Proposal / Application

for

ICT-Related Development and Research Grant

End-to-End Mobility Management Framework (EMF)

for Multihomed Mobile Devices

Dr Amir Qayyum

Professor, M. A. Jinnah University, Islamabad
List of Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EE</td>
<td>External Evaluators</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>JPD</td>
<td>Joint Project Director (Co-Director)</td>
</tr>
<tr>
<td>MC</td>
<td>Milestone Chart</td>
</tr>
<tr>
<td>MD</td>
<td>Monitoring Department</td>
</tr>
<tr>
<td>MoIT</td>
<td>Ministry of Information Technology</td>
</tr>
<tr>
<td>PAC</td>
<td>Project Appraisal Committee</td>
</tr>
<tr>
<td>PD</td>
<td>Project Director</td>
</tr>
<tr>
<td>PI</td>
<td>Principal Investigator (Organization)</td>
</tr>
</tbody>
</table>

"Principal Investigator" means the person, company, partnership, undertaking, concern, association of persons, body of individuals, consortium or joint venture which receives funding from the Company to execute a research and development project."

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>SED</td>
<td>Solicitation and Evaluation Department</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Description</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Project Identification...........................................................................</td>
<td>3</td>
</tr>
<tr>
<td>A. Project Title:</td>
<td>3</td>
</tr>
<tr>
<td>B. Project Director (PD):</td>
<td>3</td>
</tr>
<tr>
<td>C. Organization (The Principal Investigator):</td>
<td>3</td>
</tr>
<tr>
<td>D. Other Organizations Involved in the Project:</td>
<td>4</td>
</tr>
<tr>
<td>E. Key Words:</td>
<td>4</td>
</tr>
<tr>
<td>F. Research and Development Theme:</td>
<td>4</td>
</tr>
<tr>
<td>G. Project Status:</td>
<td>4</td>
</tr>
<tr>
<td>H. Project Duration:</td>
<td>5</td>
</tr>
<tr>
<td>I. Executive Summary:</td>
<td>5</td>
</tr>
<tr>
<td>2. Objectives of the Project</td>
<td>7</td>
</tr>
<tr>
<td>A. Scope and Introduction of the Project (Abstract):</td>
<td>7</td>
</tr>
<tr>
<td>B. Specific Objectives Being Addressed by the Project:</td>
<td>9</td>
</tr>
<tr>
<td>3. Research Approach</td>
<td>11</td>
</tr>
<tr>
<td>A. Literature Review Summary:</td>
<td>11</td>
</tr>
<tr>
<td>B. Development / Research Methodology:</td>
<td>29</td>
</tr>
<tr>
<td>C. Project Activities:</td>
<td>41</td>
</tr>
<tr>
<td>D. Key Milestones and Deliverables:</td>
<td>43</td>
</tr>
<tr>
<td>4. Benefits of the Project</td>
<td>45</td>
</tr>
<tr>
<td>A. Direct Customers / Beneficiaries of the Project:</td>
<td>45</td>
</tr>
<tr>
<td>B. Outputs Expected from the Project:</td>
<td>46</td>
</tr>
<tr>
<td>C. Organizational / HRD Outcomes Expected:</td>
<td>46</td>
</tr>
<tr>
<td>D. Technology Transfer / Diffusion Approach:</td>
<td>46</td>
</tr>
<tr>
<td>Annexure A – Curriculum Vitae</td>
<td>48</td>
</tr>
<tr>
<td>Annexure B – References</td>
<td>55</td>
</tr>
<tr>
<td>Annexure C – Additional List of Abbreviations and Acronyms</td>
<td>57</td>
</tr>
</tbody>
</table>
1. **Project Identification**

   **A. Project Title:**
   
   *End-to-end Mobility management Framework (EMF) for multihomed mobile devices*

   **B. Project Director (PD):**
   
   **Name:** Dr Amir Qayyum  
   **Designation:** Professor  
   **Organization:** M. A. Jinnah University, Islamabad  
   **Email:** aqayyum@ieee.org

   **C1. Senior Researcher:**
   
   **Name:** Dr Shahzad A. Malik  
   **Designation:** Associate Professor  
   **Organization:** COMSATS Institute of Information Technology, Islamabad  
   **Email:** smalik@comsats.edu.pk

   **C3. Project Team:** *(Please attach the curriculum vitae of key research / development personnel, if available and PD, JPD. Please follow the format included in Annexure A.)*

<table>
<thead>
<tr>
<th>Title / Position</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Researcher</td>
<td>1</td>
</tr>
<tr>
<td>Team Leads</td>
<td>2</td>
</tr>
<tr>
<td>Researchers / Developers (Full time)</td>
<td>4</td>
</tr>
<tr>
<td>Researchers / Developers (Part time)</td>
<td>2</td>
</tr>
<tr>
<td>Researcher / Development Assistants</td>
<td>4</td>
</tr>
<tr>
<td>Support Staff</td>
<td>3</td>
</tr>
<tr>
<td>Contract Staff</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
</tbody>
</table>

   **C. Organization (The Principal Investigator):**

   *(Please indicate the name, address, telephone and fax of the Organization acting as Principal Investigator.)*

   **Name:** M. A. Jinnah University, Islamabad
Address: 74-E, Jinnah Avenue, Blue Area, Islamabad
Website: www.jinnah.edu.pk

D. Other Organizations Involved in the Project:
(Please identify all affiliated organizations collaborating in the project, and describe their role/contribution to the project.)

E1. Industrial Organizations:

<table>
<thead>
<tr>
<th>#</th>
<th>Organization Name</th>
<th>Role / Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>- -</td>
<td></td>
</tr>
</tbody>
</table>

E2. Academic Organizations:

<table>
<thead>
<tr>
<th>#</th>
<th>Organization Name</th>
<th>Role / Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>- -</td>
<td></td>
</tr>
</tbody>
</table>

E3. Funding Organizations:

<table>
<thead>
<tr>
<th>#</th>
<th>Organization Name</th>
<th>Role / Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>- -</td>
<td></td>
</tr>
</tbody>
</table>

E4. Other Organizations:

<table>
<thead>
<tr>
<th>#</th>
<th>Organization Name</th>
<th>Role / Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>- -</td>
<td></td>
</tr>
</tbody>
</table>

E. Key Words:
(Please provide a maximum of 5 key words that describe the project. The key words will be incorporated in our database.)

4G Wireless Networks, Cross Layer Design, End-to-End Architecture, IEEE 802.21 MIH, Mobility Management, Multi-homing, TCP, Vertical Handover, Willful Handover

F. Research and Development Theme:
(If the proposal belongs to a theme specified by NICT R&D Fund, please identify the Research Theme.)

NA

G. Project Status:
(Please mark ☑)

☑ New   ☐ Modification to previous Project
☐ Extension of existing project
H. Project Duration:

<table>
<thead>
<tr>
<th>Expected Starting Date:</th>
<th>August 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned Duration in months:</td>
<td>24 months</td>
</tr>
</tbody>
</table>

I. Executive Summary:

Future of telecommunication networks is broadband, wireless, ubiquitous, and personal access to a wide variety of applications that include real-time multimedia convergent services such as streaming media, real-time communications, interactive communications, VoIP, and mobile-commerce. These exciting broadband applications are expected to be offered by a number of competing service providers through next-generation wireless all-IP networks (NGN), consisting of several, potentially incompatible, wireless access technologies, such as Wi-Fi, WiMAX, GPRS/EDGE, UMTS WCDMA and cdma2000. Today, users increasingly desire to be ‘always connected’, even when they move from one access network to another. This leads to a crucial requirement for mobility management in the next generation wireless networks so as to ensure the seamless mobility and services/session continuity. Delivering on this vision requires meeting several technical challenges, one of which is the implementation of smart roaming technologies, capable of making seamless transitions within a wireless network as well as across multiple wireless networks. Emerging mobility management solutions are needed to support handovers for both mobile and stationary users. Objective of mobility management function is to provide seamless connectivity across heterogeneous wireless networks. These advanced mobility and roaming capabilities will enhance voice and video experience for users roaming between Wi-Fi networks, or across Wi-Fi, WiMAX, and cellular networks. For mobile users, handovers may occur due to a change in wireless link conditions or a gap in radio coverage area, resulting from movement of mobile node. For stationary users handovers may occur when surrounding environment of the user changes to make one network more attractive than other. Seamless handover should be supported for the user, by which any on-going session or services could continue seamlessly regardless of change of the location ID such as IP address.

At current technology scene, mobile devices with multihome capabilities are proliferating. Multihomed devices possess more than one network interfaces. These devices normally use one network interface at one time and other network interface at some other time. Current communication protocols lack in simultaneous and efficient utilization of these available network interfaces. Multihoming can enable mobile nodes to seamlessly roam across heterogeneous networks. This capability will eventually make mobile users to see isolated heterogeneous networks as a single integrated network. This integration of different network technologies would emerge as a realization of the dream of ubiquitous computing. Along with handoffs for seamless service continuation across heterogeneous networks, data striping for bandwidth aggregation is another horizon on which multihoming can be exploited. Data striping enables multihomed devices to utilize the number of available network interfaces simultaneously.

The most challenging problem associated with seamless handovers is maintaining mobility across heterogeneous networks. There are several approaches to handle mobility across heterogeneous networks that provide seamless handover. These
approaches could be classified into the link-layer, network-layer, and end-to-end transport/session/application layer. The choice of a better scheme for handover support may depend on several factors including the type of mobility considered (e.g., inter-network handover or intra-network handover), the services and application characteristics, and other features of the underlying access networking technologies, etc. Some standards groups have addressed various parts of the mobility issues, such as IEEE 802.21 which provides link layer intelligence to assist mobility, or Internet Engineering Task Force (IETF) mobile Internet Protocol (IP) for layer 3 (L3) mobility. However, these standards still have limitations for providing universal solutions that support seamless integration of these networks. Users on the move would experience service discontinuities, so such standardized solutions can only be regarded as a first step. Further these standard mobility management protocols are not interoperable with one another. There is therefore the need for a common access-independent mobility solution capable of supporting mobility in next-generation networks including multiple administrative domains, heterogeneous access technologies and a rapidly growing number of users.

The objective of this project is to develop an end-to-end framework that would be capable of handling mobility management across heterogeneous networks without requiring additional entities in the network and any change in current implementation of TCP/IP protocols. Moreover, this new framework would also support data striping for bandwidth aggregation by simultaneously utilizing multiple network interfaces resulting in better user throughput and efficient resource utilization. The proposed End-to-end Mobility management Framework (EMF) is designed to operate over the transport layer and attempts to overcome the limitations of current mobility management solutions. As applications specific solution is not an appropriate design choice therefore transport layer or session layer are most appropriate locations for the implementation of EMF framework. This framework is designed in conformance with Internet’s legacy philosophy of “smart-edges simple-network model”. EMF is designed on the principle that if the implementation of network intelligence is present, then end systems should be able to utilize this intelligence, however in the situations where network intelligence is not present; end systems should have sufficient intelligence to continue their service in a seamless way.

This proposal provides the framework for mobility management to support the seamless handover for mobile users and terminals in the next-generation wireless networks (NGN). The proposed mobility framework, EMF, is a comprehensive approach to provide seamless and pervasive end-to-end services across heterogeneous technologies, offering a broad range of pervasive services accessible regardless of the wireless or wired technology. Any user equipped with a multi-home terminal should be able to exploit multiple interfaces at the same time and move transparently from one to the other. The proposal lays down the architecture that allows seamless service continuity across heterogeneous link layer technologies for users who are running applications from their portable computing devices such as laptops, notebooks, personal data assistants (PDAs), smart phones, etc.
2. Objectives of the Project

A. Scope and Introduction of the Project (Abstract):

(Please describe the current state of the art specific to this research topic and the motivation and need for this work.)

A1. Scope

This project seeks to develop an End-to-end Mobility management Framework (EMF) that includes mechanisms, algorithms and components required to provide seamless mobility, enabling service continuity to applications in future all-IP wireless networks. EMF would be able to handle continuous connectivity requirements that may arise due to radio interface changes, address/identifier changes caused by terminal/device mobility, network conditions or user preferences. EMF aims at a comprehensive approach to provide seamless and pervasive end-to-end services across heterogeneous wireless technologies. Mobility management framework involves development of a set of functions that would enable seamless mobility within heterogeneous networks and support for multiple services. These functions may include network detection, network selection, inter-network handovers, location updates and connections with multiple access technologies simultaneously.

A2. Introduction

The ability to exchange voice, video and data, anywhere and anytime, is the basis of a new mobile lifestyle. Customers increasingly desire to stay always connected and enjoy a wide variety of voice, data and multimedia services independent of their geographical location. Continuous and ubiquitous connectivity is becoming interwoven with the lives of end-users, who increasingly rely on their communicators and other mobile devices to provide them with best-in-class service. This phenomenon is being further driven by a rapid proliferation of wireless networking in enterprises and homes, based on Wi-Fi, WiMAX and 3GPP (3rd Generation Partnership Project) standards and availability of multi-network, multifunction devices based on multiple integrated radios.

Telecommunication scenario today is characterized by the co-existence of heterogeneous wired/wireless networks. This heterogeneity relates to multiple types of access technologies ranging from the fixed network solutions, the 2G/3G networks to the IEEE 802.11 and IEEE 802.16, as well as the extension of the existing connection types to ad-hoc, multi-hop and sensor networks. Operators and manufacturers have taken up the development and introduction of multi-homed handsets to permit connectivity across 3G, WiMAX and WLAN-based networks. Figure 1 shows such a popular mobile handset with multiple network interfaces. While the arrival of these multihomed devices promises to drive enhanced voice and multimedia services, support of concurrent multiple radios also spawned unique mobility-related challenges. For better resource utilization, these devices must be capable of automatically detecting and selecting the best network and providing a seamless transition from one network to another.
Seamless connectivity requires mobility management along with support for both homogenous and heterogeneous handovers. Heterogeneous handovers involve transition across different networks such as WLAN, WiMAX and Cellular networks. Homogeneous handovers involve transition across points of attachment (PoA—such as WLAN access points or WiMAX base stations) within the same network. The capability to integrate heterogeneous access infrastructures will be the key to cope with these needs, since it will make it possible to deliver ubiquitous mobility much more efficiently and cost-effectively than realizing a global coverage with a single radio technology. Any user equipped with a multi-homed terminal should be able to exploit multiple access technologies simultaneously and move transparently from one to the other access network.

Although present standards, such as IETF’s Mobile IP or IEEE’s 802.21, specify messaging to enable mobility, they do not provide implementation solution. Moreover, some coordination is required between these mobility entities. However, this coordination has not been addressed by any standards group. Current standards still fall short of providing universal solutions that support seamless integration of diverse access networks. Users on the move will experience service discontinuities, so such standardized solutions can only be regarded as a first step. There is therefore the need for a common access-independent mobility solution capable of supporting mobility in large operational networks including multiple administrative domains, heterogeneous access technologies and a rapidly growing number of users. Emerging mobility solutions are needed to enable handovers and also to enable mobility across multiple points of attachment as changes in user environments make one network more attractive than another.
This research project is an attempt to develop a comprehensive mobility management framework that would enable the multihomed mobile devices to roam across heterogeneous wired/wireless networks for service continuation. Our proposed framework provides both forced as well as willful handovers. Studies of IP traffic patterns show that more than 90% of the Internet traffic uses Transmission Control Protocol (TCP) as a reliable transport protocol [1]. But limitation of TCP is that, it is not capable of exploiting the multihoming property of current mobile devices. Many solutions exist to overcome this limitation of TCP but these solutions either demand the support of additional network entities or require changes in current implementation of TCP. Due to these requirements, network operators and vendors had been reluctant to deploy these solutions on larger scale. The objective of this project is to develop an end-to-end framework that would be capable of handling mobility management across heterogeneous networks without requiring additional entities in the network and also it does not require any change in current implementation of TCP, thus overcoming the limitations of current mobility management protocols e.g. Mobile IP [2], MSOCKS [3], TCP-Migrate [4], etc. Another added advantage of EMF framework is that it inherently provides the facility of data striping for bandwidth aggregation thus improving the resource utilization and better users response.

B. Specific Objectives Being Addressed by the Project:

(Please describe the measurable objectives of the project and define the expected results. Use results-oriented wording with verbs such as 'to develop..', 'to implement..', 'to research..', 'to determine..', 'to identify..' Fill in the relevant sub paras below.)

B1. Research Objectives:

4G networks are opening new possibilities due to integration and merger of conventional telecom infrastructure with data communication protocols, specifically the
Internet Protocol. Deployment of a variety of heterogeneous data networks, like Wi-Fi, WiMAX, Bluetooth, etc. has opened up numerous possibilities for interaction and inter-working. This project aims to address the mobility issues arising in the integrated environment of heterogeneous, all-IP networks, which are mostly mobile and/or using wireless links. Focus of this research project is to explore and exploit the availability of multi-interface mobile devices for better resource utilization, service continuation and integrated operation of different network architectures.

Objective of this EMF project is to develop a framework with the following characteristics:

- To provide both components of mobility management i.e. handover management as well as location management of mobile devices.
- To provide both forced as well as willful handover service for mobile devices.
- To design the soft handovers mechanism for seamless service continuation while moving across heterogeneous networks.
- To develop necessary security services so as to thwart certain network security attacks related to the dynamic updates e.g. session hijacking, denial of service, etc.
- To utilize the link layer intelligence provided by the upcoming IEEE 802.21 MIH function.
- To simultaneously utilize multiple available network interfaces for bandwidth aggregation for bandwidth intensive applications.
- To develop an end-to-end architecture that neither requires support of additional network entities nor demand any change in current implementation of TCP/IP protocols.
- To design a cross layer design for an efficient implementation of the framework.

B2. Academic Objectives:

Following are the academic objective of the EMF project:

- This project would help to flourish the quality R & D culture in the academia. Research publications resulting from the project would improve overall repute/ranking of local academia in the international research community.
- EMF project would create opportunity to conduct applied research in academia rather than just conducting theoretical research.
- Development of an industrially viable product would help to bridge the gap between local industry and academia.
- R & D facilities established during this project, in the form of test bed formation & software tools, would help academia to conduct same sort of future technology projects.
- As EMF is a research oriented project so a number of MS and PhD scholars will be able to complete their research thesis as part of this project.
- The successful implementation of this project will boost the confidence of Pakistani educational and research institutes to conduct the high-tech research with local resources.

B3. Industrial Objectives:

Following are the main areas in which industry (local as well as international) can
benefit from the EMF project:

- **Service Providers/ Operators**
  - Simplified network infrastructure would enable service providers to offer new services without additional cost of extra supporting entities in the network.
  - Seamless vertical handovers would help to bridge gaps in the coverage area of different networks.
  - More utilization of access networks would help to increase the operator’s overall revenues.

- **Software Development Industry**
  - Professionals from the industry would have the opportunity to work in high-tech projects thus; industry professionals would be able to develop skills in networking protocols software development.

- **Vendors/ Manufacturers**
  - More interest in multiple network interfaces would increase sales of multihomed mobile devices. This increased demand would result in increase of industrial growth and creation of more jobs.

B4. Human Resource Development Objectives:

HRD objectives of the project includes the followings:

- This project would provide the internees/ students an exposure to practical research and development activity.
- Project would help to create product design & development experience and improved project management skills for the people from academia.
- Professionals from the industry would have the opportunity to work in high-tech projects thus; industry professionals would be able to develop skills in networking protocols software development.

B5. Other Objectives:

NA

3. Research Approach

A. Literature Review Summary:

*(Give a summary of your literature review in the proposed area with evidence to support the conclusion.)*

As IP networking technology has become cheaply and readily available, and is capable of connecting diverse types of physical networks, it can be a cost-effective solution for networking mobile hosts, with the added benefit of enabling access to the global Internet. A problem with applying the Internet suite in mobile situations, however, is that the protocols were originally not designed to handle the challenges of
mobility. Due to Internet suite’s loose description of duties of specific layers, some unique challenges may arise while providing certain services at multiple layers (e.g., reliability is often present at both the link and transport layers). Some of the services have not been associated with any particular layer (mobility support is one such example). Replication of services at multiple layers is inefficient in terms of computational cost and network resource utilization. Services that do not clearly belong to a particular layer, can pose problems in that their unexpected implementation in lower layers might cause problems at higher layers and be difficult to either detect or disable due to their absence from the poorly defined interfaces between layers.

Mobility affects the whole communication protocol stack, from the physical, data link, and network layers up to the transport and application layers [5]. Examples include radio resource reuse at physical layer, encryption and compression at data link layer, congestion control at transport layer, and service discovery at application layer. Network layer offers routing from one network to another through an independent link. Since mobility is modeled as change in node’s point of attachment, network layer supports mobility by changing the routing of packets destined to the mobile node to arrive at the new point of attachment. There are numerous solutions to cater the mobility management. In the following, these solutions are categorized according to the different layers of the communication protocol stack, at which these solutions operate. First link layer solutions have been discussed. Afterward network layer solutions have been discussed. Almost 70% of the proposed solutions lie in this category which all revolve around Mobile-IP protocol. Some of the researches have proposed the transport layer solutions. SIP-based application layer solutions are also getting popularity in the research community. In the end, new approach of cross layer design for mobility management has also been discussed.

A1. Link Layer Mobility Management Solutions

Most of the wireless access technologies have their own mobility management procedures. E.g. IEEE 802.11 family of WLANs has well defined handover mechanisms [6]. With the introduction of IEEE 802.16e, WiMAX also defines mobility service at link layer [7]. Similarly cellular networks (e.g. GSM, GPRS, CDMA, WCDMA, CDMA2000)
also have mature methods for handling location management and handover management. But almost all the link layer solutions only provide horizontal handoff procedures. There is no mature vertical handoff solution for the link layer. To explain the approaches to manage mobility at link layer let’s take the example of handover procedures of Code Division Multiple Access (CDMA).

A1.1 Preparing for Handover in CDMA

To realize the handover process, a typical CDMA access network defines four types of channel sets [8].

- **Active Set**: The active set contains those channels that are carrying forward traffic to the MS. During normal operation there is usually only one channel in the active set. However, during a soft handover when the MS is communicating with more than one BS, there will be at least two channels in the active set. In CDMA, a forward pilot channel is fully defined by its PN offset index and its frequency assignment.

- **Candidate Set**: The channels that are likely candidates for soft handover are held in the candidate set. A channel is added to this set if its received pilot power exceeds a threshold value $T_{ADD}$ and it is removed if the power falls below a threshold value $T_{DROP}$ for a fixed period of time, or if the channel is transferred to the active set during the handover process.

- **Neighbor Set**: The neighbor set contains pilot channel offsets of BSs that are close to mobile station. Initially this set is composed of channels received in a neighbor list message from the current BS. Members are added to this set in a number of circumstances. For example, a neighbor list update message may be received by the MS. Also, if an active set member, i.e. the current BS, becomes inactive due to a handover, then the current BS is now a neighbor and is added to the list. Finally, if received signal strength of a pilot in candidate set falls below $T_{DROP}$ for a given period of time, then it is also added to the neighbor list. All members of the neighbor set are assigned a variable that relates to their duration in the set. The variable is incremented when a handover occurs, or a neighbor list update message is received. Members are dropped from the set when their age exceeds a threshold, or when they become a member of the candidate set as a result of their pilot power exceeding $T_{ADD}$.

- **Remaining Set**: The final type of channel set is the remaining set. This contains all possible pilot offsets in use on the current CDMA frequency, excluding those contained in other sets.

A1.2 Types of Handover in CDMA

With respect to scope of the mobility CDMA defines following types of handovers:

- **Idle Mode Handover**: An idle mode handover occurs when an MS moves from coverage area of one BS into the coverage area of second BS while MS is in idle mode. MS determines that an idle mode handover should occur when it detects a sufficiently strong pilot channel signal from a BS other than its current BS.

- **Softer Handover**: Handover between two sectors of the same cell is termed as softer handover. During this handover, user data is combined at the BS.

- **Soft Handover**: Handover between two Base Stations is termed as soft handover.
During this handover, user data is combined at the Base Station Controller (BSC). A **soft handover** is used between BSs having CDMA carriers with identical frequency assignments. MS communicates simultaneously with these BSs until it is evident that only one BS is required.

- **Hard Handover:** Hard handovers occur when a mobile is switched between two BSs using different carriers. This handover also occurs when a mobile is switched between IS-95 BS and an AMPS BS.

### A1.3 Message Exchange During Soft Handover:

The messages exchanged between BS and MS during a typical soft handover are:

1. When pilot strength exceeds $T_{ADD}$, mobile station sends a pilot strength measurement message and transfers the pilot to the candidate set.
2. BS sends a handoff direction message.
3. MS transfers the pilot to its active set and sends a handoff completion message.
4. When pilot strength drops below $T_{DROP}$, MS starts the handoff drop timer.
5. When handoff drop timer expires, MS sends a pilot strength measurement message.
6. BS sends a handoff direction message.
7. MS moves the pilot from active set to the neighbor set and sends a handoff completion message.

### A2. IEEE 802.21 (Media Independent Handover - MIH)

IEEE 802.21 WG is developing a specification that facilitates handover optimization between heterogeneous media by providing link-layer intelligence and network information to upper layers.

Working Group was approved in March 2004 and its current scope includes a Media Independent Handover Function (MIHF) consisting of three basic services and corresponding SAPs and primitives:

1. Media Independent Event Service (MIES)
2. Media Independent Command Service (MICS)
3. Media Independent Information Service (MIIS)

Support for multiple access technologies (e.g., IEEE 802.3, IEEE 802.11, IEEE 802.16 and Cellular (3GPP and 3GPP2)) is being considered for both network and device initiated handovers. Specification clearly recommends that mobility across heterogeneous networks should be handled at upper layer of TCP/IP protocol stack.
A3. Network Layer Mobility Management Solutions

Network layer mobility management solutions can be broadly classified into two categories: Macro-mobility and micro-mobility management solutions [9] that are explained below:

A3.1 Macro-Mobility Solutions

The movement of mobile users between two network-domains is referred to as macro-mobility, for example, the movement from domain 1 to domain 2. One domain is an administrative body, which may include different access networks, such as WLAN, second-generation (2G), and third-generation (3G) networks of one service provider. In the Internet, a node is identified by an IP address that uniquely identifies its point of attachment to the Internet, and packets are routed to the node based on this address. Therefore, a node must be located on the network indicated by its IP address in order to receive datagrams. This prohibits the node from moving and remaining able to receive packets using base IP protocol. Mobile IP has been proposed to solve the problem of node mobility by redirecting packets for the mobile node to its current location.

A3.1.a Handoff Management in Mobile IP:

When a Mobile Node (MN) moves from one subnet to another then the handoff procedure is carried out by the following steps [10]:

- MN obtains a new Care-of-Address (CoA) when it enters a new subnet.
- MN registers new CoA with its Home Agent (HA). The HA sets up a new tunnel up to end point of new CoA and removes the tunnel with old CoA.
- Once the new tunnel is set up, afterward HA tunnels packets destined to the MN using MN’s new CoA.
A3.1.b Paging Extension for Mobile IP:
In order to save battery power consumption at MN, IP paging is proposed as an extension for Mobile IP. Under Mobile IP paging, an MN is allowed to enter a power saving idle mode when it is inactive for a period of time. During idle mode, the system knows the location of MN with coarse accuracy defined by a paging area composed of several subnets. MN may also deactivate some of its components for energy-saving purposes. An MN in idle mode does not need to register its location when moving within a paging area. It performs location update only when it changes paging areas. When packets are destined to MN in idle mode, they are terminated at a paging initiator. The paging initiator buffers the packets and locates the MN by sending out IP paging messages within paging area. After knowing the subnet where MN resides, paging initiator forwards data packets to the serving Foreign Agent (FA) of the subnet and further to MN. When an MN is in active mode, it operates in the same manner as in Mobile IP, and system keeps the exact updated location information of MN.

A3.1.c Problems with Mobile IP
Mobile IP has following shortcomings:
- Packets sent from a Corresponding Node (CN) to an MN are first intercepted by HA and then tunneled to MN. However, packets from MN are sent directly to CN. This ‘triangular routing’ problem results in communication routes significantly longer than the optimal routes and introduces extra delay for packet delivery.
- When an MN moves from one subnet to another, new FA cannot inform old FA about the movement of MN. Hence, packets already tunneled to old CoA and those that are in flight are lost.
- Mobile IP is not a satisfactory solution for highly mobile users. Mobile IP requires an MN to send a location update to its HA whenever it moves from one subnet to another. This location registration is required even though the MN does not communicate with others while moving. The signaling cost associated with location updates may become very significant as number of MNs increases. Moreover, if distance, between visited network and home network, is large enough then signaling delay would be large as well. Mobile IP supports mobility across both homogeneous and heterogeneous systems. It is well suited for macro mobility management, but less suited for micro mobility management.
- Mobile IP does not provide any mechanism to simultaneously utilize the availability...
of more than one network interfaces for bandwidth aggregation by data striping.

- Mobile IP requires the presence of extra network entities i.e. home agent and foreign agent thus requiring more network intelligence. Without support of HA and FA, mobile not cannot benefit from the Mobile IP.

A3.1.d Enhancement to Mobile IP

The problem of triangular routing can be solved by ‘Route Optimization’ [11]. The basic idea behind route optimization is to use a direct route between MN and its CN to bypass the HA. CN maintains a binding cache of the CoAs of MN. When CN sends packets to an MN, it first checks if it has a binding cache entry for the MN. If yes, CN tunnels the packets directly to CoA of MN. If no binding cache entry is available, CN sends the packets following the basic Mobile IP procedure, that is, via HA of MN. CN learns about most recent CoA of an MN in either of the following two ways:

- When HA intercepts and tunnels packets destined to an MN, it sends a Binding Update message to the source of packets about current CoA of MN. When tunneled packets reach an FA which no longer has destination MN in its visitor list, FA sends a Binding Warning message to HA asking HA to send a Binding Update message to source node.

- Route optimization also takes care of the ‘packets already tunneled to old CoA’ and in flight. When an MN registers with a new FA, it requests new FA to notify previous FA about movement of MN. This ensures that packets in flight to old CoA are successfully forwarded. It also ensures that packets from CN with out-of-date binding cache entries for MN are successfully delivered to MN’s new CoA. Moreover, route optimization also ensures that any resources consumed by MN at old FA are released immediately, rather than waiting for registration time to expire. Beside these enhancements, some changes to mobile IPv4 have also been proposed [12]. These changes include creating a new error code for use when a Foreign Agent can detect that Home Agent address field is incorrect. Also it prohibited the use of Foreign-Home Authorization Extension on deregistration messages.

A3.1.e Basic Operation of Mobile IPv6

A mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to mobile node within its home subnet prefix on its home link. While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses. A "care-of address" is an IP address associated with a mobile node with a subnet prefix of some foreign link. Mobile node can acquire its care-of address through conventional IPv6 mechanisms, such as stateless or stateful address auto-configuration [13]. As long as mobile node stays in this location, packets addressed to this care-of address will be routed to mobile node. Mobile node may also accept packets from several other care-of addresses, such as when it is moving but still reachable at the previous link.

The association between a mobile node's home address and care-of address is known as "Binding" for mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function
as the "home agent" for mobile node. Mobile node performs this binding registration by sending a "Binding Update" message to the home agent. Home agent replies to mobile node by returning a "Binding Acknowledgement" message.

Any node communicating with a mobile node is referred to as "Correspondent Node" of mobile node, and may itself be either a stationary node or a mobile node. Mobile nodes can provide information about their current location to correspondent nodes. This happens through the correspondent registration. As a part of this procedure, a return routability test is performed in order to authorize the establishment of binding.

There are two possible modes for communications between mobile node and a correspondent node.

- **Bidirectional Tunnelling:** The first mode, bidirectional tunneling, does not require the Mobile IPv6 support from correspondent node and is available even if mobile node has not registered its current binding with correspondent node. Packets from correspondent node are routed to home agent and then tunneled to mobile node. Packets to correspondent node are tunneled from mobile node to home agent ("reverse tunneled") and then routed normally from home network to correspondent node. In this mode, home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to mobile node's home address (or home addresses) on home link. Each intercepted packet is tunneled to mobile node's primary care-of address. This tunneling is performed using "IPv6 encapsulation".

- **Route Optimization:** The second mode, "route optimization", requires mobile node to register its current binding at correspondent node. Packets from correspondent node can be routed directly to care-of address of mobile node. When sending a packet to any IPv6 destination, correspondent node checks its cached bindings for an entry for packet's destination address. If a cached binding for this destination address is found, node uses a new type of IPv6 routing header to route packet to mobile node using care-of address indicated in this binding.

Routing packets directly to mobile node's care-of address allows the shortest communications path to be used. It also eliminates congestion at mobile node's home agent and home link. In addition, the impact of any possible failure of home agent or networks on path to or from is also reduced. When routing packets directly to mobile node, correspondent node sets the Destination Address in IPv6 header to care-of address of mobile node. A new type of IPv6 routing header is also added to packet to carry the desired home address. Similarly, mobile node sets Source Address in the packet's IPv6 header to its current care-of addresses. Mobile node adds a new IPv6 "Home Address" destination option to carry its home address. The inclusion of home addresses in these packets makes use of the care-of address transparent above the network layer (e.g., at the transport layer).

Mobile IPv6 also provides support for multiple home agents, and a limited support for reconfiguration of home network. In these cases, mobile node may not know the IP address of its own home agent, and even home subnet prefixes may change over time. A mechanism, known as "dynamic home agent address discovery" allows a mobile node to dynamically discover the IP address of a home agent on its home link, even when mobile node is away from home. Mobile nodes can also learn new information about home subnet prefixes through the "mobile prefix discovery"
mechanism.

**A3.1.f Addressing Handover Latency**

The ability to immediately send packets from a new subnet link depends on the "IP connectivity latency", which in turn depends on the "movement detection latency" and "new CoA configuration latency". Once an MN is IP-capable on new subnet link, it can send a Binding Update to its Home Agent and one or more correspondents. Once its correspondents successfully process the Binding Update, which typically involves the "Return Routability" procedure, the MN can receive packets at new CoA. So, the ability to receive packets from correspondents directly at its new CoA depends on "Binding Update latency" as well as the "IP connectivity latency" [11].

Mobile IPv6 enables MN to quickly detect that it has moved to a new subnet by providing new access point and associated subnet prefix information when MN is still connected to its current subnet. For instance, an MN may discover available access points using link-layer specific mechanisms (i.e., a "scan" in WLAN) and then request subnet information corresponding to one or more of those discovered access points. MN may do this after performing router discovery or at any time while connected to its current router. The result of resolving an identifier associated with an access point is a [AP-ID, AR-Info] tuple, which MN can use in readily detecting movement. When attachment to an access point with AP-ID takes place, the MN knows the corresponding new router's coordinates including its prefix, IP address, and L2 address. The "Router Solicitation for Proxy (RtSolPr) Advertisement" and "Proxy Router Advertisement (PrRtAdv)" messages are used for aiding movement detection.

Through the RtSolPr and PrRtAdv messages, the MN also formulates a prospective new CoA (NCoA) when it is still present on the Previous Access Router's (PAR) link. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to new subnet link (i.e., New Access Router's (NAR) link) when the MN has received a "Fast Binding Acknowledgment (FBack)" message prior to its movement. If it moves without receiving an FBack, the MN can still start using NCoA after announcing its attachment through a "Fast Neighbor Advertisement (FNA)" message. NAR responds to FNA if the tentative address is already in use thereby reducing NCoA configuration latency. Under some limited conditions in which the probability of address collision is considered insignificant, it may be possible to use NCoA immediately after attaching to new link.

To reduce Binding Update latency, Mobile IPv6 specifies a tunnel between Previous CoA (PCoA) and the NCoA. An MN sends a "Fast Binding Update" message to its Previous Access Router to establish this tunnel. When feasible, the MN should send an FBU from PAR's link. Otherwise, it should be sent immediately after attachment with NAR. As a result, PAR begins tunneling packets arriving for PCoA to NCoA. Such a tunnel remains active until the MN completes the Binding Update with its correspondents. In the opposite direction, MN should reverse tunnel packets to PAR until it completes the Binding Update. PAR should forward the inner packet in tunnel to its destination (i.e., to MN's correspondent). Such a reverse tunnel ensures that packets containing PCoA as a source IP address are not dropped due to ingress filtering. It should be noted that even though MN is IP-capable on new link, it cannot
use NCoA directly with its correspondents without the correspondents first establishing a binding cache entry (for NCoA). Forwarding support for PCoA is provided through a reverse tunnel between the MN and the PAR.

A3.2 Micro-Mobility Solutions

Mobile nodes usually move frequently between subnets of one domain. To reduce signaling load and delay to home network during movements within one domain, many micro-mobility solutions have been proposed. They can be broadly classified into two groups: tunnel-based and routing-based micro-mobility schemes:

- **Tunnel-based schemes** use local or hierarchical registration and encapsulation concepts to limit the scope of mobility-related signaling messages, thus reducing global signaling load and handoff latency. Mobile IP regional registration (MIP-RR), hierarchical Mobile IP (HMIP) [14], and intra-domain mobility management protocol (IDMP) [15, 16] are tunnel-based micro-mobility protocols.

- **Routing-based schemes** maintain host-specific routes in routers to forward packets. Host-specific routes are updated based on host mobility. Cellular IP (CIP) [17] and handoff aware wireless access Internet infrastructure (HAWAII) [18] are routing-based micro-mobility protocols.

In the following we will describe Hierarchical Mobile IPv6 as a working example of the protocols for handling micro-mobility.

A3.2.a Hierarchical Mobile IPv6

HMIPv6 concept is simply an extension to the Mobile IPv6 protocol [11]. HMIPv6 introduces a new Mobile IPv6 node, called “Mobility Anchor Point” (MAP). It is used and can be located at any level in a hierarchical network of routers, including the Access Router (AR). Unlike Foreign Agents in IPv4, a MAP is not required on each subnet. A Mobility Anchor Point is a router located in a network visited by mobile node. The MAP is used by MN as a local HA. One or more MAPs can exist within a visited network. The MAP will limit the amount of Mobile IPv6 signalling outside the local domain. Introduction of MAP reduces signaling overhead and handover latency in the following way:

- Mobile node sends Binding Updates to local MAP rather than HA and CNs.
- Only one Binding Update message needs to be transmitted by MN before traffic from HA and all CNs is re-routed to its new location. This is independent of the number of CNs that MN is communicating with.

A MAP is essentially a local Home Agent. The aim of introducing hierarchical mobility management model in Mobile IPv6 is to enhance the performance of Mobile IPv6 while minimizing the impact on Mobile IPv6 or other IPv6 protocols. It also supports Fast Mobile IPv6 Handovers to help MNs for achieving seamless mobility [19].

A mobile node entering a MAP domain will receive Router Advertisements containing information on one or more local MAPs. MN can bind its current location (on-link CoA) with an address on the MAP’s subnet (RCoA). Acting as a local HA, MAP will receive all packets, on behalf of mobile node it is serving, and will encapsulate and forward them directly to mobile node's current address. If mobile node changes its current address within a local MAP domain (LCoA), it needs to register new address with MAP
only. Hence, only the Regional CoA (RCoA) needs to be registered with correspondent nodes and the HA. The RCoA does not change as long as the MN moves within a MAP domain. This makes the mobile node's mobility transparent to correspondent nodes it is communicating with.

![Hierarchical Mobile IPv6](image)

**Fig.6 – Hierarchical Mobile IPv6**

**A4. Transport Layer Mobility Management Solutions**

Mobility solutions described so far allow mobile nodes to move between subnets, or to change interface thus enabling vertical handoffs but they do not support the simultaneous use of multiple interfaces, nor do they have the ability to specify which interface each individual type of traffic should be carried on. There are some other limitations of the network layer mobility management solutions e.g. these solutions cannot support some mobility services e.g. session mobility. To support such services upper layer information is required thus such mobility services are provided at the transport or session layer of the protocol stack. Moreover pure network layer solutions do not provide the willful handovers. To overcome these limitation/drawbacks many researchers has proposed the transport layer mobility management solutions. [20] provides a good survey of such transport layer solutions. This survey categorize transport layer solutions in four categories i.e. i) Connection Migration Protocols, ii) Handoff Protocols, iii) Gateway Based Mobility Schemes, & iv) Mobility Manager.

Connection Migration protocols are not in real sense the mobility management protocols as they do not provide necessary mobility management service i.e. handoff management. Rather they provide the mechanisms that can aid the mobility management protocols. Examples of such protocols include Freeze TCP and TCP-Redirection. TCP-R however also proposes to use DNS as location manager. As both Freeze-TCP and TCP-R do not specify the handoff procedure therefore we will not discuss these protocols in this proposal. Radial Reception Control Protocol (R2CP), Mobile Multimedia Streaming Protocol (MMSP) and Mobile-SCTP (mSCTP) are the transport layer protocols that provide the handoff service to the mobile devices. Moreover these protocols also support IP diversity. But they do not specify the location
management procedures for mobile servers. In the following we will describe the working of Cellular-SCTP (cSCTP) as an example of this class of protocols [21]. cSCTP is an enhanced version of the mSCTP protocol. Most important drawback of gateway based mobility management solutions is that they require the support of some additional entity in the network, thus making such solution infrastructure dependent. As such intermediate entities i.e. mobility gateway or proxy, need to process the packet at intermediate location thus causing conflict with some of the security protocols. Examples of such solutions include MSOCKS, Indirect TCP, M-TCP, M-UDP and BARWAN. MSOCKS is more mature of this class of protocols so in the following we describe the working of MSOCKS+ protocols [22]. Seamless IP diversity based Generalized Mobility Architecture (SIGMA) and TCP-Migrate are the transport layer protocols that provide complete mobility management solutions as both of these protocols provide handoff management as well as location management for mobile servers. Moreover they do not require the support of any additional network entity in the network infrastructure. In the following we provide the working of TCP-Migrate as an example of this class of protocols.

A4.1 Cellular SCTP

Stream Control Transmission Protocol (SCTP), from 3GPP, has been accepted by IETF as a general-purpose transport layer protocol [23]. SCTP is designed to transport PSTN signaling messages over IP networks, but is capable of broader applications. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- Acknowledged error-free non-duplicated transfer of user data
- Data fragmentation to conform to discovered path MTU size
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages
- Optional bundling of multiple user messages into a single SCTP packet
- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association

The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks. The protocol has TCP like features of reliable service delivery over IP network. Besides these features, it has other features that support mobility such as partial reliability, multi-homing & multi-streaming.

- **Partial Reliability**: Partial reliability mechanism allows SCTP to configure the reliability level. This helps, for example, traffic that has high QoS requirements and has only a limited time to live.
- **Multi-Homing**: Using multi-homing SCTP allows a MN to specify a set of IP addresses as primary IP addresses and another set as secondary IP addresses, along with a port number for primary and secondary set, to the CN and/or HA. This way one of the addresses can be used as secondary address. The protocol also allows the deletion and addition of new addresses on the fly. In this way, when a handover is detected, the secondary address can be automatically used.
- **Multi-Streaming**: SCTP multi-streaming allows data to be partitioned into multiple streams, and each stream to be sequentially delivered to the destination end point independently of other streams. Hence, a packet loss in one stream does not incur head-of-line blocking to other streams.
SCTP-based vertical handover schemes do not require additional components in the network such as home/foreign agents or SIP server. Therefore, it provides a network-independent solution, which is always preferred by the service providers [24].

![SCTP Header with 'H' Flag](image)

**Fig.7 – SCTP Header with ‘H’ Flag**

In Cellular SCTP (cSCTP), a Mobile Node (MN) has three main components [21]:

- **Host-Agent Component**: Host-Agent component communicates with Access Router(s) (ARs) mainly to help cSCTP component learn about reaching a new AR and/or leaving previous AR.
- **cSCTP component**: The cSCTP component is basically an SCTP protocol entity with dynamic address reconfiguration extension plus handover procedure. The Correspondent Node (CN) also needs to have a cSCTP component.
- **SIP User Agent**: To facilitate mobility management, there is a SIP User Agent running at application layer of both MN and CN.

Moreover, each AR will need to support a neighbor discovery protocol. Cellular SCTP handover works as follows:

- Detecting and obtaining a new IP address
- Adding new IP address into association
- Data transfer during handover
- Deleting old IP address from association

**A4.2 Proxy-based Transport Layer Solution**

MSOCK+, Transport Layer Mobility architecture is built around a proxy that is inserted into communication path between mobile node and static correspondent node [3, 22]. For each data stream from mobile node to static correspondent node, the proxy is able to maintain one stable data stream to/from the static host, isolating it from any mobility issues. Meanwhile, proxy can simultaneously make and break connections to mobile node as needed to migrate data streams between network interfaces or subnets. MSOCKS+ protocol is designed to allow roaming within an enterprise network. It may be possible to extend it to handle global roaming, by designing an inter-proxy protocol, but the need for such an extension seems to be limited at this point, since MSOCKS+
does not expect the users to keep their laptops powered while moving to remote locations.

Proxy-based architecture places an intermediate unit called a proxy in the communication path between mobile node and the servers with which mobile node’s applications converse. Proxy can then mediate communication between server and client, and provide services on behalf of either. As examples of possible proxy services, proxies can: provide processing resources the client may not have; reformat information from the server to fit the mobile node, such as resizing GIF images for small screens; or use compression to reduce the bandwidth required between the mobile node and proxy, which is frequently a low quality link. Since the proxy is typically under the control of the same organization that owns the mobile nodes it serves, the proxy can be configured to support the peculiarities of its population of mobile nodes. The servers that mobile nodes access may be under the control of other organizations, who have little incentive to change their code to support the newest mobile nodes.

Most proxies operate on a split-connection model, where mobile nodes desiring to communicate with static server first make a connection to the proxy and tell it which server they want to communicate with. Proxy makes a second connection to static server and then reads data from one connection and writes it into the other, thereby allowing the client and server to communicate. Each logical communication session between mobile node and server is split into two separate TCP connections. Proxies can support mobility by providing a way of switching mobile-proxy connection while maintaining proxy-static connection unchanged. Imagine a mobile node starting a TCP connection while using its wired network interface, so that the connection between mobile node and proxy uses mobile node’s wired IP address as its endpoint. If mobile node is disconnected from its wired network, it could potentially contact proxy using IP address of its radio interface and ask proxy to subsequently copy data from server-proxy connection to new mobile-proxy-via-radio connection, instead of the old mobile-proxy-via-wire connection. In this way, mobile node can migrate its sessions from one network interface to the other. The case in which mobile node moves from one subnet to another subnet on same interface can be handled in the same way, so long as the mobile node can obtain an address for use on that subnet via a protocol such as DHCP or stateless address autoconfiguration in IPv6 [25], [26], [13].

Each network interface on mobile node has its own IP address. We can therefore control over which interface data would travel from static to mobile node by choosing IP address used by mobile node as its endpoint in mobile-proxy connection. We can also control network interface over which data moves in opposite direction, from mobile to static server, by assigning the proxy several IP addresses — it does not matter which interface on proxy the addresses are bound to. Mobile node creates a host route for each of proxy’s addresses, such that packets sent to that address would go out a different interface of mobile node. Mobile node can choose which interface that data to proxy will flow out by picking appropriate proxy address as peer address for mobile-proxy connection.

Communication session composed of two TCP connections spliced together appears to mobile and to static server as a single TCP connection, and so is defined in terms of IP addresses and port numbers of connection’s endpoints. Thus, changing endpoint address of an existing session effectively breaks the session. Connecting and
reconnecting two connections, normally risks the loss of any data in flight while reconnection is in progress, which would breach end-to-end semantics of logical mobile-to-server communication session. MSOCK+ is built around a technique called TCP Splice. TCP Splice allows the machine where two independent TCP connections terminate to splice two connections together, effectively forming a single end-to-end TCP connection between endpoints of two original connections. Although two TCP connections appear as a single TCP connection, the protocol cannot cope with IP layer cryptography, like IPSEC. Therefore higher layer crypto protocols like SSL and TLS would be used with MSOCK architecture.

MSOCK+ architecture consists of three pieces:

- A user-level MSOCKS proxy process running on proxy machine.
- An in-kernel modification on proxy machine to provide TCP Splice service.
- A shim MSOCKS library that runs under the application on mobile node.

No modifications are required in static server application, static server kernel, mobile node kernel, or Mobile application.

**A4.3 TCP Migrate**

In [4] a new end-to-end TCP option has been designed to support secure migration of an established TCP connection across an IP address change. Using this option, a TCP peer can suspend an open connection and reactivate it from another IP address, transparent to application that expects uninterrupted reliable communication with peer. In this design, security is achieved through the use of a connection identifier, or token, which may be secured by a shared secret key negotiated during initial connection establishment. The presented idea is general and can be implemented in a like manner for specific UDP-based protocols such as Real-time Transport Protocol (RTP) to achieve seamless mobility for those protocols as well.
The proposed Migrate TCP option is included in SYN segment, that identifies a SYN packet as part of a previously established connection, rather than a request for new connection. This Migrate option contains a token that identifies previously established connection on same destination_address – port pair. Token is negotiated during initial connection establishment through the use of Migrate-Permitted option. After successful token negotiation, TCP connections may be uniquely identified by either their traditional (source address, source port, destination address, destination port) 4-tuple, or a new (source address, source port, token) triple on each host. Mobile node may restart a previously established TCP connection from new address by sending a special Migrate SYN packet that contains the token identifying previous connection. Static host would than re-synchronize the connection with mobile node at new end point. A migrated connection maintains same control block and state (with a different end point, of course), including sequence number space, so any necessary retransmissions can be requested in standard way.

A4.4 Other Transport Layer Protocols

Tsukamoto [27] proposed a transport layer mobility management protocol that can support multiple connections. This solution also support multihoming and is able to perform soft handover. Multiple connections also enable the bandwidth aggregation thus efficiently utilizing the system resources. Solution also supports a cross layer mechanism *Interlayer Signalling Pipe (ISP)* that provides data link interface information to the upper layer for facilitating the handover decisions. Although cross layer nature of Tsukamoto solution support lower layer information but current protocol does not specify the usage of IEEE 802.21 Media Independent Handover function. Other limitation of this solution is that it does not support the willful handovers that would play vital role in a multi-subscription 4G environment. Moreover this solution is not a complete mobility management solution in a sense that it does support the location management. Applications are not transparent to this solution and support at both ends i.e. at mobile node as well as corresponding node is required to utilize this solution.

A5. Session Layer Mobility Management Solutions

Landfeldt et al. presented a session layer end-to-end mobility management solution [28]. SLM was designed with the provision of QoS management in mind. It introduces a new semantic where open data streams are treated as being separate sessions. This new semantic can provide necessary system support for application that demand some specific operational environment. In its current proposal, solution does not support the handovers however it has the support for location management through a *User Location Server (ULS)*. ULS is an additional network entity along with DNS server. So in this sense it is a drawback of SLM that it requires another support entity in the network infrastructure. Other drawbacks of SLM are that it does not have any mechanism to exploit the multihoming property of modern mobile devices. Also it is not capable of providing the bandwidth aggregation. It also does not specify any cross layer mechanism that may be capable of utilizing the lower layer intelligence for making the efficient mobility management decisions. Applications using SLM for mobility management are not transparent. Further more SLM require changes at both ends i.e. at mobile node and corresponding node for facilitating the mobile nodes. In
short although SLM provides a rudimentary session layer model but it is not mature enough to be declared as a complete mobility management solution for upcoming 4G heterogeneous wireless networks.

A6. Application Layer Mobility Management Solutions

Conceptually 4G wireless network architecture can be viewed as many overlapping wireless Internet access domains. In this heterogeneous environment, a mobile node is equipped with multiple (often called multi-mode) wireless interfaces to connect to any or all of the wireless access networks, anytime, anywhere. Dependency of mobility management protocols on access networks reduces progressively as we move up on the protocol stack. Application layer protocols are transparent to lower layer characteristics. They maintain true end-to-end semantics of a connection and are expected to be right candidate for handling mobility in a heterogeneous environment. SIP has been accepted by Third Generation Partnership Project (3GPP) as a signaling protocol for setting up real-time multimedia sessions [29]. SIP is not only capable of supporting terminal mobility but also session mobility, personal mobility and service mobility. Therefore, SIP seems to be an attractive candidate as an application layer mobility management protocol for heterogeneous 4G wireless networks [30]. However, SIP uses TCP or UDP to carry its signaling messages and hence is limited by the performance of TCP or UDP over wireless links. In addition, SIP entails application layer processing of messages, which may introduce considerable delays. These are prime factors behind handoff delays while using SIP as mobility management protocol.

Performance of SIP as a mobility management protocol in a heterogeneous access-networking environment, predicted for 4G wireless networks, has been investigated in [31]. In particular, a case study has been performed on SIP-based handoff delay analysis using SIP to handle terminal mobility in an IP-based network. Two different types of access technologies i.e. UMTS and IEEE 802.11b based WLAN have been considered for IP-based network. Analytical results show that for WLAN networks, handoff delay is suitable for streaming media but for UMTS network, minimum handoff delay does not meet the specifications. More precisely, handoff to an UMTS network from either another UMTS network or a WLAN, introduces a minimum delay of 1.4048 seconds for 128 kbps channel, while a handoff to a WLAN access network from another WLAN or an UMTS network, the minimum delay is 0.2 ms. Clearly, in former case the minimum delay is unacceptable for streaming multimedia traffic and requires deployment of soft-handoff techniques to reduce handoff delay and keep it within a desirable maximum limit of 100 ms. As indicated in [32], 3GPP implementation of SIP is optimized for the 3G wireless telecommunication environment and has some minor differences with IETF SIP specification. In a 4G heterogeneous all-IP environment these differences can arise some interoperability issues that are needed to be addressed.
A6. Cross Layer Mobility Management Solutions

A number of cross-layer solutions have also been proposed for mobility management. A cross-layer manager is introduced in [33] that interacts with multiple layers of communication protocol stack to create an inter-layer coordination model. This idea is further extended in [34] in form of Mobility Manager. This Mobility Manager utilizes IEEE 802.21 Media Independent Handover (MIH) events, commands & information from the lower layers [35] and provides handover commands to Mobile IPv6. Furthermore, Mobility Manager also provides notifications to upper layers for application adaptations. Both of these solutions use MIPv6 for mobility management that has inherent limitations of requiring number of network entities. MIPv6 also doesn’t support data striping. A cross layer decision model has been recently proposed in [36] to facilitate the vertical handovers. But this solution has not specified the procedures for handover and location management of mobile nodes.

Fig. 9 – Cross Layer Coordination Plane for Mobility Management

Fig. 10 – Cross Layer Mobility Manager
B. Development / Research Methodology:

(Please describe the technical details and justification of your development and research plan.)

Although almost all wireless access technologies e.g. IEEE 802.11 WLAN, IEEE 802.16 WiMAX, GSM/GPRS, WCDMA/CDMA2000, etc. have their own well-defined handover procedures, as described in previous section, but these procedures are applicable only when mobile nodes move from one cell to another cell of the same access technology. This is known as horizontal handoff. For handovers from one type of access network to a different type of access network, upper layer solutions are usually incorporated. This kind of handoff is known as vertical handoff [37]. Most prominent upper layer mobility management solution is Mobile-IP that is a network layer solution. Variants of Mobile-IP (MobileIPv4 as well as MobileIPv6) provide solutions for both macro and micro mobility management. Although these are most mature among all mobility management solutions, they have some limitations that are common to all the variants of network layer solutions. First, end-nodes using Mobile-IP require some supporting entities in network to support end-node’s mobility; examples include home agent, foreign agent and mobility anchor point (MAP) [14]. This means that users would demand more functionality from the network. We argue that mobility is such a service that can be effectively provided without sacrificing the “smart-edges simple-network” theme of Internet. Secondly, not all kind of mobility services can be implemented at network layer. For example, session mobility from one terminal to another terminal requires some upper layer processing that cannot be implemented at network layer [27]. Thirdly, Mobile-IP is not able to exploit multihoming for bandwidth aggregation by data striping [38].

Many researchers believe in end-to-end handling of mobility management thus provide solutions at transport layer of TCP/IP protocol stack. Examples of such solutions include TCP-Migrate [4], MSOCKS [3], [22], pTCP [39] and SCTP [23]. TCP-Migrate, pTCP and MSOCKS require changes in current implementation of TCP. Moreover, for MSOCKS, in order to splice TCP connection, an additional entity i.e. proxy is required in network. SCTP, with its mSCTP [24] and cSCTP [21] extensions, has good potential to cater mobility management issues in an elegant manner. But problem for applications running over TCP is still unsolved. Solutions also exist that resolve these issues at session layer. For example [40] discusses the advantages of implementing bandwidth aggregation/data striping at session layer, but mobility management was not discussed in it. Session Initiation Protocol (SIP) also facilitates mobility services with its location update option [29], [30]. SIP has gained popularity in the 3GPP community, but SIP too does not provide complete set of mobility services [31]. SIP implementation of 3GPP is optimized for cellular networks thus some minor differences exists between IETF’s SIP and 3GPP’s SIP. In heterogeneous 4G wireless networks, these differences can create interoperability issues [32]. SIP also requires some additional network entities e.g. Proxy Server, Registrar, etc. Moreover, SIP does not provide mobility solution for applications using TCP.

This project of End-to-end Mobility management Framework (EMF) is an attempt to overcome the limitations of current mobility management solutions. As link layer and network layer solutions has some inherent limitations therefore, EMF framework is designed to operate at the upper layers. But as applications specific solution is also not an appropriate design choice therefore transport layer or session layer are most
appropriate locations for the implementation of EMF framework. Our framework is designed in conformance with Internet’s legacy philosophy of “smart-edges simple-network model”. The simple, flexible and scalable design along with deployment of low cost equipment enabled Internet to emerge as a blockbuster of the century. Earlier network designers strongly believed in the design that most of the intelligence should be implemented in end nodes. At that time the major concern of Internet was to merely provide the connectivity. However with the advancements in computing as well as communication technologies, user expectations from communication networks has changed to a large extent. Today’s user demand services like mobility, quality of service, security, etc. that were not provided by Internet in early ages. In order to provide such services, network designers are putting more and more intelligence in network [41]. It emerged as a hot debate that whether the intelligence should be implemented in network or in end hosts [42]. However, in spite of changing network requirements, many researchers still believe in End-to-End design philosophy of Internet [43]. Rather than waiting for the settlement of this “end-to-end or network intelligence debate”, our EMF framework is designed on the principle that if the implementation of network intelligence is present, then end systems should be able to utilize this intelligence, however in the situations where network intelligence is not present, end systems should have sufficient intelligence to continue their service in a seamless way. In the following first, we described the design objectives and then the technical details of our EMF framework.

B1. Design Objectives of EMF Framework

Although basic objective of a mobility management protocol is to provide handoff management and location management services to mobile nodes, however to develop an efficient and comprehensive mobility management framework, we draw following guidelines that serve as design objectives of End-to-end Mobility management Framework (EMF):

i) If network intelligence is present then end nodes can utilize this intelligence for mobility management. However, if network support is not present then EMF framework should overcome this limitation and enable mobile nodes to manage the mobility.

ii) EMF framework should be designed in conformance with the end-to-end design philosophy of Internet. It should not require any extra entity in network to provide mobility service.

iii) Objective of EMF framework should be to facilitate the TCP rather than to change the current implementation of TCP.

iv) Applications using TCP, as reliable transport protocol, should continue having confidence of reliable data delivery for applications using EMF framework.

v) Current standards lack in providing willful handovers. Therefore EMF framework should overcome this limitation and should support both forced handover as well as willful handover.

vi) In order to provide service continuation, EMF framework should support soft handoffs. At upper layers it can be provided in the form of connection diversity.

vii) Mobile node should remain able to serve as mobile server. So, EMF framework should also provide location management service.

viii) Overhead regarding handoff and location management should be minimized.
ix) EMF framework should provide minimal handoff delays.
x) Applications that do not require mobility support should not incur mobility support overhead.
x i) Appropriate security measures should be taken to avoid certain security attacks regarding handoff and location update messages e.g. session hijacking attacks, denial of service attacks, etc.
x ii) As current mobile devices possess multiple network interfaces therefore, along with providing vertical handoffs, EMF framework can also efficiently utilize the presence of these multiple network interfaces for supporting other services e.g. data striping for bandwidth aggregation.


The architecture of EMF framework is shown in figure 11. This architecture includes three main components:

i) EMF Core Protocol
ii) EMF Host Agent
iii) EMF User Agent

B2.1 EMF Core Protocol

EMF Core Protocol consists of two sub-parts:

i) EMF Control
ii) EMF Data Handler

EMF Control part would be used to exchange handover messages among communicating peer hosts. EMF Control would also be responsible for sending location updates using secure DNS dynamic update messages [44], [45]. While EMF Data Handler would have ability to simultaneously handle multiple data streams.

EMF control part establishes an association between two EMF aware applications. By “EMF aware” we mean that end hosts have implementation of EMF framework and applications are using this framework. Each EMF association is identified by a unique identifier. A single EMF association can have multiple TCP connections. The emphasis is on reliable delivery of user data rather than on conservation of TCP connection. Due to network interface change or location change, if TCP connection is affected, then EMF Control establishes a new TCP connection with same previous association identifier but with possibly new network layer/transport layer identifiers. It is responsibility of EMF Data Handler to assure in-sequence reliable transportation of user data. In [46], similar theme is used by SCTP-based solution that maintains multiple streams for a single association.
Whenever an EMF compliant client requests a TCP connection, EMF Core Protocol holds the connection request and checks whether the peer end is also EMF compliant or not by sending an EMF Association Initiation Request to corresponding server. EMF control messages like Association Initiation Request and Association Change Request messages are of request-response type messages where no bulk data transfer is required. Therefore, these control messages can be exchanged over UDP [47]. This design choice reduces the latency that would be involved in establishing the subsequent data connection. If client does not receive positive EMF response, it concludes that peer end is not EMF compliant and proceeds with a normal TCP connection establishment for user’s request. However, if peer end responds as EMF compliant, then both ends will agree on certain parameters. One such parameter is the unique EMF association ID. Client can send it in Association Initiation Request message. To make sure the uniqueness, this ID can be derived from parameters like random number, client’s IP address, timestamp, etc. The peer end should check that this suggested ID has not been used for any already established association. Although probability of having such match is rare but still if found then peer end can send its suggested unique association ID to client node. In this way, peer entities can agree on unique ID. This ID needs to be unique only among mutually communicating parties and need not be globally unique. Due to certain security concerns (e.g. session hijacking) some Public-Key cryptographic procedures may be adopted to assure the uniqueness, randomness and secure agreement of association ID. For example, algorithms like Elliptic Curve Cryptosystems for shared key exchange may be used to establish the shared association ID among peer nodes [48].
After agreement on association parameters, client can now initiate TCP connection as per user's request. In this way an umbrella of EMF association is established beneath which multiple TCP connections can be maintained as depicted in figure 14. There are two main objectives of this umbrella association. First is to hide the effects of mobility from user application. On change of network interface address, EMF Control part initiates handover mechanism and establishes a new TCP connection with the previous association ID but with new IP address. Details of this handover mechanism are discussed in subsequent sections. Second objective of EMF umbrella association is data striping for bandwidth aggregation. For files with considerably larger size, EMF Core Protocol divides the file in number of chunks and then transmits these different chunks on multiple TCP connections via multiple available network interfaces simultaneously. EMF Data Handler will assure the in-order delivery of transmitted data to user application. Software components that will constitute the EMF Control and EMF Data Handler part are depicted in the diagrams 12 and 13 respectively.

**B2.2 EMF Host Agent**

EMF Host Agent is the entity that collects local host information and statistics that are helpful for handover procedure. Primary objective of EMF Host Agent is to assist EMF Core Protocol for handovers. Two kind of handover decisions are possible: i) Forced Handovers & ii) Willful Handovers.

Forced handovers are handovers in which mobile terminal has no other choice except to handover its connection to the only available network. This kind of handovers are usually required when mobile terminal moves away from the network in which it has initiated the connection and enters in coverage area of another network. As previous network is no more accessible, thus in order to enjoy the service continuation, mobile terminal is forced to handover its connection to new network. These forced handovers are most often triggered due to changes in lower layer parameters. EMF Host Agent is responsible to monitor these changes of lower layer parameters. Events corresponding to these changes e.g. include access router discovery, obtaining new IP address or usage of IEEE 802.21 events/triggers.
Willful-handovers are initiated, for example, when application or user preferences, obtained from upper layers demand connection migration. With multihomed mobile devices in heterogeneous 4G wireless environment, mobile users would have subscription to a number of network operators. If user has access to multiple networks simultaneously, then handover decisions would largely be affected by user preferences. User preferences would depend upon parameters like available bandwidth, quality of operator’s service, cost of connection, etc. This type of handover is called Willful Handover. EMF Host Agent is required to interact with upper layers in order to get necessary information to initiate willful handovers. Current mature mobility management solutions, e.g. Mobile-IP variants, lack this facility of willful handovers. In this regard, our proposed solution is comprehensive enough to incorporate both types of handovers i.e. forced as well as willful handovers.

As EMF Host Agent is required to interact with multiple layers of network protocol stack, an efficient and optimized implementation design choice is the cross-layer solution. Figure 11 depicts the interaction of EMF Host Agent with corresponding layers of protocol stack. At lower layer, it interacts with IEEE 802.21 MIH layer, and at application layer, it interacts with EMF User Agent to get user preferences. On the basis of this information, it interacts with EMF Control module to assist the handover procedure. In its design, EMF Host Agent can be seen as cross-layer manager of [33] and mobility manager of [34]. Difference, however, is that the cross-layer manager and mobility manager interact with Mobile-IPv6 as mobility management protocol, while EMF Host Agent interacts with EMF Control module for mobility management.

**B2.3 EMF User Agent**

To assist willful handovers, we propose that there should be an application layer utility that would interact with users. We call such utility as EMF User Agent. User can provide the details such as connection subscriptions, preferences, default settings, etc. in two ways: one is manual and other is automated. It is likely that users will not be changing their network subscriptions and preferences frequently, e.g. on daily or hourly basis. Hence, users are required to interact with EMF User Agent only when there is a change in user’s network subscription or there is a change in user’s preferred or default network interface. These changes may be affected by a number of
parameters e.g. service levels provided by network operator, monetary cost of connections, availability of a particular type of access network, etc. On the basis of these parameters, user can define its default and alternative network interfaces. EMF User Agent must be able to provide the status information of ongoing connections to the user. Status information might include, for example, current data rate, packet loss ratio, estimated time to complete the transfer of current data (e.g. in case of file transfer) and the available alternative links on which the ongoing connections can be migrated. It is responsibility of EMF Host Agent to provide such information to EMF User Agent. As this information would be available, the user, if not satisfied by the performance of currently serving link, can initiate the transfer of connection to an alternative link. This is a scenario of willful handover. EMF Core Protocol is responsible to handle connection migration under such willful handovers.

To avoid frequent user interventions and to automate the migration procedure, some service level thresholds can be defined. User would be able to change these thresholds any time. Whenever these thresholds are crossed, a notification may be sent to EMF Host Agent and in turn EMF Host Agent can trigger EMF association change procedure.

B2.4 Interaction between EMF Host Agent & IEEE 802.21 MIH layer

IEEE 802.21 is being developed in an effort to standardize an abstraction layer that would provide Media Independent Handover (MIH) function for enabling handover and interoperability between heterogeneous networks [34]. Objective of the standard is to simplify handover management for multihomed mobile devices having not only wired and wireless IEEE network interfaces but also having 3GPP and 3GPP2 cellular network interfaces. MIH function basically provides three services i.e. i) Media Independent Event Service, ii) Media Independent Command Service & iii) Media Independent Information Service.

Applications subscribe to the event service, and in response to this subscription, both local and remote events are notified to the upper layer. These events may include “Link parameter change”, “Link Up”, “Link Down”, etc. Command service is responsible for gathering status information of connected links. Commands can be used to poll the connected links for their status and to configure new links. Information service can be used to provide information about available networks and services they provide. As shown in Figure 11, EMF Host Agent interacts with 802.21 MIH function for these three services and on basis of information received by MIH function, EMF Host Agent can notify EMF Control module for initiation of EMF association change procedure.

B3. Handovers with EMF Architecture

Whenever EMF Host Agent notices some change i.e. change in IP address or change in user preferences, it signals this change to EMF Control module. EMF Control checks the ongoing EMF associations and sends an EMF Association Change message to peer node. In order to avoid session hijacking attacks, this association change message includes the previous association ID. After necessary authentication, peer EMF Control updates its EMF association parameters. Then a new TCP connection is established with new parameters. EMF Data Handler will maintain
sequence numbers for assuring in-order delivery of user data over multiple TCP connections.

B3.1 Managing Forced Handovers

Forced handover scenarios can occur when mobile node is moving out of the coverage area of serving network and entering in the coverage area of another network. In such situations, user has only one working IP address and has no other option except to migrate the connection to new network. When mobile node discovers new network and gets new IP address, EMF Host Agent detects this change and triggers the EMF association change message.

B3.2 Managing Willful Handovers

Willful handover scenarios can occur when a node has access to more than one network, e.g. simultaneous access to Ethernet, WLAN, WiMAX, GPRS, etc. As depicted in figure 1, modern mobile terminals (Laptops, PDAs, etc.) possess more than one network interfaces. User may wish to use one network interface at one time and other network interface at other time or may wish to utilize all available network interfaces simultaneously. As discussed earlier, such decisions may be triggered from upper layers. Whenever user manually gives commands to EMF User Agent to initiate handover or when serving network’s parameters cross preferences threshold, this information is passed to EMF Host Agent. EMF Host Agent then notifies EMF Control to initiate EMF association change procedure. We assume that the acquisition of new IP addresses for each network interface is implicit. Dynamic Host Configuration Protocol (DHCP) may be used for acquiring IPv4 addresses [25] and in case of IPv6 as underlying network protocol, either DHCPv6 (for tighter control over address assignment) or IPv6 address autoconfiguration can be used for generating globally unique IPv6 addresses [26], [13]. Under already established EMF association, EMF Control initiates new TCP connection using new IP address but with previous association ID.

B4. Location Management with EMF Architecture

Handover management, described in previous section, is only one component of mobility management. Second major component of mobility management is location management of mobile nodes. Although location management may not be an issue for mobile nodes that act only as clients, however, it is a concern for the nodes that also act as server. When a mobile server changes its location, its IP address also changes. DNS dynamic updates provide the facility to dynamically update the name-address mapping of the hosts [44]. BINDv8 and BINDv9 (Berkeley Internet Name Domain) provide the implementation of DNS dynamic update standard [49]. Many mobility management solutions have used the DNS dynamic update option for tracking location of mobile servers [4], [50]. In most cases, DHCP server sends DNS dynamic update message describing the changes in assignment of IP addresses. But if there is no DHCP server and IP addresses are generated using IPv6 address autoconfiguration [13], mobile nodes would be allowed to send DNS dynamic updates. In this case, when EMF Host Agent detects the change of IP address, it issues a command to EMF Control to send a DNS dynamic update message. Sending of this DNS dynamic
update message doesn’t affect the ongoing connection(s) because the problem for maintaining ongoing connection(s) is resolved with EMF handover mechanisms as described in previous section. Location update mechanism is helpful for new connection requests only.

In contrast to the initial concerns regarding the scalability and overhead involved in DNS dynamic updates, studies proved viability of using DNS dynamic updates [46]. Incremental zone transfer of DNS data helps to reduce the update overhead [51]. Moreover, Notify option is useful for reducing the delays involved in the dynamic updates [52]. The security concerns regarding DNS dynamic updates has been addresses in [45]. For authentication purposes, secure DNS dynamic updates require the use of Transaction Signature (TSIG) Message Authentication Code (MAC) and SIG(0) public-key encryption. A minor issue regarding the use of shared secret key based TSIG MAC algorithm is that, the real time distribution of shared secret key is expensive. So we suggest the usage of digital certificates for DNS message integrity. However, this performance optimization of authentication/integrity of DNS update messages is out of scope of this project.

B5. Handling Network Security Issues

While designing a new framework we always keep two important aspects regarding security issues in mind. First is that new framework should not create any conflict with existing network security protocols e.g. IPsec or SSL/TLS. And the other is that new framework should not introduce new network security concerns. In the following we discuss both of these aspects in some detail:

B5.1 Conflicts with Existing Network Security Protocols

For network security services currently IPSec and SSL/TLS are being largely used on Internet. IP Security (IPSec) is a network layer security solution that provides authentication and confidentiality services to the IP traffic [53]. IPSec provides authentication service through the Authentication Header (AH) protocol. AH provides the data integrity, data origin authentication and limited anti replay services. While Encapsulating Security Protocol (ESP) provides the authentication as well as confidentiality services to the IP traffic. Both of these protocols can be used in either transport mode or tunnel mode. A security association (SA) is established from sender to the receiver for using either of these AH or ESP protocol. SA is a unidirectional association thus for full duplex communication, two SAs are needed to be established in both the directions. Each SA is uniquely identified by three parameters that are: i) Security Parameter Index, ii) Destination IP address & iii) AH or ESP identifier.

Mobility Management protocols that require the processing of IP packets at some intermediate node i.e. at proxy or gateway causes conflicts with IPSec datagrams especially when used in tunnel mode of IPSec. [20] discusses such protocols in detail. Thus MSOCKS, Indirect TCP, M-TCP & BARWAN causes to create conflict with such security protocols. As EMF framework does not require any intermediate entity for providing mobility service thus EMF does not create any conflict with such security protocols. However one of the identifier for uniquely identifying the IPSec SA is destination IP address and in a mobility scenario this IP address is likely to be changed. Therefore, with every change in IP address, one-way IPSec association i.e.
from fixed node to mobile node is needed to be re-established. And other way SA i.e. from mobile node to fixed node will remain unchanged. It is quite valid to establish a new SA for some ongoing session. IPSec itself recommend to establish a new SA in a number of scenarios e.g. if soft lifetime of SA would have expired then Internet Key Exchange (IKE) protocol is invoked for establishing a new SA. Similarly if the sequence number field of IPSec header would have overflowed then again IKE is invoked to establish a new SA. As establishing a new SA is allowed therefore whenever a mobile node acquires new IP address it invokes IKE for establishing a new SA. This provision does not require any change in current implementation of IPSec. However for highly mobile environments IPSec can be optimized to dynamically add/delete IP addresses in a given SA. Provision for this optimization is already there, as IPSec allows more than one IP addresses for a given SA. However this optimization is out of scope of this EMF project.

SSL/TLS is a transport layer protocol that provides security services to the upper layer data. Transport Layer Security (TLS) is enhanced version of Secure Socket Layer i.e. SSLv3.1. SSL/TLS architecture contain four protocols i.e. i) SSL Record Protocol, ii) SSL Handshake Protocol, iii) SSL Change Cipher Spec Protocol, and iv) SSL Alert Protocol [54]. SSL maintains session between two communicating peer entities. This SSL session is established by the SSL Handshake Protocol. Transport layer connections are established under this SSL session. SSL maintains session and connection states to identify and properly process the secure web traffic. As these session and connection states do not use network layer identifier i.e. IP address to identify the session or connection thus the change of IP address of a mobile node does not create any conflict with the SSL/TLS security mechanism.

Tunneling techniques are used in many mobility management protocols. This tunneling can cause conflicts with many network security procedures e.g. ingress filtering at the firewalls. These tunneling techniques are normally used by the network layer mobility solutions. As transport layer solutions in general and our EMF framework in particular does not use tunneling techniques thus there is no such conflict with ingress filtering at the firewalls.

B5.2 Introducing New Security Concerns

Mobility management solutions generally require update messages to be sent to the corresponding node or some intermediate nodes. It is possible that some attacker would misuse these messages for hijacking ongoing data sessions. An attacker can send binding update message to indicate corresponding nodes that mobile node has changed its location and subsequent packets would be delivered to the new location (attacker’s location). Therefore, proper authentication of update messages is necessary to avoid such hijacking attacks. EMF project uses these authenticated update mechanism for both location update messages as well as for handover messages. For location update messages EMF framework uses the Secure Dynamic DNS Updates. And for authenticated handover updates, EMF uses the Association Identifier. This association identifier is unique within the communicating host systems. This identifier is exchanged with cryptographically secure mechanism using for example public key cryptographic algorithms. Public key cryptographic methods e.g. Diffie Hellman Key Exchange Protocol, Elliptic Curve Cryptographic (ECC) Key Exchange Mechanism, etc. have been used to securely exchange the share session keys. In EMF project we will
use such algorithm for exchanging the shared EMF association identifier. Although this shared identifier would not be used for any encryption however this association identifier is used in subsequent EMF association update messages. These association update messages are actually used for handovers in the EMF framework. Therefore it can be said the EMF framework has been designed by keeping the session hijacking attacks in mind and enough cryptographic primitives has been used to counter such attacks. Hence in its current context EMF framework is resilient enough and does not introduce any new security vulnerability in overall data communication architecture.

B6. Qualitative Comparison With Existing Solutions

End-to-end Mobility management Framework (EMF) has been designed in the light of guidelines provided in section B1 of proposed development / research methodology. These guidelines set the attributes that are desirable for any mobility management solutions for 4G heterogeneous wireless networks. Before actual implementation, development and testing we provide a qualitative analysis that depict the services provided by current mobility management solutions and set of services provided by the EMF framework. We will see that there are many services that are non-existing in other protocols, so in that case we can compare EMF with other protocols. In such cases our EMF framework has a clear advantage on already proposed mobility solutions. However for those mobility services that are common in EMF framework and in other mobility solutions, a detailed quantitative performance analysis is required. But such analysis would be possible only after the development of this project. Until actual implementation of EMF project only qualitative comparison can be provided. As a research activity we also plan to develop simulation modules of this project so that off line simulation can be performed. Moreover we also plan to develop some mathematical / stochastic models for the analytical performance analysis of the EMF framework. It will not only enable us to compare our EMF framework analytically with other already proposed solutions but also provide us the tool for performance tuning of different components of EMF framework and thus achieving the optimal performance of the framework. Although analytical performance modeling is not part of this ICT R&D EMF project however, this is part of our long-term research plan on EMF framework.

Although in literature review section we had identifies many shortcomings / limitations of current mobility management solutions in general. Here we provide a qualitative comparison table depicting the number of services provided by our EMF framework and other transport layer and upper layer mobility management solutions. Table 1 clearly depicts the advantage of EMF framework in terms of set of mobility services provided by this mobility solution. The only shortcoming of EMF framework is that in its current form it is not application transparent. We are doing research in devising the methods to make this EMF framework as application transparent. Such schemes may include the techniques like interception/translation of called APIs and/or to use web browser based solutions. Web based solutions may incorporate the proposed EMF architecture within the web browser. Beside this application transparency limitation, which can be overcome via above-mentioned techniques, our EMF framework has clear advantage of providing much richer set of mobility services. Specialty of EMF framework is the provision of services like Willful Handover, Bandwidth Aggregation, Support of upcoming IEEE 802.21 MIH function, etc. such services are not present in current mobility management solutions. Thus in this way EMF framework overcome the limitations of current mobility management protocols.
Table-1: Comparing desirable services provided by End-to-End protocols

<table>
<thead>
<tr>
<th>Services</th>
<th>EMF</th>
<th>SLM</th>
<th>Tsukamoto</th>
<th>MSOCKS</th>
<th>TCP- Migrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willful Handovers</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Soft Handovers</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Bandwidth Aggregation</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Location Updates</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Support of 802.21 MIH function</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Cross Layer Manager</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Multihoming</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Require changes in TCP</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Require additional network entities</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Application Transparency</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Support required at both Ends</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

B7. Summary of Research & Development Plan

Following areas have been identified in which extensive research is required:

1. Exploration of commands, events, information and interfaces provided by IEEE 802.21 MIH function and the ways to utilize this function with EMF Host Agent.
2. Research on devising a mechanism for establishment and exchange of Association Identifier in a secure manner probably using cryptographic primitives.
3. Research on developing a Handover Manager and defining message exchange format as well as parameters that would be exchanged through these messages.
4. Research on developing a Location Update Manager that would be able to interact with DNS server in a secure manner.
5. Research on designing an efficient Bandwidth Aggregation function that would be able to exploit the multihomed property of mobile devices.
6. Research on development of an efficient Soft Handover function above transport layer by the way of connection diversity mechanism.
7. Research on designing a reliable function that would ensure the in-order delivery of user data in a connection diversity environment.

From the software development perspective, we identify following core software components that would constitute the EMF framework:

1. EMF Host Agent
2. EMF User Agent
3. Interface with IEEE 802.21 MIH function
4. EMF Control Module
4.1 Secure Association Establishment Module
4.2 Handover Manager
4.3 Location Update Manager

5. EMF Data Handler Module
   5.1 Bandwidth Aggregation Handler
   5.2 Soft Handoff Handler
   5.3 Sequenced Delivery Handler

C. Project Activities:
(Please list and describe the main project activities, including those associated with the transfer of the research results to customers/beneficiaries. The timing and duration of research activities are to be shown in the Gantt chart in Section 7.)

Complete research and development of EMF framework project is estimated to span up to two (2) years. Complete implementation of the project can be partitioned into four (4) logical phases of six (6) months each. A set of deliverables is defined, to be produced at the end of each phase. These phases can be identified as following:

Phase-1 = Project Setup, Research and Planning Phase
Phase-2 = Prototype Development Phase
Phase-3 = Integration & Optimization Phase
Phase-4 = Portability Testing, Documentation & Final Release Phase

Testing of EMF framework will follow the standard software testing techniques. At the completion of phase 1 of the project, detailed test cases will be designed for EMF framework software testing. These test cases will be used rigorously throughout the subsequent phases of the project. In phase 2 and 3, White Box testing techniques will be used, in which procedures are examined in detail. Logical paths through the software are tested by providing test cases. And in the end i.e. during phase 4 thorough Black Box testing will be used to test the operational functionality of the project [55].

Phase-1 – Research, Planning & Setup Phase

Following tasks will be performed in phase-1 of the project:
- Project Setup
- Requirements Identification
- Team Setup and specification of responsibilities of each team member
- Project Planning, Equipment purchase
- Research Phase will include an extensive research on the areas identified in section 3.B.5 - Summary of Research and Development Plan, that are:
  - Exploration of IEEE 802.21 Media Independent Handover (MIH) function
  - Designing a secure mechanism for establishment and exchange of Association Identifier
  - Designing Handover Manager and message exchange along with parameters included in these handover messages
  - Designing Location Update Manager for transmission of secure DNS dynamic updates in appropriate situations
  - Designing a Bandwidth Aggregation mechanism on the transport layer
  - Designing an efficient mechanism to make sure the soft handoffs
  - Designing a reliable function for sequenced delivery of user data
Phase-2 – Prototype Development Phase
Following activities will be performed in second phase of the project:
- Software Development Plan of the project
- EMF Prototype Development
  - EMF Host Agent component
  - EMF User Agent component
  - Secure Association Establishment Module
  - Handover Manager
  - Location Update Manager
  - Bandwidth Aggregation Handler
  - Soft Handoff Handler
  - Sequenced Delivery Handler
- Development of framework components for simulations
- Monitoring of Development Plan in the light of EMF Design Objectives

Phase-3 – Integration & Optimization Phase
Following activities will be performed in third phase of the project:
- Testing and verification of EMF components through simulations
- Test bed formation
- Integration of individual components developed in phase-2 of the project
- Prototype testing with standard software testing tools and mechanisms
- Framework re-evaluation in the light of results obtained in testing phase and updation of the architecture, if required
- Optimization of framework functions

Phase-4 – Portability Testing, Documentation & Final Release Phase
Following activities will be performed in fourth and final phase of the project:
- Portability Testing of EMF framework on different platforms
- Design Document featuring design structure and design philosophy of the complete EMF framework
- Software Packaging
- User Manual explaining the EMF User Agent user interface
- Installer Guide
- Developers Guide explaining script/APIs provided by the EMF framework for application developers
- Technical Report along with performance analysis and comparison with other competitive mobility management solutions for multihomed mobile devices
- Release Document featuring implementation details and testing summary
- Final Release

Summary of tasks performed in each phase is given in the table below.
Table-2: Project Phases along with major tasks in each phase

<table>
<thead>
<tr>
<th>Phase-1</th>
<th>Requirements Identification, Planning, Setup</th>
<th>ADS, DDS</th>
<th>Research on areas identified in section 3.B.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase-2</td>
<td>Development Plan</td>
<td>EMF Prototype Development</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Phase-3</td>
<td>Test bed Formation</td>
<td>Integration of Components</td>
<td>Prototype Evaluation, Updation &amp; Optimization</td>
</tr>
<tr>
<td>Phase-4</td>
<td>Portability Testing</td>
<td>Packaging</td>
<td>Documentation</td>
</tr>
</tbody>
</table>

D. Key Milestones and Deliverables:

(Please list and describe the principal milestones and associated deliverables of the project. A key milestone is reached when a significant phase in the project is concluded, e.g. selection and simulation of algorithms, completion of architectural design and design documents, commissioning of equipment, completion of test, etc.) The timing of milestones is also to be shown in the Gantt chart in Section 7.

The information given in this table will be the basis of monitoring and release of funds by the National ICT R&D Fund.

Phase-1 – Milestones and Deliverables

Milestones:
A-1: Detailed description of roles of individual project team member
A-2: Summarizing the research work and design of mechanisms and algorithms for the solution of problem areas identified in section 3.B.5
A-3: Describing the Architecture Design Specification (ADS) of EMF framework
A-4: Describing the Detailed Design Specification (DDS) of EMF framework
A-5: Explaining the goals and objectives of the EMF project in full detail

Deliverables:
A-D1. Report describing the Architecture Design Specification (ADS) of EMF framework
A-D2. Report describing the Detailed Design Specification (DDS) of EMF framework

Phase-2 – Milestones and Deliverables

Milestones:
B-1: Report describing complete development plan of the project
B-2: Software implementation of EMF prototype. This includes the following core components of the EMF framework:
   B-2-a: Implementation of EMF Host Agent
   B-2-b: Implementation of EMF User Agent
B-2-c: Implementation of Secure Association Establishment function for EMF Control Module
B-2-d: Implementation of Handover Manager for EMF Control Module
B-2-e: Implementation of Location Update Manager for EMF Control Module
B-2-f: Implementation of Bandwidth Aggregation Handler for EMF Data Handler Module
B-2-g: Implementation of Soft Handoff Handler for EMF Data Handler Module
B-2-h: Implementation of Sequenced Delivery Handler for EMF Data Handler Module

Deliverables:
B-D1: Code, software implementation of EMF prototype

Phase-3 – Milestones and Deliverables

Milestones:
C-1: Report describing the details of Test bed formation for the project
C-2: Report describing the testing and evaluation results of EMF framework
C-3: Report describing the updation and optimization of EMF prototype in the light of design objective of the project
C-4: Code Updated and optimized, software release of prototype

Deliverables:
C-D1: Report describing the updation and optimization of EMF prototype
C-D2: Updated and optimized software code of prototype

Phase-4 – Milestones and Deliverables

Milestones:
D-1: Portability test results
D-2: Final software release Package
D-3: Installer Guide
D-4: User manual explaining the EMF User Agent user interface
D-5: EMF framework design document
D-6: Developer’s guide explaining the script/APIs provide by EMF framework for developers developing the mobility aware user applications
D-7: Release document describing the implementation details and testing summary of EMF framework

Deliverables:
D-D1: Final software release package
D-D2: EMF framework design document
D-D3: Installer Guide
D-D4: User manual explaining the EMF User Agent user interface
D-D5: Developer’s guide

Following table shows the summary of tasks, milestones and deliverables for each of the four (4) phases, along with the expected time to complete each phase of the project:
<table>
<thead>
<tr>
<th>No.</th>
<th>Elapsed time from start (in months) of the project</th>
<th>Milestone</th>
<th>Deliverables (Labeled as mentioned above)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>6 months</td>
<td>Requirement Analysis, Planning, Setup, Research, Architecture Design Specifications (ADS), Detailed Design Specification (DDS)</td>
<td>A-D1, A-D2</td>
</tr>
<tr>
<td>2.</td>
<td>12 months</td>
<td>EMF Prototype Development</td>
<td>B-D1</td>
</tr>
<tr>
<td>3.</td>
<td>18 months</td>
<td>Test bed Formation, Integration, Framework Evaluation, Prototype Updation, Optimization</td>
<td>C-D1, C-D2</td>
</tr>
<tr>
<td>4.</td>
<td>24 months</td>
<td>Portability Testing, Packaging, Documentation, Final Release</td>
<td>D-D1, D-D2, D-D3, D-D4, D-D5</td>
</tr>
</tbody>
</table>

4. Benefits of the Project

A. Direct Customers / Beneficiaries of the Project:

(Please identify clearly the potential customers/beneficiaries of the research results and provide details of their relevance, e.g. size, economic contribution, etc.)

Multiple segments of the society would be the direct beneficiaries of this EMF project.

- **End Users**
  - End users already having multihomed mobile devices but currently are not able to enjoy full range of benefits from multihoming property. This project will help them to efficiently utilize the existence of these multiple network interfaces.
  - Vertical handovers across different networks would enable end users to enjoy seamless continuation of services
  - Dynamic location updates would enable end users to be reachable irrespective of their location
  - Willful handovers would enable end users to benefit from different access technologies according to their preferences in an efficient and cost effective manner.
  - Bandwidth aggregation would enable end users to enjoy better throughput experience for data rate intensive applications.

- **Service Providers/ Operators**
  - Simplified network infrastructure would enable service providers to offer new services without additional cost of extra supporting entities in the network.
  - Seamless vertical handovers would help to bridge gaps in the coverage area of different networks.
  - More utilization of access networks would help to increase the operator’s overall revenues.

- **Vendors/ Manufacturers**
  - More interest in multiple network interfaces would increase sales of multihomed mobile devices. This increased demand would result in increase of industrial growth and creation of more jobs.
B. Outputs Expected from the Project:

Following would be the outputs from the EMF project:
- Software patch for EMF services.
- Application for the facilitation of willful handovers.
- Complete documentation along with user as well as developer’s guide.
- Research publications in internationally reputed conference/magazines/journals.
- Internet Drafts of EMF framework for IETF standardization

C. Organizational / HRD Outcomes Expected:

Organizational Benefits
- This project would help to flourish the quality R & D culture in the academia. Research publications resulting from the project would improve overall repute/ranking of local academia in the international research community.
- EMF project would create opportunity to conduct applied research in academia rather than just conducting theoretical research.
- Development of an industrially viable product would help to bridge the gap between local industry and academia.
- R & D facilities established during this project, in the form of test bed formation & software tools, would help academia to conduct same sort of future technology projects.

HRD Benefits
- This project would provide the internees/ students an exposure to practical R & D activity.
- Project would help to create product design & development experience and improved project management skills for the people from academia.
- Professionals from the industry would have the opportunity to work in high-tech projects thus; industry professionals would be able to develop skills in networking protocols software development.

D. Technology Transfer / Diffusion Approach:

(Please describe how the outputs of the project will be transferred to the direct beneficiaries/customers. Please also state if the project outputs are sustainable, i.e. if they can be utilized without further external assistance.)

Following components would help the technology transfer developed during the project development:
- EMF project will be released as open source thus enabling a large community to benefit from the outcomes of the project.
- Comprehensive documentation including user manual, installation guide, developer’s kit, etc. would accompany the final release of the project.
- Research Publications in reputed international conferences and journals.
- A very convenient way of technology transfer / diffusion in Internet community is to standardize EMF framework by the IETF body. After complete implementation/development/testing of EMF framework, we plan to submit Internet Drafts as our
standardization effort. Effort to get EMF framework be approved as IETF RFC (Request for Comments) is included in our long-term research plan. As recognition of a protocol as IETF RFC is a time taking effort thus for the time being RFC standardization is not part of this project. However research / development will pave the way towards the IETF RFC of EMF framework.

- HRD from academia as well as industry would help to further propagate the skill developed during the project.
- Trainings/seminars/workshops can be arranged to disseminate the finding/results of conducted research.
Annexure A – Curriculum Vitae

Please provide relevant information and also attach CVs of key research / development personnel (if available) and PD, JPD.

A. Professional Information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Name: Dr. Amir Qayyum</td>
</tr>
<tr>
<td>2.</td>
<td>Title or Position Held: Professor</td>
</tr>
<tr>
<td>3.</td>
<td>Experience: (yrs) 12 years</td>
</tr>
<tr>
<td>4.</td>
<td>Email Address: <a href="mailto:aqayyum@ieee.org">aqayyum@ieee.org</a></td>
</tr>
</tbody>
</table>

B. Research Papers in Relevant Area

- A. Qayyum, Comparison of CSMA and CSMA with Active Signaling in Wireless LANs, Proc. 6th Open Workshop on High Speed Networks (HSN’97), Stuttgart, Germany, 8-9 October 1997
- A. Qayyum, L. Viennot and A. Laouiti, Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks, 35th Hawaii International Conference on System Sciences (HICSS-35) Big Island, Hawaii, USA, 7-10 January, 2002
Conference (Joint ICN 2002 and ICWLHN 2002), Atlanta, USA, 26-29 August, 2002


- A. Qayyum and F. Amjad, Internet Gateway Connectivity using OLSR protocol on MANET nodes, 2nd International Conference on Information Technology and Applications (ICITA 2004), Harbin, China, 8-11 January, 2004

- A. Iqbal and A. Qayyum, Algorithmic Techniques for Unidirectional Link Support in Mobile Ad Hoc Networks, IASTED International Conference on Parallel and Distributed Computing and Networks (PDCN 2004), Innsbruck, Austria, February 17-19, 2004


- Paul Muhlethaler, Mikael Salaun, Amir Qayyum, and Yasser Toor, Comparison Between CSMA and Aloha Throughput in Multihop Ad Hoc Networks, Proceeding of the 2004 International Conference on Wireless Networks (ICWN'04), Las Vegas, USA, June 21-24, 2004 (also available as INRIA Research Report http://www.inria.fr/rrrt/rr-5129.html)


- Farooq Umer and Amir Qayyum, Architecture for De-centralized, Distributed Event Communication Mechanism through Overlay Network, Proceeding of the 2005 International Conference on Emerging Technologies (ICET’05), Islamabad, Pakistan, September 17-18, 2005

<table>
<thead>
<tr>
<th>C. Courses Taught in Relevant Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Computer Communication and Networks</td>
</tr>
<tr>
<td>• Computer Network Security</td>
</tr>
<tr>
<td>• Advanced Computer Networks</td>
</tr>
<tr>
<td>• Mobile Networking</td>
</tr>
<tr>
<td>• Network and System Programming</td>
</tr>
<tr>
<td>• Multimedia Services over IP Networks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D. Thesis / Projects Supervised in Relevant Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Architecture for Decentralized and Distributed Event Management Mechanism for Ubiquitous Computing Environments Using Overlay Networks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E. Grants Received in Relevant Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>• National ICT R&amp;D Grant for the project “Design &amp; Implementation of the Core Components of 4G Telecom Infrastructure”, November 2007</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F. Industrial Work Done in Relevant Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title: Design and development of long-range, mesh-based secure mobile ad hoc network for tactical communication</td>
</tr>
<tr>
<td>From: 2003 To: 2004</td>
</tr>
<tr>
<td>Position held: Senior Member Technical (CARE Pvt Ltd)</td>
</tr>
<tr>
<td>Description of the Project: Design of the complete architecture of a long-range MANET, development of all routing and communication protocols plus actual deployment of a robust and secure network providing communication between mobile and stationary nodes in a military environment</td>
</tr>
<tr>
<td>Major output(s): Design document, functional code, complete running and operational mobile ad hoc network</td>
</tr>
</tbody>
</table>

| Title: Networking protocol stack for a RISC based packet processor |
| From: 2001 To: 2003 |
| Position held: S.M.T.S. (Enabling Technologies) |
| Description of the Project: Design and implementation of a complete TCP/IP protocol stack for a RISC-based packet processor. The stack included all companion IP protocols (ICMP, IGMP, ARP, etc.), RTP and RTCP for real time voice/video transport, IPSec for security, IP Precedence and |
DiffServ for Quality of Service, MP and PPP for serial link communication, RoHC and CRTP for header compression, plus AAL2 and AAL5 for IP to ATM interface

Major output(s): Design documents, functional code

Title: Simulation, implementation and deployment of multi-hop mobile ad hoc network

From: 1996
To: 2000
Position held: Research fellow (INRIA, France)

Description of the Project: Simulation of several MANET routing protocols (AODV, OLSR, DSR, TBRPF, TORA, etc.) for performance comparison, then implementation of a proactive routing protocol (OLSR) on Linux, and then actual deployment of a MANET (at INRIA Rocquencourt) using this OLSR protocol for multi-hop communication

Major output(s): Simulation code on MoWiNet and NS-2, research papers, multiple Internet Drafts and RFC 3626, protocol stack of OLSR on Linux and WindowsNT, OLSR test bed of 10s of routers at INRIA
## A. Professional Information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name:</td>
</tr>
<tr>
<td></td>
<td>Dr. Shahzad A. Malik</td>
</tr>
<tr>
<td>2</td>
<td>Title or Position Held:</td>
</tr>
<tr>
<td></td>
<td>Associate Professor</td>
</tr>
<tr>
<td>3</td>
<td>Experience: (yrs)</td>
</tr>
<tr>
<td></td>
<td>11 years</td>
</tr>
<tr>
<td>4</td>
<td>Email Address:</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:smalik@comsats.edu.pk">smalik@comsats.edu.pk</a></td>
</tr>
</tbody>
</table>

## B. Research Papers in Relevant Area

- Shahzad Malik and Djamal Zeghlache, "Dynamic Rate Adaptation for Packet Data in Mixed Services WCDMA Networks", Proceedings of CIC 2001, October 30 - November 02, 2001, Seoul, South Korea.
• Saleem Akhtar, Shahzad Malik and Djamal Zeghlache, "Prioritized admission control for mixed services in UMTS WCDMA networks", IEEE PIMRC, September 30 - October 3, 2001, San Diego, CA, USA.

C. Courses Taught in Relevant Area

• Mobile Broadband Networks
• Mobile Cellular Networks
• Mobile Computing
• Advanced Computer Networks
• Wireless Communications
• Computer Network Design and Systems Security
• Selected Topics in Computer Networks and Distributed Systems
• Performance Evaluation of Computer Networks

D. Thesis / Projects Supervised in Relevant Area

• Mobility Management in heterogeneous wireless networks
• Seamless Handoff using Layer 2 triggers based on IEEE 802.21 MIH
• Performance analysis and QoS in IEEE 802.16 WiMax Networks
• Differentiated Services in IEEE 802.11 based Wireless LANs
• Radio Resource Management and Quality of Service (QoS) Provisioning for Multimedia in UMTS mobile cellular networks
• Performance Analysis of SCTP and DCCP for Video Transport over Heterogeneous Network
• Performance Evaluation of DCCP and SCTP for MPEG4 over wireless networks
• Comparison of Energy Efficient MAC Protocols for Wireless Sensor Networks
• Seamless Handoff Performance and analysis in Mobile IP
• QoS and performance in IEEE802.11 WLANs
• TCP performance in MANETs - Mobile Ad Hoc Networks

E. Grants Received in Relevant Area

<type here>

F. Industrial Work Done in Relevant Area
Nortel Networks/ INT, Evry, France - Collaboration Project for GPRS Simulator, designed and developed software modules in OPNET Modeler and C/C++ for GPRS RLC/MAC and LLC layer protocols in Nortel Network’s future generation mobile network testbed (GPRS Simulator); Integrated, tested and validated the code with other protocol modules developed in house by Nortel.
Annexure B – References

34. F. Cacace & L. Vollero, "Managing Mobility and Adaptation in Upcoming 802.21 enabled Devices", In Proceedings of the 4th International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, Los Angles, CA, USA, 2006
37. J. Manner & M. Kojo, "Mobility Related Terminology", RFC 3753, IETF, June 2004
41. M. S. Blumenthal & David Clark, "Rethinking the design of the Internet: The End-to-End Arguments vs. the Brave New World", ACM Transactions on Internet Technology, Vol. 1, No. 1, August 2001
42. M. Yabuksi, T. Okagawa & K. Imai, "Mobility Management in All-IP Mobile Network: End-to-End Intelligence or Network Intelligence", IEEE Radio Communications Magazine, December 2005
44. P. Vixie, S. Thomson, Y. Rekhter & J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, IETF, April 1997
46. T. Goff & D. Phatak, "Unified transport layer support for data striping and host mobility", IEEE Journal on Selected Areas in Communications, Volume 22, Issue 4, Pages 737-746, May 2004
52. P. Vixie, "A mechanism for Prompt Notification of Zone Changes (DNS Notify)", RFC 1996, IETF, January 1996
Annexure C – Additional List of Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>4G</td>
<td>4th Generation wireless network</td>
</tr>
<tr>
<td>ADS</td>
<td>Architecture Design Specification</td>
</tr>
<tr>
<td>AMPS</td>
<td>Advanced Mobile Phone Service</td>
</tr>
<tr>
<td>AR</td>
<td>Access Router</td>
</tr>
<tr>
<td>BS</td>
<td>Base Station</td>
</tr>
<tr>
<td>BSC</td>
<td>Base Station Controller</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CIP</td>
<td>Cellular IP</td>
</tr>
<tr>
<td>CN</td>
<td>Corresponding Node</td>
</tr>
<tr>
<td>CoA</td>
<td>Care of Address</td>
</tr>
<tr>
<td>DAB</td>
<td>Downlink Audio Broadcast</td>
</tr>
<tr>
<td>DDS</td>
<td>Detailed Design Specification</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DVB</td>
<td>Downlink Video Broadcast</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data rate for GSM Evolution</td>
</tr>
<tr>
<td>EMF</td>
<td>End-to-end Mobility management Framework</td>
</tr>
<tr>
<td>FA</td>
<td>Foreign Agent</td>
</tr>
<tr>
<td>FBack</td>
<td>Fast Binding Acknowledgement</td>
</tr>
<tr>
<td>FBU</td>
<td>Fast Binding Update</td>
</tr>
<tr>
<td>FNA</td>
<td>Fast Neighbor Advertisement</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communication</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>HAWAII</td>
<td>Handoff Aware Wireless Access Internet Infrastructure</td>
</tr>
<tr>
<td>HMIP</td>
<td>Hierarchical Mobile IPv6</td>
</tr>
<tr>
<td>HSDPA</td>
<td>High Speed Downlink Packet Access</td>
</tr>
<tr>
<td>IDMP</td>
<td>Intra Domain Mobility management Protocol</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineering</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IS-95</td>
<td>Interim Standard 95</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>L2</td>
<td>Layer 2 of communication protocol stack</td>
</tr>
<tr>
<td>LCoA</td>
<td>Local Care of Address</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobility Anchor Point</td>
</tr>
<tr>
<td>MIH</td>
<td>Media Independent Handover</td>
</tr>
<tr>
<td>MIP-RR</td>
<td>Mobile IP Regional Registration</td>
</tr>
<tr>
<td>MN</td>
<td>Mobile Node</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Station</td>
</tr>
<tr>
<td>NAR</td>
<td>New Access Router</td>
</tr>
<tr>
<td>NCoA</td>
<td>New Care of Address</td>
</tr>
<tr>
<td>PAR</td>
<td>Previous Access Router</td>
</tr>
<tr>
<td>PCoA</td>
<td>Previous Care of Address</td>
</tr>
<tr>
<td>PoA</td>
<td>Point of Attachment</td>
</tr>
<tr>
<td>RCoA</td>
<td>Regional Care of Address</td>
</tr>
<tr>
<td>SAP</td>
<td>Service Access Point</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunication System</td>
</tr>
<tr>
<td>WCDMA</td>
<td>Wideband CDMA</td>
</tr>
<tr>
<td>WG</td>
<td>Working Group</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
</tbody>
</table>