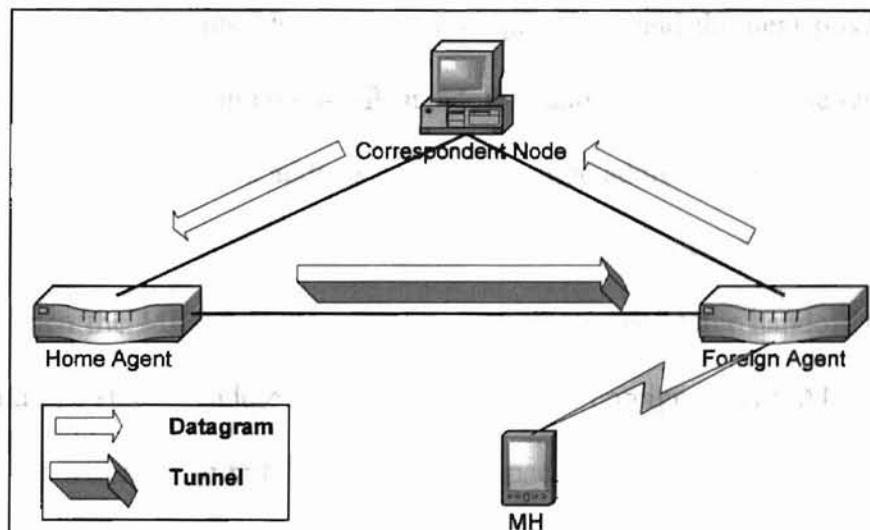


Fig.1 Triangle Routing Problem with MIP

There is a route optimized mobile IP (ROMIP) protocol that has been proposed to solve the triangle routing problem. In ROMIP, the source is informed of MH's handover and the source tunnels directly all the packets destined to MH. Although this solves the

triangle routing problem, the problem of additional overhead in every packet due to tunneling still remains.

2.1.1 Handover in MIP

This section explains how handover has been dealt with in MIP. Actually, MIP has been proposed for macromobility between subnets. But for micromobility within a subnet, HAWAII and Cellular IP (CIP) [32] have been suggested. The entire wireless network is designed such that there are frequent micromobilities than macromobilities. HAWAII [32] is capable of doing smooth handoff and has been considered a potential protocol for micromobility.

For macromobility with MIP, MIP requires buffering and transferring stacks of data between the Foreign Agents (the previous Foreign Agent and the next possible Foreign Agent) for achieving smooth (semi-soft) handoff is another problem. The requirement of the MH to buffer stacked data address pairs (the source address and identification) of all the packets it received will result in a significant waste of processing time and memory especially when the MH stays longer in the same network. After handoff the MH will have to send this stack of address pairs to its previous Foreign Agent. Also the previous Foreign Agent will have to buffer all of the data packets that are destined for the Mobile Agent from the time the connection was established, which also includes the packets received during handoff and after. Then the previous Foreign Agent will have to conduct a comparison of the stacked packets with the stack of address pairs sent by the MH in order to identify the old and new packets that were received during the handoff procedure and then will send only the new packets to the MH. If either the Foreign Agent or the MH

is to run out of memory and not able to buffer this stack of forwarding packets then the stack of packets may be lost in whole or in part, which will result in a low reliability performance.

2.2 Brief Introduction to HAWAII

This section has been explained based on [32]. While MIP has been suggested for macromobility, HAWAII is a protocol that has been strongly considered for micromobility. HAWAII makes use of specialized path setup schemes in order to do micromobility. These schemes require some of the routers in the network to store host-based forwarding. HAWAII assumes IP address of MH to remain unchanged, which also solves the problems related to QoS and TCP connections.

In HAWAII, MHs retain their network address while moving within a domain. Both the home agent and the correspondent node are unaware of micromobility of MHs. The requirement of storing forwarding entries at the routers may be a challenge while discussing scalability issues.

HAWAII requires the entire wireless network to be divided into hierarchical domains (Refer to Fig. 2). For the mobility within a domain, the MH does not change its IP address. Every domain has a gateway that is called the domain root router, which receives the packets destined for MH first and then forwards them to the appropriate MH through dynamically established paths.

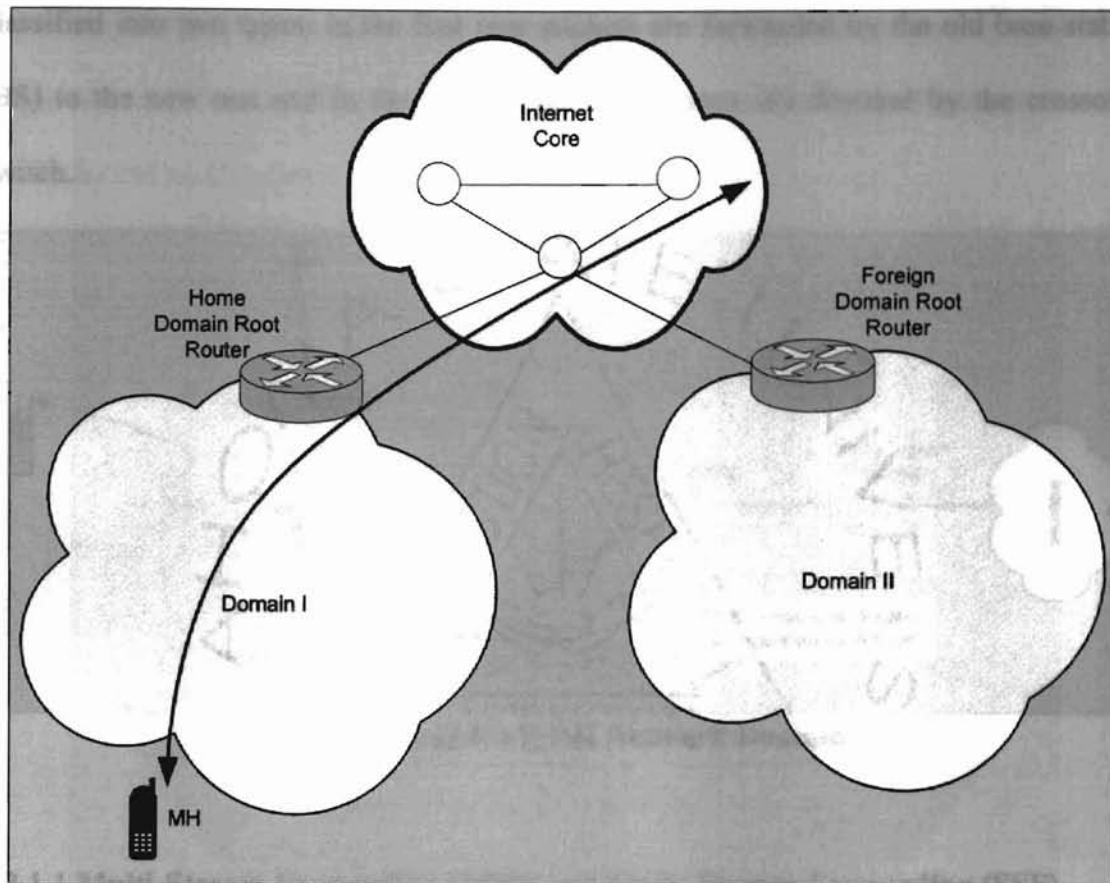


Fig.2 Domain Hierarchy in HAWAII

As soon as a MH powers up, it sends a *path setup power-up* message. This message will be used to establish a path between the MH and its domain root router. When the MH is moving to a foreign domain, HAWAII uses *path setup* messages to establish and update host-based routing entries for the MH. MH has to occasionally keep refreshing its path to its base station in order to keep it alive. The base station and the intermediate routers will then send periodic *aggregate hop-by-hop refresh* messages towards the domain root router.

2.2.1 HAWAII Path Setup Schemes

Four path setup schemes have been proposed for the establishment of a path while the MH is moving to a foreign agent within a subnet [32]. They can be broadly

classified into two types: in the first type packets are forwarded by the old base station (BS) to the new one and in the second type the packets are diverted by the crossover switch.

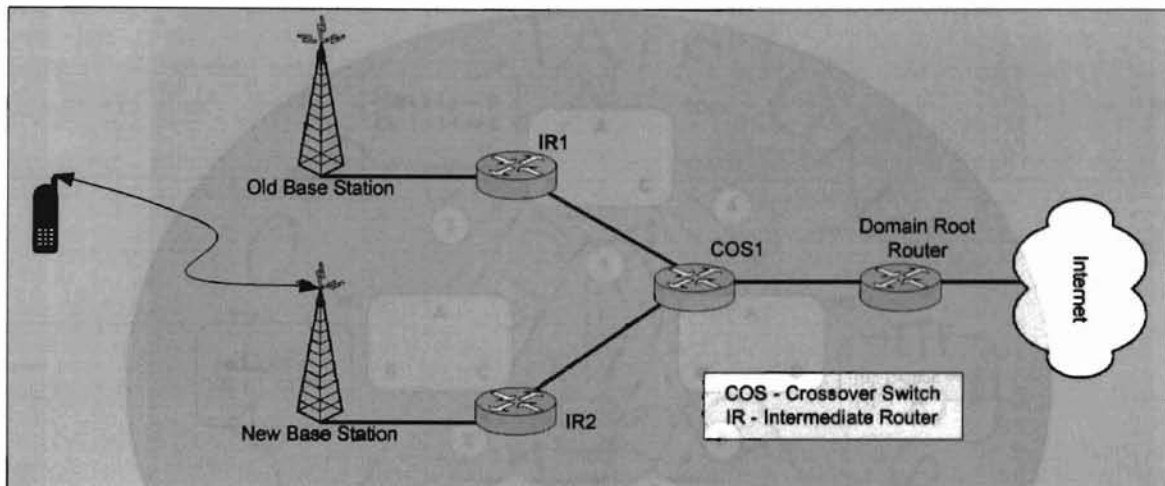


Fig.3 Typical HAWAII Network Domain

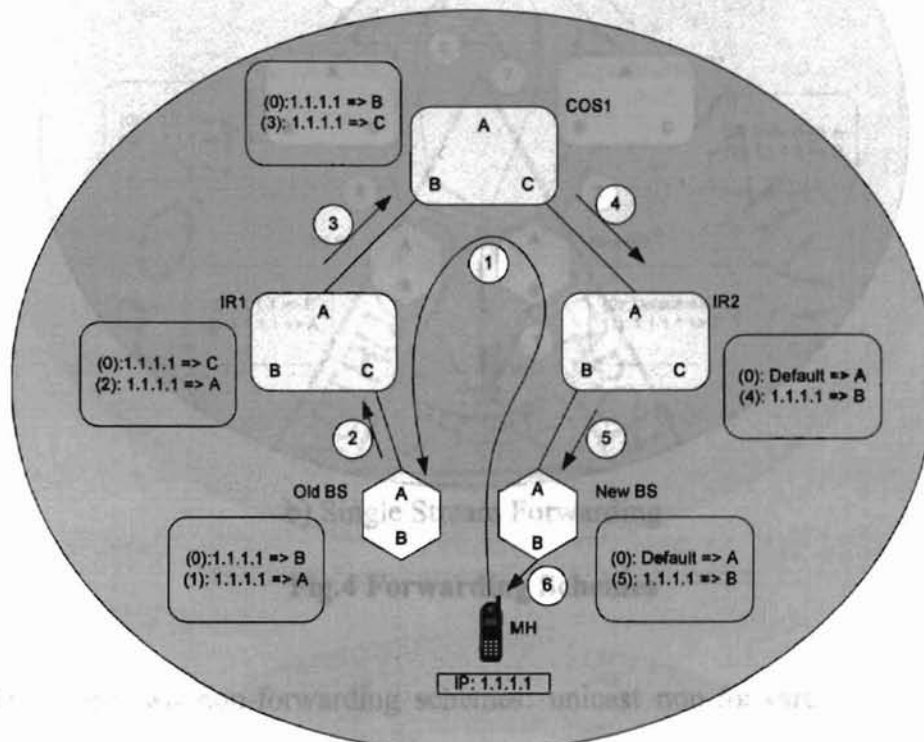
2.2.1.1 Multi-Stream Forwarding (MSF) and Single Stream Forwarding (SSF)

Under the forwarding scheme, there are two protocols namely the multi-stream and the single stream forwarding schemes. In these schemes, the packets are first forwarded by the old BS and then are diverted by the crossover switches.

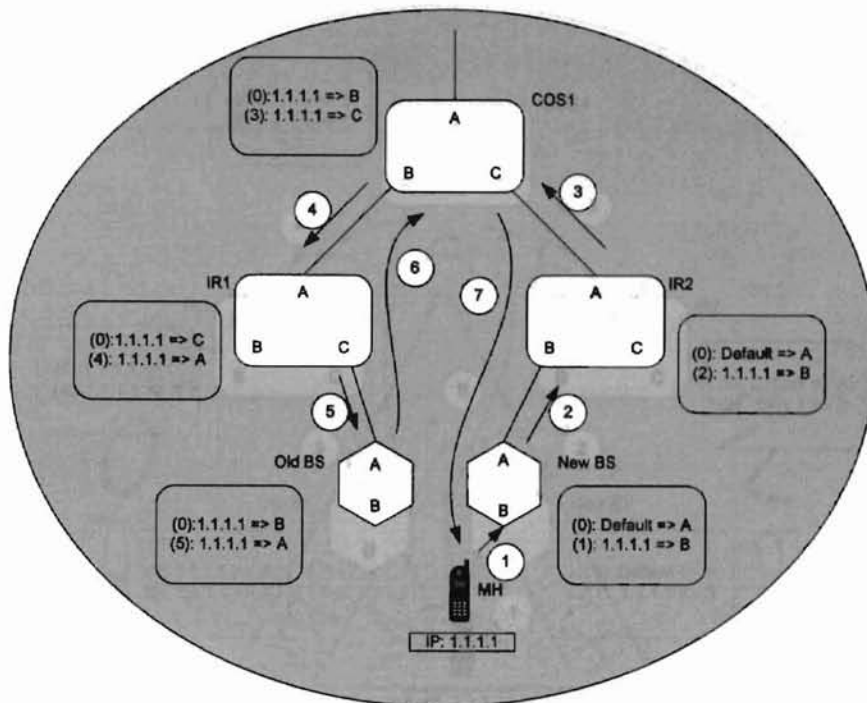
In MSF (Refer Fig. 4a) scheme, MH will send a path setup message to old base station through new base station. Once this message reaches the old base station, the old base station will change its forwarding table accordingly and forward this message to its next hop router. The next hop router does the same and finally the message reaches the new BS through the crossover switch. The new base station also adjusts its forwarding table and sends an acknowledgement to MH.

The disadvantage in the MSF is that the packets may arrive in different orders at the MH. The packets from COS1 may arrive earlier than the packets from BS1. To

overcome this problem, single stream forwarding (Refer Fig. 4b) has been proposed. In single stream forwarding the forwarding table is adjusted first by new base station and finally by old base station.



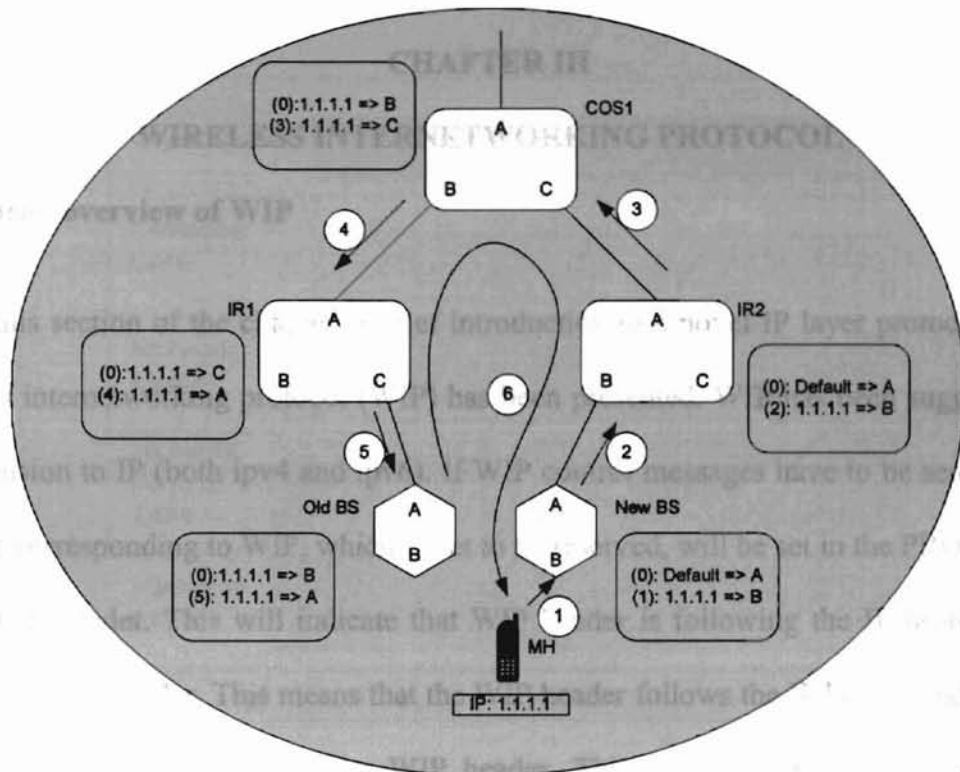
a) Multi-Stream Forwarding



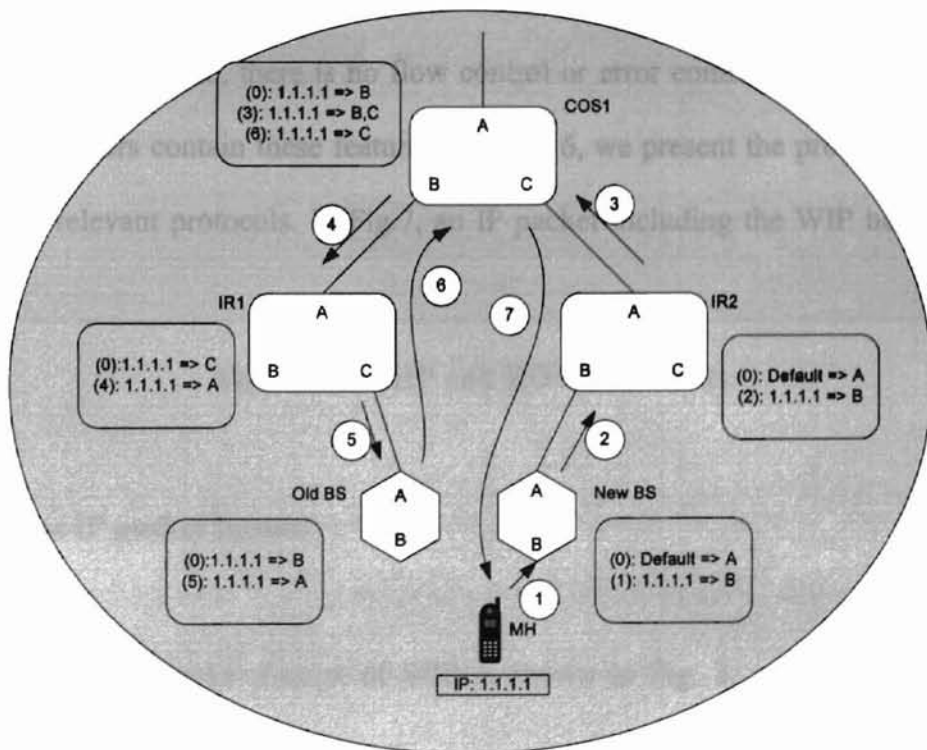
b) Single Stream Forwarding

Fig.4 Forwarding Schemes

There are two non-forwarding schemes: unicast non-forwarding and multicast non-forwarding. The unicast non-forwarding (UNF) is optimized for networks where the MH can listen to more than one BS. The multicast non-forwarding (MNF) is suitable for the MHs that cannot listen to two BSs simultaneously. Actually in MNF scheme, dual-casting takes place in which the COS dual-casts packets to both old BS and new BS. In this case, when the new base station receives the path setup message, it adds a forwarding entry for the mobile host's IP address with the outgoing interface set to the interface on which it received this message. It then performs a routing table lookup for the old base station and determines the next hop router, IR2. The new base station then forwards Message 2 to IR2. This router performs similar actions and forwards Message 3 to COS1.



a) Unicast Non-Forwarding (UNF) Scheme



b) Multicast Non-Forwarding (MNF) Scheme

Fig.5 Non-Forwarding Schemes

CHAPTER III

WIRELESS INTERNETWORKING PROTOCOL

3.1 A brief overview of WIP

In this section of the chapter, a brief introduction to a novel IP layer protocol called wireless internetworking protocol (WIP) has been presented. WIP has been suggested as an extension to IP (both ipv4 and ipv6). If WIP control messages have to be sent, then a number corresponding to WIP, which is yet to be reserved, will be set in the PROTOCOL field of IP header. This will indicate that WIP header is following the IP header as an extension to IP header. This means that the WIP header follows the IP header and that the transport layer header follows the WIP header. This enables WIP to work with the network access layer protocols providing WIP with more controllability over the network physical resources. Also, there is no flow control or error control in WIP as the IP and the transport layers contain these features. In Fig. 6, we present the protocol layer stack of WIP and relevant protocols. In Fig.7, an IP packet including the WIP header field is shown.

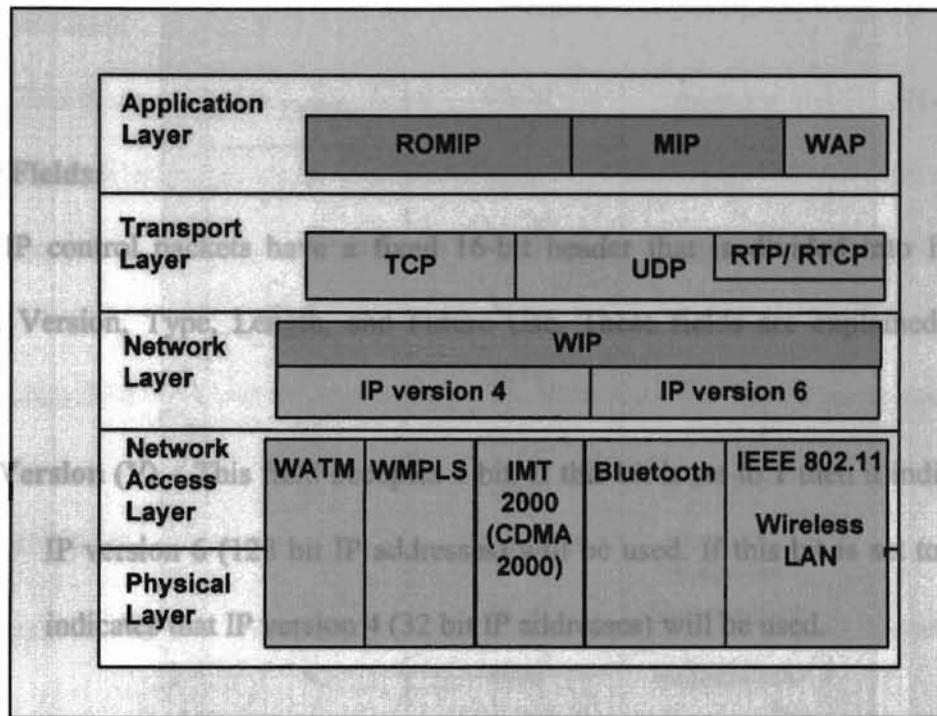


Fig.6 Protocol layer stack of WIP and relevant networking protocols.

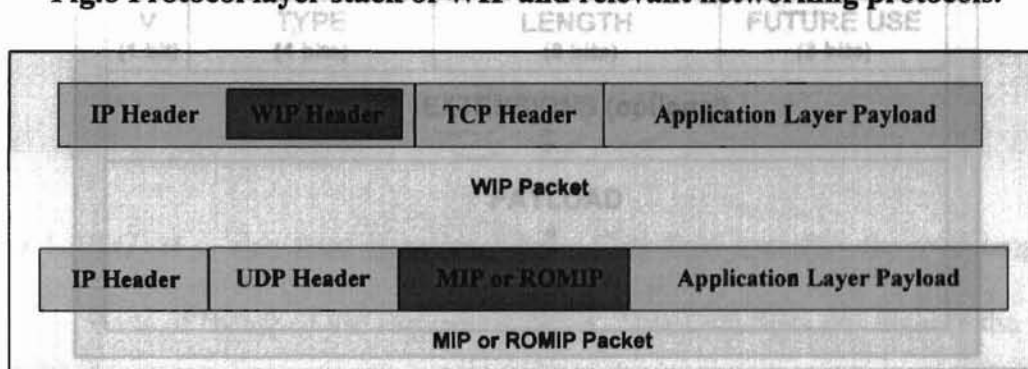


Fig.7 WIP, MIP and ROMIP Packets

3.2. Wireless IP packet format

The general packet format of WIP is shown in Fig. 8, and the fields of WIP protocol are introduced below.

Header Fields:

WIP control packets have a fixed 16-bit header that is divided into five fields namely: Version, Type, Length, and Future Use. These fields are explained in detail below.

- **Version (V)** – This field occupies 1 bit. If this bit is set to 1 then it indicates that IP version 6 (128 bit IP addresses) will be used. If this bit is set to 0 then it indicates that IP version 4 (32 bit IP addresses) will be used.

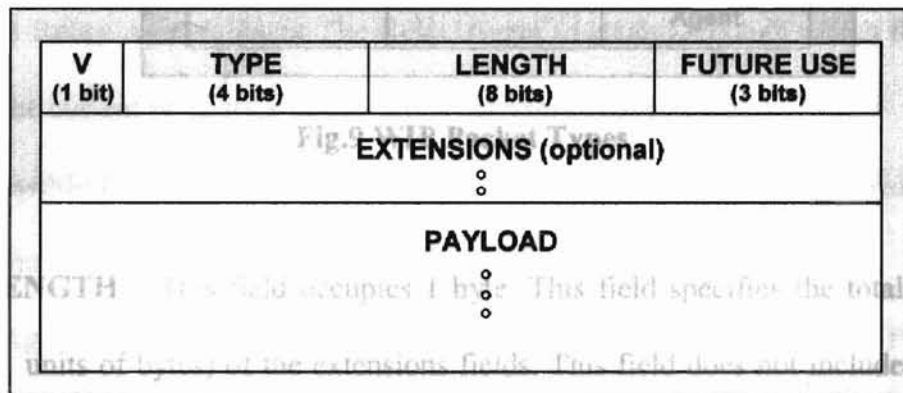


Fig.8 WIP Packet Format

- **TYPE** – This field occupies 4 bits that indicate the type of the packet. The following table lists the types of packets and their codes from Type 0 to Type 9. Type 10 to Type 15 are reserved for future use.

Extension Field

This is an extension to the header. This field may contain the Min's new address or stack IP address or any other useful information. This field may be followed by a payload depending on the WIP control packet.

Payload Field

TYPE	CODE (in binary)	PACKET
0	0000	CNI
1	0001	CNIACK
2	0010	COI
3	0011	COIACK
4	0100	FLUSH
5	0101	ENQUIRY
6	0110	ENQUIRY Response
7	0111	DISCONNECT
8	1000	Registration
9	1001	Advertisement Agent

Fig.9 WIP Packet Types

- **LENGTH** – This field occupies 1 byte. This field specifies the total length (in units of bytes) of the extensions fields. This field does not include the length of the payload, since the actual length of the payload part can be found from the “Length” field of the IP packet.
- **Future Use** – This field occupies 3 bits and is reserved for future applications. For example, this field could be used to support priority class assignments in differentiated services.

Extension Field: This is an extension to the header. This field is optional. This field may contain

the MH's new IP address or its old IP address or any other useful information. This field may or may not be followed by a payload depending on the type of WIP control packet.

Payload Field:

This field will hold the application data to be sent, if necessary with padding. This field will hold the application data to be sent by the MH, although the control packet was actually sent

3.3. WIRELESS IP OPERATIONS & ARCHITECTURE

Wireless IP defines three types of Relay Agents and eight types of control packets.

The three Relay Agent types are:

- **Current Relay Agent (RAc):** The Relay Agent (a router) through which the MH has obtained the current IP address in use and is currently connected to.
- **Next possible Relay Agent (RAn):** The Relay Agent (a router) through which the MH will be communicating with its correspondent node.
- **Home Agent (HA):** This relay agent is the same as it is described in MIP and is the router in the home network of a MH. Home address and home network are the terminologies that remain same as they are in MIP.

The ten control packet types are:

- **CNI (client's new IP address):** This packet informs the destination host of the MH's new IP address. The name "client" has been used just for convenience and always refers to MH. This packet is sent by the MH to the correspondent node. This packet will contain the header followed by the client's (MH's) new IP address and its home address

in the extension of the header. It has been assumed that all the routers can read into WIP headers and so will be able to distinguish different types of WIP packets. The RAc will look into the packet and then forward it to the correspondent node that is communicating with the MH. This packet can also have data (and some padding if needed).

- **CNIACK** (CNI acknowledgment): This packet is transmitted by the RAc to the MH in response to the CNI packet sent by the MH. Although the CNI packet was actually sent by the MH to the correspondent node, since all the routers are allowed to read into WIP headers, the RAc will be able to identify a CNI packet. This packet will have the header followed by data if necessary (and padding if needed).
- **COI** (client's old IP address): This packet will inform the target host of the MH's previous or old IP address. This packet is sent by the MH to the RAn. This packet will have the header followed by the client's old IP address and its home address in the extension of the header. This packet will not have any payload field.
- **COIACK** (COI acknowledgment): This packet is sent by the RAn in response to the COI packet. This packet will have only the header. Data will not follow the header.
- **FLUSH**: This packet is sent by the correspondent node to both RAc and the MH in response to the CNI packet forwarded by the RAc. This packet will not have the extension field. Data may follow the header for the packet that is sent to the MH through RAn. However, for the packet that is sent to the RAc, there will be no data field.
- **ENQUIRY**: This packet is sent by a node that wants to communicate with MH. This packet will be sent using MH's home address. Hence, this packet will be intercepted by

MH's home agent. The home agent after receiving this packet should send an enquiry response message with MH's new IP address. This node can now directly try to access the MH using its new IP address. This packet will have nothing but the WIP header with type field indicating '5'. There is no extension field in the header and no payload field.

- **ENQUIRY Response:** This packet is sent by a home agent of a MH to a node that enquired about MH. This packet will include MH's new IP address in the extension field of WIP. This packet will have no payload following the header.
- **DISCONNECT:** This packet is sent by the MH to inform all the devices involved in the connection between itself and the correspondent host about the termination of the connection. This packet will have just the header field.
- **Registration:** This packet is sent by the MH to its home agent in order to register its new IP address. This packet has the header followed by the MH's IP and its home address in the extension of the header. This packet will have no payload following the header.
- **Agent Advertisement:** This packet is sent by all the relay agents on their local links to advertise themselves. This packet will have the header followed by the IP address of the relay agent in the extension of the header. This packet will have no payload following the header.

In the following section, WIP procedures have been explained in detail. The procedures explained below assume DHCP protocol for IP address allocation for a subnet. Using DHCP has been suggested and is not a requirement for WIP. Also, the use of collocated care-of address for MH has been suggested and assumed, although foreign

agent care-of address is also possible. If the foreign agent care-of address were to be used, the following procedures will be different, in that the CNI packet will not hold MH's new address instead it will hold IP address of RAN and the end point of the tunnel would be RAN, not the MH.

3.4. Fetching an IP address for the next possible subnet

When a MH remains in the same subnet, it receives packets from the correspondent node (identified as Src/Dstn in the figures) through the RAN. The handoff procedure will be triggered if the MH identifies the need for a handoff. The identification of a need for a handoff is very commonly done in the physical layer based on the received signal strength at the MH. This is referred to as mobile host initiated handoff. The need for handoff can also be informed by the BS to the MH in which case the handoff procedure is called BS initiated handoff. Once it is about to enter (not after entering) a different subnet, it sends a DHCP REQUEST to the RAN. The RAN sends the request to a DHCP server that allocates an IP to the clients for that subnet. The DHCP RESPONSE with the new IP is sent by the DHCP server to the RAN, which is then forwarded to the client. Now the client has a valid IP address for the next possible subnet. This is shown in Fig. 10.

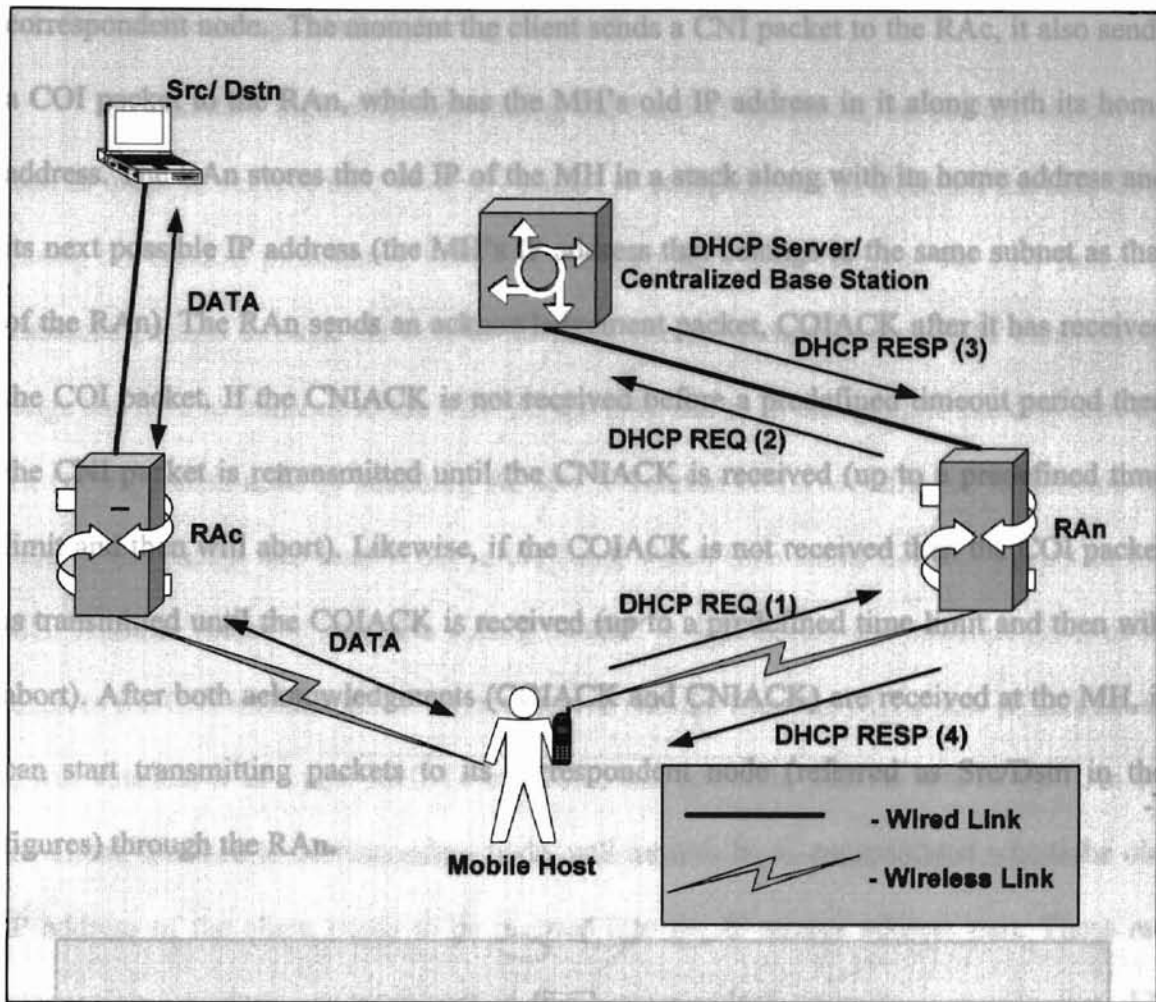


Fig.10 Fetching an IP for the next possible subnet

3.5. Preparing for Handoff

After obtaining an IP address for the next possible subnet, the MH sends a CNI packet to the correspondent node to inform it about a successful handoff and also about its new IP as shown in Fig. 11. The CNI packet contains the new IP address of the MH. Since the RAc can read into the packets, if it finds the packet to be a CNI packet it will store the new IP of the client in a stack along with the MH's home address and its old IP address (the MH's IP that belongs to the same subnet as that of RAc). The RAc sends an acknowledgement packet CNIACK back to MH. It also forwards the CNI packet to the

correspondent node. The moment the client sends a CNI packet to the RAc, it also sends a COI packet to the RAn, which has the MH's old IP address in it along with its home address. The RAn stores the old IP of the MH in a stack along with its home address and its next possible IP address (the MH's IP address that belongs to the same subnet as that of the RAn). The RAn sends an acknowledgement packet, COIACK after it has received the COI packet. If the CNIACK is not received before a predefined timeout period then the CNI packet is retransmitted until the CNIACK is received (up to a predefined time limit and then will abort). Likewise, if the COIACK is not received then the COI packet is transmitted until the COIACK is received (up to a predefined time limit and then will abort). After both acknowledgments (COIACK and CNIACK) are received at the MH, it can start transmitting packets to its correspondent node (referred as Src/Dstn in the figures) through the RAn.

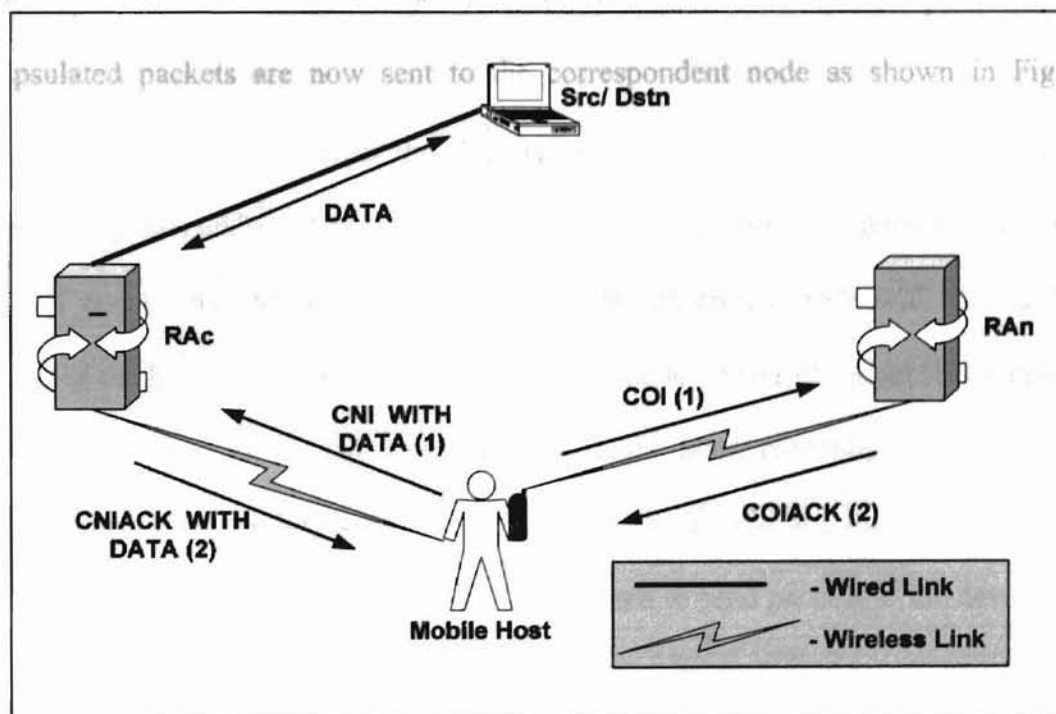


Fig.11 Client IP notification for WIP handoff procedures

3.6. Packet Re-encapsulation during handoff

To maintain high reliability during the handoff operation, no packets should be lost. In order to achieve this, we apply packet re-encapsulation to maintain the data flow during the handoff procedures. Until the correspondent node receives the CNI packet it transmits packets through the RAc to the MH. The client may be out of the transmitting range for RAc to transmit to the MH. So the RAc has to re-encapsulate the data sent by the correspondent node by attaching the new IP address of the MH into the destination IP field of the packet and send it out to the RAn, which then sends the data packet to the MH. Another factor to consider during handoff is that before the correspondent node receives the CNI information, it cannot receive packets from the MH's new IP address as it will consider it as a new MH. To overcome this problem, packets sent to the RAn by the client, destined to correspondent node, will have to be re-encapsulated where the old IP address of the client needs to be inserted into the IP source address part. These re-encapsulated packets are now sent to the correspondent node as shown in Fig. 12.

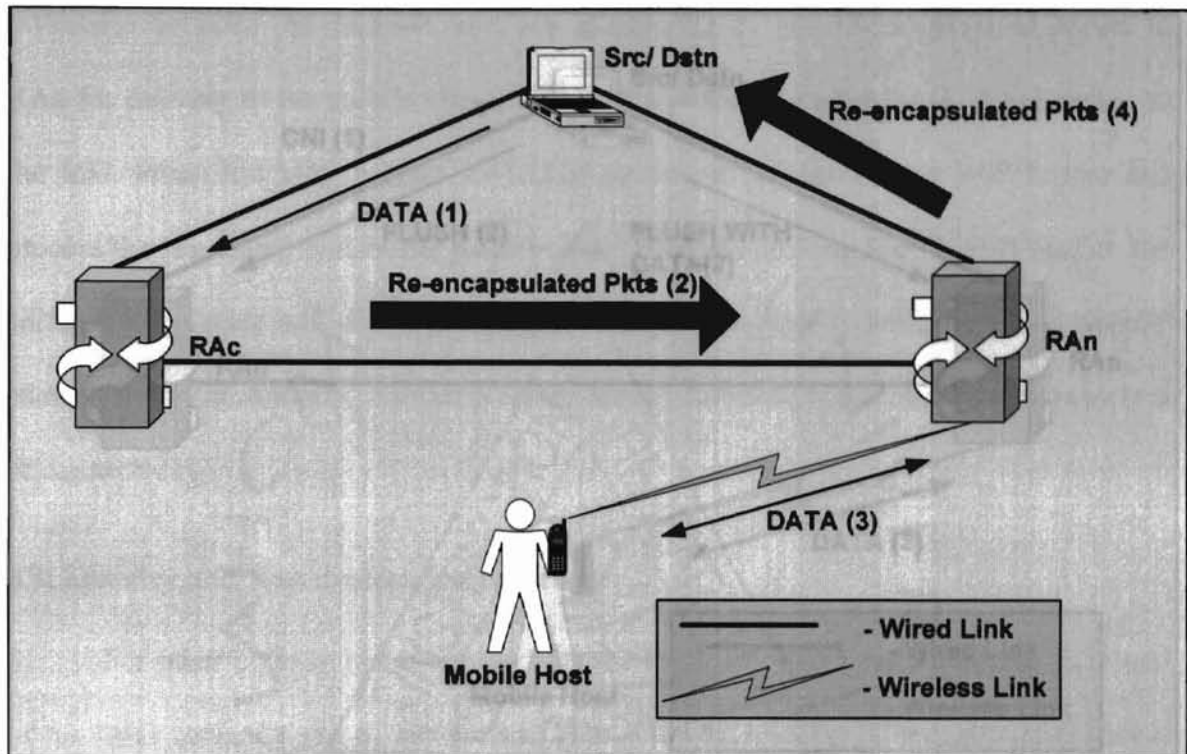


Fig.12. Packet Re-encapsulation for data forwarding over WIP Networks

3.7. Handoff Completion

When the RAc forwards the CNI packet to the correspondent node, the new IP address and home address pair of the MH is notified at the correspondent node as the new point of contact for the MH of interest. The correspondent node will use the home address of the MH to recognize that the new IP is due to a handoff, rather than a new user trying to connect to it. The correspondent node after receiving the CNI packet acknowledges it by sending a FLUSH packet to both the MH and the RAc as shown in Fig. 13. Following this, the correspondent node starts to send packets to the new location of the client.

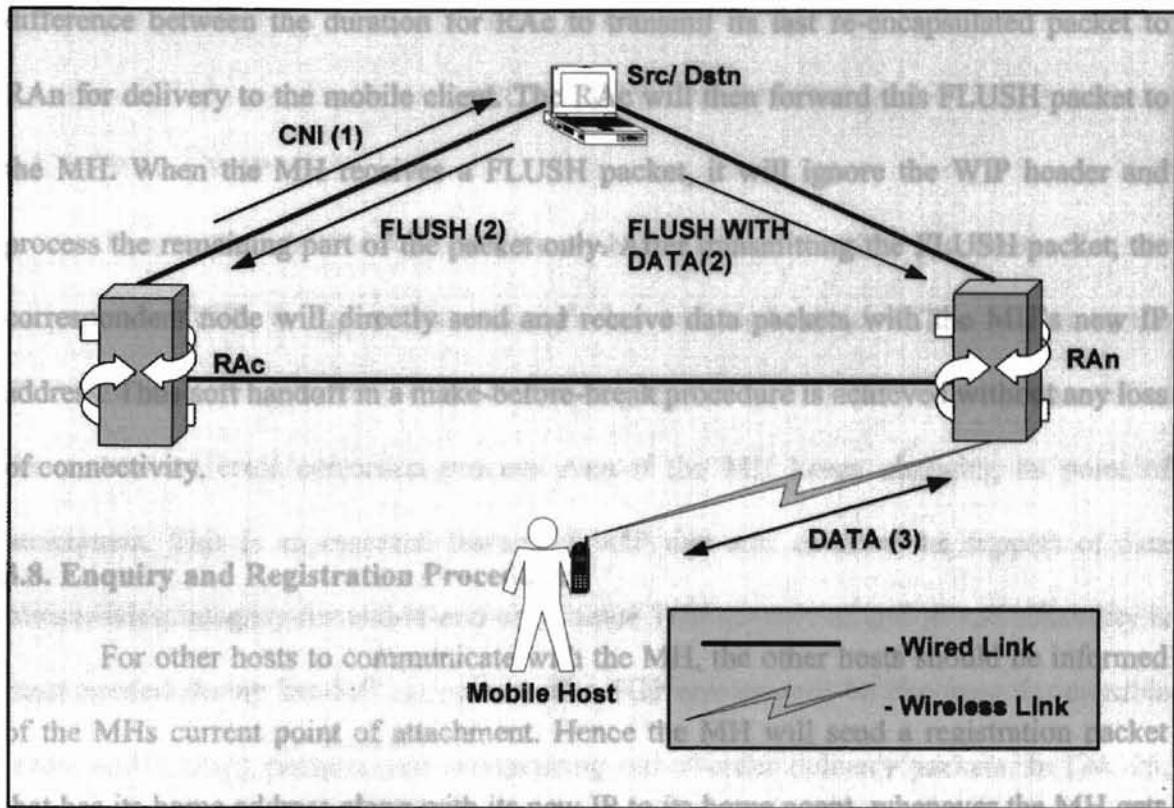


Fig.13 Src/Dstn routing table information update process

When the RAc receives the FLUSH packet, it removes the entry of the new IP of the MH from the stack, as it no longer needs to re-encapsulate and send the packets through RAn since the correspondent node will now directly transmit data packets to the new IP address of the MH through RAn. Since RAn can look into the packet header sent by the correspondent node to the MH, it can identify a FLUSH packet. When the RAn identifies the FLUSH packet, it will establish routing connections for the new IP address for the MH and will also wait for a couple more packet arrival durations and then will remove the entry of the old IP of the client. This waiting time for a couple of packet arrival durations is necessary since the time that the RAc and RAn receive the FLUSH packet may be different. In addition, there will be a processing and propagation time

difference between the duration for RAc to transmit its last re-encapsulated packet to RAn for delivery to the mobile client. The RAc will then forward this FLUSH packet to the MH. When the MH receives a FLUSH packet, it will ignore the WIP header and process the remaining part of the packet only. After transmitting the FLUSH packet, the correspondent node will directly send and receive data packets with the MH's new IP address. Thus soft handoff in a make-before-break procedure is achieved without any loss of connectivity.

3.8. Enquiry and Registration Procedures

For other hosts to communicate with the MH, the other hosts should be informed of the MHs current point of attachment. Hence the MH will send a registration packet that has its home address along with its new IP to its home agent, whenever the MH gets a new IP address. The home agent pairs the home address with the new IP address of the MH in its memory. Any network user (correspondent node) that needs to communicate with the MH will have to send an ENQUIRY packet requesting to know the current point of attachment of the MH. The home agent will look into the recorded database and will return an ENQUIRY Response packet to the correspondent node, which includes the current IP address of the MH. The node can now communicate directly to the MH using its new IP address.

4.1. TCP over WIP

Due to the inherent soft state “make-before-brake” handoff procedures that are proposed for WIP, in case of data transmission with end-to-end TCP connections, the TCP link will have to remain connected managing the session reconstruction as well as the end-to-end error correction process even if the MH keeps changing its point of attachment. This is an essential feature of WIP that will enhance the support of data transmission integrity for end-to-end users since TCP support of end-to-end reliability is most needed during handoff operations. The TCP session will be checking for possible errors and missing packets, and reorganizing out-of-order delivery packets. In [24, 25, 26] not much is mentioned about how the TCP sessions are handled in Mobile IP or ROMIP.

For the TCP connections between WIP-supportive sources (Src/Dstn that support WIP functionalities) and the MH, TCP will not be able notice the changes that occur in the source or the destination addresses of the IP packet. When the MH enters a different subnet and gets a new IP, WIP forces the RAc and RAn to re-encapsulate the packets during handoff. So there exist two routes: one from the correspondent node through the RAc to the MH and the other from the MH through the RAn to the correspondent node. Both of these routes will be carrying valid IP packets between the MH and the correspondent node. TCP will not be able to notice the changes made in the IP header for the reason that it is above IP layer. Since the TCP session is the same for both the routes, TCP will help the connection to be end-to-end reliable until the connection is terminated

by either the MH or by its correspondent node. After the handoff, there exists only one route that is between the MH and the correspondent node through the RAN. This route will be used until the MH needs to be handed over again, still maintaining the same TCP session. The traditional socket programming will terminate the TCP connection if the IP address of the MH changes. Hence it is obvious that WIP requires a more sophisticated socket programming that can allow for the TCP session to remain same even if the MH's IP keeps changing. Another issue to notice is that the Checksum field in the TCP header includes a pseudo header that has the source IP and destination IP addresses in calculating the checksum. So if either one of the addresses changes, the packet will be discarded assuming errors in the packet. To overcome this, the following is suggested. After the enquiry procedure, the correspondent gets an enquiry response message that includes the current IP address of the MH. After receiving this address, the correspondent node is required to store this address in cache. This address is stored till the end of communication, even if the MH's IP keeps changing in the mean time. So whenever, TCP requires the IP address of a MH, WIP will respond with this address that was stored when the communication actually began. This way TCP will assume that the same connection is being maintained. On the MH's side, it has to store its IP address that it had in the beginning of the TCP connection. WIP will respond to TCP with the stored IP address even if the MH changes its IP before the termination of connection. This way the TCP connection is maintained through out and efficient data flow can thus be guaranteed.

For the TCP connections between WIP supportive and WIP non-supportive sources (Src/Dstn that do not support WIP functionalities), there should exist a translator that makes WIP compatible. Here, the source need not be informed about the mobility of

the MH. The translator between WIP-supportive and WIP non-supportive networks will have to then remove the WIP headers and then forward those packets into the non-supportive environment.

In [7], a method to make TCP more compatible with the wireless environment, called indirect TCP (i-TCP), was introduced which involves the TCP connection between the MH and the correspondent node to be split into two separate connections: one TCP connection between the correspondent node and a mobile support router (MSR) and the other between the MSR and the MH applying wireless TCP. So whenever the MH moves to a different cell, the actual connection between the correspondent node and the MSR remains unchanged and only the connection between MSR and MH is changed. A similar architecture that can maintain the TCP connection even if the MH changes its IP address is possible. For the case of TCP in support of WIP, the TCP connection between the correspondent node and the MH is split into two: one between the correspondent node and the WIP translator and the other between the WIP translator and the MH. Refer to Fig. 14. This issue is being analyzed and so remains as a future research topic.

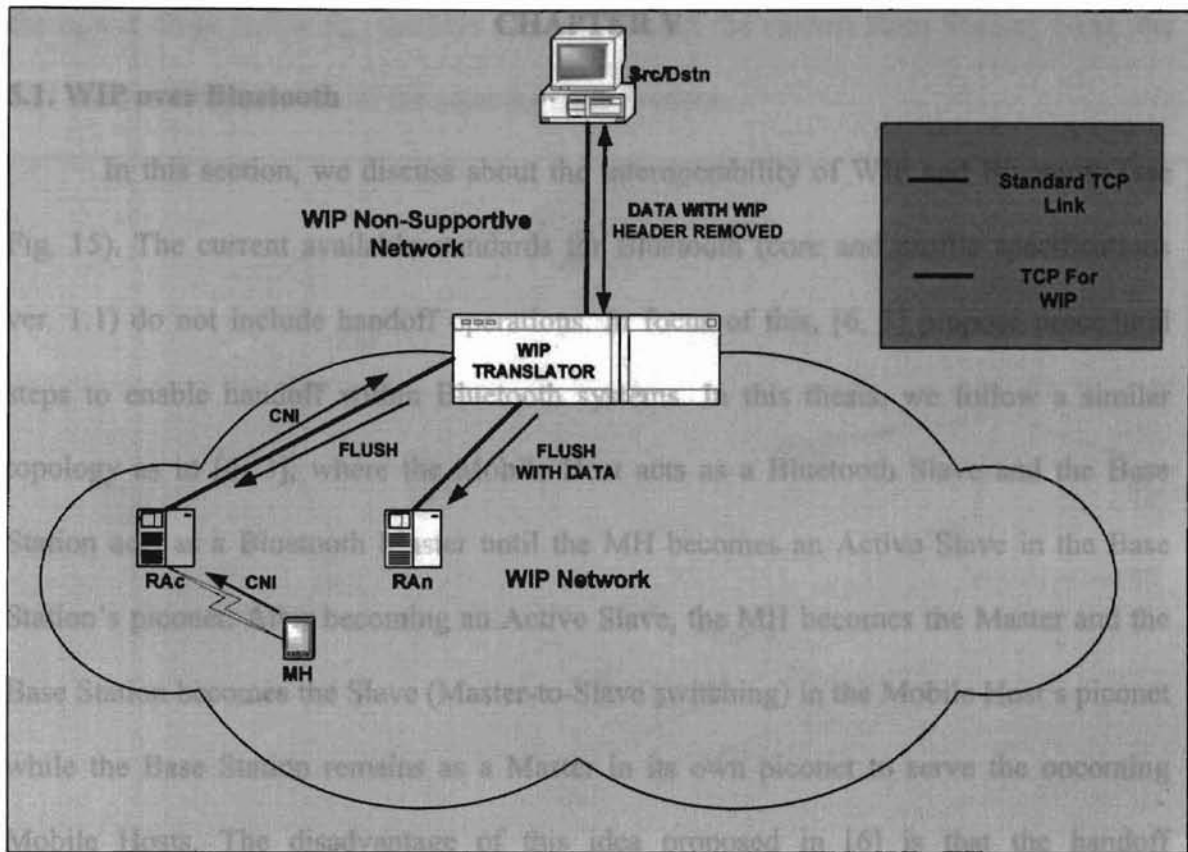


Fig.14 TCP operations with a WIP translator interoperating between the WIP non-supportive network and the WIP network.

In case that real-time voice or video data is being transmitted the real-time transport protocol/real-time transport control protocol (RTP/RTCP) may be used to manage the packet inter-arrival jitter as well as for packet loss control. In this case, a TCP connection will not be established. Instead the RTP/RTCP protocol will collaborate with the user datagram protocol (UDP) to receive source/destination port information, length information, and checksum information of the entire UDP segment. For cases where no session control is necessary UDP can be used alone.

5.1. WIP over Bluetooth

In this section, we discuss about the interoperability of WIP and Bluetooth (see Fig. 15). The current available standards for Bluetooth (core and profile specifications ver. 1.1) do not include handoff operations. In focus of this, [6, 3] propose procedural steps to enable handoff within Bluetooth systems. In this thesis, we follow a similar topology as in [6, 3], where the Mobile Host acts as a Bluetooth Slave and the Base Station acts as a Bluetooth Master until the MH becomes an Active Slave in the Base Station's piconet. After becoming an Active Slave, the MH becomes the Master and the Base Station becomes the Slave (Master-to-Slave switching) in the Mobile Host's piconet while the Base Station remains as a Master in its own piconet to serve the oncoming Mobile Hosts. The disadvantage of this idea proposed in [6] is that the handoff procedures are hard-handoff procedures since the search procedures for another Base Station to connect with will begin only after the connection with the current Base Station is lost. This will lead to momentary disconnection in the packet transmission and reception that is unsuitable for real time applications. Hence a method to solve this problem is described below.

The Mobile Host conducts reception signal power estimation, always. This will not require any additional designing due to the fact that Bluetooth systems have built-in functionalities where the received signal power is measured and recorded as the Receiver Signal Strength Indicator (RSSI) variable. Once the instantaneous power of the received signal (from Base Station) equals or drops below a threshold power level (P_{th}), the Inquiry is initiated in the common access channel. It is important to notice that even after

the power drops below P_{th} , the MH can still contact the current Base Station. Next, the MH receives responses from the adjacent Base Stations.

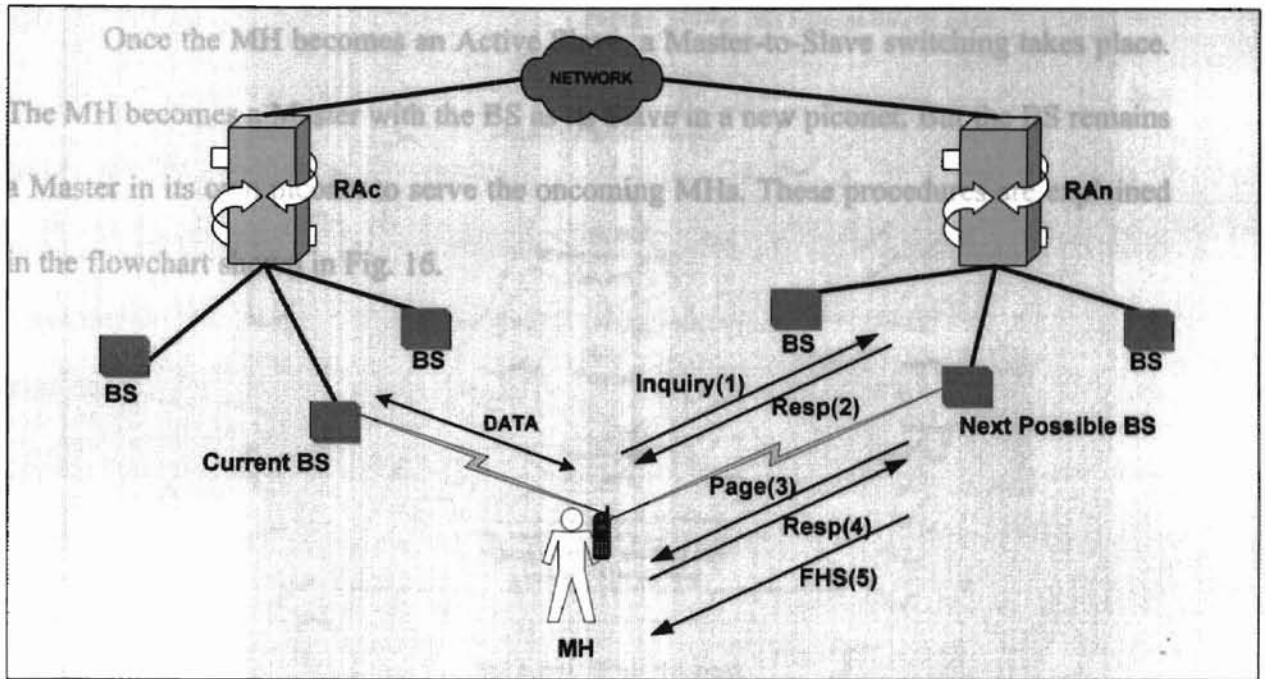


Fig. 15. WIP handoff operations in support of Bluetooth system connectivity.

5.2. Selection of a next possible Base Station (BS)

The MH will choose the first BS that sends a response to the inquiry with the signal power greater than P_{th} . If it did not receive any response (with a power level greater than P_{th}) then it will retransmit the Inquiry message until a response is obtained. Once the BS is selected, the MH has to wait to be paged by that BS. Then the MH becomes an Active Slave in the BS's piconet after basic parameter negotiations and agreements are established between the BS and the MH (e.g., MTU, packet type, connection type, etc.).

5.3. Master-to-Slave Switching

Once the MH becomes an Active Slave, a Master-to-Slave switching takes place. The MH becomes a Master with the BS as its Slave in a new piconet. But the BS remains a Master in its own piconet to serve the oncoming MHs. These procedures are explained in the flowchart shown in Fig. 16.

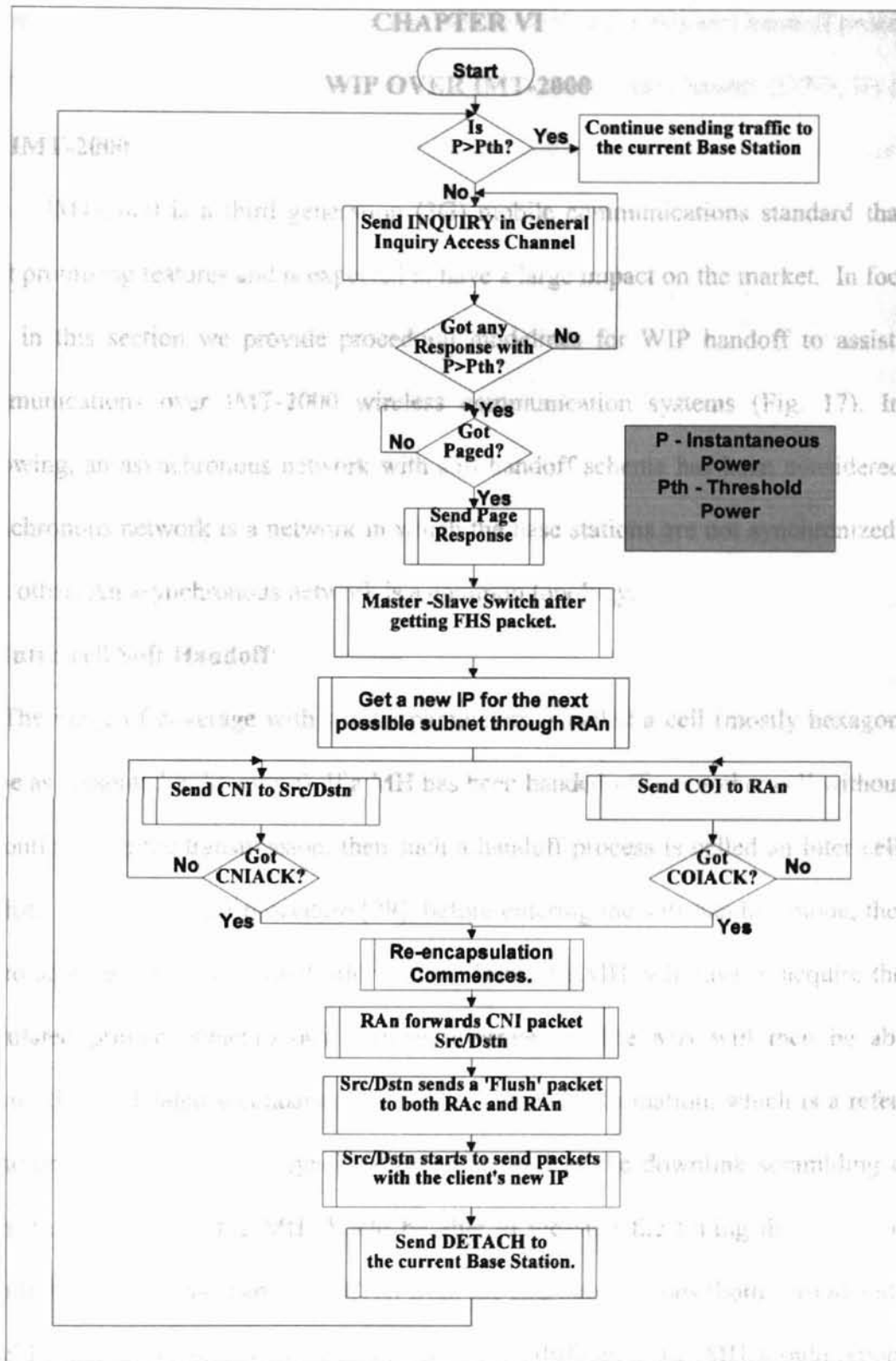


Fig.16 Flow chart of WIP handoff procedures in support of Bluetooth system connectivity.

CHAPTER VI

WIP OVER IMT-2000

6.1. IMT-2000

IMT-2000 is a third generation (3G) mobile communications standard that has most promising features and is expected to have a large impact on the market. In focus of this, in this section we provide procedural guidelines for WIP handoff to assist data communications over IMT-2000 wireless communication systems (Fig. 17). In the following, an asynchronous network with soft handoff scheme has been considered. An asynchronous network is a network in which the base stations are not synchronized with each other. An asynchronous network is a common topology.

6.2. Inter-cell Soft Handoff:

The range of coverage with similar parameters is called a cell (mostly hexagonal in shape as presented in literature). If a MH has been handed-off to another cell without any discontinuity in the transmission, then such a handoff process is called an inter-cell soft handoff. In this handoff procedure [29], before entering the soft handoff mode, the MH has to acquire the pilot channel information. Then, the MH will have to acquire the unmodulated primary synchronous channel information. The MH will then be able to acquire the modulated secondary synchronous channel information, which is a reference to the chip, slot, and frame synchronization as well as the downlink scrambling code. With this information the MH should be able to measure the timing difference of the downlink synchronous channels (SCHs) from the two base stations (both current and next possible base stations). After measuring this timing difference, the MH should report this timing difference to its current base station. The timing of a new downlink soft handover

connection is adjusted with a resolution of one symbol. After this soft handoff procedure, the MH will be able to send traffic on the dedicated physical channel (DPDCH) of the new cell. We should remember that the connection with the current base station still exists for some time.

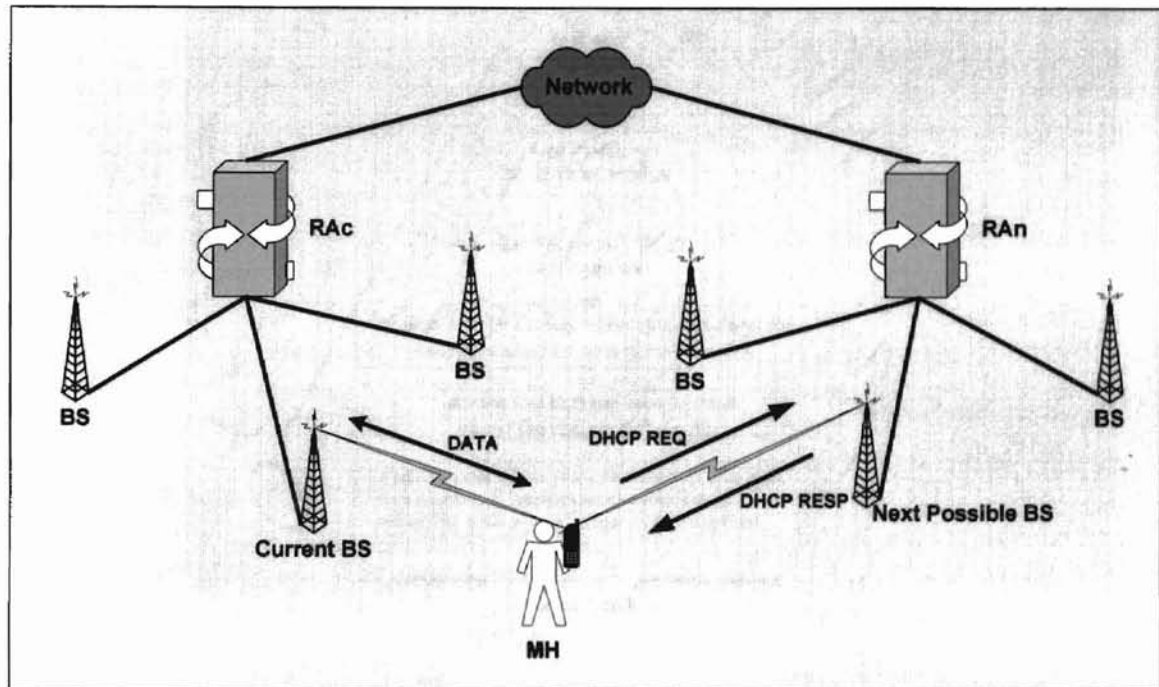


Fig.17 WIP handoff operations in support of IMT-2000 mobile communications services.

6.3.WIP Over IMT-2000

After the soft handoff in the IMT-2000 layer there should also be a soft handoff in the IP layer. If the IP layer is not capable of supporting a soft handoff then the true benefits of having soft handoff procedures in the lower layer (IMT-2000 physical layer) will be lost. This is due to the fact that the IP layer connection will break momentarily during handoff procedures, which can easily lead to loss of packets.

WIP, as discussed above, enables a soft handoff to be established in the IP layer which can avoid packet loss due to momentary loss of connectivity. Hence, with soft handoff in both the IMT-2000 layer and the IP layer, the overall connection is reliably maintained without any interruptions. These procedures are explained using a flowchart in Fig. 18.

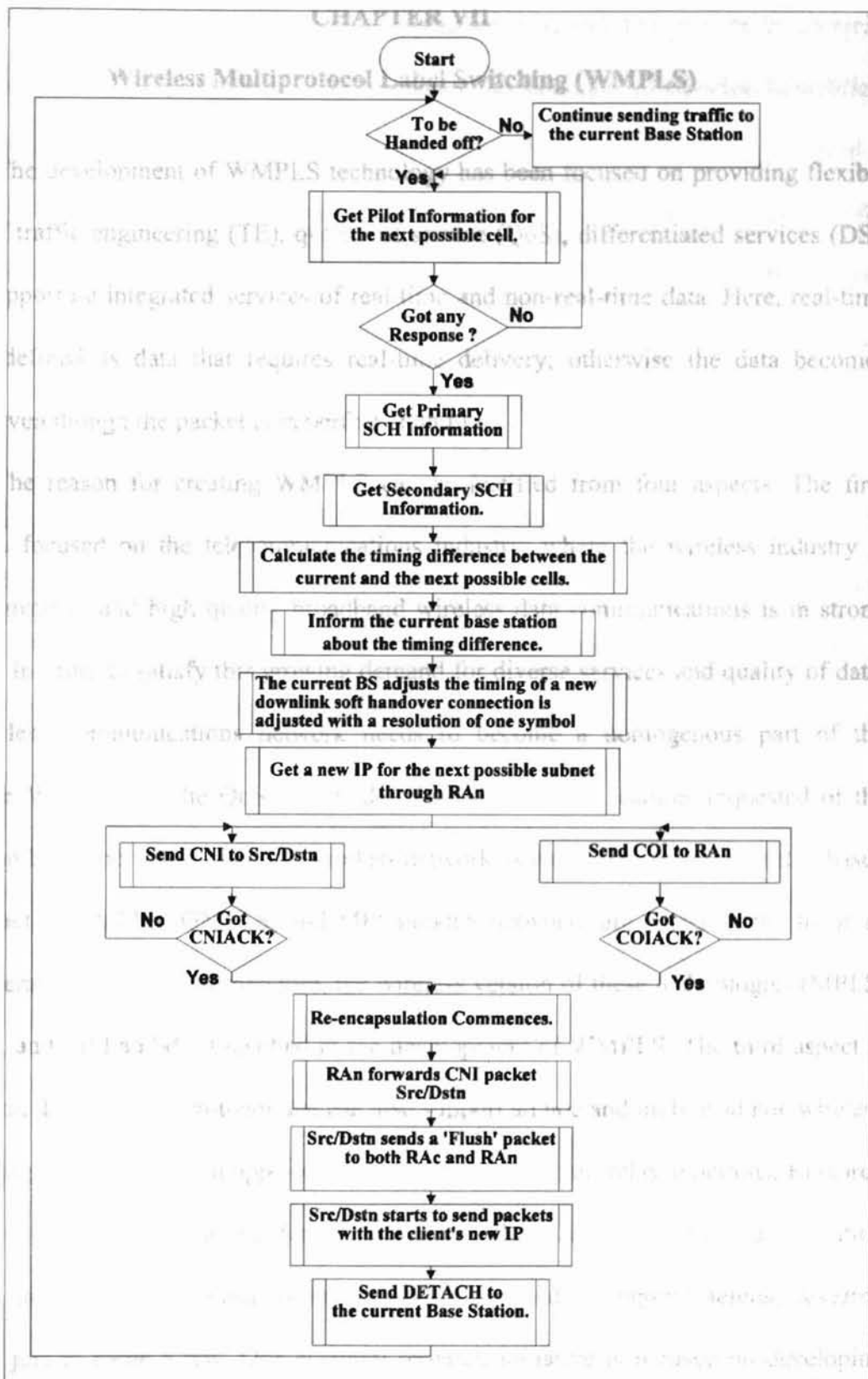


Fig.18 Flow chart of WIP handoff procedures in support of IMT-2000.

CHAPTER VII

Wireless Multiprotocol Label Switching (WMPLS)

The development of WMPLS technology has been focused on providing flexible levels of traffic engineering (TE), quality of service (QoS), differentiated services (DS), while supporting integrated services of real-time and non-real-time data. Here, real-time data is defined as data that requires real-time delivery; otherwise the data becomes useless even though the packet is in perfect condition.

The reason for creating WMPLS can be justified from four aspects. The first aspect is focused on the telecommunications industry, where the wireless industry is rapidly growing and high quality broadband wireless data communications is in strong demand. In order to satisfy this growing demand for diverse services and quality of data, the wireless communications network needs to become a homogenous part of the backbone WAN. Then the QoS and grade of services (GoS) features requested of the WAN can be supported through the wireless network as well. The second aspect is based on the fact that MPLS, GMPLS, and MPLambdaS networks are currently the focus of next generation WANs, and therefore, the wireless version of these technologies (MPLS, GMPLS, and MPLambdaS) resulted in the development of WMPLS. The third aspect is focused on the need of a protocol that can also support ad hoc and mobile ad hoc wireless networking functions, which apply effective and efficient data relay functions. Research initiatives of this kind can be found in various places including the transportation industry, the government transportation organizations, and in ongoing defense research projects, just to name a few. One essential research initiative is focused on developing applied information technology wireless communication systems in support of more

effective traffic management services. This initiative is intended to provide commercial and emergency information to both commercial and noncommercial vehicles. In addition, protective systems to prevent vehicle collisions are also being developed that will need to apply mobile ad hoc wireless networking technology. The fourth aspect is focused on the application of wireless differentiated services. One example of wireless differentiated services employed in military applications is the data transportation of C4I (command, control, communications, computers, and intelligence) priority data. Wireless differentiated services can be accomplished through capture effect, signal transmission power control, code control, signal polarity control, priority assignments of time/frequency segments in TDM/FDM multiple access networks, directional signal transmission, and other technologies.

7.1. Wireless ATM (WATM)

The standardization efforts of WATM have been carried out by the ATM Forum and the Broadband Radio Access Network (BRAN) committee (which was formerly the RES 10) of the European Telecommunications Standards Institute (ETSI). In Japan, high-speed wireless ATM has been under investigation under the Multimedia Mobile Access Communication Systems Promotion Council (MMAC-PC). In June of 1996, fifty companies collaborated in forming the wireless ATM working group within the ATM Forum. WATM evolved from the need for the same applications where the only difference is that the user is mobile [1, 5, 8, 33]. Wireless ATM uses the cellular approach of dividing the service area into radio cells where each cell has a base station and the cells reuse the available spectrum. Wireless ATM is a technique wherein user

information, which has originated with arbitrary format and comprises of continuous or variable bit rate voice, data, image or video, is converted and presented to the network as a sequence of ATM cells [1, 5, 8, 33].

WATM has several advantages that make it attractive. First, WATM provides the convenience of delivering voice, data, image or video applications to a mobile user. Second, it uses the ATM technique where the information is converted and presented to the network as a sequence of ATM cells. Third, the WATM protocol gives the advantage of sharing the limited communications bandwidth in an efficient way. Fourth, WATM enables the efficient use of the frequency spectrum and minimizes the delay experienced by mobile systems. And fifth, ATM cells encapsulated with error control coding reduce the time volatility of the radio link between itself and its serving base station, thus being able to provide a low bit error rate (BER) service [1, 5, 33].

The WATM header format adds two bytes (one header and one trailer byte) to the ATM cell to support wireless communications. The sequence number is added to each cell (in the header part) to identify each cell uniquely for acknowledgements and automatic retransmission request (ARQ) purposes. An 8 bit FEC field in cyclic redundancy check (CRC) format is added as the trailer to the ATM cell for cell error detection purposes. The 7 bytes of overhead compared to the overall 55 byte format results in 12.73% of overhead. Due to this the standard ATM cell header can be compressed, resulting in a header length of 2 to 4 bytes. In this case, the cell will have 7.69% to 11.11% of overhead, respectively. In addition, based on the ATM cell type, before the payload field is processed through the segmentation and reassembly (SAR) operations of the ATM adaptation layer (AAL), the payload may include a trailer and a

padding field based on AAL type. This will result in an even higher overall overhead percentage.

7.1.1. WATM Limitations and Challenges

In this section, the limitations and challenges of ATM and WATM networks are listed.

(1) ATM and WATM networks do not support differentiated services. The current generation network is commonly described as a fully deployed integrated service network, where as the next generation network is focused on adding differentiated services and real-time data services in WANs. In addition, wireless differentiated services in military applications are also being developed. Wireless differentiated services can be accomplished through many ways and wireless networks will have to be able to recognize the priority assignment of the packets and provide corresponding control based on the data packet class of service (CoS) field indications.

(2) ATM networking has some disadvantages in supporting dynamic multicasting control of real-time data delivery services. Based on the focus of providing a solution to these problems and also due to recent advancements in optical networking technology (e.g., lambda-switches and optical cross connects (OXC)), MPLS, GMPLS, and MPLambdaS networking protocols and topologies were conceptualized, which became the basis of the next generation networking technology. Multicasting has also been one of the main problems that ATM networks suffered due to the complexity of the signaling and management mechanisms [14, 15]. In the future, increasing demands of dynamically

controlled multicasting services by wired and wireless end-users is expected, where the scalability and complexity of WATM-ATM networks will be challenged.

(3) WATM does not specify any inherent automatic retransmission request (ARQ) error recovery mechanism to enhance reliability; instead it relies on the upper or lower layer protocol to control ARQ reliability services. Thus, WATM is not capable of providing hop-by-hop error or flow control, which is a necessary function in some applications of mobile ad hoc networks.

(4) WATM is not suitable for connectionless or connection-oriented ad hoc and mobile ad hoc wireless networking that require efficient data relay functions. This is due to the inflexible procedures and operational complexity of the signaling protocol.

(5) WATM cells have a fixed payload size of 48 bytes where the type of application specifies the payload AAL SAR format. This puts a limit to the flexibility of applications to various wireless systems. Shorter packet sizes are known to have advantages over longer packets for wireless mobile communication channels due to the time varying channel characteristics. The longer the frame, the more vulnerable the packet will be to errors. On the other hand, when errors are not abundant and the reception channel status is good and stable, using longer packets can enable the transmission data transfer efficiency to increase. In comparison, if the reception channel conditions are good then using smaller packets will result in more overhead than necessary, which will result in lower transmission efficiency. This type of adaptive transmission-control technology is

found in advanced wireless systems, such as, wireless local area networking technologies (IEEE802.11 standards) and also in IMT-2000. WATM only allows one cell payload size of 48 bytes. Having only one payload format will be beneficial in some cases, but in general, the fixed payload size prevents the original application service packet unit from being used effectively. This can result in delays where the packet reconstruction system is waiting for dependent segments of the application data to arrive for AAL SAR reassembly operations. In addition, special encryption applications require different lengths of redundancy or parity information to be added to the packet. In addition, the error control coding also adds different lengths of parity information based on the code applied. In adaptive error control coding, based on observations of the time varying channel status, the code length will change as the coding technology changes. Limiting the cell size brings on limitations to the applied encryption coding and error control coding. For example, some packets will need to contain its full code (inner and outer concatenated code) to be decodable. If packets always need to be segmented into 48 bytes of a payload length, then a complete error control coding package or encryption codeword set will most likely not fit into this predefined 48 byte size. In cases where segmentation is demanded and multiple cells are required to be decoded together at the receiver, then missing one cell is equivalent to missing all cells of the packet session due to the decryption of the codeword process. The WATM solution to this is cell concatenation after segmentation of the cell units, which is still limited by the complexity of the AAL operations.

(6) WATM has interoperability problems when overlay network models are applied. For physical layer applications, based on the modem technology or networking protocol applications, in order to get the true benefit of the combined technologies, commonly there will be a need for the physical layer and the network access layer (or data link layer application) to closely interoperate with each other. WATM shows some limitations due to its complex and strict-controlled nature, where neither does it provide a mechanism to control the lower layer resources flexibly, nor does it have good interoperability characteristics with other protocols.

(7) Mobility imposes a significant challenge to current ATM protocols because they are designed for fixed terminals. To handle mobility within ATM, the following three issues have to be considered: Location management, Connection management and Handover management [5]. Location management focuses on tracking the location of a mobile user and handling all the requests it makes. Connection management deals with issues relating to the connections that all users have and how they have to be treated when moving from one base station to another (i.e., moving from one cell to another). Connection management also deals with the QoS parameters and its constant negotiation. Since ATM is a connection-oriented protocol, it assumes that all the parameters are going to be guaranteed for the duration of the virtual circuit (VC) connection. WATM, however, has to face the problem that when roaming users enter a new cell, the QoS parameters they were serviced within the cell they are leaving might not be available in the new cell they are entering. The handover management deals primarily with delivering the ATM cells to the mobile hosts in the sequence they were generated. There are several initiatives to

overcome these problems, and most of the WATM test beds employ different mechanisms in order to ensure the QoS parameters in mobile environments.

In WMPLS, future research will be focused to solve these types of technical challenges. One advantage of WMPLS is that the traffic engineering and differentiated services features of negotiating a QoS, GoS, and traffic parameters are well provisioned. This can be observed in the operations and the protocol structure of the signaling protocols and how they operate to perform flexible traffic engineering features.

7.2. WMPLS Networking

MPLS represents the next level of standards-based evolution in combining the layer 2 “data link layer” switching technologies with the layer 3 “network layer” routing technologies. The primary objective of the MPLS standardization process is to create a flexible networking architecture that provides increased performance and scalability. The MPLS label switching router (LSR) that conducts the differential services is required to conduct a three-stage procedure to enable traffic engineering. These three basic CQS operational stages of an MPLS router are shown in Fig. 19.

Wireless MPLS applies two fundamental protocol header formats, which are shown in Fig. 20. Within the WMPLS network, the first 2 bits of the 20 bit Label field will be read as a Flag field. This field will determine if a Control field and cyclic redundancy check (CRC) field are applied or not, and it will also indicate the length of the applied Control field either being 1 or 2 bytes, corresponding to the number of sequence bits used, either 3 or 7 bits, respectively. In an overlay model, where the lower

layer protocol provides error and flow control, the WMPLS header format with no Control field and CRC field. To identify this label format, the first two bits of the label will be set to zero, which will imply that no control field and no CRC field is being used (Fig. 20 (a)).

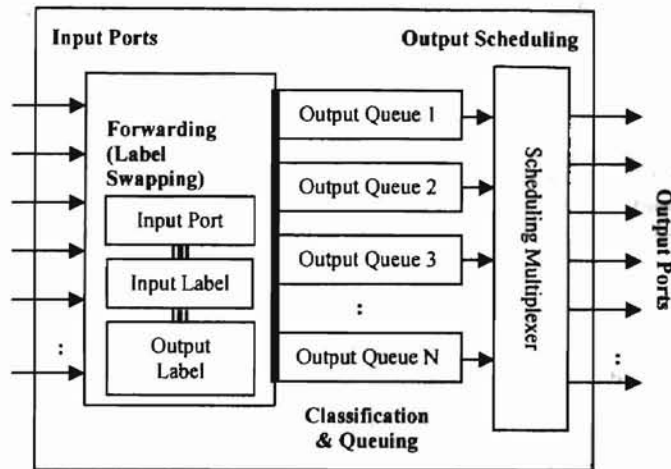
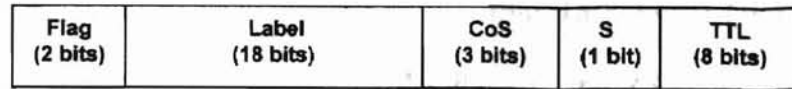


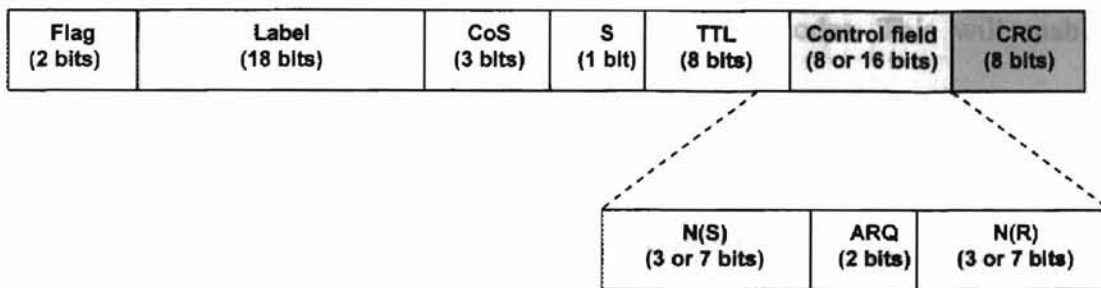
Fig.19 Functional diagram of the LSR CQS operation [8, 9]

In the Control field, shown in Fig. 20 (b), $N(S)$ is the sending sequence packet/frame number and $N(R)$ is the automatic retransmission request (ARQ) or flow control acknowledging frame sequence number. Using more sequence numbering bits will allow larger flow control windows to be established in support of high-speed sequential frame transmission. This option will enable end-to-end or hop-by-hop error and flow control to be provided when necessary on a labeled packet basis. The Control field of the WATM header will include error and flow control functionalities. In applications of mobile ad hoc networking, it is necessary to have the option of hop-by-hop error and flow control. As discussed earlier, WATM is not capable of hop-by-hop

error and flow control, where this functionality is left for the end-to-end users to conduct, or if an overlay model is used, hop-by-hop error and flow control may become possible if the underlying lower layer protocol can provide this service.



(a) WMPLS Header with no control field or CRC field.



(b) WMPLS Header with control field and CRC field.

Fig.20 MPLS protocol structure. The payload field (not drawn) will follow the TTL/CRC field (variable length).

Flag		Control Field Sequence Numbers N(R) & N(S) and 2 bit FEC & ARQ control field.
0	0	No Control and CRC Field.
0	1	3 bit N(R) and 3 bit N(S).
1	0	7 bit N(R) and 7 bit N(S).
1	1	Reserved for future applications.

Table.1 WMPLS header Flag bits.

The label distribution protocol (LDP) and the resource reservation protocol with traffic engineering extensions (RSVP-TE) are the two signaling protocols for MPLS networks. Currently, constraint-based routed LDP (CR-LDP) is also under development through Drafts submitted to the Internet Engineering Task Force (IETF). Both strict-routing and loose-routing is possible for LDP, CR-LDP, and RSVP-TE. In this thesis, we focus on the applications of the loose-routing topology in WMPLS to enable reliable soft handover procedures for mobile communications. The loose section of the wireless mobile network will be defined as the group of abstract nodes. This will enable the wireless network to do handover from one base station to another within the mobile cellular environment without breaking the LSP connection. In addition, alternative methods applying strict-routed CR-LDP and RSVP-TE connections are also being investigated. In the following subsections, the proposed extensions to the signaling protocols (i.e., CR-LDP and RSVP-TE) to enable WMPLS networking are presented.

ARQ flow control Bits	Flow Control and Error Control Acknowledgement of Frames.	Control Symbol
00	Accumulative acknowledgment of N(R-1).	RR
01	Receiver Not Ready flow control and accumulative acknowledgment of N(R-1).	RNR
10	Go-Back-N ARQ REJECT N(R) signal & accumulative acknowledgment of N(R-1).	REJ
11	Selective Reject/Repeat N(R) signal.	SREJ

Table.2 WMPLS header flow control and error control acknowledgement control bits.

7.3. Extensions to RSVP-TE for WMPLS

RSVP-TE has been made and proposed to support explicit route LSP (ER-LSP) as well as to provide additional features to RSVP. Since the RSVP protocol was proposed to support MPLS LSP setups, a considerable amount of modifications and extensions have been made to the original protocol to cope with the traffic engineering requirements. The major modifications and extensions fall into the areas of adding traffic engineering capabilities and resolving scalability problems. The revised RSVP protocol has been proposed to support both strictly and loosely explicitly routed LSPs (ER-LSP) [34]. For the loose segment in the ER-LSP, the hop-by-hop routing can be employed to determine where to send the Path message. Or if the networking group is governed by a specific router (peer group leader [30] or network management sever/system), then that LSR

could assign the local connections of the loosely routed LSP using an unsolicited downstream label distribution topology [34].

For WMPLS LSP setup, a Path message will be transmitted by the source router. In the Path message, the LABEL_REQUEST object will request the desired label types for WMPLS setup operations informing the nodes of the desired LSP to reserve the requested traffic parameters. Based on RFC 3209 [24], the LABEL_REQUEST object is defined as class 19, and there are three LABEL_REQUEST class types (C-Type) defined, which are, without label range (C-Type = 1), with ATM label range (C-Type = 2), and with Frame Relay label range (C-Type = 3). The extension necessary to trigger a WMPLS LSP through RSVP-TE will need to have new C-Type assignments within the LABEL_REQUEST object such that proper wireless traffic parameters and connection types can be recognized in the Path message. In addition, in the Path message and the Resv message, the SESSION object can be used with new C-Type assignments. Based on RFC 3209, the SESSION object of RSVP-TE is assigned the class SESSION and C-Types 7 and 8 are assigned for IPv4 and IPv6 LSP tunnel applications, respectively [4]. C-Types 1 and 2 of the SESSION object are assigned for IPv4 and IPv6 sessions for RSVP in RFC 2205 [9]. Through the identification of WMPLS applications, the network routers will provision WMPLS packets and the corresponding control fields, instead of MPLS packets.

Common Header
INTEGRITY (opt.)
SESSION
RSVP_HOP
TIME_VALUES
EXPLICIT_ROUTE (opt.)
LABEL_REQUEST
SESSION_ATTRIBUTE (opt.)

(a) Path message

Common Header
INTEGRITY (opt.)
SESSION
RSVP_HOP
TIME_VALUES
RESV_CONFIRM (opt.)
SCOPE (opt.)
POLICY_DATA (opt.)
STYLE
Flow descriptor list

(b) Resv message

Fig.21 Format of the RSVP-TE. (Not drawn to scale. Each field may be variable length based on protocol subfields applied)

7.4. Extensions to CR-LDP for WMPLS

The extensions to CR-LDP [2, 22] that need to be made include the WMPLS label request and mapping, since the protocol format needs to be considered, and the mobility and CoS based operations for WMPLS services. The fields shaded in the CR-LDP format shown in Fig. 22 are the operators that will play the essential role of servicing the LSP setup for WMPLS networks. The encoding of the Label Request Message needs to be extended with CoS and label information of the WMPLS network. In addition, the encoding for the CR-LDP Label Mapping Message needs to be extended to include the resolved channel information from the wireless link.

Applying CR-LDP signaling, the wireless system can establish a LSP for supporting WMPLS TE applications through the FEC TLV or the Traffic TLV. In the case where the Traffic TLV is used, the specification of the traffic parameters are

included in the signaling message. The parameters of TE negotiation to the LSR services are CDR (Committed Data Rate), CBS (Committed Burst Size), PDR (Peak Data Rate), and the PBS (Peak Burst Size). In cases where the FEC is used to signal the LSP connection for WMPLS, the CoS assignment will be acknowledged instead of specific data rate parameters.

0	WMPLS Label Mapping (15 bits)	Message Length (2 bytes)
Message ID (4 bytes)		
FEC TLV		
LSPID TLV (CR-LDP, mandatory)		
ER-TLV (CR-LDP, optional)		
Traffic TLV (CR-LDP, optional)		
Pinning TLV (CR-LDP, optional)		
Resource_Class TLV (CR-LDP, optional)		
Pre-emption TLV (CR-LDP, optional)		

(a) Label Request message

(b) Label Mapping message.

Fig.22 Format of the CR-LDP. (Not drawn to scale. Each field may be variable length based on protocol subfields applied)

7.5. Handover in WMPLS Mobile Communication Networks

For data communication between two hosts, the forward and the reverse paths can be either symmetric or asymmetric with respect to data rates and/or bandwidth. For example, the bandwidth required to download data is commonly higher compared to the bandwidth required for requests and control messages. The same is not true for voice

communication, where the bandwidth required for both forward and reverse paths are the same.

First, we summarize some of the terminologies that will be used:

- **Mobile Host (MH)**: A host that is nomadic in nature.
- **Base Station (BS)**: A service provider that governs all the users connected to it.
- **Mobile Switching Office (MSO)**: The routers that provide access points to MHs enabling connection to the network.
- **Mobile Switching Office Gateway (MSO GW)**: This is an MSO that lies at the border of the mobile communication network and the backbone (WAN) network.

7.5.1. The Proposed Network Topology

As described in the previous sections, WMPLS works with the signaling protocols like LDP, CR-LDP, RSVP and RSVP-TE. LDP and CR-LDP are hard state protocols, i.e., once a label switched path (LSP) is established it is assumed that this LSP stays alive until the end of communication, until it is intentionally disconnected. On the other hand, RSVP and RSVP-TE are soft state protocols, i.e., once a path is established it has to be refreshed every few seconds for this LSP to stay alive. Both of these protocols can be either strictly explicitly routed or loosely explicitly routed [34]. In strictly explicit routing, each node to be traversed to reach a destination is explicitly specified. Whereas in loosely explicit routing, not all nodes to be traversed to reach the destination are specified [34]. The nodes that are not specified in the explicit path list in loose routing are called the abstract nodes. In this thesis, we propose a network configuration method that

applies loosely explicitly routed LSP setup for WMPLS networks. The topology is as illustrated in Fig. 23.

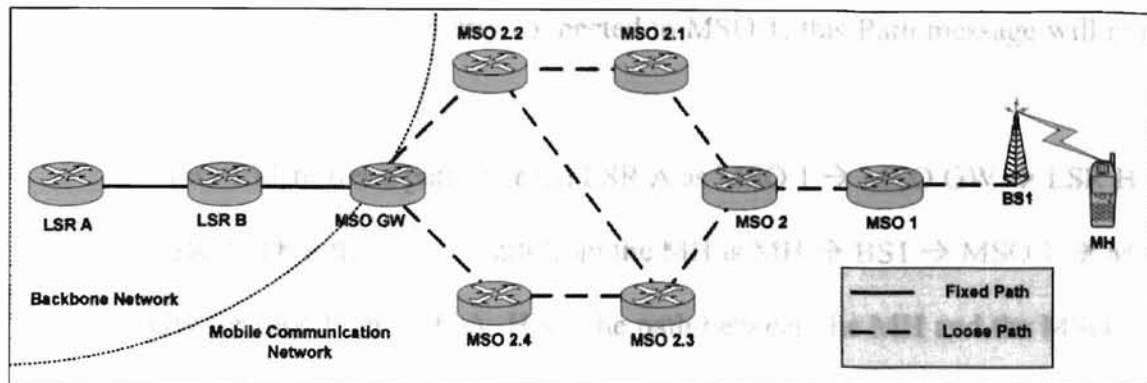


Fig.23 The proposed WMPLS networking topology.

7.5.1.1. Initial Path Setup

In this section, initial path setup is explained based on Fig. 23, where, the MH requests a connection to LSR A. Here, the MSO GW is an MSO that exists at the border of the mobile communication network and the backbone network. Since the MH continues to roam and thus requests connection to different BSs, the path between the MH and the MSO GW keeps changing. Hence, it would be beneficial for the path that exists between the MH and the MSO GW to be defined as the loosely explicitly routed part of the overall LSP that exists between the MH and LSR A. The steps involved in establishing the LSP from the MH to LSR A have been discussed in detail in the following with reference to Fig. 24. In Fig. 24, the processing time and the other system delay times have been neglected. In the following example we assume that the proposed RSVP-TE extensions are being used as the signaling protocol for WMPLS.

1. The MH first identifies and connects to its service-providing base station (BS1).
2. The MH requests for a connection to LSR A by sending a Path message to BS1. Since BS1 is directly connected to MSO 1, this Path message will reach the MSO 1.
3. MSO 1 identifies a path to reach LSR A as $MSO\ 1 \rightarrow MSO\ GW \rightarrow LSR\ B \rightarrow LSR\ A$. Thus the overall path from the MH is $MH \rightarrow BS1 \rightarrow MSO\ 1 \rightarrow MSO\ GW \rightarrow LSR\ B \rightarrow LSR\ A$. Here, the path between the MH and the MSO GW is the loosely explicitly routed part and the path between the MSO GW and LSR A is the fixed part of the overall LSP from the MH and LSR A.
4. Then, a path between the MSO 1 and the MSO GW is chosen (see Fig. 24). In this example, to reach the MSO GW from the MSO 1, there are four possible paths, where, for this example, we will assume that the path selected is $MSO\ 1 \rightarrow MSO\ 2 \rightarrow MSO\ 2.1 \rightarrow MSO\ 2.2 \rightarrow MSO\ GW$. Thus the complete overall path is $MH \rightarrow BS1 \rightarrow MSO\ 1 \rightarrow MSO\ 2 \rightarrow MSO\ 2.1 \rightarrow MSO\ 2.2 \rightarrow MSO\ GW \rightarrow LSR\ B \rightarrow LSR\ A$.
5. The Path message sent by the MH traverses the selected path through all the nodes until it reaches LSR A.
6. The Resv message is then sent by LSR A, which traverses the selected path to MH. At all nodes, the reservation and allocation of resources takes place. Labels are also assigned to individual links in the LSP. The path established will support traffic flowing from the MH and LSR A only as RSVP-TE, as well as RSVP, LDP, and CR-LDP, are all unidirectional signaling protocols.

7. Along with the Resv message, LSR A also sends a PATH message in order to establish a path from LSR A to MH for the packets sent by LSR A to reach the MH.
8. MH sends back a Resv. Then, resource allocation and label assignments for individual links are performed for the path from LSR A to MH.

As mentioned earlier, the resource requirements for these two paths may be different, thus creating an asymmetric or symmetric connection based on the request. In the initial path setup, when applying the proposed CR-LDP extension, all the steps are similar to the RSVP-TE case described above. The difference is that the Label Request message will be used instead of the Path message and the Label Mapping message will be used instead of the Resv message. In addition, CR-LDP will reserve all required traffic bandwidth and service features as the Label Request message traverses the downstream path. In the upstream path of the Label Mapping message, only the labels will be assigned to the individual LSP links. Compared to this, in RSVP and RSVP-TE, the bandwidth, service features, and labels will all be reserved when the Resv message is sent in the upstream path.

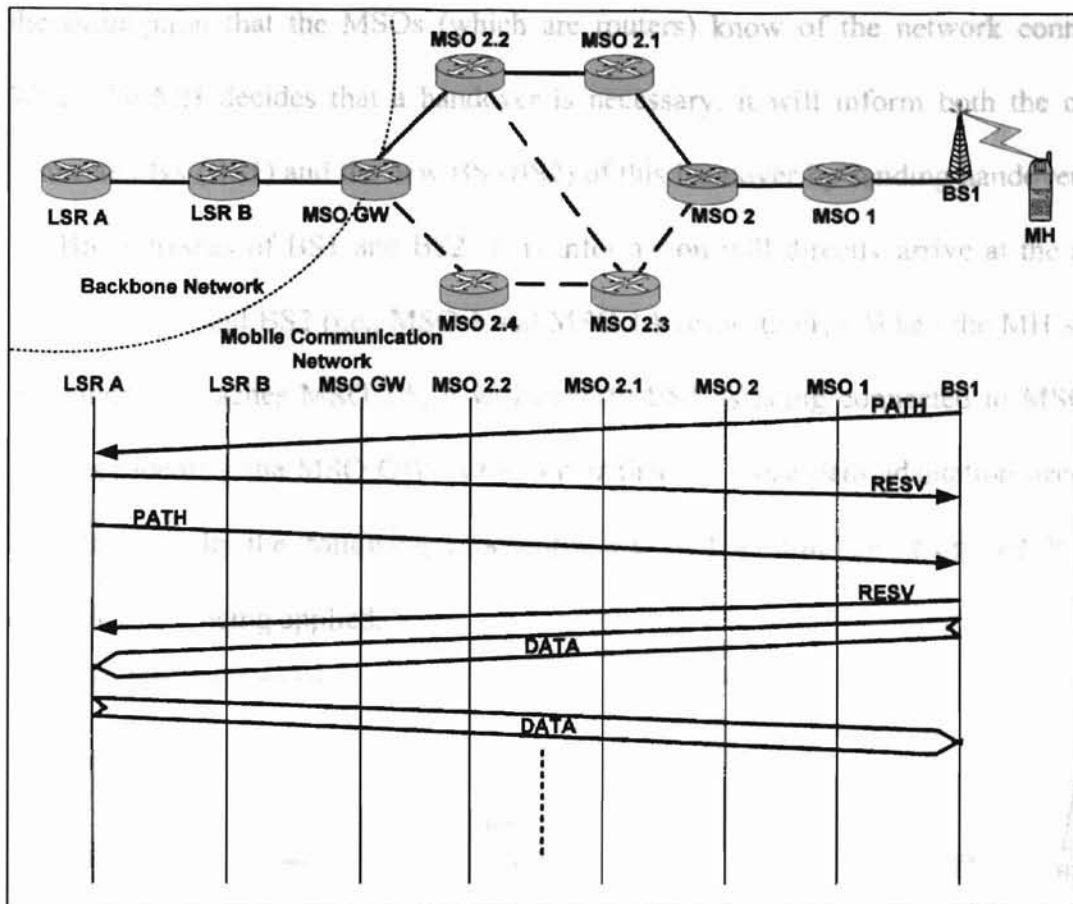


Fig.24 Initial Path Setup

7.5.1.2. Path Establishment during Handover

A soft handover procedure is initiated as soon as a need for handover is detected by the MH. As soon as a need for handover is detected, the MH identifies the new BS (BS2) in its reception area. While the currently established connection through BS1 is still kept alive to receive and transmit packets during handover, the MH tries to find another path to reach the MSO GW through BS2 [Fig. 25 & Fig. 26]. In the examples, where there is an intermediate router in the overall LSP that can support changes of the handover switching paths, then, the path from the MH to that MSO may be the part of the overall LSP that will be requested to change. In the operations described below, we make

the assumption that the MSOs (which are routers) know of the network connections. When the MH decides that a handover is necessary, it will inform both the currently connected BS (BS1) and the new BS (BS2) of this handover by sending handover data of the BS addresses of BS1 and BS2. This information will directly arrive at the adjacent MSOs of BS1 and BS2 (i.e., MSO 1 and MSO 1A respectively). When the MH's request for handover reaches MSO 1A, it will identify BS1 as being connected to MSO 1 and will also identify the MSO GW as the router that the loose path adaptation needs to be requested to. In the following procedures we will assume the proposed RSVP-TE extensions are being applied.

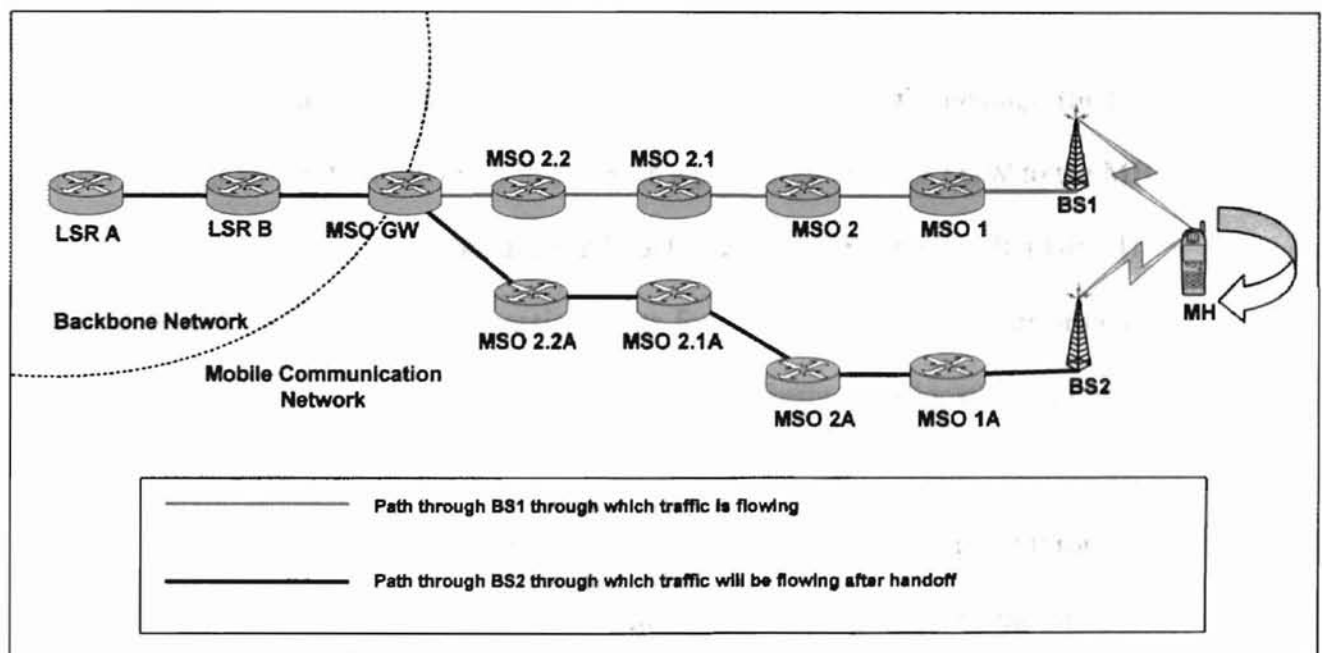


Fig.25 Path Establishment during Handover

1. The MH sends a Path message (or Label Request message in CR-LDP) to BS2, requesting connection to LSR A. Since MSO 1A is directly connected MSO supporting BS2, it will receive the Path message (or Label Request message in CR-LDP). Since MSO 1A identifies that the MSO GW is the common node where the LSPs meet, it selects a path to reach the MSO GW as MSO 1A → MSO 2A → MSO 2.1A → MSO

2.2A → MSO GW. The overall path from the MH through BS2 thus being MH → BS2 → MSO 1A → MSO 2A → MSO 2.1A → MSO 2.2A → MSO GW.

2. A Path message (or Label Request message in CR-LDP) sent by the MH traverses the selected path through the nodes in the selected path only up to the MSO GW. The path from the MSO GW to the LSR A remains fixed.

3. The Resv message (or Label Mapping message in CR-LDP) is then sent by the MSO GW, which traverses the selected path to the MH. At all nodes, the reservation and allocation of resources takes place. (In CR-LDP, the reservation of the resources would have taken place along with step 2.) Labels are also assigned to individual links in the new LSP.

4. Along with the Resv message, the MSO GW also sends a Path message (or Label Request message in CR-LDP) in order to establish a path from the MSO GW to the MH.

5. The MH sends back a Resv message (or Label Mapping message in CR-LDP). Then the resource allocation and the label assignments for individual links are performed for the LSP from the MH to the MSO GW. (In CR-LDP, the resource allocation would have taken place along with step 4.)

6. Once this path is successfully established, data packets will be forwarded through the newly established path and the former path from the MH through BS1 to the MSO GW (MH → BS1 → MSO 1 → MSO 2 → MSO 2.1 → MSO 2.2 → MSO GW) is disconnected.

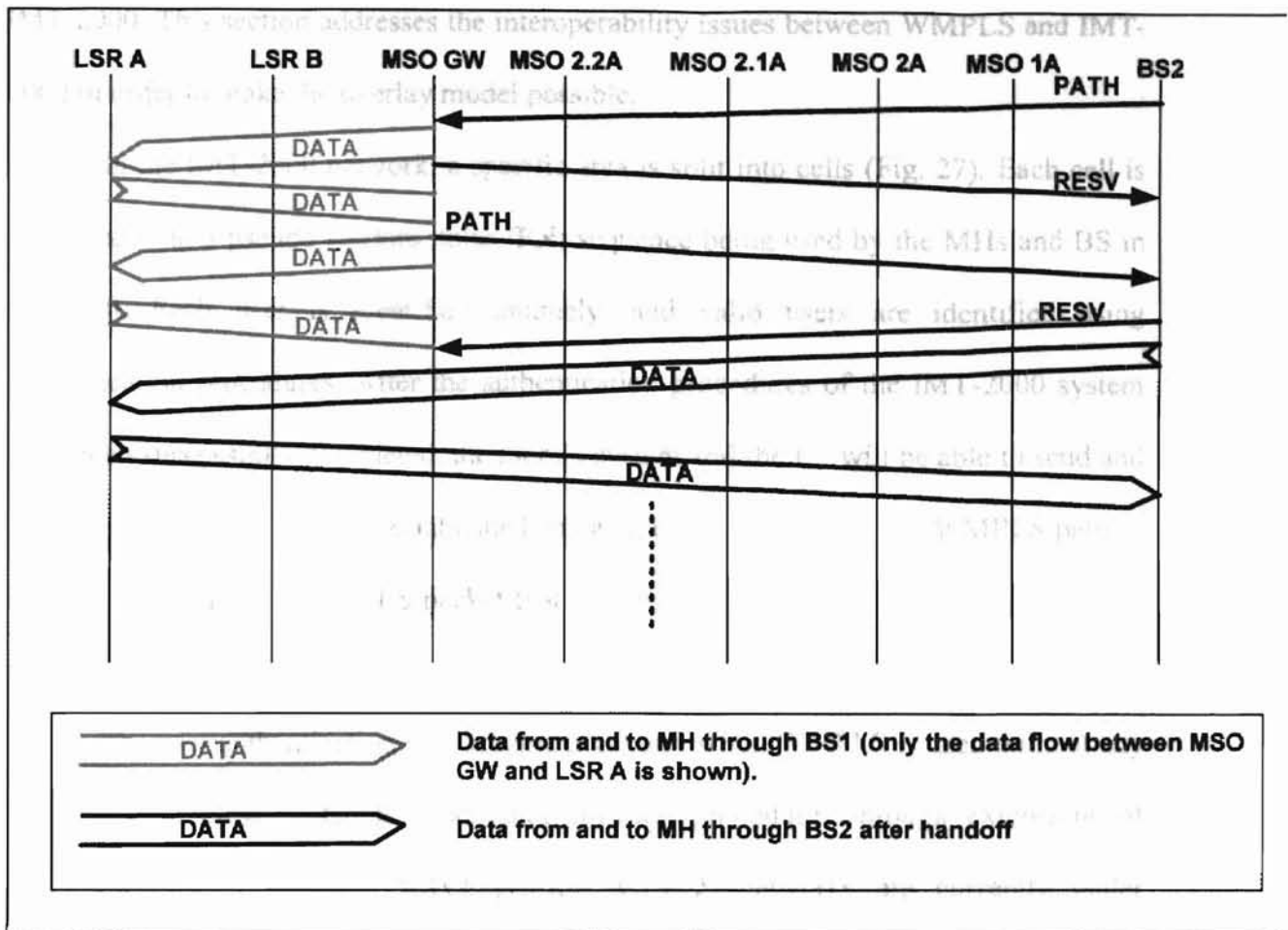


Fig.26 Message and Data Flow during and after Handover

7.5.2. WMPLS over IMT-2000

In this section we look into the operations of WMPLS applied in an overlay model having the International Mobile Telecommunications-2000 (IMT-2000) wireless communication network architecture as the lower layer system.

The objectives of IMT-2000 are to provide a maximum data rate of 144/384 Kbps under roaming conditions and a peak data rate of 2 Mbps under stationary conditions, both with a bandwidth of 5 MHz. To provide QoS, dedicated bandwidth, and differentiated services over the network; WMPLS can work in an overlay fashion with

IMT-2000. This section addresses the interoperability issues between WMPLS and IMT-2000 in order to make the overlay model possible.

In the IMT-2000 network, a specific area is split into cells (Fig. 27). Each cell is identified with a pseudo random noise (PN) sequence being used by the MHs and BS in that cell. Each user is identified uniquely, and valid users are identified using authentication procedures. After the authentication procedures of the IMT-2000 system have been successfully completed, the mobile system and the BS will be able to send and receive packets. Through this established channel, the MH establishes a WMPLS path as explained earlier. Any WMPLS packet that is sent is encapsulated within the IMT-2000 protocol payload.

The user authentication will become necessary when WMPLS is used without any underlying wireless protocols. User authentication procedures through extensions of LDP, CR-LDP, RSVP and RSVP-TE for WMPLS networks are currently under investigation.

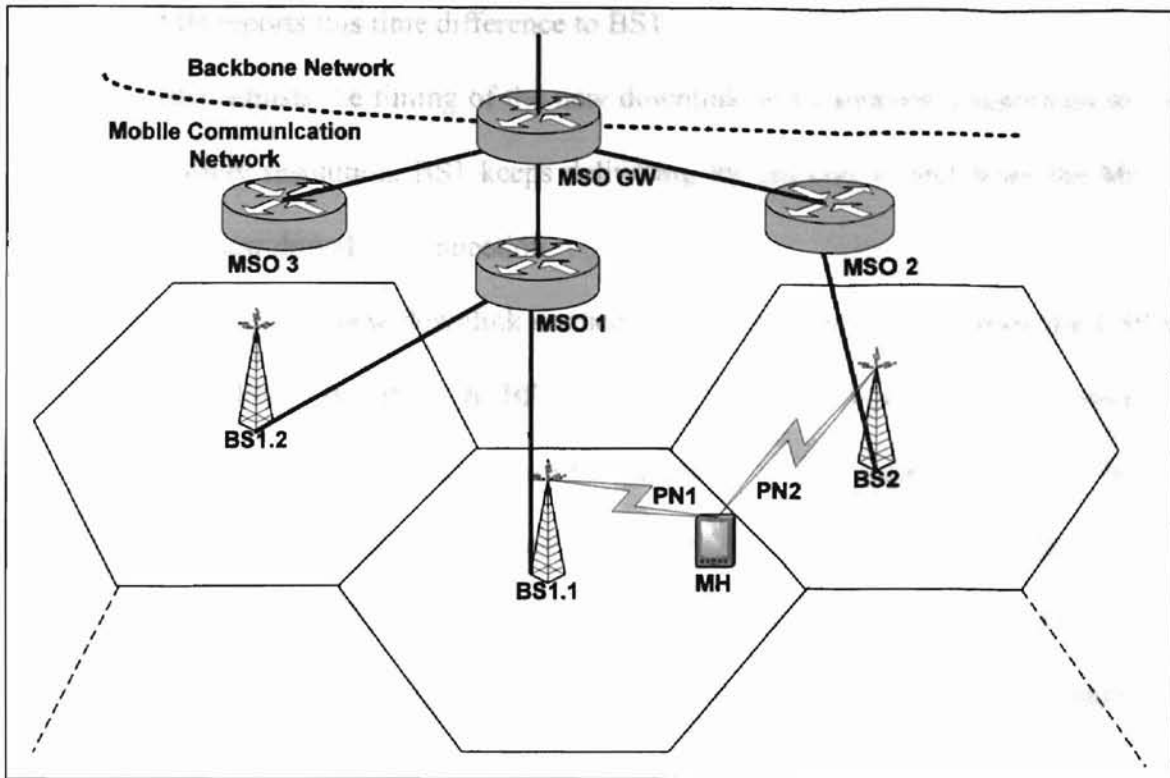


Fig.27 WMPLS Over IMT-2000

As an example shown in Fig. 27, the MH is connected to BS1.1. The PN sequence used in that cell is assumed to be PN1. Additionally, we also assume that the MH detects a need for handover/handoff and is expecting the communication link to be handed off to BS2, which belongs to another cell with a different PN sequence, is PN2. Assuming overlapping coverage ranges of the BSs, the following steps [29] are carried out:

1. The MH performs the initial cell search and acquires the scrambling code for BS2. Thus the MH will be able to find the broadcast control channel (BCCH).
2. The MH then acquires the primary unmodulated synchronous channel (SCH) and obtains the timing information for the secondary SCH.
3. Once acquiring the secondary SCH, the MH achieves synchronization to BS2.
4. The MH then calculates the timing difference between two downlinks of BS1 and BS2.

5. MH reports this time difference to BS1.
6. BS1 adjusts the timing of the new downlink soft handover connection to one symbol resolution. BS1 keeps delivering the packets to and from the MH in this new downlink connection.
7. Keeping this new downlink connection alive, the MH establishes the LSP to the MSO GW through BS2 with the help of MSO 1A. The resource requirements of this new path to the MSO GW through BS2 should be the same as that of the current path to the MSO GW through BS1. Since WMPLS uses RSVP-TE or CR-LDP as the signaling protocols, such negotiation procedures can be performed during handover in order to get the same TE parameters.
8. Once the new path through BS2 to the MSO GW with same TE parameters is established, the path through BS1 to MSO GW is terminated.

Thus, soft handover with same TE parameters is achieved in the overlay model of WMPLS over IMT-2000. As explained earlier, in general, WATM is not as flexible as WMPLS is in negotiating TE parameters, which can become a significant problem during handover procedures. Another benefit of applying WMPLS procedures over IMT-2000 link is that the IMT-2000 connection in support of the wireless network is focused on the connection of the BS to the MH, while WMPLS is capable of providing a single connection or multiple connections over a single wireless link. This is especially beneficial when a MH needs to establish a point-to-multipoint connection or when it needs to conduct simultaneous data communication functions of other devices attached to

the MH system, where the MH is communicating over the network simultaneously with these attached devices. Other benefits can be seen when multiple devices may be communicating through a MH using the MH to BS connection as a relay path. In addition, interoperability of the networking protocols with future MPLS, GMPLS, or MPLambdaS networks is another essential reason that this technology has been developed.

CHAPTER VIII

WMPLS Performance Analysis

8.1. WMPLS Performance Analysis Based on GoBackN Technique

In this subsection, we analyze the performance of WMPLS protocol with GoBackN technique for error control. We also compare WMPLS with WATM to prove that WMPLS with adaptive packet size capability has better throughput efficiency over WATM. For this analysis, [10] has been used. In [10] only ATM has been considered. We extend this analysis for a general case in order to compare WMPLS and WATM.

For this analysis, no error correction capability is assumed for WMPLS and WATM. A packet is discarded even if there is a single bit error in the header. If the header does not have any bit errors and the payload has a single bit error, then a packet is still considered useless.

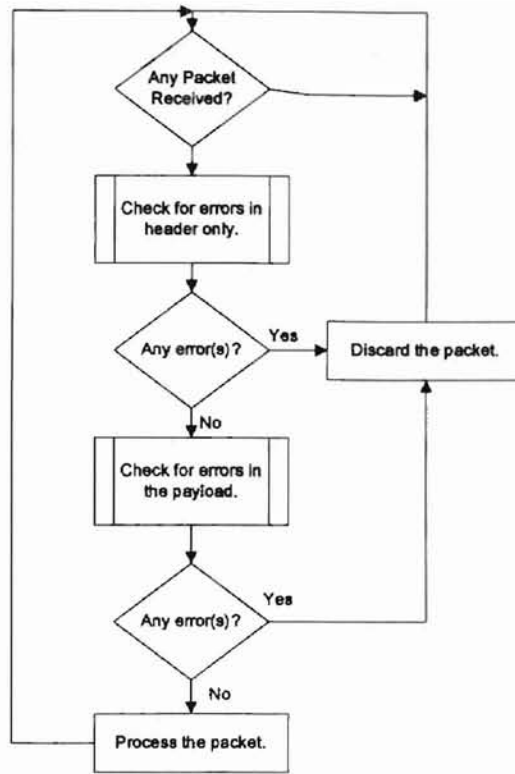


Fig.28 Error Control Algorithm

From [10], the throughput efficiency of a protocol is defined to be,

$$\eta_{WATM} = \frac{1 - R_{OverHead}}{P_C + (1 - P_C) \cdot N_{Win}} \cdot P_C \quad (1)$$

where,

$$R_{OverHead} = \frac{h}{h + T} \text{ with } h \text{ as header size (in bits), } T \text{ as payload size (in bits),}$$

P_C = Probability {total packet is received without any errors}, and

N_{Win} = Window Size (number of data link layer packets per window).

If N is assumed to be the number of data link layer packets per original packet and N_{pkt} is assumed to be number of bits per data link layer packet, then

$$P_C = \{(\text{Probability of correct data link packet})^{N+1}\}, \quad (2)$$

and

$$N_{pkt} = h + T. \quad (3)$$

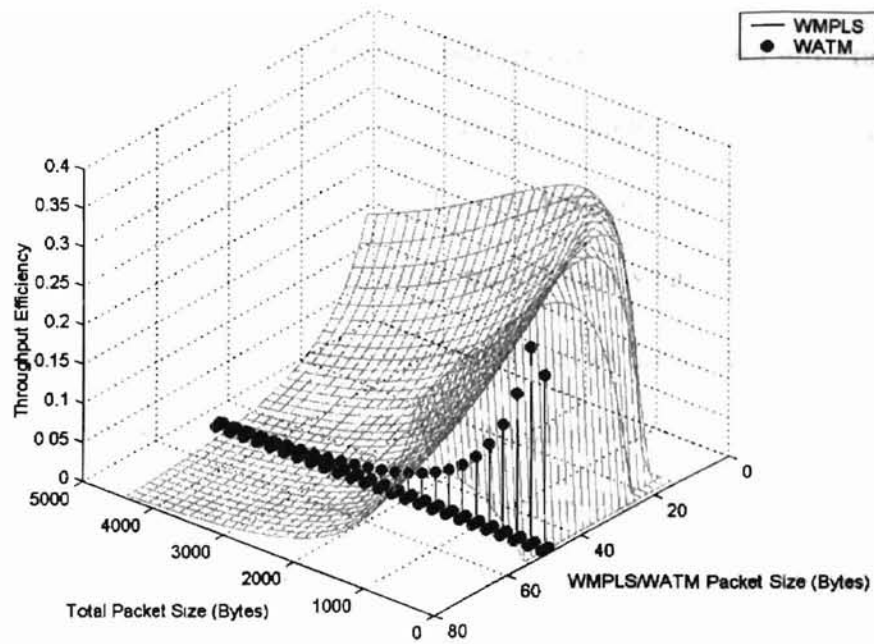
Here, $N+1$ data link packets are used to calculate P_C because, to receive an original packet (also referred as total packet) the last data link packet of the previous original packet should have been received successfully.

Now, assuming that the probability of error in any bit as independent of the probability of bit error in any other bit, we can write the probability of correct data link packet (P_{pkt}) as the probability of no error in header ($1 - P_h$) and probability of no error in the payload.

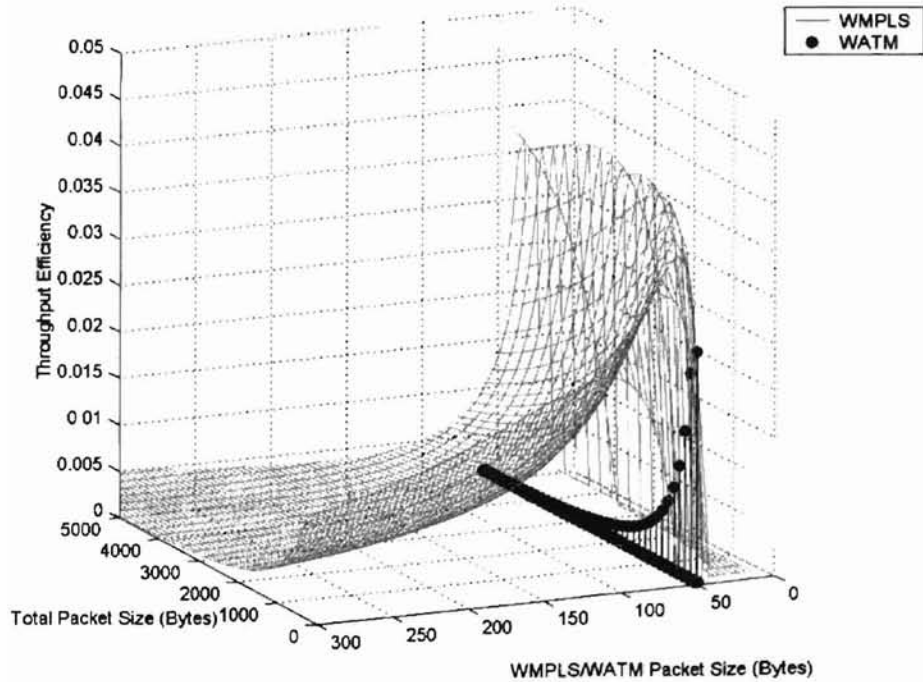
$$P_{pkt} = (1 - P_h) \cdot (1 - p)^T \quad (4)$$

where, p is the probability of a bit error and $P_h = (1 - p)^h$.

The above analytical model can be used to analyze and compare WMPLS and WATM technologies. In this article, a total packet size is the size of all the data link packets contained in it. In other words, a total packet should have at least one data link layer packet (WMPLS/WATM).



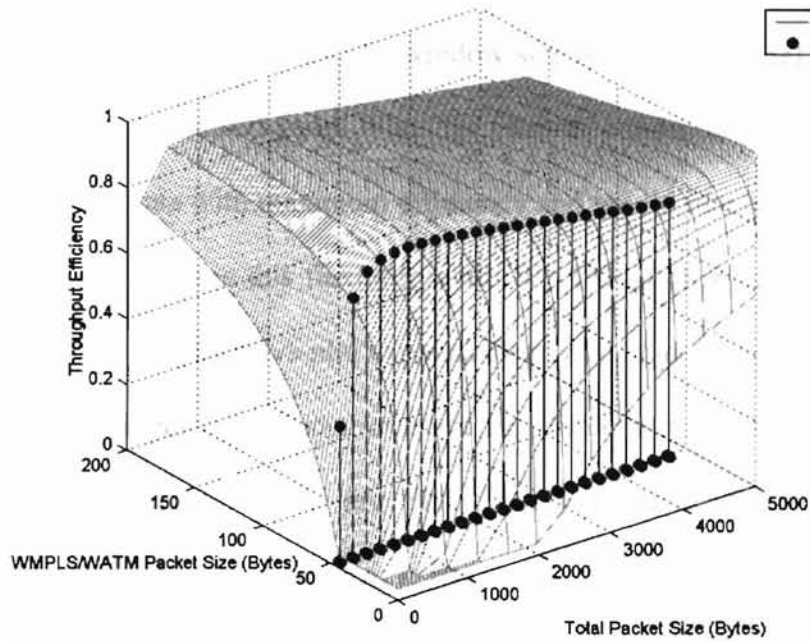
a) Throughput Efficiency for Window Size = 7, 6 Byte WMPLS Header



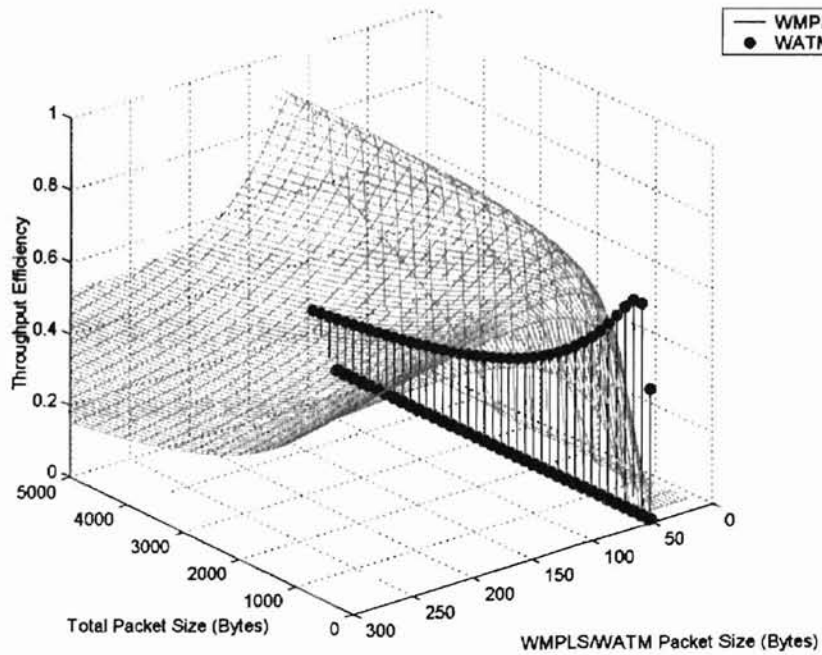
b) Throughput Efficiency for Window Size = 7, 7 Byte WMPLS Header

Fig.29 WMPLS Performance with GoBackN for BER = 10^{-4}

The above figures give a plot of throughput efficiency for different WMPLS packet sizes (just payload) and for different total packet sizes, at a bit error rate of 10^{-4} . It is clear from the above figures that WMPLS has much higher throughput efficiency than WATM when the number of bytes in a WMPLS packet keeps decreasing. This is because we would like to keep the data link layer packet size small in order to have good throughput efficiency when the channel conditions are not favorable ($BER = 10^{-4}$). From the figures, it can be seen that for small WMPLS packet sizes, we have better throughput efficiency for relative long total packet sizes. For very high total packet sizes, due to retransmission of corrupted packets, the efficiency decreases. From the figure, we can select the best WMPLS packet size for a known total packet size such that the efficiency is maximized. For WATM, we do not have packet size adaptability and so has fixed efficiency profile. In fact, for total packet sizes greater than a few hundred bytes, the efficiency of WATM drops significantly. This is true for WATM with 7 byte header also. In Fig. 29a, WMPLS with 6 byte header and WATM with 5 byte header were assumed. In Fig. 29b, both WMPLS and WATM with 7 byte header were assumed. For the latter case, the efficiency of both the protocols is significantly less compared to the former one. This is because of an increase in the header size of these protocols. As the header size increases, the probability of errors in the header increases, in turn increasing the probability of packet discard.



a) Efficiency for Window Size = 7, 6 Byte WMPLS Header



b) Efficiency for Window Size = 7, 7 Byte WMPLS Header

Fig.30 WMPLS Performance with GoBackN for BER = 10^{-6}

The above figures give the plot of throughput efficiency for the case when probability of bit error is 10^{-6} and the window size is 7. The channel with such a bit error rate is generally considered good. When the channel condition is good, we would like to send as much of data with maximum efficiency and would like to send them in big sized packets. We do not have this flexibility with WATM of changing packet size based on channel conditions. The above plot explains clearly this fact. Even for large size WMPLS packets, the efficiency is almost constant for different total size packets. Hence, we would be able to send packets of large size when the channel condition is good. Too large of packets may lead to poor efficiency. But the above plot may be used to determine the maximum packet size for maximum efficiency. In the following section WMPLS performance analysis for selective reject (SREJ) ARQ has been assumed. Selective reject will lead to better performance than GoBackN as only the packets that were in error are to be retransmitted.

8.2. WMPLS Performance Analysis Based on SREJ Technique

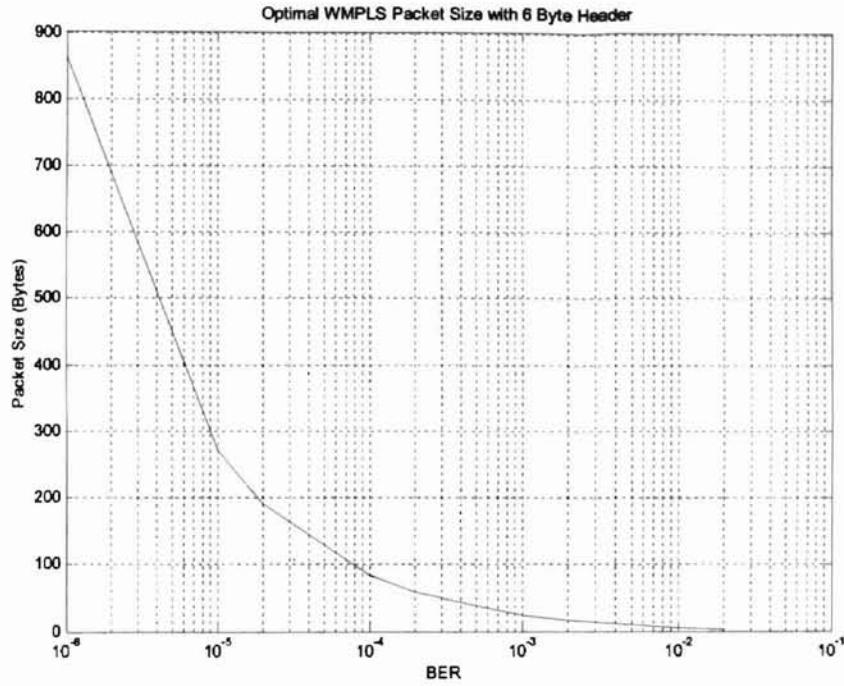
For the analysis of WMPLS performance, in this section, we make use of a direct equation from [23]. In [23], a detailed packet size optimization has been given. The basic equation for optimal packet size for SREJ is given by,

$$k_{opt} = \frac{-h \cdot \ln(1-p) - \sqrt{-4h \cdot \ln(1-p) + h^2 \cdot \ln(1-p^2)}}{2 \ln(1-p)} \quad (5)$$

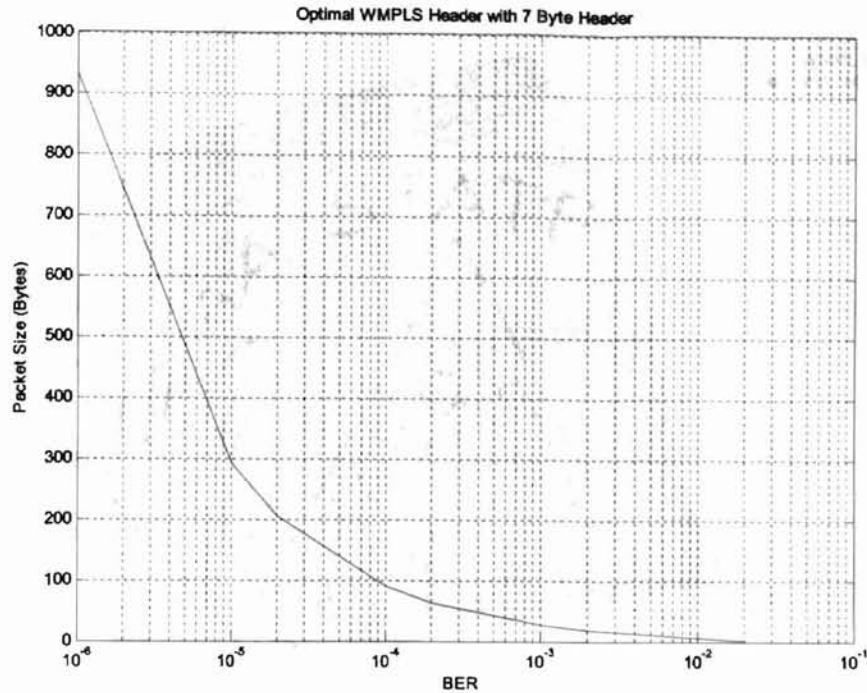
where, k_{opt} is the optimal packet size.

The throughput efficiency of a protocol using SREJ is given by,

$$EFF = \left(\frac{T}{T+h} \right) \frac{1}{(1-p)^{-(T+h)}} \quad (6)$$



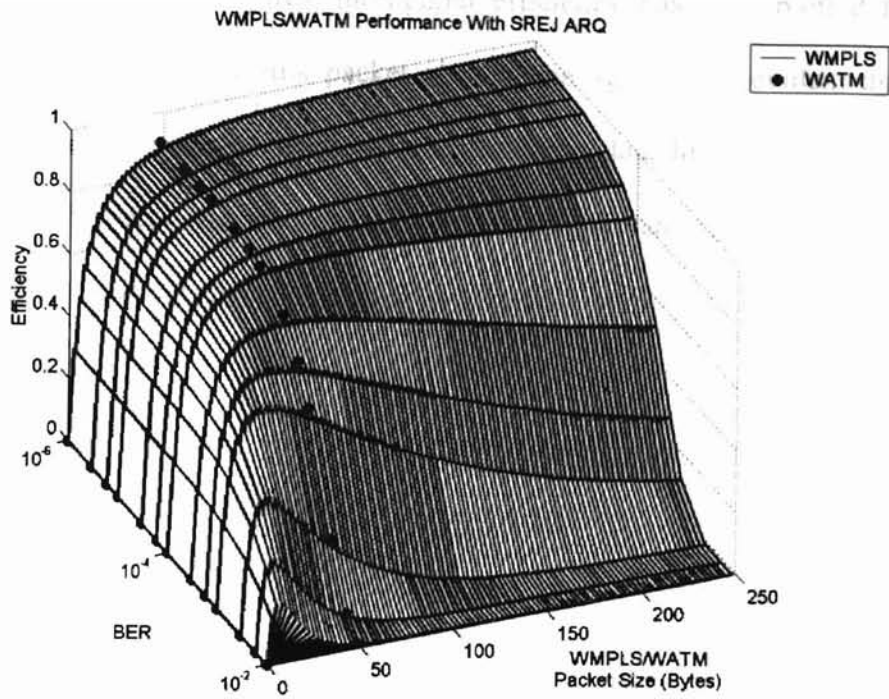
a) Optimal Packet Size with 6 Byte Header



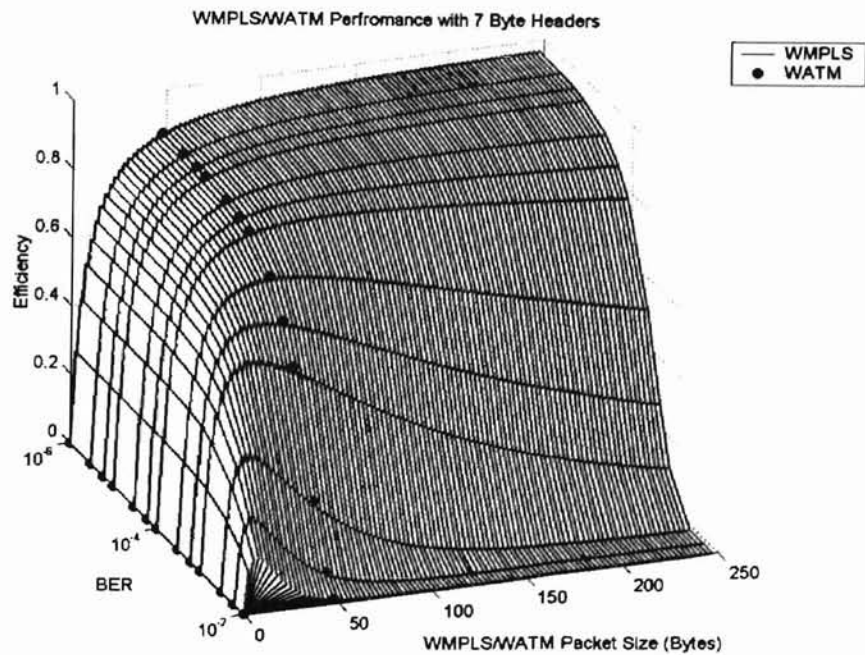
b) Optimal Packet Size with 7 Byte Header

Fig.31 Optimal WMPLS Packet Size

The above two plots give the optimal packet sizes for WMPLS under various channel conditions. Selective Reject ARQ technique has been assumed for error control. As can be seen, the optimal WMPLS packet size increases as the channel condition gets better. Packet size optimization has been done to maximize the efficiency. This packet size adaptability is not possible with WATM and so is limited to fixed throughput efficiencies for different channel conditions.



a) WMPLS Performance with SREJ for 6 Byte Header



b) WMPLS Performance with SREJ for 7 Byte Header

Fig.31 WMPLS Performance with SREJ ARQ

In the above two figures, throughput efficiency has been plotted for different channel conditions and data link packet sizes. Once again, it is evident that when the channel condition is bad, we would like to limit our data link packet size in order to improve the efficiency. As the channel gets better, we can also increase the data link packet size.

CHAPTER IX

CONCLUSION

In this thesis, a novel internetworking protocol, called wireless internetworking protocol (WIP) and a novel network access layer protocol, called wireless MPLS (WMPLS) were presented to support enhanced reliability for mobile wireless voice/video/data communications.

WIP utilizes a “make-before-brake” soft handoff procedure to support continuous reliable data transmission over the network under handoff situations. WIP requires for a network server or management module to announce mobile client IP address changes on request for other network users. It has been shown that WIP also helps to avoid triangle routing problems that MIP has, and eliminates the need for the transferring of stacks of data packets and the comparison process of address pairs that are required due to handoff procedures in ROMIP and MIP based networks. WIP also eliminates the need to do encapsulation of all the packets. Even if minimal header encapsulation can be used for encapsulation, this is still a waste of resources. In addition, when desired, the soft handoff enables a continuous end-to-end TCP session to be maintained throughout the connection enhancing the link reliability (error control, flow control, and session control). In addition, through the procedural flow charts provided, it is proved that WIP is also supportive of providing IP layer reliable and efficient soft handoff support over wireless systems such as Bluetooth communications and IMT-2000 mobile communications.

WMPLS being the wireless version of MPLS, MPLambdaS and GMPLS, provides the wireless network with differentiated services with quality of service (QoS) and traffic engineering features. WMPLS requires a simple translator at border of

wireless and backbone network, to translate the WMPLS headers in to MPLS, MPLambdaS or GMPLS header format. To prove that WMPLS is interoperable with latest wireless technologies, WMPLS over IMT-2000 was also discussed in detail. Using adaptive packet size WMPLS, it has been shown that WMPLS has better throughput efficiency than WATM under varying channel conditions.

REFERENCES

- [1] A. S. Acampora and M. Naghshineh, "An architecture and Methodology for Mobile-Executed Handoff in Cellular ATM Networks," *IEEE JSAC*, vol.12, no.8, Oct. 1994.
- [2] L. Andersson, P. Doolan, N. Feldman, A. Fredette, and B. Thomas, "LDP Specification," RFC 3036, The Internet Society, Jan. 2001.
- [3] Albrecht, M.; Frank, M.; Martini, P.; Schetelig, M.; Vilavaara, A.; Wenzel, A, "*IP services over Bluetooth: leading the way to a new mobility*", Local Computer Networks, 1999. LCN '99. Conference, 1999
- [4] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209, The Internet Society, Dec. 2001.
- [5] E. Ayanoglu, K. Y. Eng, and M. J. Karol, "Wireless ATM: Limits, Challenges, and Proposals," *IEEE Personal Communications*, vol. 12, Aug. 1996.
- [6] Baatz, S.; Frank, M.; Gopffarth, R.; Kassatkine, D.; Martini, P.; Schetelig, M.; Vilavaara, A, "*Handoff support for mobility with IP over Bluetooth*", Local Computer Networks, 2000. LCN 2000. Proceedings. 25th Annual IEEE Conference, 2000.
- [7] A. Bakre and B. R. Badrinath, "*Handoff and system support for indirect TCP/IP*", in *Proc. of the 2nd USENIX Symposium on Mobile and Location-Independent Computing*, pp. 11-24, Apr. 1995.
- [8] B. Bing, *High-Speed Wireless ATM and LANs*. Norwood, MA: Artech House, 2000.
- [9] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1, Functional Specification," RFC 2205, The Internet Society, Sept. 1997.

- [10] J. B. Cain and D. N. McGregor, "A Recommended Error Control Architecture for ATM Networks with Wireless Links," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 1, Jan. 1997.
- [11] A. T. Campbell, J. Gomez, and A. G. Valko, "An overview of cellular IP," in *Proc. of IEEE Wireless Communications and Networking Conference 1999 (WCNC'99)*, vol.2, 21-24 Sept. 1999.
- [12] J.-M. Chung, (Invited Paper) "Wireless Multiprotocol Label Switching," in *Proc. of the 35th Asilomar Conference on Signals, Systems & Computers 2001*, Pacific Grove, California, U.S.A., Nov. 4-7, 2001.
- [13] J.-M. Chung "Wireless Multiprotocol Label Switching (WMPLS) Applications in Broadband Wireless Communications," submitted to *IEEE Networks*.
- [14] J.-M. Chung, (Invited Paper) "Analysis of MPLS Traffic Engineering," *Proceedings of the IEEE Midwest Symposium on Circuits and Systems 2000 Conference (IEEE MWSCAS'00)*, East Lansing, MI, U.S.A., Aug. 8-11, 2000.
- [15] J.-M. Chung, E. Marroun, H. Sandhu, and S.-C. Kim, "VoIP over MPLS Networking Requirements," in *Proc. of the IEEE International Conference on Networking 2001 (IEEE ICN'01)*, Colmar, France, July 9-13, 2001.
- [16] J.-M. Chung, M. A. Subieta Benito, H. Chhabra, G. Y. Cho, and P. Rasiah, "Extensions to CR-LDP for MPLS Multicasting," work in progress, *Internet Draft*, Internet Engineering Task Force (IETF), The Internet Society.
- [17] J.-M. Chung, M. A. Subieta Benito, H. Chhabra, G. Y. Cho, and P. Rasiah, "Extensions to RSVP-TE for MPLS Multicasting," work in progress, *Internet Draft*, Internet Engineering Task Force (IETF), The Internet Society.

- [18] T. Clausen, P. Jacket, A. Laouiti, P. Minet, P. Muhlethaler, A. Wayyum, L. Viennot, "Optimized Link state Routing Protocol," work in progress, *Internet Draft*, Internet Engineering Task Force (IETF), The Internet Society.
- [19] Core Specifications ver. 1.1, The Bluetooth Special Interest Group (SIG), www.bluetooth.com.
- [20] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, The Internet Society, Jan. 1999.
- [21] R. Droms, "Automated configuration of TCP/IP with DHCP," *IEEE Internet Computing*, vol. 3, issue 4, July-Aug. 1999.
- [22] B. Jamoussi, et al., "Constraint-Based LSP Setup using LDP," work in progress, *Internet Draft*, Internet Engineering Task Force (IETF), The Internet Society.
- [23] E. Madiano, "An adaptive algorithm for optimizing the packet size used in wireless ARQ protocols," *Wireless Networks*, 1999.
- [24] C. E. Perkins, "Mobile IP," *IEEE Communications Magazine*, vol. 35, issue 5, May 1997.
- [25] C. E. Perkins and K.-Y. Wang, "Optimized smooth handoffs in Mobile IP," in *Proc. IEEE International Symposium on Computers and Communications 1999 (ISCC'99)*, 6-8 July 1999.
- [26] C. E. Perkins, "Mobile networking through Mobile IP," *IEEE Internet Computing*, vol. 2, issue 1, Jan.-Feb. 1998.
- [27] C. E. Perkins and T. Jagannadh, "DHCP for mobile networking with TCP/IP," in

Proc. of IEEE Symposium on Computers and Communications 1995 (ISCC'95), 27-29 June 1995.

- [28] C. E. Perkins, E. M. Belding-Royer, S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," work in progress, *Internet Draft*, Internet Engineering Task Force (IETF), The Internet Society.

- [29] R. Prasad and T. Ojanpera, "An Overview of CDMA Evolution toward Wideband CDMA," *IEEE Communications Surveys*, vol. 1, no. 1, 4th quarter, 1998.

- [30] "Private Network-Network Interface Specification 1.0 (PNNI 1.0)," af-pnni-0055.000., The ATM Forum, Mar. 1996.

- [31] Profile Specifications ver. 1.1, The Bluetooth Special Interest Group (SIG), www.bluetooth.com.

- [32] R. Ramjee et al, "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless networks," *Proceedings of the Seventh Annual International Conference on Network Protocols*, ICNP '99.

- [33] D. Raychaudhari and N. D. Wilson, "ATM based transport architecture for multiservice wireless personal communication networks," *IEEE JSAC*, vol. 12, pp. 1401-1414, Oct. 1992.

- [34] E. Rosen and A. Viswanathan, "Multiprotocol Label Switching Architecture," RFC 3031, The Internet Society, Jan. 2001.

- [35] C.-K. Tok, "Wireless ATM and Ad-Hoc Networks: Protocols and Architectures," Kluwer Academic Publishers, 1997.

VITA 2

Kannan Srinivasan

Candidate for the Degree of

Master of Science

Thesis: PROTOCOL DEVELOPMENT AND PERFORMANCE ANALYSIS OF WIP
AND WMPLS WIRELESS NETWORKING TECHNOLOGIES

Major Field: Electrical Engineering

Biographical:

Personal Data: Born in Madras, India, On June 5, 1978, the son of
R. Srinivasan and S. Rama.

Education: Received a Bachelor of Engineering degree in Electronics and
Communication Engineering from the University of Madras, India in May
2000. Completed the requirements for the Master of Science degree with a
major in Electrical Engineering at the Oklahoma State University in August
2002.

Experience: Employed as a Research Assistant by the ACSEL Laboratories at the
School of Electrical and Computer Engineering, Oklahoma State University,
Aug. 2000 to present.

Employed as an Intern in TechTrol Inc., Pawnee, Oklahoma, May 2002 to
Aug 2002.

Professional Membership: Student member of the honorary Institute of Electrical
and Electronics Engineers, Inc. (IEEE) for the academic years 2001 and 2002.