Handoff Between Homogeneous and Non-Homogeneous Mobile Network Environment

by

Zia Mansoor

This dissertation is submitted to I.I.U. in partial fulfillment of the requirements for the degree of

MS Electronic Engineering

Department of Electronic Engineering

Faculty of Engineering and Technology

International Islamic University, Islamabad.

2008

14/7/10

M8 $g

1. Communication
2. Electronic measurements
3. Electric measurements
4. Rigid guard channel; Conventional guard channel
5. Electrometry and electronic test equipment

Certificate of Approval

It is certified that we have read the project report submitted by **Zia Mansoor [132-FET/MSEE/F-07]**. It is our judgment that this report is of sufficient standard to warrant its acceptance by the International Islamic University, Islamabad for degree of MS Electronic Engineering (MSEE).

Supervisor
Dr. Tanweer Ahmed Cheema
Dean, FET, IIU Islamabad.

External Examiner
Dr. Abdul Jalil
Associate Professor
PIEAS, Islamabad.

Internal Examiner
Dr. Aqdas Naveed Malik
Assistant Professor, IIU, Islamabad.

Declaration

I hereby declare that this research and simulation, neither as a whole nor as a part thereof has been copied out from any source. It is further declare that I have developed this research, simulation and the accompanied report entirely on the basis of my personal effort made under the guidance of my supervisor and teachers.

If any part of this report to be copied or found to be reported, I shall standby the consequences, no portion of this work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Zia Mansoor
132-FET/MSEE/F-07

Dedicated to My Parent
And Friends

Acknowledgement

First of all I would like to extend my sincere and humble gratitude to Almighty Allah whose blessings and guidance has been a real source of all my achievements in my life.

I am grateful to thank my Teacher ***Dr. I. M. Qureshi*** *and supervisor* ***Dr. Tanveer Ahmed Cheema*** *for his sincere help and guidance during my studies and thesis work. He always remained a source of Learning for me.*

I would also like to thank all my fellows, seniors and juniors who have been remained encouraging for all the period that came in my university life, Special thanks to Mr. Jamil Kahut & Mr. Muhammad Shoaib for his important suggestions and valuable advice throughout my research work. They helped me to get into the bottom of the problems I faced in course work and research.

I am indebted to my parents and other family members for their prayers and moral & financial support during my studies.

At the end I would like to thank all of my class fellows for their cooperation and help.

(Zia Mansoor)

Abstract

This dissertation explores various schemes to solve the problem of vertical handoff. Most of the schemes explained in the thesis use Mobile IP (MIP), Session Initiation Protocol (SIP), Host Identification Protocol (HIP) and Network Mobility Protocol. I purpose that the vertical handoff through extension of Host Identification Protocol (HIP) can give us better performance as compared to other schemes. Because it does not suffer from the routing overhead, since the home agent is not used. Also we do not need to change anything in the network to support handover which is preferred by service providers, as home/foreign agents are required in the MIP schemes and SIP server is required in the scheme proposed through SIP.

In this thesis, I propose some improvement over previous work about network mobility using different protocols using MR implementation in Linux O.S. Also presenting architecture for reduces handoff impacts on the communication of nodes in the varied network. The purposed architecture is independent of infrastructure support with using caching and route optimization techniques to improve the communication between nodes.

Keywords: Network mobility, Vertical Handoff, Mobility management, Mobile IP

Table of Contents

List of Figures

Chapter 1

Introduction

In the recent years, the trend has been changed to make the computers mobile and to make such mobile devices powerful enough to have computer like capabilities. Therefore, a lot of wireless technologies have emerged in recent years in order to support mobility, competing with one another e.g. WiMAX, WiFi, UMTS [1] and CDMA. Proliferations of these wireless technologies have raised a number of questions. One of these questions is how to maintain seamless mobility within these technologies so that one technology will not be able to dominate all other technologies and future will consist of combination of these technologies. In order to obtain mobility, the moving user has to be connected to the network which is obtained by handoffs or handovers. These handoffs may be horizontal and vertical handoffs. Mobile devices typically have limited battery capacity due to the design objective of minimizing their weight and size. In order to reduce the power consumption, the processing power of mobile devices, such as Personal Digital Assistants (PDAs) and smart phones, is only a fraction of the processing power of the most modest personal computer. However, the increased processing power of low power processors will increase the limit of applications which can be run on low power mobile devices.

The limited size and processing power of the mobile devices reflects on the way users can interact with them. The small screen and lack of a proper keyboard limit the text reading and entering capabilities of PDAs. In order to address such limitations, new types of user interfaces such as projected keyboards [2] and multimodal interfaces have been proposed. However, the limitations of communication capabilities are in part due to the inherent physical characteristics of wireless networks which make communication over these networks several magnitudes less reliable and slower than communication over wired networks. The restrictions on antenna size, number of antennae, limited transmitted power, the range and throughput of wireless communications for a mobile device. Furthermore, the radio communications utilize a shared medium which limits the communication [3].

The network architectures and protocols which are used to enable the communications limit the way mobile users can take advantage of the available wireless networks. Many mobile devices, especially smart phones and PDAs, are already being equipped with multiple radio interfaces enabling them to connect to multiple access networks at the same time. This would enable them to use a wireless overlay consisting of multiple access network types of complementing characteristics. However, in spite of these advanced hardware capabilities, the devices cannot currently take full advantage of the heterogeneous access networks effectively due to the lacking support for handoffs, i.e. handing over of communications from one network to another one, on the protocol level. This prevents users from starting a voice call over a low cost network, such as IEEE 802.11 Wireless Local Area Networks (WLANs) and when leaving the limited coverage of the WLAN network performing a so called vertical handoff, i.e. inter-technology, handoff to a wider coverage, but more expensive Wireless Wide Area Network (WWAN), e.g. an UMTS network.

In single type of network i.e. horizontal handoffs, has been conventionally handled below the network level. This is possible as long as the new and old networks are part of the same IP network. However, handoffs between different IP networks require the mobility management to be handled on the IP layer or above it. This would be the case at least for vertical handoffs and for handoffs between networks operated by different providers.

1.1 Ubiquitous Wireless Services

Ubiquity refers to the ability of subscriber to obtain wireless telecommunications services everywhere. Ubiquitous is also a characteristic of radio coverage. It implies that there are no gaps or holes in a coverage area. Personal area networks and vehicle networks provide network access services to the user during journey. Central management servers are used to connect vehicle networks and use other network resources. MR is one of the most important devices in mobile network which is used to connect to the mobile nodes to the internet using wire or wireless connection. Using a MR allows all the MN in the network to take advantage of the communication capabilities of the Mobile Router. The external antenna of vehicle is used to communicate among the MN using power from the power system of vehicle. In addition, extra features of MR minimize the protocol overheads during the mobility.

Mobile Router using NEMO for managing the mobile networks designed by Internet Engineering Task Force. In NEMO,[4] handling of the mobility related signaling and management of routing of packets to and from the mobile network are aggregated into the Mobile Router, as shown in Figure 1. The Mobile Router runs the NEMO protocol with a special router, the Home Agent. It acts as a fixed anchor point for maintaining the reach ability of the Mobile Router and the devices within the mobile network. NEMO hides the mobility from the Mobile Network Nodes (MNNs), i.e. nodes within the mobile network. This enables Mobile Network Nodes to communicate with nodes outside the mobile network in spite of the Mobile Router moving between different networks without any mobility management capabilities.

1.2 Thesis Structure

The following are contributions of this thesis:

- Structural design

  * The SIP and HIP protocol [5] have been enhanced for mobility management enhancement in heterogeneous network environment.
  * Mobile Router has been enhanced by adding the feature bootstrapping. The thesis also improves the use and configuration of the mobility management services.

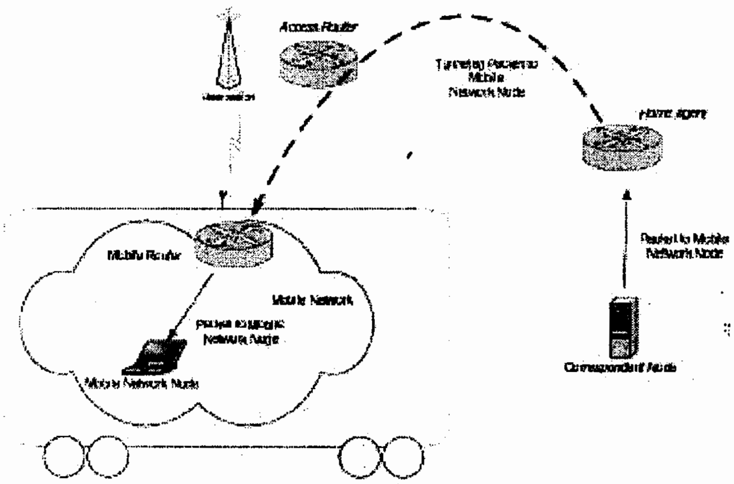


Figure 1 Basic architecture of mobility.

* In novel architecture is proposed which is based on the use of proactive caching in order to increase the efficiency of mobile communications in a varied wireless environment.

- Management schemes for Mobility
  * Network mobility has been enhanced by relaxing certain overheads of network Mobility Management protocol with IPv6 using OptiNets.
  * A Make-Before-Break hand-off scheme with two network interfaces is proposed for NEMO.
  * In this thesis, a mobility management is proposed by localized forwarding scheme which combines Make-Before-Break handoffs with loss recovery [6] using buffering and selective delivery of lost packets from a buffer after completion of the handoff. The basic idea of the localized mobility management protocol for Make-Before-Break handoffs is combined with a novel handoff timing algorithm for vertical handoffs based on application or transport protocol context.
- designing of Protocol
  * This thesis proposes a new LMM protocol for handling Make-Before-Break handoff capable Mobile Nodes.
  * This thesis proposes a protocol extension to NEMO and Mobile IPv6 for supporting Make-Before-Break handoffs in Mobile IPv6.

* Protocol overhead is avoided by proposing an improved version of the OptiNets protocol.

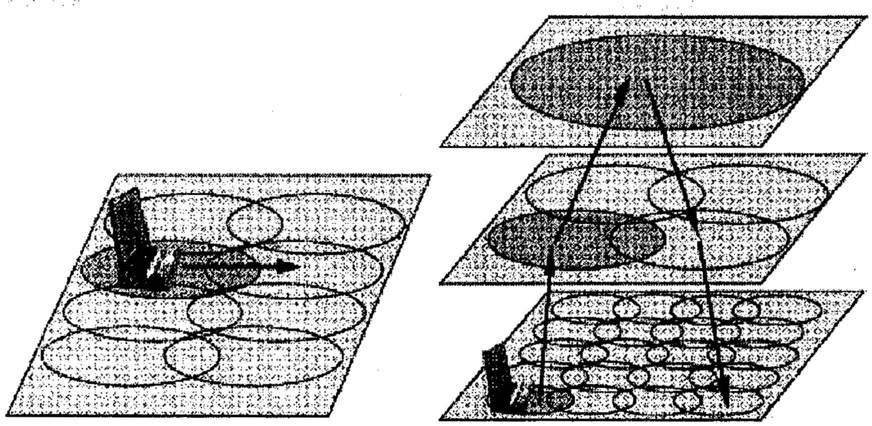
- Test bed

  * Design and building of a configurable test bed uses Linux plate form with NS2 for implementation my purposed architecture.

Chapter 2

Background and Motivation

It is worth noting that the personalized communication and information technology is progressively growing during the recent years. Today, a user has the ability to choose among different available ways of communication as compared to a few years ago. Instead of using one telephone connected to only one provider, one has the option to choose between several providers and services. In case of several available network links, a selection has to be made in such a way that the desired Quality of Service (QoS) is met. In highly dynamic wireless and mobile environments, involving varying numbers of users and volatile transmission conditions, the characteristics of streams of data packets change all the time which imposes the need of end-to-end monitoring. The amount of simultaneous users who could be connected to the same Access Point (AP) also has some major impact on the overall performance. Moreover, the problem with interference in the 2.4GHz Industrial Scientific and Medical (ISM)-band, shared amongst Wireless Local Area Network (WLAN), ZigBee, Bluetooth and microwave ovens, needs to be addressed. Today, several other technologies are competing in transferring information in the same frequency band causing interference.



Horizontal Handoff Vertical Handoff

Figure 2 Horizontal Vs Vertical Handoff.

Figure 2 shows a situation in which different wireless networks coexist. Lower levels are comprised of high bandwidth wireless cells that cover a relatively small area. Higher levels in the hierarchy comprise a lower bandwidth but over a larger geographic area.

2.1 Horizontal Handoff

A horizontal handoff can be defined as a handover between base stations that are using the same wireless technology. This is the traditional definition of handoff for homogeneous cellular systems such as cellular telephone systems. This type of handoff can also occur between wireless local area networks.

2.2 Vertical Handoff

A vertical handoff can be defined as handover between base stations that are using different wireless technologies. The terms horizontal and vertical are derived from the network structure that is followed during handoff. Networks with increasing cell sizes are placed at higher levels in the hierarchy. During horizontal handoff the handover is at the same level and in vertical handoff its direction is either upside or downwards. This can be easily understood from the figure 2.

The vertical handoff can also be sub classified as upward vertical handoff and downward vertical handoff. An upward vertical handoff is a handoff to a wireless network with a larger cell size and a downward vertical handoff is a handoff to a wireless overlay with a smaller cell size. A vertical handoff may occur to an immediately higher or lower level network or the mobile host may skip a network [7]. This sub classification is also useful because the upward and downward vertical handoff have different characteristics with respect to the time required for handoff.

2.3 Horizontal Vs Vertical Handoff

In horizontal handoff systems, a mobile host performs a handoff from cell A to cell B while moving out of the coverage area of cell A into the coverage area of cell B. However, this is not necessarily the case in vertical handoff. A user can perform a downward vertical handoff from cell B to cell A. It means that the user is not moving out of the coverage of cell B. This implies that downward vertical handoffs are less time-critical because a mobile can always stay connected to an upper overlay while handing off to a lower overlay.

Many network interfaces have an inherent diversity that arises because they operate at different frequencies. For example, a room-size overlay may use infrared frequencies, a building-size overlay network may use one set of radio frequencies, and a wide-area data system may use another set of radio frequencies. Another way in which diversity exists is in the spread spectrum techniques of different devices. Some devices use Direct Sequence Spread Spectrum (DSSS), while others use Frequency Hopping Spread Spectrum (FHSS).

In a network of homogeneous base stations, the choice of "best" base station is usually obvious: the mobile chooses the base station with the highest signal strength after incorporating some threshold and hysterics. In a multiple-overlay network, the choice of the "best" network cannot usually be determined by channel-specific factors such as signal strength because different overlay levels may have widely varying characteristics. For example, an in-building RF network with low signal strength may yield better performance than a wide-area data network with high signal strength. There are also considerations of monetary cost (some networks charge per minute or byte) that do not arise in a homogeneous handoff system". So vertical handoff is very different from the horizontal handoff and also the requirements of upward and downward vertical handoff are different from each other.

2.4 Stream Control Transmission Protocol (SCTP)

SCTP is a reliable transport protocol operating on top of a potentially unreliable connectionless packet service such as IP. It offers acknowledged error-free non duplicated transfer of datagram. Originally, SCTP was designed as a specialized transport protocol for call control signaling in voice over IP (VOIP) networks and has been specified by the 3rd Generation Partnership Project (3GPP) to carry call signaling traffic in UMTS. It has been designed by the IETF SIGTRAN working group, which has released the SCTP standard draft document (RFC2960) in October 2000.

The decisive difference between SCTP and TCP is multi-homing and the concept of several streams within a connection. SCTP supports multiple, independent logical streams of messages within an SCTP association. Each message sent over an SCTP association is assigned to a particular stream. Other core features of SCTP is multi-homing which means that a node can have multiple IP addresses each of which can be used for communication with that node. Normally in SCTP we use two configurations which are single-homing and dual-homing. In single-homing node has only one IP address and in dual-homing node has two IP address for communication. One or both the nodes can be in single or dual homing configuration as shown in the figure 3. If both sides have dual homing configuration then there are four independent paths for communication. One of the paths is the primary path and the remaining paths are called secondary paths. We can change our primary path during the communication. This feature was provided to support fault tolerance which can be achieved by configuring the IP address from physically different networks. But this feature of multi-homing can be used to support mobility both in horizontal and vertical handoff.

In the base version of SCTP all the IP addresses at the end points had to be exchanged in the start of the communication. We can say that in base version we could not add IP addresses dynamically which is required to support mobility. When a host is mobile it does not know or have all the IP addresses in advance. So in order to support mobility an extension was required in the base version of SCTP for dynamically adding or deleting the IP addresses. This extension was named Dynamic Address Reconfiguration (DAR) [8].

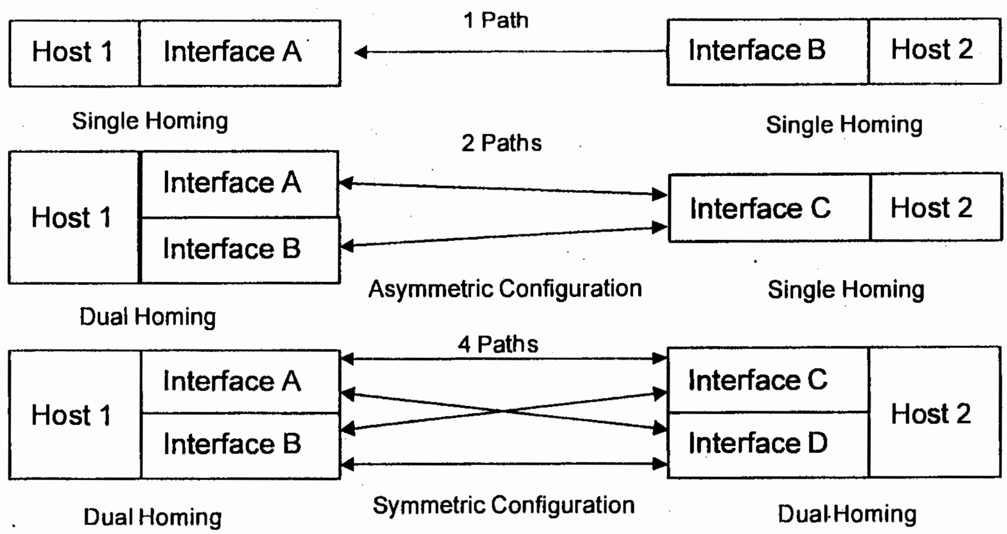


Figure 3 Different Configurations in M-SCTP

2.5 Problem Definition

Problem is to support seamless connectivity of the user as it moves from one technology to another technology due to the limited range or for better bandwidth to which the user wants to switch. Seamless means that the delay and the packet loss during the handoff should be as low as possible. This problem can be decomposed into two sub problems. First problem is to identify when to switch from one technology to another. There can be a number of factors which can be used to identify when to switch to another technology e.g. received signal strength of the current network and the other network to which user wants to switch. But a vertical handover to/from a different wireless network causes a change in the connection parameters as perceived by the mobile user (e.g., in terms of throughput and end-to-end RTT). On long term, several continuous vertical handoffs among heterogeneous networks, and therefore frequent fluctuations of the connection parameters, affect the performances of the application sessions running on the mobile user's device. This effect is called ping pong effect which refers to frequent unnecessary vertical handoffs when a number of wireless networks exist and the user is continuously switched between these networks. We require efficient algorithms to solve this problem because of the ping pong effect.

After the necessary decision of switching to other technology has been made, then come to the problem of moving from one network to other network while maintaining connectivity. The protocol or steps required to move from one network to another network are estimated. During the vertical handoff there should be minimum number of packet loss and minimum amount of delay [9]. Also the message exchanges should be as low as possible because with each message there comes number of delays e.g. propagation delays, queuing delay.

The impact of handoff is further increased by the conservative resending mechanism which is designed for congestion avoidance instead of dealing with packet loss from wireless errors or a handoff in case of TCP. Furthermore, in a NEMO mobile network setting, the devices in the mobile network would not be aware of the mobility of the Mobile Router and could not determine that the impact on their connections was a result of mobility instead of congestion. This significant disruption of traffic has made it unfeasible to take full advantage of all available networks, since the large impact of a handoff between different IP networks combined with the cost of signaling could mitigate any gains achieved from switching to a faster network for a potentially short time. The use of higher cost wireless technologies has slowed the deployment of on board mobile networks and limited their applications. The ability of a Mobile Router to perform seamless handoffs, i.e. handoffs which do not have a noticeable negative impact on application performance, in a heterogeneous network environment is crucial for enabling more wide-spread use of mobile networks.

In order to seamless switching between the varied networks, mobile router have to minimize the utilization of high cost networks. This can be achieved by correct timing of the vertical handoffs between the different technologies and use of caching. However, it also requires that the protocols used for achieving the seamless mobility do not create unnecessary signaling and data traffic overheads.

In this thesis, architecture for enabling seamless and improved handoffs in varied wireless networks is developed. The architecture consists of a mobility management protocol for supporting seamless Make-Before-Break handoffs with and without support from the access network, caching and optimized routing mechanisms for increasing the efficiency of communications of Mobile Network Nodes and security architecture to secure the operation and configuration of the protocol in the architecture. The focal points of this thesis are improvement in protocol and architectural for reducing the impact of the handoffs of MR in a varied wireless network environment on communications between mobile network nodes and fixed network counter parties. Furthermore, the thesis aims to limited the usage of high cost networks to increase the scope of applicability of the proposed solutions.

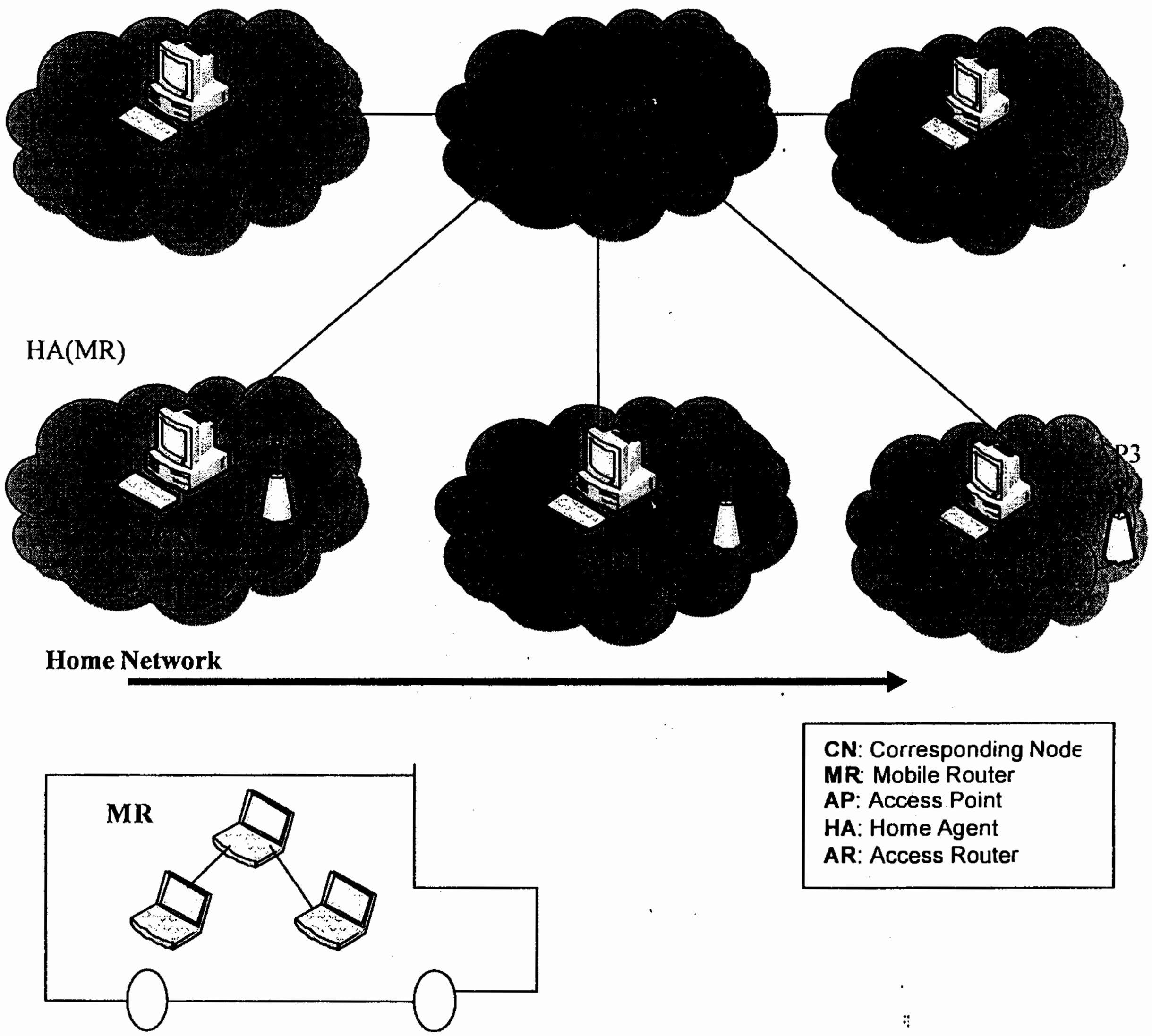


Figure 4 Logical Network Topology.

2.6 Solution Criteria

A lot of solutions have been proposed to support seamless mobility within different technologies but most of the solutions have taken three approaches. Categorization of these approaches can be made depending on the layer which has been selected to solve this problem of mobility. These layers are Network Layer, Transport Layer and Application Layer.

The purposed architecture will be evaluated according to the following criteria.

- The purpose solutions should reduce interruptions from the mobility of the Mobile Router or the Mobile Nodes to the communications between the Correspondent Nodes and the Mobile Nodes.
- The purpose solutions should utilize available unused capacity of networks.
- The purpose solutions should have negligible performance impact on communications and should optimize usage of wireless resources.
- The given architecture should not introduce new vulnerabilities.
- The purposed solutions should require changes to a minimal number of entities in the network.

Chapter 3

Handovers

In this chapter, we will discuss different solutions of the handover problem stated at the end of the previous chapter. These solution will be explained according to the layer they have been used.

3.1 Network Layer Solutions

3.1.1 Mobile IP

If user of a PC equipped with a wireless network interface is running some application while he roams the countryside. The PC might detach itself from one network and attach to another with some frequency, but the user would want to be oblivious to this. In particular, the applications that were running when the PC was attached to network A should continue to run without interruption when it attaches to network B. If the PC simply changes its IP address in the middle of running the application, the application cannot simply keep working, [10] because the remote end has no way of knowing that it must now send the packets to a new IP address. Ideally, we want the movement of the PC to be transparent to the remote application. The procedures that are designed to address this problem are usually referred to as "Mobile IP".

3.1.2 Routing for Mobile Hosts

In Mobile IP was proposed to support mobility by providing an indirection in the routing architecture. In this approach we need to add some new functionality in one of the router which is known as *home agent.* This router exists in the home network of the mobile node. In this approach home agent has a permanent IP address in his home network. This IP is called *home address.* This IP address has to be permanent because this IP address will be used by other nodes for communicating with the mobile node.

In order to have additional functionalities in MIP we also need to have a special router which is called *foreign agent* in the foreign network where the mobile node wants to have mobility. Both the agents foreign and the one at home have to announce their presence on their respective network by periodically sending advertisement messages [11]. By these messages a mobile node may know which router at its home network is working as home agent. When mobile node leaves his network he has to save the address of its home agent.

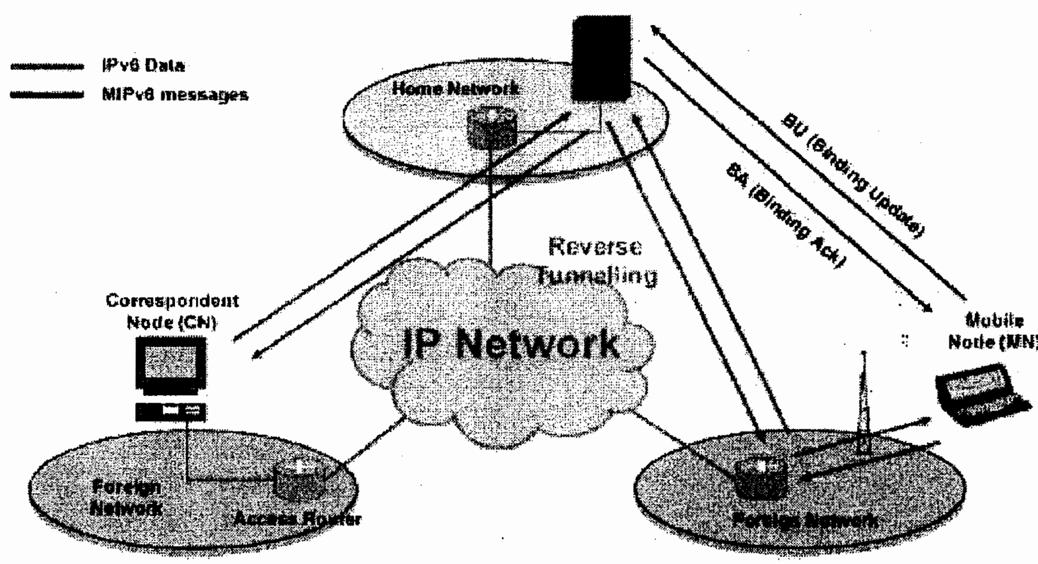


Figure 5 Link Established between CN and MN using Binding Updates

The mobile node can move to a foreign network as he listens for the advertisement message which announces the presence of a foreign agent in the foreign network. If a foreign agent is present then the mobile node registers with this foreign agent by providing him the address of his home agent. Foreign agent then contacts with the home agent of the mobile node and provides him with his own IP address. Home agent then adds the IP of the foreign agent in the *care-of address* for the mobile node. Any packet which is destined for mobile node is intercepted by the home agent. Home agent then wraps this packet inside an IP header and sends this packet to the foreign agent. Foreign agent removes this extra IP header and sends the packet to the registered mobile node. We can say that an IP tunnel is established between the home agent and the foreign agent. Home agent simply intercepts the packets destined for mobile node and drops those packets in the tunnel. Foreign agent gets the packets form the tunnel and sends it to mobile node.

In the absence of foreign agents in the foreign network then the mobile node himself has to work like foreign agent. In this situation, mobile node will send his new IP address in the foreign network to its home agent [12]. This new IP address will then work as a *care-of address* for the mobile node. Now a tunnel will be established between home agent and mobile node. One significant draw back in the above approach was that the packet from the other node does not take a small route to the mobile node. It always first reaches home agent then it goes to the foreign agent. It may be the case that other node and mobile node are close to each other. This problem is referred to as "triangle routing problem" because a triangle is formed between other node, home node and mobile node. Our goal should be to send the packets to mobile node as directly as possible.

This problem was solved by sending the care of address of the mobile node to the sending node. By using this care of address sending node and mobile node can form a tunnel between themselves. When the sending node is not using the optimal route then home agent sends the *binding update* message to the source. Source then uses *binding cache [13]* to send the packets to the mobile node. Binding cache contains the care of address of the mobile node. This cache is deleted after a certain time because this cache could be out of date as mobile node can move to any other network with out informing the sender.

3.1.3 Cellular IP

In Cellular IP , no node knows the exact location of a mobile node in the foreign network. Packets addressed to mobile node are sent to the gateway in the foreign network. Gateway then sends the packets to appropriate base station of the mobile node by the routing information. Routing information is obtained by each base station by monitoring the sender address and incoming port on which the packet is received. Routing information is referred to as mappings in cellular IP. These mappings are cleared after a certain amount of time. So in order to maintain path of a mobile host it must periodically transmit dummy packets even when it has no data to send. When the mobile host moves to a new base station then it is possible that it may have two mappings for some interval of time. Within this time interval if any packet is destined for the mobile node then it will be send on both the base stations.

PCs are only used to search for mobile host while RCs are used to route packets. Network operator has to place PCs in a small number in well positioned nodes and other nodes can broadcast search messages to find the mobile host. Short control packets called paging-update packets are send periodically by an idle mobile host. These packets are destined for the gateway and on their way; nodes having PC update their mappings. When a packet arrives at the gateway router destined for the mobile host for which no up to date routing information is available PCs are used to find the host through a control packet called *paging packet.*

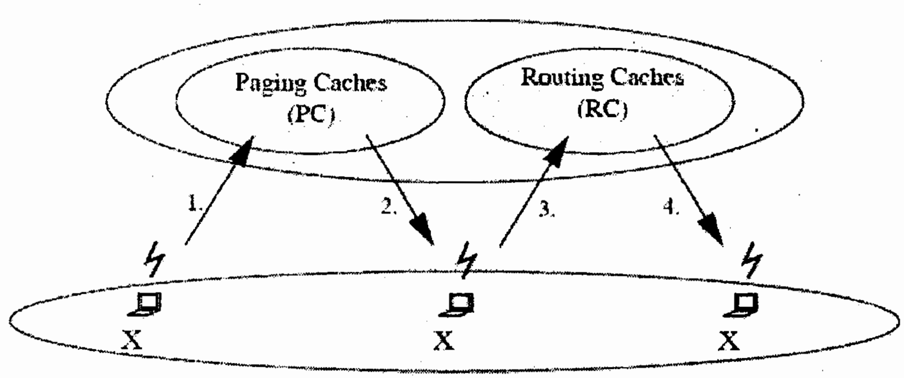


Figure 6 Paging & Routing Caches in CIP

In Cellular IP, [14] the binding update problem of MIP was partially solved by not updating the care-of-addresses at Home Agent every time host moves to a new address. In this approach a gateway router is used to send packets to the host in the foreign network and when the host moves within the network it only causes the gateway router to change the base station where the packets are to be sent. Although this optimization procedure smoothes the handoff, but it works only within the same network because the mobile host moves from one network to another same Mobile IP is used.

3.1.4 Wireless Overlay Networks

In hierarchical structure of networks the mobility between these networks is proposed using same Mobile IP concept. In this concept, the handoff latency is dominated by the discovery time which is the amount of time before a mobile discovers that it has moved into or out of a new wireless network. Mobile Hosts (MHs) and Base Stations (BSs) are connected to a wired infrastructure. BSs act as Foreign Agents (FAs). The basic structure is similar to the MIP. The only difference in their scheme is that instead of unicast address a multicast address is used as a care-of address. This multicast address is composed of a number of BSs. BSs are selected by the mobile host. As HA sends packet to a multicast address therefore all the BSs in the group receive the packet. But only one BS sends the packet to the mobile host. This BS is called forwarding BS and is selected by the mobile host. However, the remaining BSs in the group are called *buffering BSs*, as they are buffering data for mobile host in a circular buffer. This type of system can be seen in figure 7.

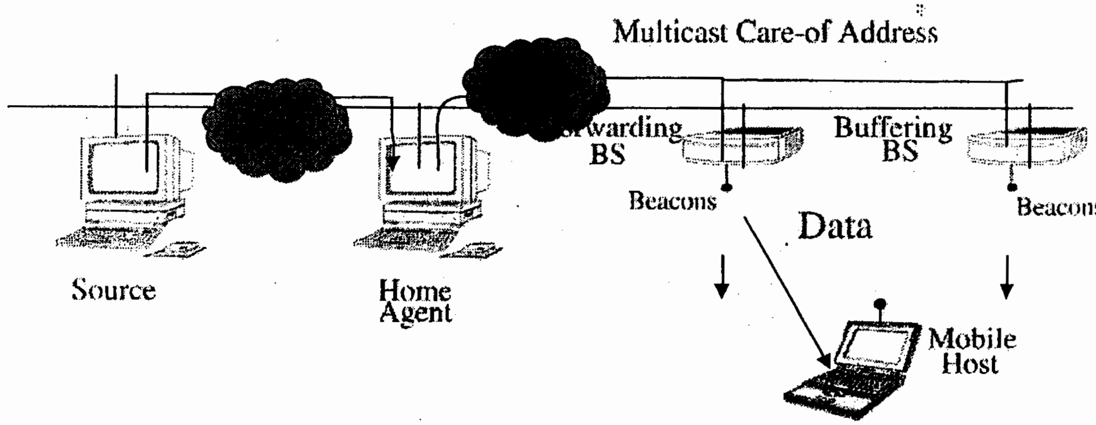


Figure 7 Handoff Systems in Overlay Networks.

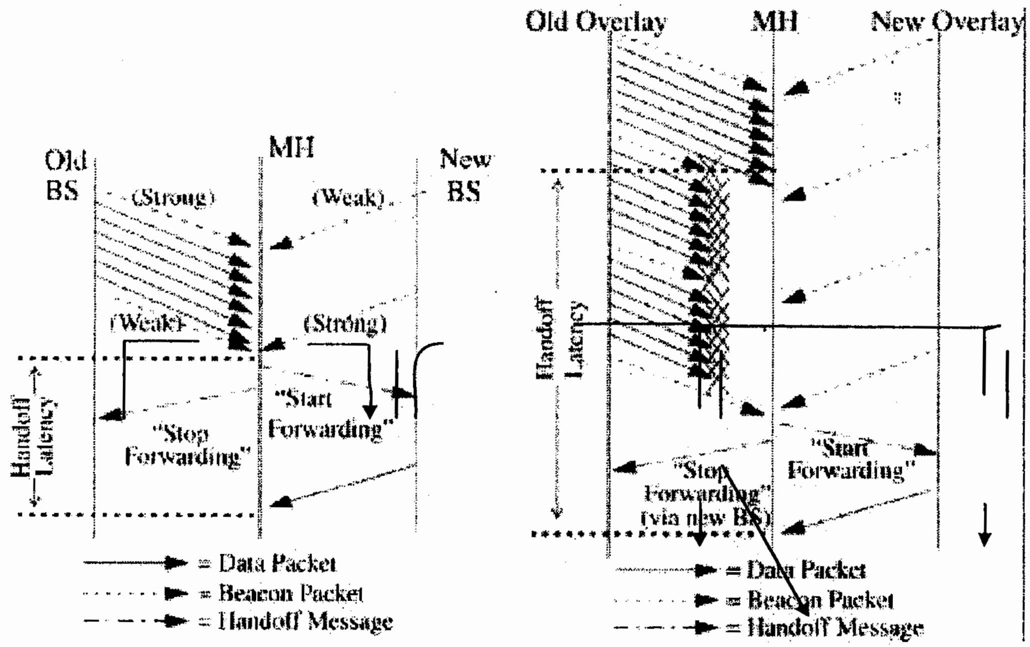


Figure 8 Breakdown of Horizontal and Vertical Handoff.

3.1.5 HOPOVER

HOPOVER (Handoff Protocol for Overlay Networks) [15] performs handoff in three stages, pre-resource reservation, buffering and forwarding. When the mobile host detects that it may need a handover in the near future then it sends a *Handoff-Prepare (HP)* packet to a small group of BSs after selecting them on the basis of signal strength, bandwidth, pricing and other factors. Each BS then sends this HP packet to its authentication server. If the mobile host is authenticated then the resources are reserved in the target cells and along the path from mobile host's current sender to the target cells. Each of the target BSs allocates a small buffer for the mobile host and sends a HP_ACK packet to the current BS. Current BS then starts forwarding packets to the target BSs.

3.1.6 WiFi Bridge

In a combination of CIP and IP Tunneling is used to achieve horizontal and vertical handoff between GPRS and WLAN called WiFi Bridge. WiFi Bridge is based on the establishment of two IP tunnels. One tunnel exists between home gateway and mobile host on the GPRS Link. Other tunnel exists when the mobile host moves to a foreign WLAN. This tunnel is formed between the home gateway and foreign gateway. When the MH receives the dynamic IP in the GPRS domain then it sends this IP to its Home WLAN Gateway (GW). Home GW maintains a cache for each mobile host called *tunneling cache* which contains the mapping between static and dynamic IP addresses of the MH. Then an IP tunnel is established between Home WLAN GW and the MH on the provided dynamic IP address. This tunnel is called GPRS tunnel and is permanently kept alive. This tunnel is used when WLAN is not available.

When the MH is in foreign WLAN then an IP tunnel is created between the GWs at its home domain and foreign domain similar to GPRS Tunnel. Packets destined for the MH first reach home GW and then through the tunnel created reach foreign gateway. When the packets reach foreign gateway they are send to the MH using Cellular IP. Within a home and foreign domain CIP is used to manage horizontal handoffs.

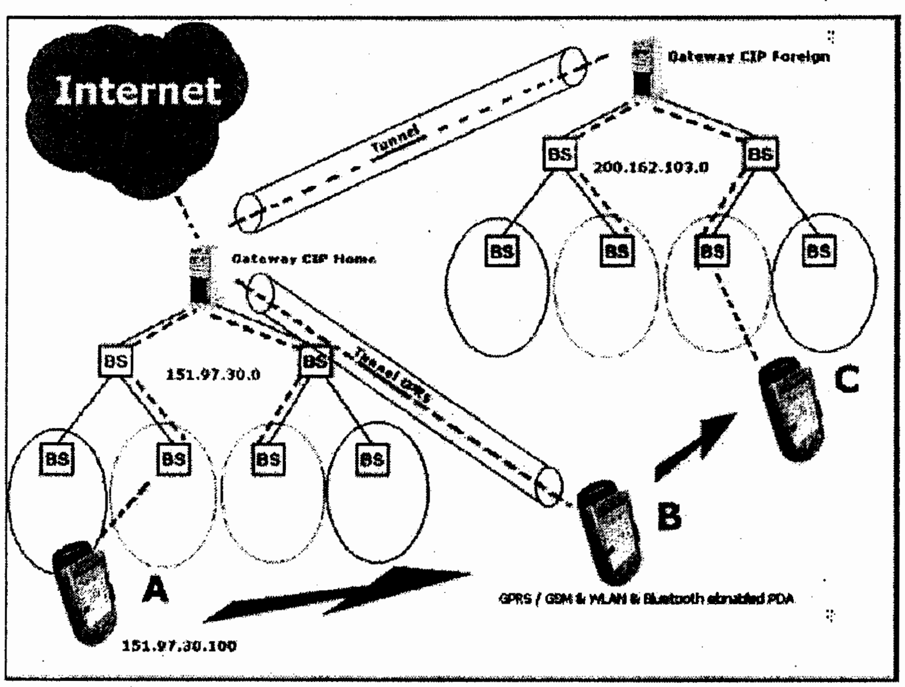


Figure 9: Working of WiFi Bridge

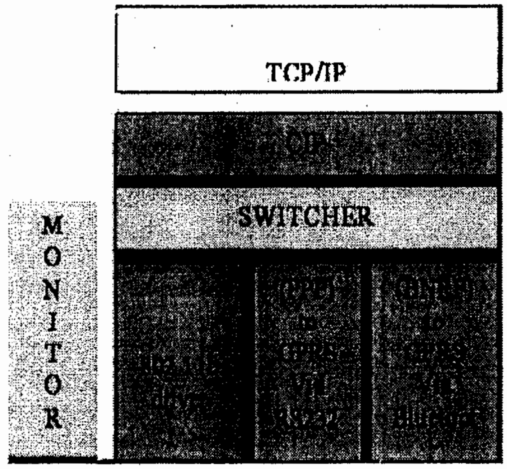


Figure 10 ProtocolStack for WiFi Bridge

This solution has the same problem as with MIP. Data always has to come first at the home domain and then pass through a tunnel to foreign gateway and then to MH. Let us suppose that MH is connected to one foreign domain and during an active communication between MH and some other node MH moves into another foreign domain then first we will have to create a new IP tunnel between the home and new foreign gateway before the two nodes can communicate with each other. So, this might not provide seamless continuity in this case. They have only considered a scenario in which GPRS is involved between the home and foreign WLAN domains. In same WiFi Bridge [16] is used for the vertical handoff procedure. They have changed the procedure for the detection of vertical handoff.

3.1.7 TAKEOVER

A new vertical handoff concept is given in which neighboring node (NN) takes over the mobile node's handover operations and is named as Takeover. In this concept, mobile node first sends Ready-to-Takeover message to discover a NN to perform handover operations. When a NN is ready it sends Clear-to-Takeover message with its address. After finding the NN there are other five steps that complete the Takeover process of vertical handover.

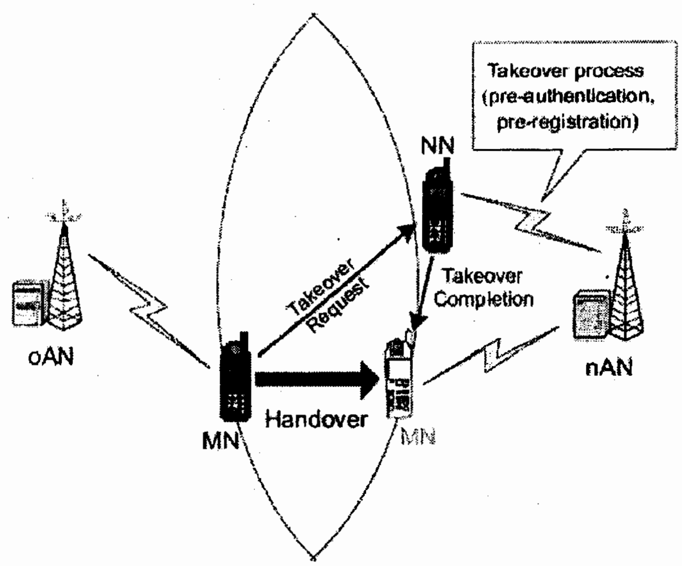


Figure 11 Takeover Process

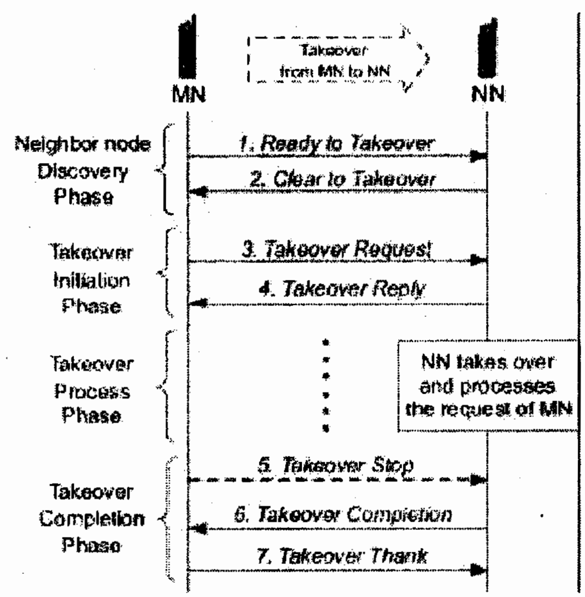


Figure 12 Basic operations of Takeover

When "the MN confirms its NN by this message, it starts takeover initiation procedure with the NN through exchange of Takeover Request and Takeover Reply messages. The Takeover Request message includes specific contents of the request and information needed according to a kind of request (e.g profile). At this time, the NN can process the takeover request instead of the MN. If the MN wants to interrupt the takeover operation, it can send Takeover Stop message to the NN. When the NN finishes the takeover operation, it delivers to the MN Takeover Completion message together with the final information created as a result of successful takeover execution. Finally, the MN transmits Takeover Tha nk message to the NN".

In this concept the whole handover procedure is completely dependent on the neighboring node. There are many questions relating to this concept.

- What will happen if there is no NN?
- If there is a NN, is he willing to participate in TAKEOVER?
- How can we make every NN understand the whole protocol of TAKEOVER?
- How can we authenticate a NN whether he is really connected to required network?
- How can we completely trust a NN and supply him security key and other information?

This concept has seven different message exchanges before the handover can occur and is using a mediator which will bring delays in the handover procedure.

3.1.8 Universal Seamless Handoff Architecture

USHA consist of a handoff server (HS) to which several mobile hosts (MHs) are connected. USHA is implemented using IP tunneling technique. At one end of the tunnel is HS and at the other end MH. *"An IP tunnel is maintained between every MH and the HS such that all application layer communications are "bound" to the tunnel interface instead of any actual physical interfaces. All data packets communicated through this IP tunnel are encapsulated and transmitted using the connectionless UDP protocol."*

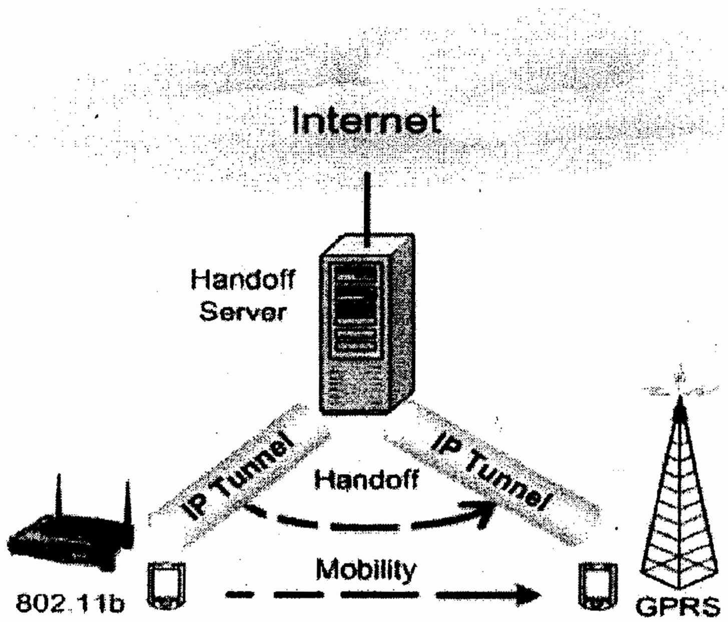


Figure 13 USHA Architecture

"The IP tunnel above utilizes two pairs of virtual/fixed IP addresses, one on HS and one on MH. The fixed IP addresses are necessary for an MH to establish a physical connection to the HS. When the handoff event occurs and the physical connection from MH to HS changes, the MH is responsible for automatically switching the underlying physical connection of the virtual tunnel to the new interface, as well as notifying the HS of its change in physical connection. Upon handoff notification, the HS immediately updates its IP tunnel settings so that any subsequent data packets will be delivered to MH's new physical link.

Since all data packets are encapsulated and transmitted using UDP, there is no need to reset the tunnel after the handoff. Therefore, end-to-end application sessions (e.g. TCP) that are bound to the IP tunnel are kept intact. This provides handoff transparency to upper layer applications."

This architecture uses the same indirection approach in the network layer using IP tunneling. It forces to uses UDP protocol which may not be suitable for some applications as they may require error free delivery.

3.2 Transport Layer Solutions

3.2.1 Migrate TCP

An extension was made to TCP in and was named as Migrate TCP (MTCP) to support host mobility. This option added the ability to move from one IP address to another IP address during an active TCP connection. One can use secure or insecure option in the migration. Mobility support was provided by using M-TCP and Domain Name System (DNS) update protocol. When the MH moves from one IP address to another then change in the IP was reflected using dynamic updates to DNS to track host location.

In this architecture, three components: addressing, mobile host location and connection migration have been used The first component of obtaining an IP address in a foreign domain can be achieved by manual assignment or using DHCP protocol [17]. So in a foreign network mobile host uses a locally obtained address which is valid in foreign domain. The second component deals with locating the Mobile Host. When mobile host changes its attachment point, it must detect this and change the hostname-to-address mapping in the DNS by using DNS update protocol. DNS uses a cache for name mappings. As a MH can regularly change his name mapping we could have a wrong entry in the DNS cache. In order to avoid this, it was suggested that DNS should not cache entry for the MH.

The third part deals with the migration of TCP connection. In original TCP we cannot move an active connection to another IP address. They have added a new Migrate TCP option in the SYN segment to support migration in TCP. In MTCP SYN packet is considered a part of previously established connection rather than a request for a new connection. The figure 14 shows an example of migrating TCP connection. MH starts the communication by sending a SYN packet to the server including the Migrate-Permitted option and some token information which is used for security purpose. Fixed servers then accept migrate permitted option by sending a response message. MH then sends an ACK packet to complete the three way handshake process.

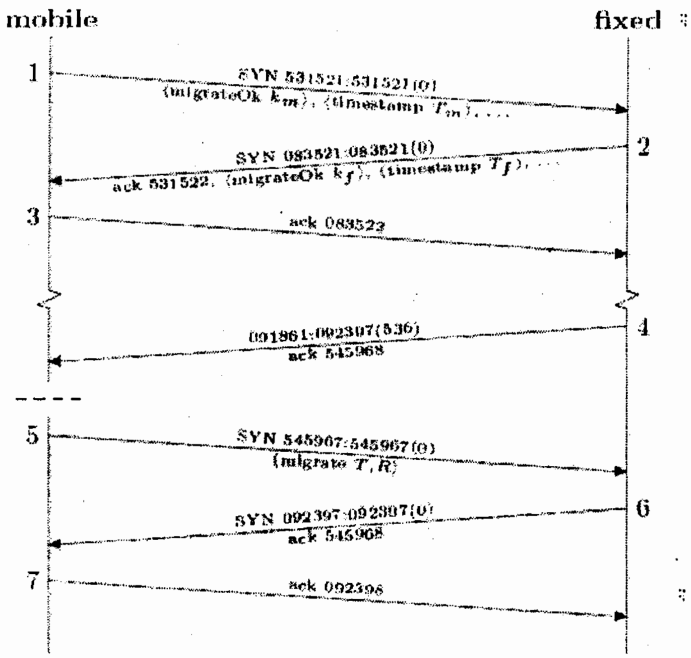


Figure 14 Steps of Migrate TCP

Message 4 is the last packet received by MH from fixed server at the old IP address of MH, as shown in the figure 14. After some time MH moves to a new address and wants to resume his old connection. He sends the SYN packet along with previously computed token as indicated in message 5. After validating the token fixed server sends the response of SYN packet. MH then sends an ACK packet to complete the handshake process. After that fixed server starts sending the data from where the connection was broken.

3.2.2 VHOST

Vertical Hand-Off through Seamless TCP-Migration (VHOST) was proposed in [18]. They have proposed a handoff-aware TCP adaptation scheme to adapt TCP protocols to cope with different network characteristics. VHOST has three basic modules: Migration monitor, Resumption module and Handoff-aware TCP core, as shown in the figure 15.

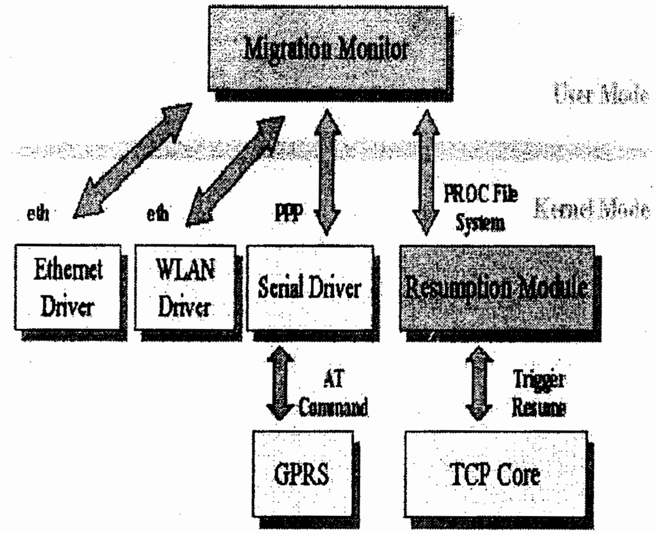


Figure 15 VHOST Architecture

Migration Monitor as the name suggests monitors the status of all network interfaces and if a vertical handoff is going on then activates the connection migration procedure to migrate all TCP connection form old network to the new one.

Resumption module *"provides interface to migration monitor for obtaining information about suspensible TCP connections and for triggering connection migration. After receiving the migration requests from migration monitor, resumption module asks the handoff-aware TCP core to perform the connection migration".*

The handoff-aware TCP core performs two tasks: one is to migrate the current connection from a network interface to another one using M-TCP. The other is to agilely adapt the migrated TCP connection according to the new network characteristics. The same M-TCP proposed in to perform the handoffs and changed the BSD socket interface of TCP core to customize it according to the wireless environment. The main shortcoming of using this TCP extension have been mentioned above and also it does not exploit concurrently available access points for performance enhancement.

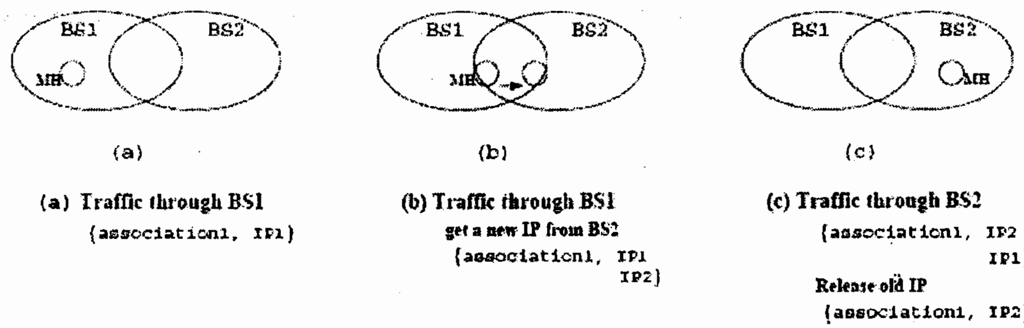


Figure 16 Mobile SCTP Mechanism

3.2.3 M-SCTP for End to End Mobility Concept

In [19] Mobile Stream Control Transmission Protocol (M-SCTP) was used to perform horizontal handoffs. In M-SCTP a connection can have a set of IP addresses which can be changed dynamically. Initially MH is in the coverage of BS1 having an IP1. As it detects BS2 it gets new IP2 and adds it in the SCTP Association. Later when the MH is no longer in the range of BS1 it deletes its old IP1.

3.2.4 Use of SCTP for IP Handover Support

The experimental analysis of SCTP handover for the dual-homing and single-homing mobile terminals has also been proposed for IP Handover. Figure 17 shows the sketch of the SCTP handover where the MT is moving from BS A to B.

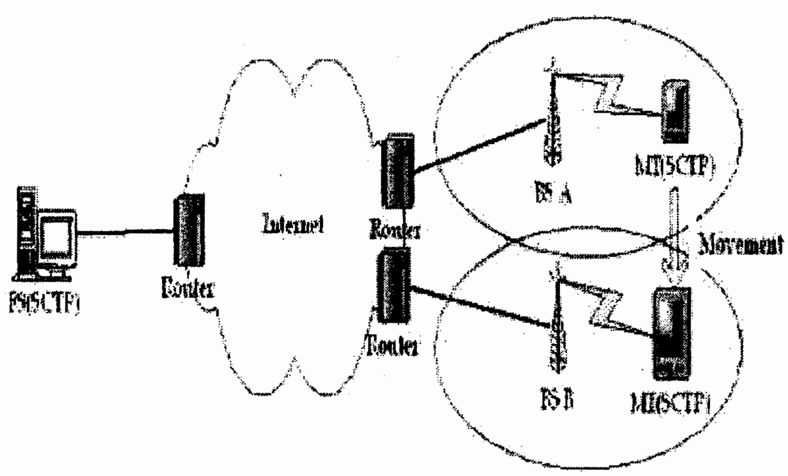


Figure 17 SCTP Handover

3.3. Application Layer Solution

3.3.1 Application Layer Mobility Using SIP

The use of SIP have also been explored for supporting four modes of mobility which are terminal, session, personal and service mobility. The SIP-based mobility is less suitable for TCP-based applications. The terminal mobility for TCP-based applications is difficult if applications are to maintain TCP connections across different networks [20].

3.3.2 SIP -Based Vertical Handoff

Delay associated with vertical handoff using SIP in the WLAN-UMTS inter-network. Analytical results of this show that "WLAN-toUMTS handoff incurs unacceptable delay for supporting real-time multimedia services, and is mainly due to transmission of SIP signaling messages over erroneous and bandwidth- limited wireless links. On the other hand, UMTS-to WLAN handoff experiences much less delay, mainly contributed by the processing delay of signaling messages at the WLAN gateways and servers [21].

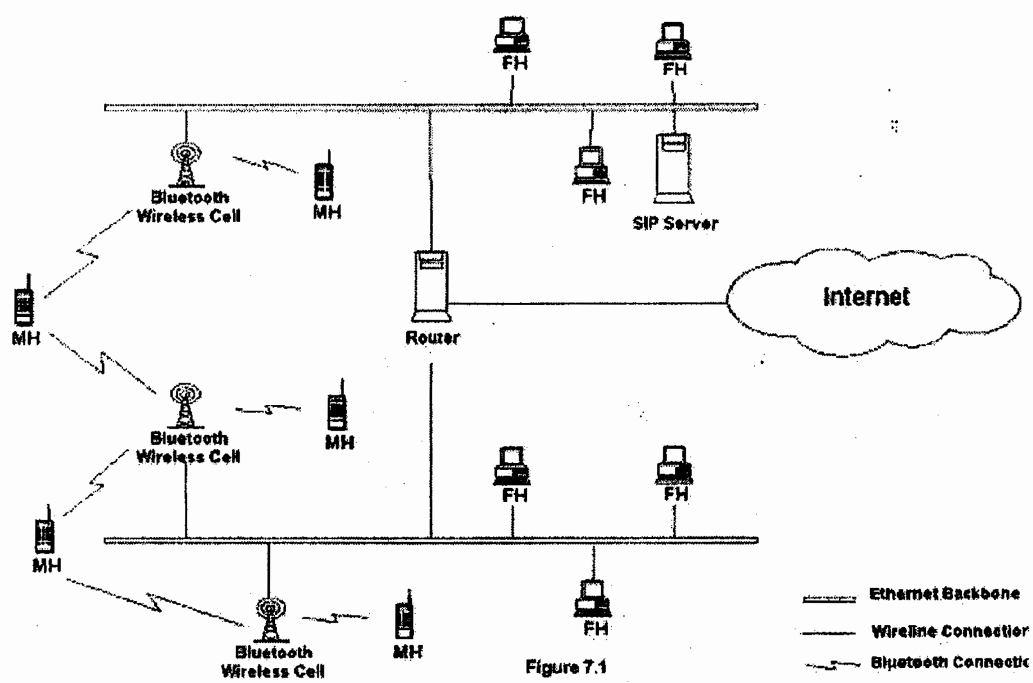


Figure 18 Mobility Architecture using SIP Server

3.3.3 HIP -Based Vertical Handoff

Host Identity protocol (HIP), and SHIM layer for IPv6 (SHIM6) are alternative approaches to Mobile IP. Mobile IP and IP in general use an IP address as both an identifier and as a locator; HIP defines a new identifier, which is derived cryptographically from the identity of the host. In HIP, the Mobile Node and the Correspondent Node communicate directly and reach ability of the Mobile Node is achieved using a redirection agent, [22] the rendezvous server, which informs the Correspondent Node of the current location of the Mobile Node.

3.5 Scope

In this thesis, I am restricted only to the second part of the vertical handoff which is related to the protocol or steps required to move from one technology to another. I will not be identifying when to switch from one technology to another. I will assume that there exist some efficient algorithms which will give us just the right time to execute our steps to move from one technology to another. Also when the decision is made for the vertical handoff then there are only two to three candidates to which the user wants to switch.

Another important requirement for the support of vertical handoff is that the two different networks within which the vertical handoff support is provided must be integrated to authenticate the user and for billing infrastructure. There may exist loose coupling and tight coupling. In this thesis we will not be going into the details of how the two networks are integrated and how the authentication of the user is done because these are completely different issues.

Chapter 4

Proposed Handoff in Mobile Network Environment

In order to understand our suggested improvement first we need to understand the scenario for the vertical handoff which is simlar to the scenarios used in [23]. Let us suppose a Mobile Client (MC) is connected to a Fixed Server (FS) through a router R1 having an IP1. After a certain time MC moves to a new location and senses a new router R2. It gets a new IP address IP2 and adds this IP address to SCTP association by sending a message of Add IP address IP2 to FS. FS then sends acknowledgment to MC. When the strength of the signal from R2 is considered strong enough for communication then MC sends a message of Set Primary Address IP2 to FS. When the acknowledgment of this message is received by MC then R2 becomes the primary router for the MC's traffic. Before sending this message MC's traffic was coming through router R1 having an IP1 address. Later when MC is out of the range of R1 then he deletes IP1 from its association by sending Delete IP Address IP1. This scenario is explained in figure 19. The above scenario is possible only when there is overlapping range of R1 and R2. If one router is using a technology like UMTS and other is using some other technology such as WLAN then it becomes a vertical handoff and if both router are using same technology then it is horizontal handoff.

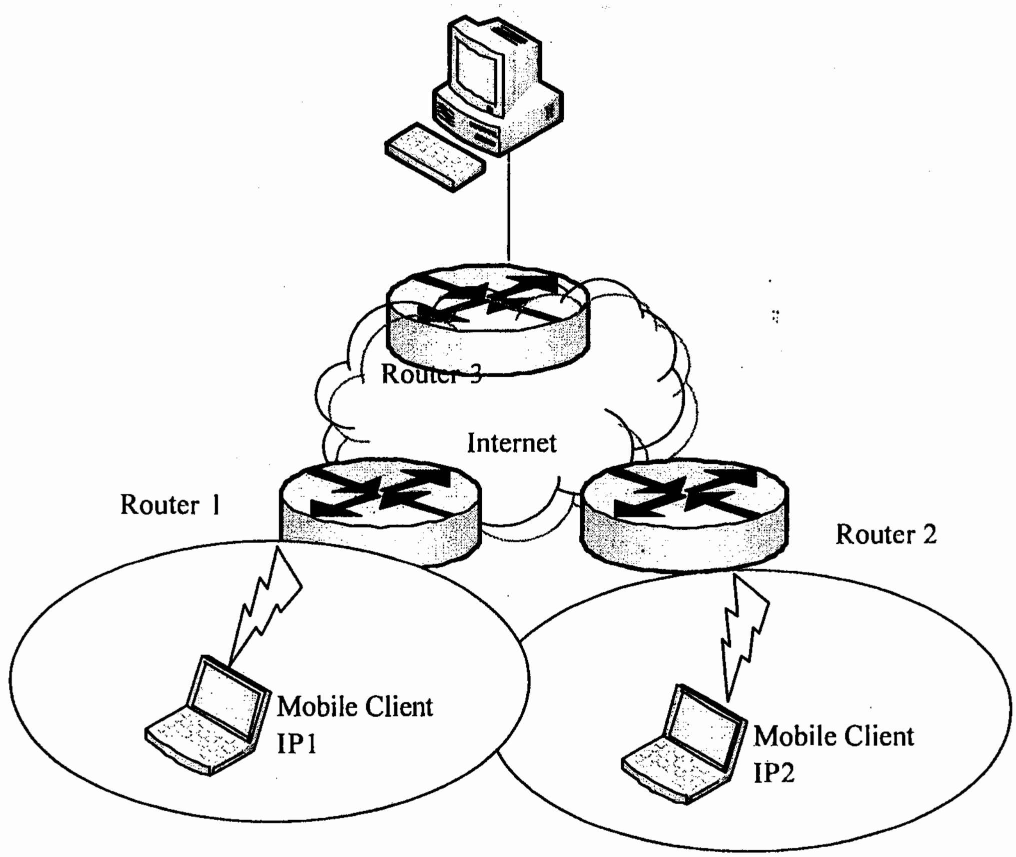


Figure 19 Typical Handover Process in M-SCTP

In two configurations are used for vertical handoff. In both the configurations MC is in dual-homing configuration because in both configurations MC is using two IP addresses. The first configuration is called single-homing in which FS has only one IP address and the second is referred to as dual-homing because FS has two IP addresses.

4.1 Handover Delay in Single-Homing

"When the FS is in single-homing configuration, the handover delay is the time interval in which the FS receives the first packet on the new primary link and last packet on the old primary link. According to the simulation results, the UMTS-to-WLAN handover delay is 533 ms and WLAN-to-UMTS de lay is 513 ms".

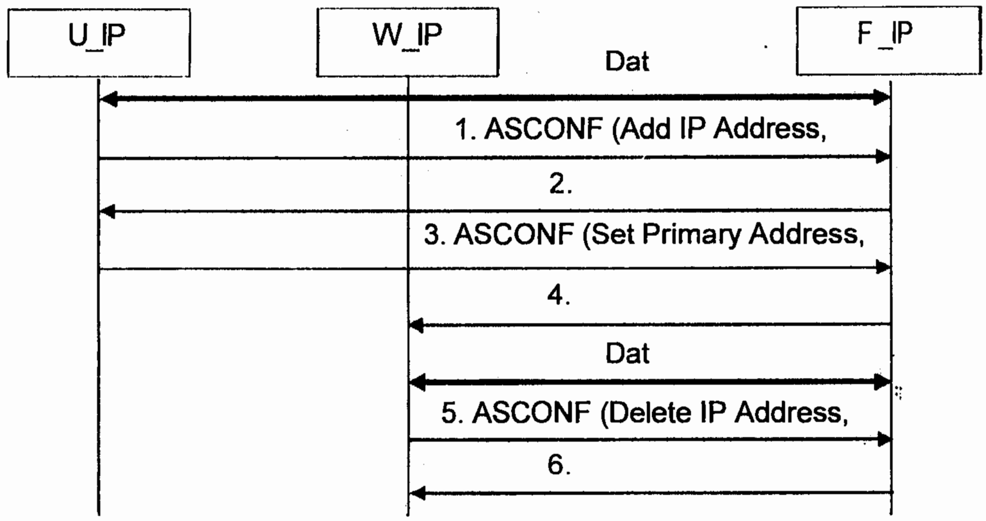


Figure 20 UMTS-to-WLAN Single-Homing

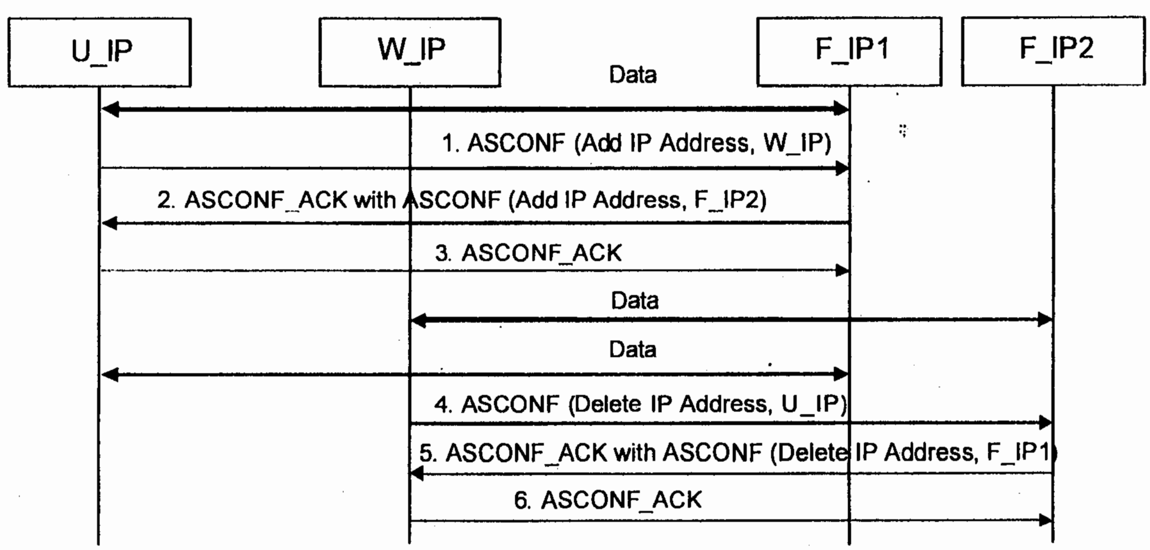


Figure 21 UMTS-to-WLAN Dual-Homing

4.2 Handover Delay in Dual-Homing

"When FS is in dual-homing configuration, the handover delay is the time interval in which the FS receives the same transmission sequence number on both links. These two handover delays are reduced to 234 ms and 212 ms respectively. This is because when the FS is in single-homing configuration, the MC sends a set primary address request to trigger a handover, thus increasing the overall delay with a handshake processing time. However, when the FS is in dual-homing configuration, the MC can trigger a handover by directly setting the FS's secondary address; therefore, the handover delays in both directions are reduced significantly".

By using two IP's for the FS in dual-homing, the handover delay was reduced by 299ms and 301 ms for UMTS-to-WLAN and WLAN-to-UMTS. The main difference for the reduction of the delay was that of handshake process. The propagation delay in the testing environment was set to 1 00ms. So 200ms comprises the propagation delay. The remaining 1 00ms comprise the time to generate the packet at ends, the queuing delays suffered by the packet and time required to acquire the wireless medium for sending the acknowledgment packet. Although in dual-homing configuration has a very small handover delay but this can not be used in real world which is even accepted in.

"Configuring each server with more than one IP address is not an easy task." On the other hand if we observe single-homing configuration it can easily exist in real world. A MC who requires mobility can have two different devices for example of UMTS and WLAN. In the single-homing configuration of FS, after W_IP address has been added as a secondary path between FS and MC, there exist two independent paths between FS and MC. These independent paths are shown in the figure 22:

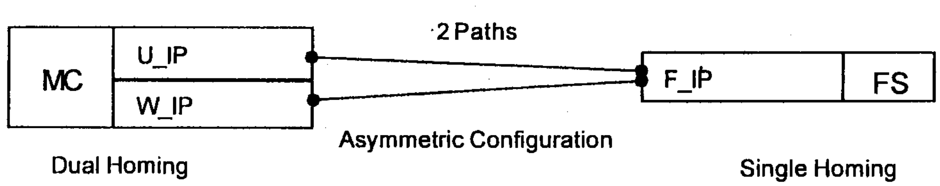


Figure 22 Paths between MC& FS

By using these independent paths and multi-streaming feature of SCTP we can achieve same performance as that of dual-homing in single-homing configuration of FS.

We suggest that when the FS adds the new IP address of MC then it should create two similar streams of data and send them to both primary (old) and secondary (new) IP address of the MC. MC can use one of the streams and discard the other stream. When the MC will start sending ACK packets on the new IP address then FS should set this new IP address as the primary one and the old one should be set as the secondary IP. There is no need to explicitly send *ASCONF (Set Primary Address, IP)* message to the FS. Depending on the ACK Packets received by the FS it will set secondary and primary address in its routing table.

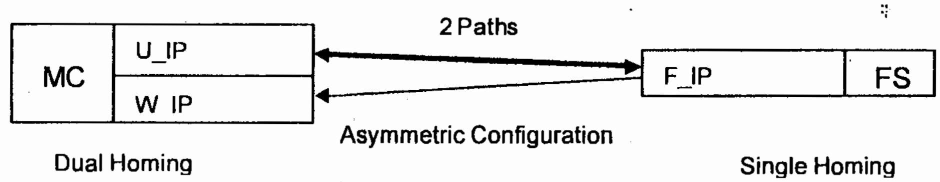


Figure 23: Primary Path is between U_IP -to-F_IP

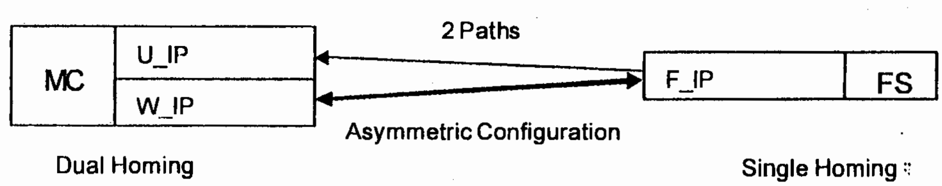


Figure 24 Primary Path is between W_IP -to-F_IP

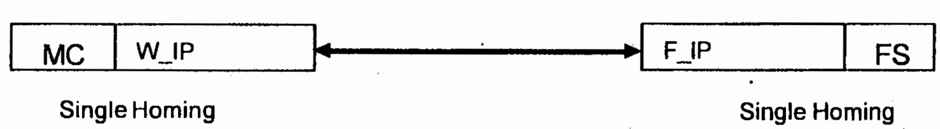


Figure 25 After Deleting U_IP

When the MC senses that there is no longer need of the old IP address, may be due to the signal strength, then it should send *ASCONF (Delete IP Address, IP)* to the FS. After receiving the delete IP message FS will stop sending the stream to that IP and will remove it from its routing table. FS could also monitor the Heartbeat packet response to check the active status of the IP addresses of MC. The figure 26 shows the steps in our proposed scheme from UMTS-to-WLAN. Similar steps are required from WLAN-to-UMTS.

In our suggested approach there are two important considerations. The first one is that in vertical handoff handover is between different technologies; let us say between UMTS and WLAN. Both of them have different network characteristics. Bandwidth of WLAN is much greater than UMTS. If FS sends data stream at the capacity of WLAN then both streams will not reach MC at the same time and will not be synchronized. So in order to synchronize stream FS should send data at the capacity of the smaller network. If data on both streams reaches the MC at the same time then we can say that there will be minimum loss of data while moving to other network.

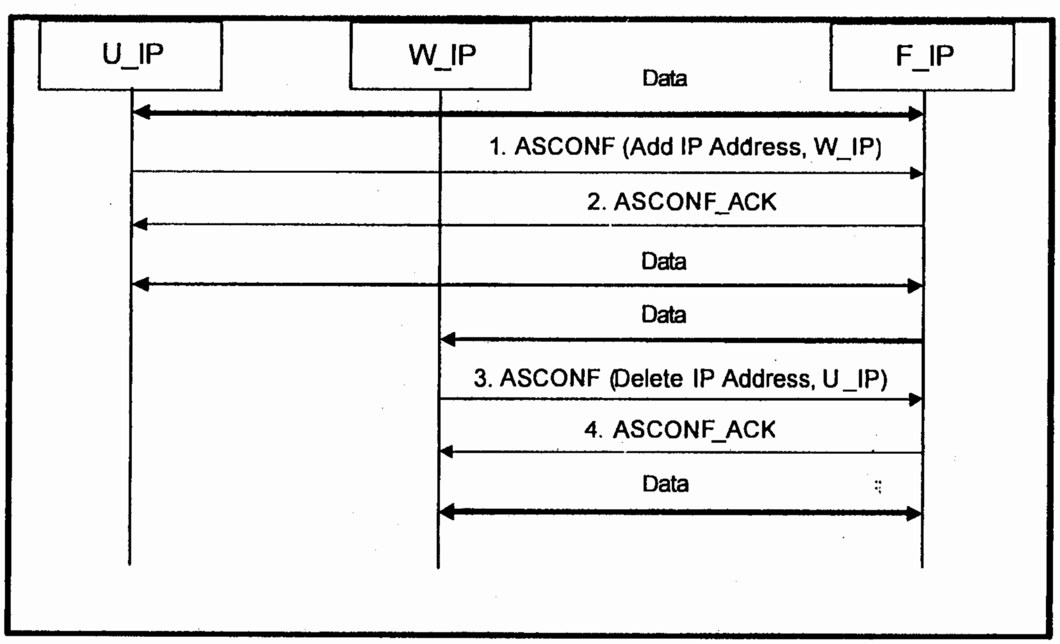


Figure 26 UMTS-to-WLAN Vertical Handover

Other consideration is that we should only add the IP address in our association when there is need of handover other wise the network utilization will be low. This is because FS will be sending data on both the addresses and as explained above data will be sending at the smaller capacity of the two available networks.

4.3 PROPOSED ARCHITECTURE

In this section, the proposed architecture for mobility will be discussed Proposed architecture is also shown in the figure 27 which introduces mobile caching for VMN and Independent handoff for vertical and horizontal handoffs use localized mobility scheme. The proposed scheme is basically independent of infrastructure for Make-Before-Break to reduce the disruption from the mobility. Mobile Router is able to provide seamless connectivity to the MNN [24], such as the WLAN networks.

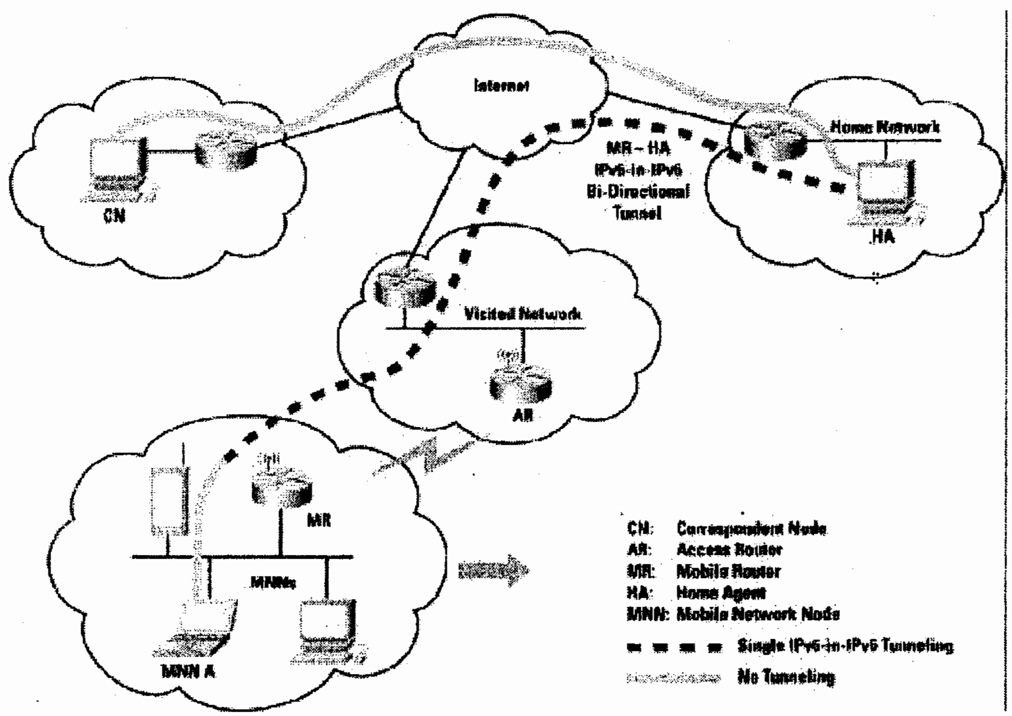


Figure 27 Proposed Architecture

4.4. Safetynet Structural Design

SafetyNet basically lightweight checkpoint/recovery mechanism to support multiple long-latency fault detection schemes. SafetyNet logically maintains multiple, globally consistent checkpoints of the state of a shared memory multiprocessor (i.e., processors, memory, and coherence permissions), and it recovers to a pre-fault checkpoint of the system and re-executes if a fault is detected. SafetyNet efficiently coordinates checkpoints across the system in logical time and uses "logically atomic" coherence transactions to free checkpoints of transient coherence state. *SafetyNet* minimizes performance overhead by pipelining checkpoint validation with subsequent parallel execution. A full-system simulation of 16- way multiprocessor running commercial workloads reveals that *SafetyNet* (a) adds statistically insignificant runtime overhead in the common-case of fault-free execution, and (b) avoids a crash when tolerated faults occur. Mobile Node can finish the handoff without losing data only when if handoff occur before losing connection with the previous Access Router (Make-Before-Break). The Fast Handovers for Mobile IPv6 protocol is designed for Break-Before-Make handoffs and does not perform well in Make-Before-Break handoffs. As I am using SafetyNet, the Fast Handovers for Mobile IPv6 protocol for my proposed architecture by extending it to support Make-Before-Break handoffs.

We design a handoff timing algorithm which exploits the SafetyNet protocol to allow a Mobile Node to maximize its use of low cost networks by delaying a vertical handoff without degrading application performance. SafetyNet improves our previously proposed Fast Handovers for Mobile IPv6 Bicasting with Selective Delivery (FMIPv6-BSD), a protocol for seamless horizontal handoffs, for vertical handoffs. In SafetyNet, the current Access Router (pAR) starts multicasting packets to candidate Access Router(s) as well as to the Mobile Node at the initialization of the handoff to ensure that any packets lost during the handoff can be recovered. Packets lost during the handoff are delivered to the Mobile Node at the finalization of the handoff from the buffer of the new Access Router. The selective delivery mechanism employed in the protocol ensures that only the lost packets are delivered from the buffer, as opposed to the entire contents of the buffer. This decreases the data transmission overhead of the protocol significantly.

A vertical handoff timing algorithm based on the signal strength finalizes the handoff immediately after the initialization of the handoff as opposed to SafetyNet handoff timing algorithm. The use of the SafetyNet handoff algorithm for upward vertical handoffs together with the SafetyNet protocol would allow the Mobile Node to maximize its use of the lower cost network without degrading the performance of on-going connections. The overview of the operation of the SafetyNet timing algorithm is shown in figure 28. The Mobile Node would initialize the handoff towards both the WLAN 2 and WWAN Access Routers. In the case of the Mobile Node moving on Path A, the delaying of the finalization of the handoff would allow it to perform a horizontal handoff to the nAR of WLAN2. In the case of Path B, the Mobile Node would eventually perform a handoff to the nAR of the WWAN. The timing of the handoff finalization is described in the SafetyNet handoff timing algorithm. The delaying of the handoff finalization would incur some packet loss. However, the use of the SafetyNet protocol would allow the Mobile Node to recover any packets lost during the handoff.

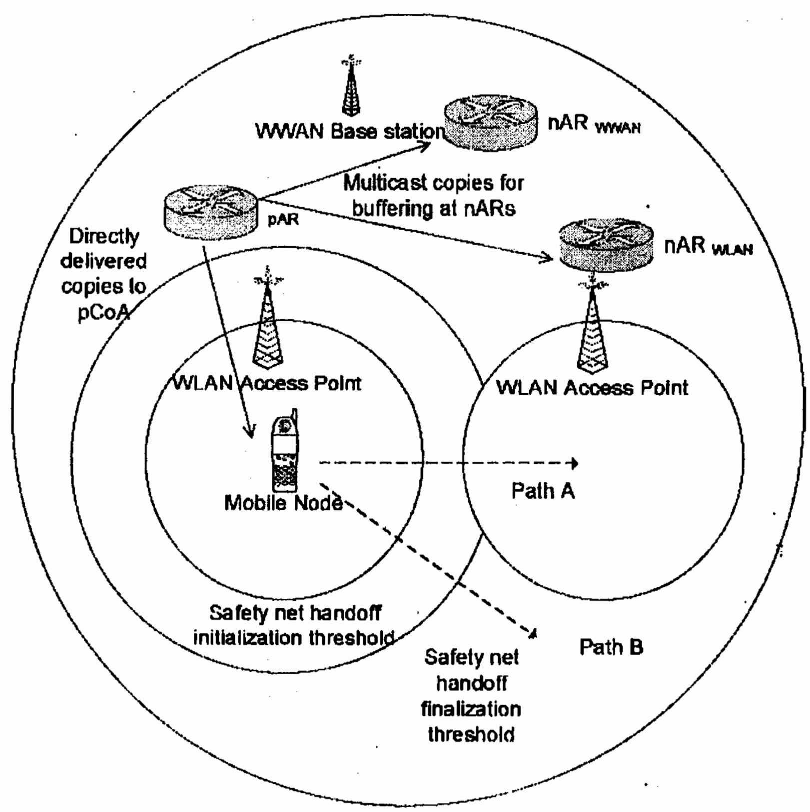


Figure 28 Mobile network using safetynet structural design.

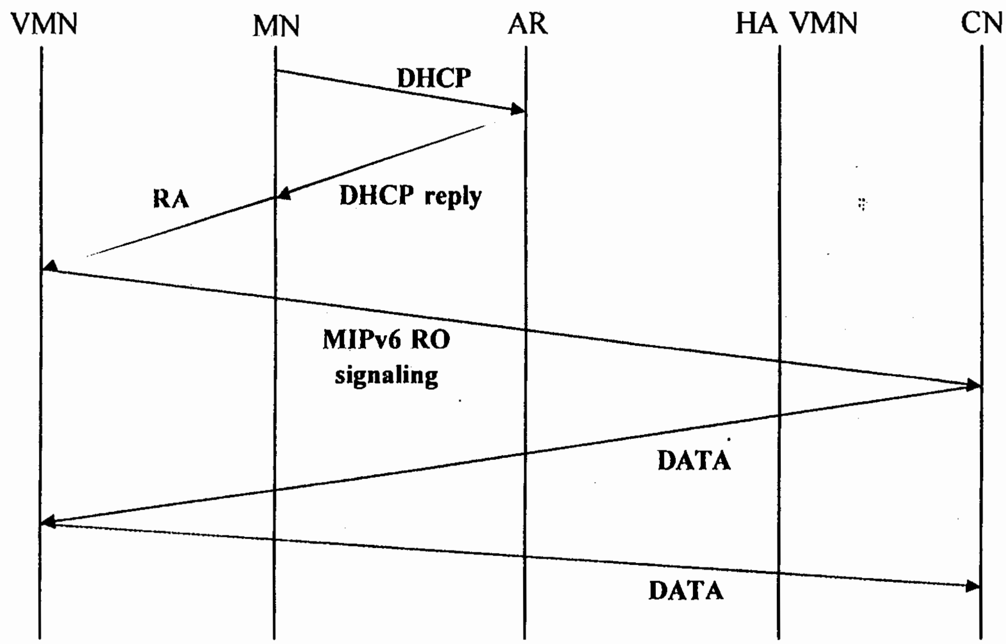


Figure 29 Steps for RO using Optinet Approach.

OptiNets and caching use the SafetyNet architecture to enable transfer of OptiNets prefix delegation context and bandwidth fuelling cache contents between the previous and new access routers. This reduces the over the air signaling required to re-establish the prefix delegation and cache state and reduces the latency of the handoff [25]. Further, the transfer of the cache contents enables the road side cache server in the Access Routers, and thus increases the benefits gained from the locality of the road side cache servers.

4.5 Optimization for VMN

The use of the NEMO protocol gives rise to non-optimal routing and protocol overheads. In this section, an optimization techniques which are used before are incorporated into the architecture to overcome non optimal routing for mobility capable nodes within the mobile network. This thesis improves the optimization technique further and implements, measures and analyzes the effects of using this technique. The NEMO Basic Support protocol hides the mobility from all the nodes in the mobile network. MIPV6 enable nodes bypass [26] HA and try to direct communicate with VMN. It is the duty of MR to advertise a network prefix getting from the FN.

4.6. Infrastructure independent Make-Before-Break handoffs

A lossless Make-Before-Break handoff can be performed between two access networks using two network interfaces using the algorithm illustrated in following Figure 30. The algorithm differentiates between an active interface and a scanning interface. The MR uses the active interface for delivering traffic between the mobile network and the Internet. The scanning interface is used to scan for new access points (APs) and perform a handoff, when a better AP than the current one is found. The algorithm for making the handoff decision is abstracted in Figure 30, and can be implemented using existing technologies such as signal to noise ratio comparisons combined with movement prediction algorithms [27]. The handoff is started when the predicted signal strength of the current access point at the time when the handoff is finished would be below an acceptable level and a candidate access point would according to the prediction have acceptable signal strength at that point. When the handoff is completed the data traffic is switched to the new interface and the original active interface becomes the scanning interface.

4.7. Mobile Cache Server

A system for caching data from an origin server, comprising: a wireless device, a wireless network, a mobile cache that is separated from the wireless device by means of the wireless network, the mobile cache including a user profile database that stores at least one user profile containing output preference data with respect to at least one of output content and output layout, an object database for storing selected data from the origin server, and a dynamic information composer coupled to the object database and the user profile database, wherein the dynamic information composer dynamically composes user-specific information as a personalized, user-specific output based on data in the object database and the user profile while simultaneously reducing network traffic; and a change trigger coupled to the user profile database and included as part of the mobile cache, the object database, and the dynamic information composer, wherein the change trigger monitors changes in the object database and triggers output delivery when a number of information changes in the object database reaches a predetermined threshold.

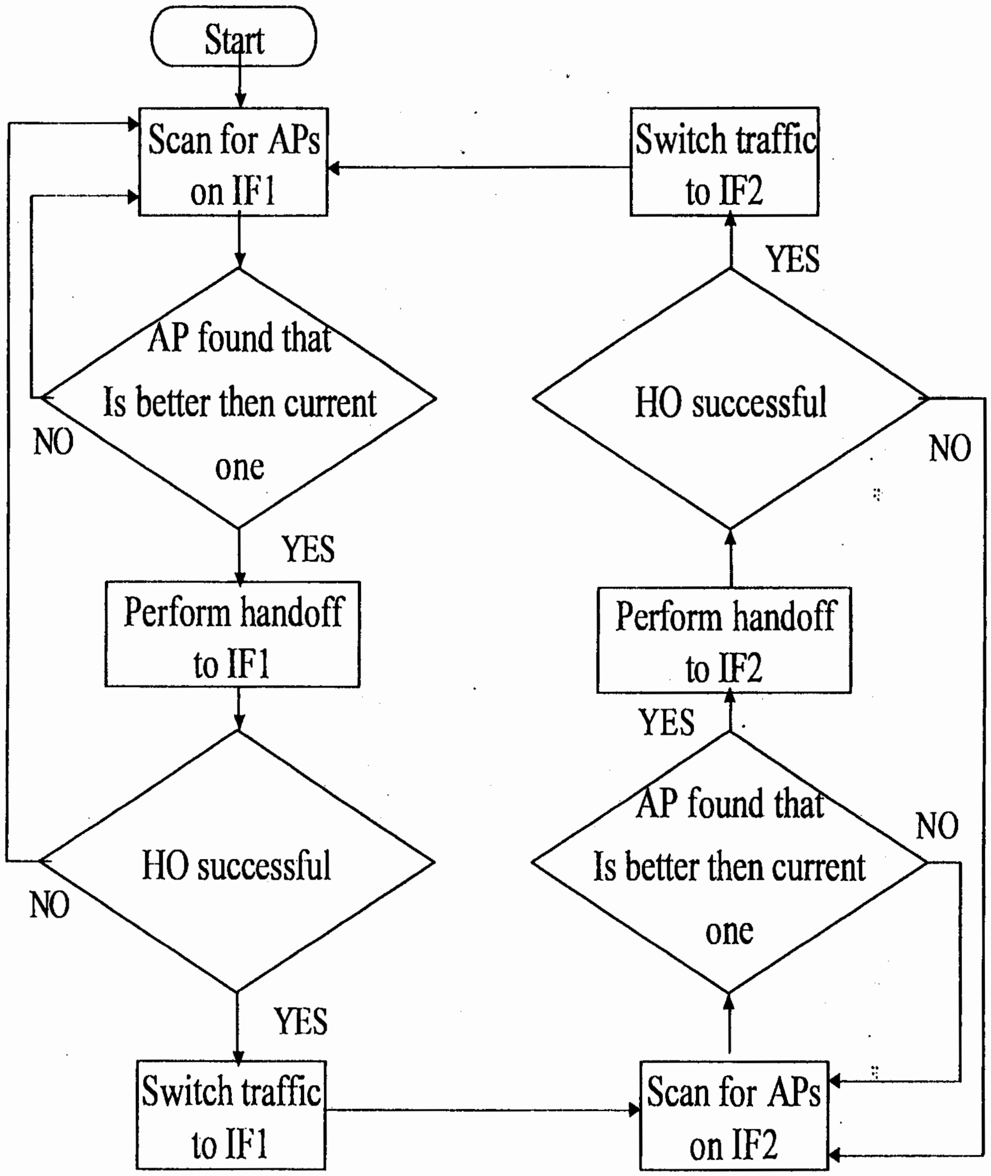


Figure 30 Algorithm for making the handoff decision.

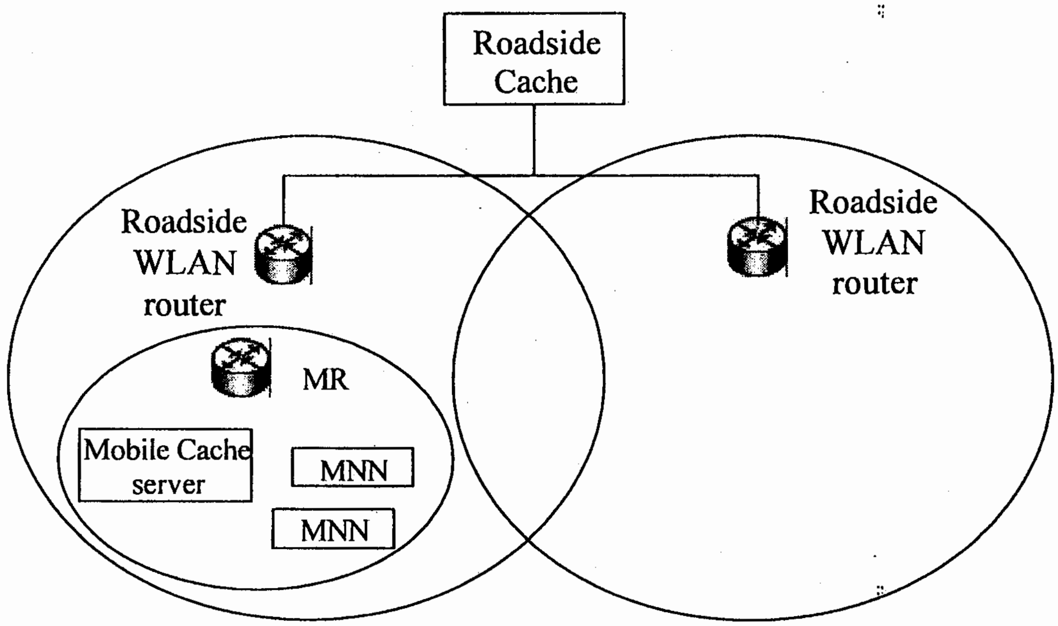


Figure 31 Bandwidth fuelling architecture

The efficiency of the communications is increased using a caching architecture, Bandwidth Fuelling together with a route optimization mechanism for NEMO, OptiNets. OptiNets RO mechanism uses the capabilities of Visiting Mobile Nodes to enable Mobile IPv6 based route optimization between the Visiting Mobile Nodes and Correspondent Nodes. The Mobile Network Nodes use topologically correct Care-of Addresses from the visited network address hierarchy for the route optimization. The Mobile Router acquires and manages the CoA from servers in the visited network.

Normally MRs already equipped with WWAN, LAN and WLAN interfaces which use to communication among the MN. The fast WLAN connection together with the localized server allows the Mobile Cache Server to be updated during the time span that the Mobile Router is in the coverage area of the Roadside network. A Roadside Network could consist of one or more Roadside Routers connected to a Roadside Cache Server. The technical aspects of the architecture are given by first considering access to a Roadside Cache Server via a single Roadside Router while the mobile network is static, i.e. the vehicle has stopped [28]. This will be followed by the case of using a cluster of Roadside Routers for access while the vehicle with the mobile network is moving.

Timely fetching of customized data to the Roadside Cache Server depends on the ability to predict mobility correctly. However, even without mobility prediction the Roadside Cache Server would be able to provide the Mobile Cache Server with fresh non-customized data, such as local news, tourist information and traffic information.

Chapter 5

Simulation Results & Discussion

First of all let us analyze network layer solutions. Mobile IP was designed to handle handoffs in a situation where the host moves at a low speed and handoff frequency is very low. Every time host moves out of the foreign network it has to update its care-of- addresses at Home Agent. Also the other party to which mobile host is communicating has to be informed of this new address when route optimization is being used. Mobile IP [29] is good for locating a mobile host but during connection migration it doesn't provide us the seamless support needed for vertical handoff.

In Cellular IP the binding update problem of MIP was partially solved by not updating the care-of-addresses at Home Agent every time host moves to a new address. In this approach a gateway router is used to send packets to the host in the foreign network and when the host moves within the network it only causes the gateway router to change the base station where the packets are to be sent. Although above mentioned optimization smoothes the handoff procedure but it works only within the same network. When the mobile host moves from one network to another same Mobile IP is used.

All the other network layer solutions HOPOVER, WiFi and Takeover are all based on indirection approach used by MIP. These approaches have limited performance and add additional complexity to the network. Even if these solutions provide a considerable amount of seamless continuity they require some considerable changes in network which may not be implement able in the real world. Now let us analyze network layer solutions. Only SIP has been used as an application layer solution. As explained earlier in the related work it has been shown that using SIP for vertical handover causes a considerable amount of delay in the handover and is not suitable approach for the vertical handoff problem.

Mobility is an end to end issue and transport layer is lowest end to end layer. Using transport layer is the best approach to solve vertical handoff problem because it can quickly detect changes in the network and customize according to the new network. Also they do not require any change in the network which is preferred by the network owners. As explained in the extended version of HIP and nemo are two competing approaches for handoffs between heterogeneous networks.

5.1 NS-2 Simulations

I used the network simulator to design a mipv6 network in Linux O.S. As several TCP implementations are implemented with network simulator, it was easier to analyze their performance regarding mipv6. I implemented this simple mechanism with NS-2. I used four machines to setup this test bed.

- Mobile Node
- Correspondent Node
- HA/Router
- Router

5.1.1 The architecture

We used a wired/wireless mixed environment. There are two base stations, one router, one correspondent node and one mobile node. We used the ns2 hierarchical addressing. In ns2 hierarchical addressing there is three different levels: Domain, Cluster and Node. It is somehow similar to IP classless addresses, but in this case there are three levels of hierarchy. For example, the Node 3 in Cluster 2, in Domain 1, will have the address 1.2.3. The Node 3 in Cluster 1, in Domain 1, will have address 1.1.3. Thus these two nodes won't be on the same cluster (you can read subnet), and then routing will be needed for the nodes to communicate. In figure 32 define:

- Correspondent Node (CN) has address 0.0.0
- Router(R) has address 1.0.0
- Base Station 1 (BS1) has address 1.1.0
- Base Station 2 (BS2) has address 1.2.0
- Mobile Node (MN) has home address 1.1.1

Base station 1 act as a Home Agent. The Mobile Node is initially in the same cluster as Base Station 1 and move towards Base Station 2, which resides in Cluster 2. The Mobile Node is communicating with the Correspondent Node, which is in another domain. The Mobile Node is a TCP Agent on the top of which an FTP application is attached, whereas the correspondent node is a simple TCP sink that acknowledges the data as soon as it receives it, but does not transmit any data.

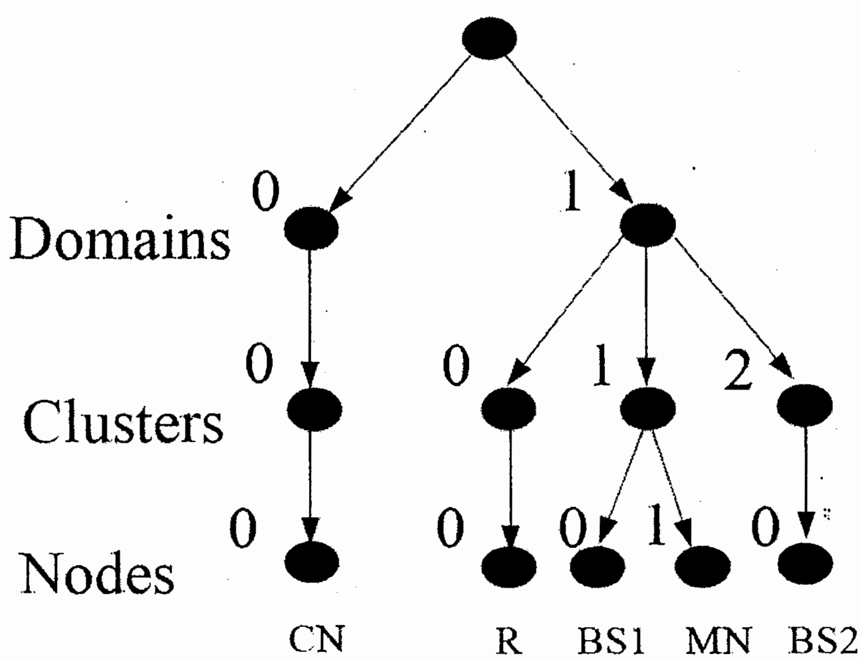


Figure 32 NS2 Architecture

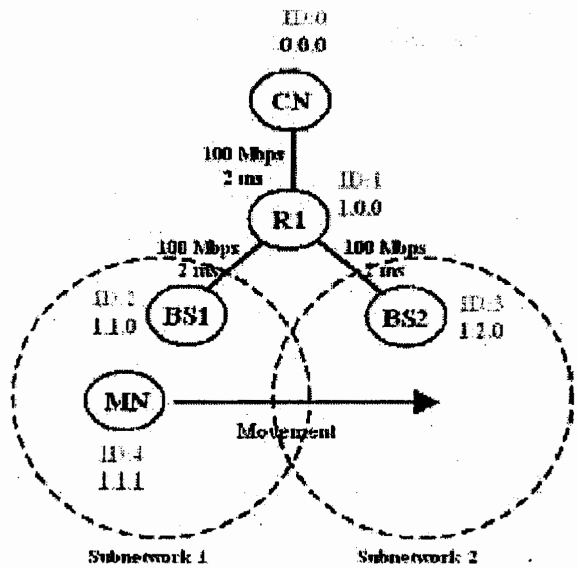


Figure 33 Simple mIPv6 simulation topology

5.2 A mIPv6 simulation scenario

We wanted to start our simulations with a simulation model as simple as possible. It was desired to start out with running simple traffic simulations in a very simple scenario, in order to limit the unknown factors. For our simple test scenario, we created a topology with just 5 nodes. Our simple simulation scenario consisted of one mobile node, two base stations (BS), one router connecting the two base stations, and one correspondent node communicating with the mobile node. The topology is shown figure 33.

The scenario consisted of two wireless networks, each served by a base station BS-1 and BS-2. The base stations function as access points connecting the wired topology to the wireless nodes, and they also have routing functionality in the sense that they exchange routing information with other nodes and they route packets towards the correct destination. The two base stations were both connected to an intermediate router, R1. The correspondent node CN is also connected to this router. The links between the nodes are set to a transmission rate of 100 Mbit/s and with a delay of 2 ms on each link. This was done to make the scenario consistent wth fast Ethernet infrastructure, so the results could be compared to hardware test results. The delay could possibly have been set to a lower value, but we wanted a certain delay to be able to do calculations on the round trip time, RTT. The mobile node MN has its home address on subnetwork 1 and BS-1 is serving as home agent for the MN.

Mobility is simply carried out by letting the mobile node move along a straight line with constant velocity until reaches a foreign subnet. When the MN is located within the coverage area of the other base station, BS-2, it performs handover to this cell. Once the MN detects it is on a foreign subnet, it does a binding update towards its home agent and receives a BU acknowledge back. Furthermore, if the MN is receiving packets from the CN, it also sends BU to this node. The BU to the CN is not acknowledged. The goal of this simple simulation was to monitor the BU procedures and to monitor the traffic performance throughout this critical period. In Ns-2, wireless simulations require the nodes to be located with x, y- and z coordinates in the simulation topography grid in order to simulate motion and radio range between nodes. The locations of the base stations and the mobile node are the only relevant positions for the wirele ss simulation. The positions of router R1 and the CN are not specified in the simulation script, as they are redundant.

An output of simulation shows the Binding Update/Binding Acknowledgement procedure. The trace file of the code did not show the Router advertisement so we see that the MN sending BU message towards the HA. Note that the Home Address is in the Source Address field in place of the care-of address. This mis-impletention does not influence the performance test. The Home Agent answers with the care of address in the Destination Address Field.

5.2.1 Result for simple mIPv6 simulation scenario

SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
1.00262 return home 1.1.0:4196352 Current location: 190.191, 194.002 Destination: 210, 610
2 Send BU to HA
66.4 Lost contact with current BS: 1.1.0:4196352 Current location: 202.633, 455.293 Destination: 210, 610
66.4358 get_coa for BS 1.2.0:4198400 Current location: 202.64, 455.439 Destination: 210, 610
67.4 Send BU to HA
Simulation finished

```
|Binding Cache for node 1.1.0 at 100 ---------------------------------------|
|Node        COA          Type  Info  Flag  Last  Time        Life  Expire
Nb|
|1.1.256          1.2.8       11    MN    1     8     95.0058     10    0
8 |

|Binding Update List for node 1.1.256 at 100 ---------------------------------------|
|Node        COA          Type  Info  Flag  Last  Time        Life  Expire
Nb|
|1.1.0       1.2.8        7     HA    1     8     95          10    2.68435e+08
9 |

|Base Station List for node 1.1.256 at 100 ---------------------------------------|
|Node        COA          Type  Info  Flag  Last  Time        Life  Expire
Nb|
|1.2.0       1.2.8        12    BS    1     -1    99.8746     1     0      69 |
```

5.3 An extended mIPv6 simulation scenario

When extending the topology further, we wanted to focus on the subnet change and the binding update procedure. This is the most important issue related to node mobility and we wanted to create a scenario where subnet changes happened more frequently to be able to determine the performance when the MN registered on new subnets repeatedly. Therefore, we created a scenario with 4 different subnetworks served by one base station each. A network of routers connecting the base stations and one correspondent node was simulated. The topology for this extended simulation scenario is shownin figure 34.

In this scenario, we constructed a hierarchical topology of routers (R1 – R6) with one mobile node (MN), one correspondent node (CN), one home agent (BS-1). The mobile node was moving along a straight line as in the simple scenario, connecting to the different wireless networks in turn. This time we also let the MN return back to its home subnet after reaching the network served by BS -4. This was done in order to see if the reconnection to the home agent went smoothly and to get more cell changes and thereby more binding updates while traffic was running. The destination was set to the point (1500, 100) in the topography grid. When the MN reached its destination, it was stationary for 5 seconds before the movement back started with the destination (100, 100).

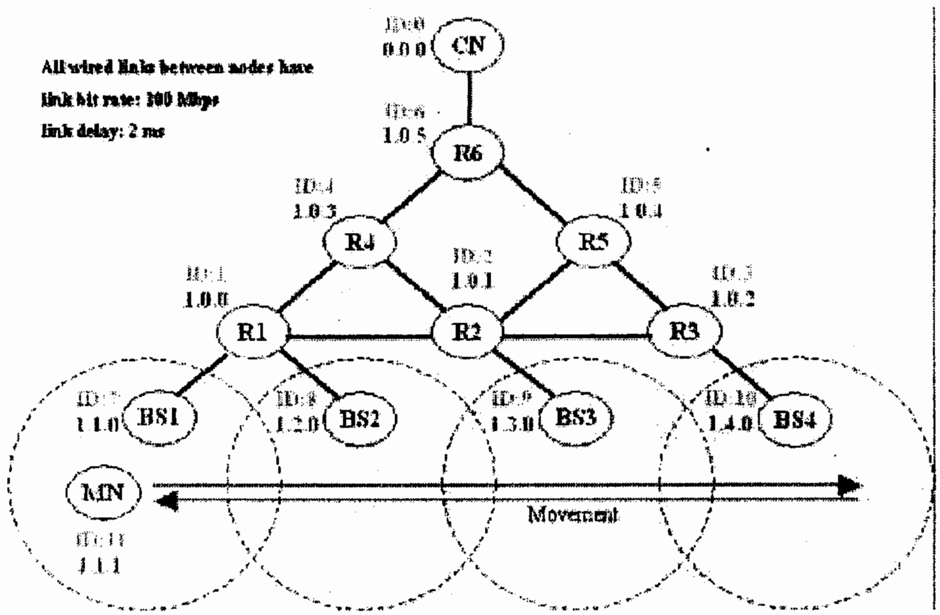


Figure 34 Extended mIPv6 network topology.

The mobile node moved from its home link and to the foreign links associated with BS-2, BS-3 and BS -4 in turn, three binding updates would take place during the movement. By monitoring throughput, delay, and packet loss for the packet flow from the correspondent node to the mobile node, we were able to determine the performance parameters in the same way as for the simple scenario. The traffic generated was ping messages and CBR traffic. CBR traffic was again generated to monitor the throughput for the flow to the MN, and we also monitored for possible packet loss, and the time delay for performing BU towards HA and CN during these movement. However, this time we decided to run CBR traffic in only one direction from CN to MN as we found this to be the most relevant traffic case. The ping command was also here used to measure RTT delay during the movement, and the time necessary to do BU and to achieve routing optimization was monitored.

5.3.1 Result for extended mIPv6 simulation scenario

Binding Cache for node 1.1.0 at 100 --|
|Node COA Type Info Flag Last Time Life Expire
Nb|
|1.1.256 1.2.9 11 MN 1 8 95.0055 10 0
8 |

|Binding Cache for node 1.4.0 at 100 --|
|Node COA Type Info Flag Last Time Life Expire
Nb|
|1.4.1 1.4.1 11 MN 1 36 66.1622 10 0 15 |

|Binding Update List for node 1.1.256 at 100 --|
|Node COA Type Info Flag Last Time Life Expire
Nb|
|1.1.0 1.2.9 7 HA 1 8 95 10 2.68435e+08
9 |

|Base Station List for node 1.1.256 at 100 --|
|Node COA Type Info Flag Last Time Life Expire
Nb|
|1.2.0 1.2.9 12 BS 1 -1 99.5434 1 0 63 |

|Binding Update List for node 1.4.1 at 100 --|
|Node COA Type Info Flag Last Time Life Expire
Nb|
|1.3.0 1.4.1 8 BS 1 -1 66.1 10 76.1 1 |
|1.1.259 1.3.6 9 CN 1 34 65 10 75.0611
9 |
|1.1.258 1.3.6 9 CN 1 35 65 10 110 10
|
|1.4.0 1.4.1 7 HA 1 36 66.1 10 2.68435e+08
15 |

|Base Station List for node 1.4.1 at 100 --|
|Node COA Type Info Flag Last Time Life Expire
Nb|
|1.4.0 1.4.1 12 BS 1 -1 99.3814 1 0 100 |

5.4 Performance

Main advantage of using HIP lets the Mobile Router act as a HIP proxy for the Mobile Network Nodes. This approach relies on the Correspondent Nodes being HIP enabled, but does not require routing of traffic via a fixed anchor point, unlike NEMO which uses the Home Agent. An extension to Session Initiation Protocol (SIP) has been proposed for network mobility management. It uses a SIP [30] Network Mobility Server to manage the mobility of the SIP nodes in a mobile network. The server acts a SIP proxy for the SIP hosts inside the mobile network enabling a NEMO like operation.

The TCP performance of a NEMO Local Fixed Node, a Visiting Mobile Node with out route optimization, a Visiting Mobile Node with Mobile IPv6 route optimization (i.e. avoiding the Home Agent of the Visiting Mobile Node), and a Visiting Mobile Node with OptiNets (i.e. avoiding both the Home Agent of the Visiting Mobile Node and the Home Agent of the Mobile Router) is compared experimentally using the Linux O.S with NS. The performance is measured in a static case, in which the Mobile Router is located in a foreign network and in a dynamic case, in which the Mobile Router moves between two foreign networks. The results for the static case indicate that the performance of the other schemes decreases as the latency between the MR and the Home Agent of the Mobile Router increases, whereas the performance of the OptiNets scheme is not affected.

Our proposed scheme is shown in the above figure. Now there is no need to have two IP address for fixed server. Our scheme also does not use set primary address command which cased delay due to handshake in the single homing configuration. Now the handover delay is reduced to only one message exchange where MC adds new IP address and the time in which same stream starts to appear in both the IP address of the Mobile Host.

Chapter 6

Conclusions & Future work

In this thesis we have presented a study of a number of vertical handoff schemes based on network layer, transport layer and application layer. We have shown that using transport layer is the best approach to solve vertical handoff problem because mobility is an end to end issue and transport layer is the lowest end to end layer. This is also in agreement with the end to end principle which says that if anything can be done in the end system should be done there. Also during vertical handoff there is considerable change in network parameters. Transport layer can quickly detect these changes and adapt flow and congestion control parameters according to the new network.

There are two vertical handoff schemes for transport layer which are using HIP and NEMO. We have shown in "Results & Discussion" that of these two schemes extension version of HIP provides better performance because it does not suffer from the routing overhead, since no home agent is used. Deployment of the purposed scheme, any person or device can communicate to the world during mobility by using a Mobile Router. Mobile Router is the most import part of purpose architecture, can fit on any vehicle and use its external antennas and its power source.

Because of using these sources it provides better connectivity with other MNN. As I have concern with communicating among varied networks technologies simultaneously so MR provides best connectivity among different network technologies simultaneously by attaching different interfaces with MR. All 3.G network technologies have different features, some are high in cost to provide mobility in higher speed but some are at low in cost but support slow speed and low data rate. Function of MR is that to selection among these technologies that which one support best speed with high low cost and best quality dynamically. When we are talking about high speed mobility and varied networks environment would result in frequent handoffs. Especially in case of WLAN causes frequently handoff between AP and WLAN networks. In this case seamless horizontal handoffs are required to provide continuous connectivity to MNN without any interruption.

Our proposed scheme offers almost the same performance in asymmetric multi-homing configuration which was previously achieved in symmetric multi-homing configuration. This is achieved by effectively utilizing the redundant path by sending duplicated data streams between mobile host and fixed server. Our proposed scheme is also realistic with respect to implementation as asymmetric configuration is easily possible in the real world.

6.1 Future Work

In the future, we will use our proposed scheme in different real world scenarios of vertical handoff in order to evaluate the performance gained in terms of delay and packet loss. The decision to implement a new simulator rather than using ns-2, is the lack of too many components in ns-2 such as IPv6 and real layer 2 handoff. Furthermore, work in MIPV6 Fast Handoff and Hierarchical MIP6 in Linux O.S. Regarding TCP, currently no real, new TCP implementations for mobile environments are in the standardization process. However extensive research is under way to change this situation. One promising research focus in the area of mobility enabled TCP is interlayer communication. However changing the current TCP implementation is a complicated task, and will take a long time before any agreement is made. Further research topics include:

– testing the new simulator presented above.

– implementation of TCP on top of it (can use the ns code).

– interaction of TCP with MIPv6 Fast Handoff, and Hierarchical MIPv6.

– Comparison of real Mobile IPv6 implantations (currently: FreeBSD/KAME, Linux/MIPL, Cisco IOS 12 beta).

– The study of interlayer communication in OS kernels.

Glossary

BS	Base Station
DAR	Dynamic Address Reconfiguration
F_IP	IP of the Fixed Server
FA	Foreign Agent
GW	Gateway
HA	Home Agent
HOPOVER	Handoff Protocol for Overlay Networks
HS	Handoff Server
IP	Internet Protocol
MC	Mobile Client
MH	Mobile Host
MIP	Mobile IP
MN	Mobile Node
M-SCTP	Mobile SCTP
M-TCP	Migrate TCP
NN	Neighboring Node
RTT	Round Trip Time
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
U_IP	IP in UMTS Network
UMTS	Universal Mobile Telecommunications System
USHA	Universal Seamless Handoff Architecture
VOHST	Vertical Hand-Off through Seamless TCP Migration
VOIP	Voice over IP
W_IP	IP in Wireless Network
MN	Mobile Node
MNN	Mobile Network Node
VMN	Visiting Mobile Node
LMM	Localized Mobility Management

References

[1] L. Ma, F. Yu, V. C. M. Leung and T. Randhawa, "A New Method To Support UMTS/WLAN Vertical Handover Using SCTP", IEEE Wireless Communications, vol. 11, no. 4, pp. 44-51, 2004.

[2] H. Roeber, J. Bacus and C.o Tomasi, "Typing In Thin Air: The Canesta Projection Keyboard - A New Method Of Interaction With Electronic Devices," In CHI '03: CHI '03 extended abstracts on Human factors in computing systems, pages 712–713, New York, NY, USA, 200 3. ACM Press.

[3] A. Calvagna and D. Modica, "A User-Centric Analysis of Vertical Handovers," In Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots, Philadelphia, USA, PP 137-146, 2004.

[4] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," internet-rfc: RFC 3963, January 2005.

[5] H. Schulzrinne and E. Wedlund, "Application-layer Mobility Using SIP," in IEEE Service Portability and Virtual Customer Environments, pp. 29-36, 2000.

[6] A. Acharya, L. Jun, B. Rajagopalan and D. Raychaudhuri. "Mobility Management In Wireless ATM Networks," IEEE Communications Magazine, vol. 35, no. 11, pp. 100-109, Nov 1997.

[7] A. C. Snoeren and H. Balakrishnan, "An End-To-End Approach to Host Mobility," In Proc. Of 6th ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Boston, MA, 2000.

[8] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," November 28, 2006.

[9] R. J. Kang, H. P. Chang and R. C. Chang, "A Seamless Vertical Handoff Scheme", Proc. of the 1st International Conference on Wireless Internet (WICON'05), pp. 64-71, 2005.

[10] H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier, "Hierarchical MIPv6 Mobility Management," Jul. 2002.

[11] G. Daley, S. Narayanan, and G. Perkins. "A Probabilistic Scheme For Fast Router Advertisement Responses In IPv6". internet-draft, feb 2005.

[12] J. P. Jeong, K. Lee, J. Park, and H. Kim, "Nd-Proxy Based Route And Dns

Optimizations For Mobile Nodes In Mobile Network," February 2004.

[13] R. Wakikawa, S. Koshiba and K. Uehara, "Optimized Route Cache Management Protocol For Network Mobility," Proceedings of the 10th International Conference on Telecommunication (ICT), Tahiti , Papeete, French Polynesia, February 2003.

[14] A. G. Valko, "Cellular IP: A New Approach to Internet Host Mobility," ACM SIGCOMM Computer Communication Review, vol. 29, no. 1, pp.50-65, 1999.

[15] C. W. Lee, "A Framework Of Handoffs In Wireless Overlay Networks Based On Mobile IPV6," IEEE Journal on Selected Areas in Communications, vol. 23, no. 11, pp. 2118-2128, Nov 2005.

[16] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," November 28, 2006.

[17] F. Du, L. Ni. and A. H. Esfahanian, "HOPOVER: A New Handoff Protocol for Overlay Networks," IEEE International Conference on Communications (ICC), vol. 5, pp. 3234-3239, 2002.

[18] W. Xing, H. Karl and A. Wolisz, "M-SCTP: Design and Prototypical Implementation of an End-to-End Mobility Concept," In Proc. of 5th International Workshop on the Internet Challenge: Technology and Applications, Berlin, Germany, 2002.

[20] A. K. Salkintzis, C. Fors and R. Pazhyannur, "WLAN-GPRS Integration For Next-Generation Mobile Data Networks," IEEE Wireless Communications, vol. 9, no. 5, pp. 112-124, 2002.

[21] A. G. Valko, "Cellular IP: A New Approach to Internet Host Mobility," ACM SIGCOMM Computer Communication Review, vol. 29, no. 1, pp.50-65, 1999.

[22] H. Kang, K. Kim, S. Han, K. J. Lee and J S. Park, "Route optimization for mobile network by using bidirectional between home agent and top level mobile router," June 2003.

[23] R. J. Kang, H. P. Chang and R. C. Chang, "A Seamless Vertical Handoff Scheme", Proc. of the 1st International Conference on Wireless Internet (WICON'05), pp. 64-71, 2005.

[24] J. P. Jeong, K. Lee, J. Park and H. Kim, "Nd-Proxy Based Route And Dns Optimizations For Mobile Nodes In Mobile Network," February 2004.

[25] R. Hsieh and A. Seneviratne, "A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP,". ACM MobiCom'03, San Diego, USA, Sep 2003.

[26] C. E. Perkins and D. B. Johnson, "Mobility Support in IPv6", Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom'96), pp. 27-37, November, 1996.

[27] Q. Guo, J. Zhu and X. Xu, "An Adaptive Multicriteria Vertical Handoff Decision Algorithm For Radio Heterogeneous Network". Proceedings of ICC 2005, vol. 4, pp. 2769–2773, May 2005.

[28] T. Zhou, H. Sharif, M. Hempel, P. Mahasukhon and C. Song, "Performance of IEEE 802.11b In Mobile Railroad Environments," Vehicular Technology Conference, 2005. vol. 4, pp. 2527–2531, Sept 2005.

[29] S. Aust, D. Proeteh, N. Fikouras, C. Paupu and C. Gorg, "Policy Based Mobile IP Handoff Decision (POLIMAND) Using Generic Link Layer Information," Proc. 5th IEEE Int. Conf. Mobile andWireless Commun. Netw., Oct. 2003.

[30] K. Basu and S. Das, "SIP-Based Vertical Handoff Between WWANs and WLANs", IEEE Wireless Communications, vol. 12, no. 3, pp. 66-72, 2005.