TOWARDS MOBILITY ENABLED PROTOCOL STACK FOR FUTURE WIRELESS NETWORKS

Fawad Nazir, Aruna Seneviratne National ICT Australia (NICTA), Australia University of New South Wales (UNSW), Australia
{fawad.nazir,aruna.seneviratne}@nicta.com.au

ABSTRACT

Future wireless networks have two widely accepted characteristics. Firstly, they will be based on all-IP based network architecture and secondly they will integrate heterogeneous wireless access technologies. As a result, there exist today a multitude of solutions aimed at managing these imminent challenges. These solutions are at varying stages of deployment, from purely analytical research, to experimentally validated proposals, right through to fully standardised and commercially available systems. In this paper we discuss the meaning, requirements, responsibilities and solutions for mobility management on all seven layers of the OSI communication stack. We identify internet mobility requirements and perform valuable three dimensional analyses between internet mobility requirements, mobility management protocols and layers of OSI communication stack. We also quantify types of mobilites possible in the future wireless networks and associate them with the responsible layers. In the end we conclude that no single layer in the OSI stack is responsible to completely address all the internet mobility requirements and support all the mobility types. We strongly believe that every layer has its own responsibilities in order to support mobility. Therefore in order to deal with mobility challenge we should have a "*Mobility Enabled Protocol Stack*" instead of mobility management solution on a specific layer. We argue that the best approach to build a complete mobility enabled protocol stack for future wireless networks is based on the concept of Co-Existence of mobility management protocols proposed on different layers, in a way that we get best out of each. In the end, in order to support our arguments, we propose a novel mobility enabled protocol stack, naming mechanism and wireless network architecture for the future wireless networks.

Keywords: Mobility, Mobility Management, OSI communication stack, mobile networking, wireless network architecture, heterogeneity.

1 INTRODUCTION

Mobility is an unmistakable truth in human lives and time is always a constraint, while communication is a necessity. Communicating while moving to save time has become a challenge. However, mobility is not just limited to communication, as historically Internet was build for communicating only, now its application are way beyond communicating. Same is becoming true for wireless networks and application of mobility. This idea is driving the research in wireless networks. An obvious question is, why traditional internet (TCP/IP) can't fulfill the requirements of future wireless networks? Two of the fundamental problems in TCP/IP stack that hinder the use of mobility are: there is no support for mobility in TCP/IP and the other problem is the tight binding of Application, transport and IP layers (Figure-1). This opens up a new and challenging area of research i.e. "Mobility Management". As a result, there exist today a multitude of solutions aimed at managing this problem. These solutions are at varying stages of deployment, from purely analytical research, to experimentally validated proposals, right through to fully standardised and commercially available systems. Most of these solutions aim to solve mobility management problems at a specific layer and questions like what layer does mobility belong? [4] are being addressed. We strongly believe that mobility handling task does not belong to any specific layer in the TCP/IP stack.

Every layer in the communication stack has its own responsibility in order to support mobility. For us mobility is functionality with its own types and requirements. Therefore, in this paper we have studied mobility management in detail while talking mobility types and mobility requirements as a reference. We also introduce a notion of mobility

management protocol co-existence. Co-existence means co-existence of different mobility management solutions proposed on different layers of OSI stack to form a "Mobility Enabled Protocol Stack".

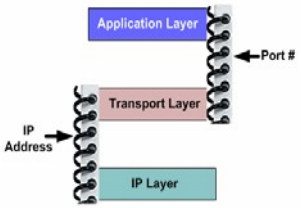

Figure 1 : Layer Binding in TCP/IP Stack

Co-existence is further divided into two types And-Based Co-existence (ABC) and Or Based Co-existence (OBC). ABC means, simultaneous existence of multiple mobility management protocols and OBC means selection of an appropriate mobility management protocol based on multiple factors like context, preference, etc. In this paper we propose an ABC based mobility enabled protocol stack, as OBC based solutions have challenges that the beyond the scope of this paper. Furthermore, we demonstrate how we can create a hybrid solutios towards mobility management using And-Based Coexistence of link layer, network layer, new layer and session layer mobility management solutions. Our proposed solution can fulfil all the mobility requirements and support physical, logical and QoS mobility. The rest of the paper is organized as follows. In the next section we describe mobility types and their relationship with the OSI stack layers. In section 3, we discuss what does mobility means on all seven layers of the OSI stack? We review the mobility management requirements in section 4. Section 5, presents mobility management solutions on different layers and analyse them according to the mobility types and mobility requirements. Finally, we introduce a new mobility management solution and architecture, followed by the conclusion and future works in the last section.

2 Mobility Types and their relationship with the OSI Stack Layers

A clear and precise definition of mobility is required in order to perform an analysis of mobility management solutions. Mobility can be categorised in different ways. On the top level we think mobility has three broad types physical, logical and QoS mobility. Throughout our paper, we will use these types as a reference for our comparisons and analysis.

Physical Mobility:

Physical mobility deals with the physical movement of the device while continuing to be reachable for incoming requests and maintaining ongoing sessions/connections. Physical mobility is further divided into two categories local and global mobility. Local mobility deals with the movement of device within a single administrative domain. On the other hand global mobility deals with the movement of device within two or more different administrative domains. Local mobility is further divided into two categories inter-subnet mobility and intra-subnet mobility. Inter-subnet mobility is moving within multiple different subnets and intra-subnet refers to the movement of device within a single subnet.

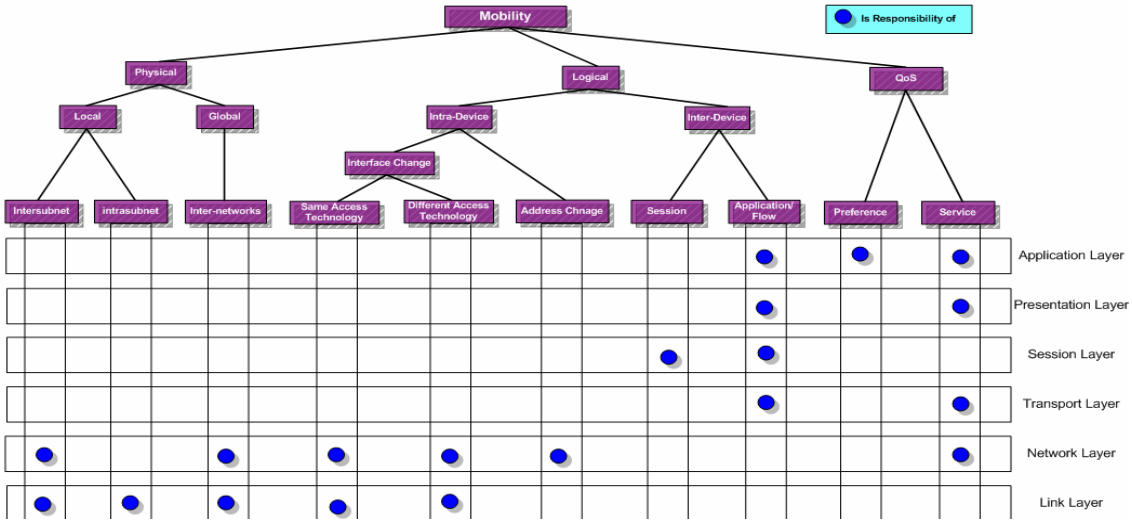

Figure 2 : Classification of Mobility Types and OSI Layer Responsibilities

Global mobility can also be referred to as inter-network mobility. Inter-network mobility is the movement of device within two different networks domains.

Now let's have a look at layers in the OSI stack that are responsible for dealing with physical mobility. At the base level, physical mobility is divided into three types' intra-subnet, inter-subnet and inter-network. In the case intra-subnet mobility,

when ever the mobile node will move it will have to re-associate itself to the new access point (AP) at the link layer. In the case of intra-subnet mobility we don't have to change our IP address so network layer may not be involved. Inter-subnet and inter-network mobility pose similar responsibilities to the OSI stack layers. In both of these cases we not only have to re-associate to new access point but also get new IP address, so both link layer and network layers are responsible. Other than these responsible layers, layer dependency rules apply as mentioned in section 1.

Logical Mobility:

Logical mobility deals with the possibility of mobility without the physical movement of the device. It is further classified into two types inter-device mobility and intra-device mobility. Intra-device mobility deals with the mobility within the device. Interface change, and address change are two types of intra-device mobility. Interface change can be further divided in two types same access technology mobility (a.k.a. horizontal handoff) and different access technology mobility (a.k.a. vertical handoff). Same access technology mobility means changing to another interface of the same access technology and different access technology mobility means changing to access interface of the different access technology e.g. changing from 802.11 to CDMA. The second type is inter-device mobility that deals with the movement of mobile objects [1] from one device to another. It can further sub-divided into session mobility and application/flow mobility. Session mobility means moving session or application/communication state to some other device for example, a user may want continue a session begun on a mobile device on to the desktop PC when entering his/her office. A user may also want to move parts of a session, e.g. if he has specialized devices for audio and video, such as a video projector, video wall or speakerphone. Application/flow mobility on the other hand means movement of application and flow state between devices. This type of mobility is also known as code mobility, agent mobility or process mobility.

At the base level logical mobility can be divided into five types namely, same access technology mobility, different access technology mobility, address change, session mobility and application/flow mobility. In logical mobility we assume that mobile device is not moving. Even being static a mobile device can change its access interfaces. If the device changes its interface, the OSI layer dependencies will depend on whether it changes interface within same subnet, different subnet or different network. Having known this the same layer dependencies will apply as in the case of physical mobility. In the case of different access technology mobility link layer is responsible for association of the mobile device with the new access technology and mobility can be handled, at the lowest, on the IP layer. Address change mobility can be handled at the network layer, as address change does not require change in the current access point association. In application/flow mobility all layers from transport to application layer will be responsible. This is because of the tight binding of application layer with that of session and transport, as discussed in section 1. Presentation layer is involved in the case in which that the new device has different presentation characteristics/abilities (content adoption). The session layer mobility only involves the session layer as we have to deal with the session states only, assuming that the device to which we are moving our sessions has all the capabilities and application as of the previous device.

QoS Mobility:

QoS mobility refers to maintaining the same operating environment during mobility, changing devices or while changing network service providers. This is further classified in to two types service mobility and preference mobility. In preference mobility the idea is that the user working preferences, working priorities, and context should move [2] with the user during mobility. Service mobility takes into account that the user should get same services and QoS level in the new visited network. For example, the IntServ and DiffServ parameters should be activated or negotiated in your new network. Both of the QoS mobility types ensure to maintain the same QoS in the new/visited network. In general QoS mobility is a tricky term in the sense that QoS can have different semantics for different networks, different service providers and different users. In general, preference mobility is dealt with at the application layer. Preference mobility solutions keep record of the user preferences and performs operations like user and network context gathering. In the case of service mobility, this could involve application layer (application based services), presentation layer (quality and level of presentation) and network layer (throughput guarantee, low latency etc).

3 Meaning of Mobility on Different OSI Stack layers

In the classical TCP/IP stack mobility has no well-defined place and meaning. Many solutions have been proposed for mobility support at different layers starting from Application to link layer. Physical layer is not involved as mobility at physical layer is handled implicitly by the wireless access technology, e.g. the physical movement of mobile nodes with respect to a single wireless access point. Every mobility management solution has its own strengths and weaknesses. To propose a new mobility solution for a specific layer it is important to understand, what does mobility mean in

association to that particular layer? In this section we will describe the meaning of mobility at different layers of the TCP/IP stack and study each layer by answering the following questions. What services are provided by this layer that are affected by mobility? What mobility types will affect this layer? How mobility can affect this layer? What is needed at this layer in case mobility? Outcome of this layer in-order to support mobility?

3.1 Physical Layer Mobility

At the physical layer message is actually sent out over the network. The basic functions of physical layer are encoding, signaling, data transmission and reception of data. Encoding and signaling takes care of transforming the data from bits that reside within the computer into signals that can be sent over the network. After transformation the physical layer actually transmits the data over the link, and of-course is also receive the signals. Mobility will not affect the function of physical layer as they have to ensure that signals are transmitted and received even when the device is moving. There are other challenges associated to physical layer like fading and multi-path on the radio channel, which are outside the scope of this paper.

3.2 Link Layer Mobility

Link layer mobility is also known as link layer handoffs. There are two types of link layer handoffs, horizontal handoffs and vertical handoffs. Horizontal handoffs may be invisible to higher layers, since it may occur within a single subnet. A vertical handoff is a handoff between different access technologies. Vertical handoffs are usually visible to network layers and cannot be handled at the link layer without substantial amount of effort. In the case of mobility the link layer perform channel scanning, detecting availability of potential access technologies, monitor channel conditions, authentication and re-association. All of these operations can be performed within access points in same or different access technologies based on the type of handoff. This layer could be affected by all kind of physical mobility types and interface change mobility (logical mobility). In the case of mobility the link layer can detect different access technologies available, signal to noise ratio of different access point's available, channel at which different access points are operating, information about the overlay networks etc. The information about channel conditions can be helpful in making decision about queuing, packet dropping and QoS[3]. Knowledge about potential links and link properties is useful in the case of overlay networks. As overlay networks have multiple heterogeneous link and involve choosing, initialing and decisions making about vertical and horizontal handoffs. Moreover, link layer techniques are also responsible for communication between different link layer devices, to enable heterogeneity and proactive context caching for fast handoffs. The information about imminent link layer handoff to network layer could significantly improve performance of IP layer handoff. In [3], the proposed low-latency mobile-IP handoff scheme utilizes the information of signal strength to detect link layer handoffs. Using this information it speeds up network-layer handoff by replaying cached foreign agent advertisements.

3.3 Network Layer Mobility

As discussed in the previous section the link layer mobility management deals with directly connected devices while network layer makes communication possible between different/remote networks. Location management (reach-ability) and naming (IP Address) are the two services provided by the network layer that could by highly effected in the case of mobility. This layer could be affected by inter-subnet mobility, inter-network mobility, interface change and address change. Network layer is also responsible for providing the required QoS services, so it will also be affected by service mobility. The major change which layer may undergo in case of mobility is the change of IP address when ever mobile device enters new network. The address change leads to the challenge of location management which apparently is another responsibility of network layer. Change of network requires the device to be configured to the new network setting, device should be able to get a new IP address and updating any naming service so that it can be reached by the corresponding hosts (location update). Protocols like DHCP and IPv6 auto-reconfiguration allows dynamic reconfiguration of hosts by providing them with a new IP address and configuration parameters in a new visited network. DNS, Dynamic DNS and home agent binding (Mobile IP) are the mechanisms for location management. Furtherore, another challenge on the network layer will be the dynamic routing of the packets to reach the destination. The following two distinct solutions for routing are possible [4], use host specific routes and updating them as each host moves or use routes to sub-networks and add indirection agents to the architecture. The first approach is not scalable as numbers of internet hosts are increasing exponentially. The second approach is being followed by all Mobile IP [5] based solution.

3.4 Transport layer Mobility

During mobility packet loss, link capacity and change of IP address affect the transport layer protocols. Packet loss affects the flow and congestion control algorithms. As in connection establishment Bandwidth Delay Product (BDP) is used to define the window size. This window size is then used for the duration of the connection. Once the device moves to a new network link capacity

might change, this will also effect the BDP. Therefore, new window size should also be negotiated again in the visited network. These issues of BDP are dealt by the mobility aware transport layer protocol. If we use the conventional transport layer implementation for mobility management, then transport layer will be the most affected layer because of its tight binding with the layer above and below it, as discussed in section 1. This layer in affected in the case of inter-subnet mobility, inter-network mobility, horizontal handoff, vertical handoff, address change, session mobility and application/flow mobility. In transport layer mobility management the reliability and integrity of end-to-end data delivery, connection reestablishment after disconnection, longer connection state maintenance, waiting for reconnection, assessing transfer rates for new link and for ongoing connections are important issues. All of these issues are responsibility of layer 4 (Transport layer) mobility management and higher layers mobility management mechanism. The distribution of these tasks between transport, session and application layer is a thoughtful process. In any case the obvious tasks of transport layer mobility management solution will be reliable data delivery, re-ordering, re-connection and integrity.

3.5 Session Layer Mobility

Main purpose of session layer is to maintain state information about the parameters involved in the session state and communication state. Mobility causes unexpected termination of transport layer service to an ongoing application communication session, which may result in the loss or invalidation of information relating to the state of the session. If session layer is used then this layer is independent of transport and lower layers. Session layer mobility protocol is only affected in the case of session mobility and application/flow mobility. Assuming that the session layer is used, then the session state information may include the number of bytes already transferred and written to disk for a file transfer application, the encryption keys and security associations set up for a secure remote login session and synchronization data for combining incoming streams. The responsibility of the session layer mobility management protocol is to ensure that this information is not lost as a result of connection termination at the transport layer. This means that application needs to provide the relevant session layer mobility handling mechanism with an access to all of the information that is required to pause, checkpoint, and restart the current session. Once transport layer service is re-established and a new communication socket is obtained, then this information can then be used to restart the application communication session in the same state as it was when the previous transport layer connection was terminated.

3.6 Presentation Layer Mobility

The presentation layer is responsible for the delivery and formatting of information to the application layer for further processing or display. It relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems. The issues like screen resolution, codec versions, application versions etc are to be dealt with at the presentation layer in the case of mobility. This might be needed in the case of session and application/flow mobility within different devices in a Personal Area Networks (PAN). As different devices in the PAN might have different presentation capabilities and options. A presentation layer mobility management protocol should be capable of content adoption and can detect the capabilities of the new device and modify the presentation of the data accordingly.

3.7 Application Layer Mobility

Application layer mobility solutions are also known as application specific mobility solutions. There are no set requirements for a mobility solution at the application layer, so we can not study it according to mobility affects on it. Application layer is highly flexible and is dependent on the underline layers for network access and socket establishment etc. Application layer can detect the changes occurred in the underline layers and can act accordingly to provide an application specific mobility solution. The important thing to keep in mind is that if the session state is maintained by the application, then the application needs to handle session mobility by itself. On the other hand if the session state is made available to a ‘session layer mobility handling protocol’ then the application doesn’t have to handle the mobility. Thus the benefit of session layer mobility is that the applications don’t need to deal with mobility handling. The drawback is that applications (or programming languages and compilers) need to be rewritten so that they can use the services provided by the session layer.

4 Mobility Management Requirements

In this section we will study the relationship between the mobility requirements and the mobility management protocols on different OSI layers. Nine major mobility requirements are listed here i.e. location management, handoff management, security, Quality of Service (QoS), connection re-establishment, end-to-end reliability, multi-homing and layer specific performance enhancement. First of all we will give a brief overview of all these requirements and then in the next section we will see how mobility management protocols fulfill these requirements at different layers.

4.1 Location Management

Location management is a process that involves identifying the location of the mobile node while it is moving within different networks. It includes two major takes [6] location registration or locations update and call delivery.

4.2 Handoff/handover Management

Handoff management is required to keep the connections alive while the mobile node is moving. Handoff management can be done on several layers for example, link layer, IP layer, transport layer and even on the application layer. Handoff management at the IP Layer is divided into two major types' inter-domain handoff and intra-domain handoff [6]. At the link layer are divided into two major categories horizontal handover/handoffs and vertical handovers/handoffs [6].

4.3 Security

Security mainly involves authentication, confidentiality, integrity and authorization to access of the network resources. Firstly, the MN needs to authorize and authenticate itself while roaming in a new environment. Secondly, when QoS resources are provided to the MN authorization should be confirmed so as to detect Denial of Service Attacks. Another important questions arise is that which layer should be responsible for security. Security solutions for wireless networks have been proposed at different layers like: link layer (WEP), IP Layer (IPSec), application layer (SSL) etc.

4.4 Quality of Service (QoS)

Transparency of QoS is a complex and important area in the future wireless network [8]. While moving within different networks, user should have guarantee of QoS. This term is also referred to as service mobility [7]. QoS provisioning also comprise data plane (mainly traffic control e.g. classification and scheduling) and control place (mainly admission control and QoS signaling) functions. Changing location during the lifetime of the dataflow introduces changed paths, thus it requires to identify the new path and install new resource control parameter via path-coupled QoS signaling. This is really a challenging problem in the wireless domain. Mobility management solutions trying to resolve QoS issues should address the above mentioned issues.

4.5 Connection Re-establishment

When mobile nodes move from one network to another they might loose their existing connection, and they need to re-establish the connections after getting the new IP layer details. This connection reestablishment is the task of transport layer in particular. This problem can only we resolved at transport layer or the layer above. In mobility management for user to have transparent view of mobility we need to have connection disconnections and reconnections seamless and transparent from the user or applications.

4.6 End-to-End Reliability

End-to-end reliability is another important research area in wireless and wired internet. This feature is more dependent on the transport layer services. In the conventional internet, transport layer protocols are dependent on the services provided by the network layer. They do not consider the link properties, thus the congestion control of transport layer does not distinguish between packet loss caused by wireless link or from the normal packet loss in wired network. This behavior degrades the performance of end-to-end connection in the wireless network. Therefore, in the mobility management protocols on transport layer should consider this factor for providing better end-to-end reliability.

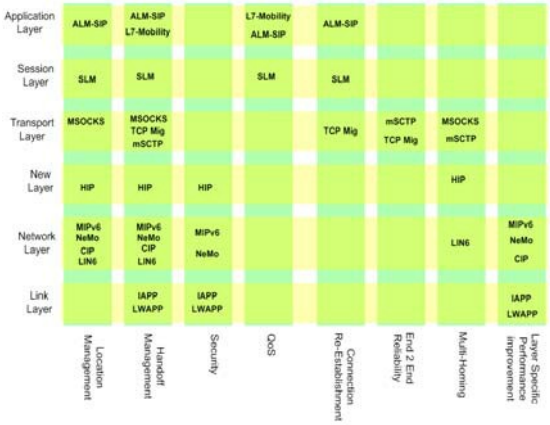

Figure 3 : Mobility Management Requirement Analysis

4.7 Multi-homing

Multi-homing is an essential component for future wireless networks. Multi-homing means that a device is capable of communicating with the help of multiple interfaces at the same time. These interfaces can be of the same or different access technologies (e.g. WiFi, GRPS, GSM, CDMA, and Bluetooth).

4.8 Layer Specific performance enhancement

There are several protocols which are built to enhance the performance or to add new functionality to the current protocols. In our discussion of internet mobility requirement analysis we will also have a look at the protocols (IAPP, LWAPP, FastMIPv6) that are developed to enhance the performance of protocols on a specific layer.

5 Mobility Management Solutions on Different Layers

In this section we will discuss mobility management protocols proposed on different layers

of the OSI Stack. First of all we will briefly see how these protocols work, then we will analyze them according to the types of mobility they support (Figure-4) and finally we will see what all mobility management requirements they fulfill (Figure - 2).

5.1 Application Layer Solutions

5.1.1 L-7 Mobility

This approach [9] introduces the concept of inter-domain mobility, that allows users to migrate their connectivity between different network domains. By adding a simple extension to current mobility practices for inter-domain mobility, L7-mobility provides support for *hot and policy mobility*. Inter-domain mobility enables handoff between two infrastructures that have nothing in common and may use totally incompatible mobility solutions. In this approach applications have to create a new TCP connection every time the device handoffs. Other link layer issues like, IP layer and transport layer issues are dealt by a Connection Diversity Framework [9]. L7-mobility provides *handoff management and QoS* using policy mobility concept. The *location management and connection reestablishment* is the responsibility of the application. The applications handle the mobility part specific to them, such as restarting their IP connection and discovering remote application proxies. The application delegates all the generic mobility functionality and link specific mobility management to the connection manager and interacts with it through a well defined API. The role of the connection manager is to discover, evaluate, setup and monitor various paths to the infrastructure on behalf of the various applications. It directly manages various link layers and includes abstraction modules specific to each link layer. The connection manager performs link discovery to find different paths to the infrastructure. It activates and configures link layers on-demand to enable their use, monitor them for failure, and disconnects them when idle. The policy manager is responsible for policy based QoS guarantee. It selects the most appropriate link to connect to the infrastructure based on the current policy, application requirement and link availability.

5.1.2 Application Layer Mobility Using SIP (ALM-SIP)

ALM-SIP uses Session Initiated Protocol (SIP) [7] to provide *terminal, personal, session and service mobility* to applications ranging from Internet telephony to instant messaging. Terminal mobility is explained in two different scenarios pre-call mobility and mid-call mobility. When ever a mobile node changes it address is registers its new address to its home Registrar. In the case of mid-call mobility in addition to registering with the home registrar it also send an INVITE request to the corresponding node with its new IP address (this is a similar concept as route optimization Mobile IPv4). The other mobility types are also discussed in detail in the paper [7]. ALM-SIP provides *location management, handoff management, QoS, and connection re-establishment.*

5.2 Session Layer Solutions

5.2.1 Session Layer Mobility Management

SLM [10] proposes a framework to manage connections to the mobile hosts. This protocol integrates the notions of Quality of Service (QoS) management and mobility management and forms a base for overall session management. The *QoS management* is carried out in a number of ways. Firstly, it maintains the normal IP routing semantics between two hosts, so it allows resource reservation using both IntServ and Diffserv, without breaking their semantics. In the case the host changes its address, the existing reservations can be torn down and a new reservation can be established. Secondly, SLM allows the placement of intermediate proxy modules for data filtering. In [1] some enhancements to SLM are proposed. It proposed to use Network Access Identifier for mobile objects [1] naming. Although this name is globally unique it is not sufficient due to the diversity of endpoints that can be created by the same mobile objects. In order to distinguish between these communication end-points, this name should be combined with another naming component for example Universally Unique Identifier (UUID). The UUID is then generated per end-point. An endpoint identity (EPID) constructed from the pair [NAI, UUID] fulfills the above requirement. This then allows the end-point to move not only within a device but also between devices so it supports both inter-device and intra-device mobility (Figure-2). SLM also provides internet mobility services like *handoff management, QoS and connection re-establishment*. SLM has introduced two entities on the session layer, one is reflector and the other is connector. The applications communicate with the reflector and the reflector redirects the connection to the connector. The connector is responsible for *handoff management and connection reestablishment*. Whenever the mobile node changes it point of attachment to the network the connector layer on the mobile device establishes a new connection with the connector layer on the corresponding node. Therefore, the handoff is transparent from the applications. SLM used a new entity called User Location Server (ULS) for *location management*.

5.3 Transport Layer Solutions

5.3.1 MSOCKS

MSOCKS [11] presents an architecture called Transport Layer Mobility (TLM) that allows mobile nodes to not only change their point of attachment to the internet, but also control which network interface to use for different kind of data leaving from and arriving at the mobile node. This

approach is implemented using split proxy mechanism and its an extension of SOCKS. In MSOCKS, when a MN changes its IP address, then it shall open a new connection to the proxy and sends a RECONNECT messages with the connection identifier of the existing connection. Upon receiving a RECONNECT message, the proxy separates the old connection between MN and Proxy (MN-Proxy) from the connection between Proxy and CN (Proxy-CN), and concatenates in the new MN-Proxy connection. The proxy then concatenates the new connection to the Proxy-CN connection in place of the old MN-Proxy connection and closes the old connection. Once the concatenation is setup, the proxy sends an ok message to MN.

MSOCKS provide *handoff and location management* using the proxy. When ever the mobile node makes a BIND or CONNECT request to the proxy asking to be connected to the corresponding node, the proxy issues a new connection identifier with which the logical session between the mobile node and the proxy are tracked. MSOCKS RECONNECT request is added to support *multi-homing* support in the mobile node. When the MSOCKS library wants to change the address or network interface that a TCP connection uses to communicate with the MSOCKS proxy, it simply opens a new connection to the proxy and sends a RECONNECT message specifying the connection identifier of the original connection. In this way MSOCKS also supports *multi-homing*.

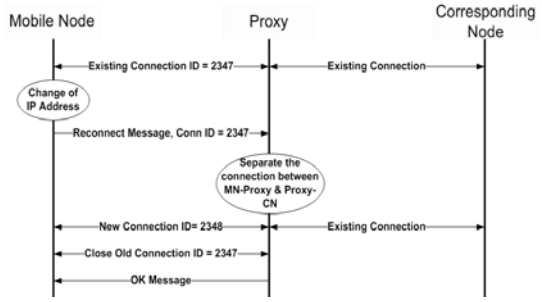

Figure 4 : Change of IP Address in MSOCKS

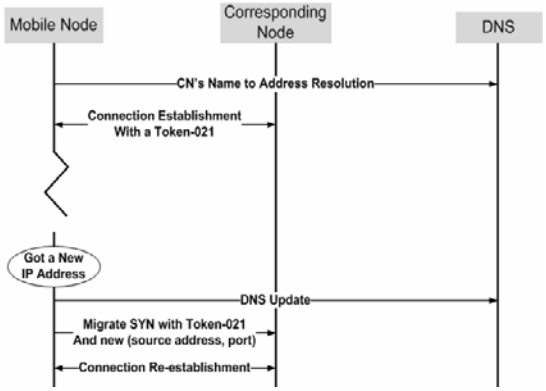

Figure 5 : TCP Connection Migration

5.3.2 TCP Migrate

TCP Migrate [12] presents the design and implementation of an end-to-end architecture for internet host mobility using dynamic updates to the Domain Name System (DNS). This protocol supports mobility management using TCP migrate option. The migrate option uses a token to identify the connection and DNS is used for location management. In TCP Migrate option the token is negotiated at the connection establishment time and after successful token negotiation and connection can be uniquely identified by (source address, source port, dest address, dest port) or (source address, source port, token). This enables a mobile node to reestablish a previously-established connection from a new address by sending a special Migrate SYN packet that contains the token. The mobility management requirements satisfied by TCP Migrate are *handoff management, connection reestablishment and end-to-end reliability*. The *location management* in TCP Migrate is done using DNS. *Handoff management* in TCP Migrate is achieved through Migrate TCP option. TCP migrate also provides end-to-end reliability as it is an enhancement of the conventional TCP and there is no middleware in between like proxy in the case of MSOCKS.

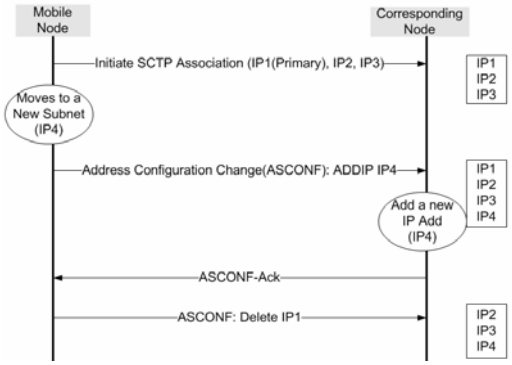

Figure 6 : mSCTP Operation

5.3.3 mSCTP

Stream Control Transmission Protocol (SCTP) [13] is a new transport protocol, existing at an equivalent level with UDP and TCP. The two major functions provided by SCTP that make it unique from other transport layer protocols are multi-streaming and multi-homing function. In particular, the multi-homing feature of SCTP enables SCTP to be used for Internet mobility support, without support of network routers or special agents. The ADDIP extension [14] enables an SCTP endpoint to add a new IP Address, delete an unnecessary IP address and also change the primary IP address used for the association in an active SCTP association. mSCTP [15] is build on top of SCTP with ADDIP extension for supporting soft handover in the transport layer. mSCTP supports *handover and multi-homing* but it does not support *location management*. mSCTP, similar to SCTP and therefore supports unicast only. In SCTP MN has only one association with the CN. At the initiation of SCTP

association the MN and CN negotiate list of IP address. Among the list of IP address one of the address is chosen as a primary address and other are specified as active address. When ever a mobile node enters into a new network it gets a new IP address, it then sends an Address Configuration Change (ASCONF) Chunk with Add IP Address parameter to inform the CN of the new IP address. On receiving the ASCONF, CN shall add the new IP address to the list of association address and reply the ASCONF-ACK chunk to MN. While MN is moving, MN may change the primary path to the new IP address by path management function. The SCTP association, therefore, can continue data transmission while moving to a new network. MN can also inform CN to delete the IP address of previous network from the address list by sending ASCONF chunk with delete IP address parameter. This is done when MN confirms that the link of the previous network has failed permanently.

5.4 Network Layer Solutions

5.4.1 MIPv6

Mobile IPv6 [16] protocol allows nodes to remain reachable while moving around in the IPv6 internet. Mobile nodes are always identified by their home address, regardless of their current point of attachment to the internet. While situated away from their home network, a mobile node is also associated with a care-of-address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of-address. This protocol is both suited for mobility across homogenous and heterogeneous media. MIPv6 supports bidirectional tunneling and route optimization (Figure - 6).

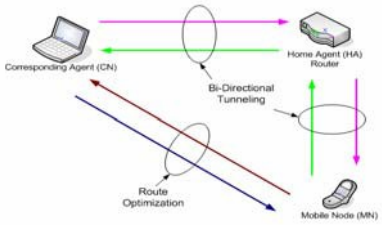

Figure 7 : Modes Supported by MIPv6

The *location management and handoff management* in MIPv6 and NeMo is almost similar, the only difference is that in the case of MIPv6 its provide location and handoff management for one host and NeMo provide the same for the whole network associated with the mobile router. For *location management* they both use binding updates to the Home Agent (HA) and Corresponding Nodes (in case of route optimization) whenever they change their point of attachment to the internet. *Handoff management* is done in the similar way, the corresponding node creates a connection with the Home Agent and in the case of handoff the Mobile Nodes open up a new connection with Home Agent. This makes handoff transparent from the corresponding node. This behavior of movement transparency of the mobile node becomes void in the case of route optimization. In the case of route optimization when ever the mobile host changing its point of attachment it sends a biding update to both the HA and the CN. In this case the architecture of corresponding node also needs to be changed. The *security* in Mobile IPv6 and NeMo is achieved by using IP Security (IPSec) tunnels between HA and the CN and the MN and the CN in the case of route optimization. Several variants of mobile IPv6 are proposed to improve its performance like FastMIPv6 [30], HMIP [31],NeMo[17] etc..

5.4.2 Network Mobility

The objective of the NEMO [17][25] is to develop a mechanisms that provide permanent Internet connectivity to all the mobile network nodes via their permanent IP addresses and to maintain ongoing sessions as the mobile network changes its point of attachment to the Internet. In the network mobility architecture the mobile router (MR) takes care of all the nodes within the network, irrespective of their capabilities. As a first step, the IETF NEMO Working Group is developing a basic protocol [18] that ensures uninterrupted connectivity to the mobile network nodes, without considering issues such as route optimization. The NEMO Basic protocol requires the MR to act on behalf of the nodes within its mobile network. Firstly, the MR indicates to it's HA that it is acting as a MR as opposed to a mobile host. Secondly, the MR informs the HA of the mobile network prefixes. These prefixes are then used by the HA to intercept packets addressed to the mobile nodes and tunnel them to the MR (at its care-of address), which in turn decapsulates the packets and forwards them to the mobile nodes. Packets in the reverse direction are also tunneled via the HA in order to overcome Ingress filtering restrictions [19].

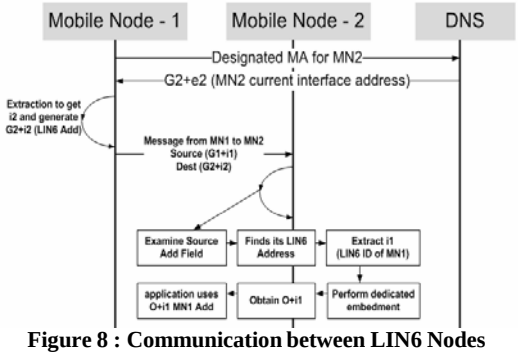

Figure 8 : Communication between LIN6 Nodes

5.4.3 LIN6

LIN6 [20] [26] is a new protocol that's

supports mobility for IPv6. LIN6 claims to have handoff in 50 milli-seconds. It is basically a Location Independent Network Architecture (LINA) [20] with IPv6 support. LINA employs separation of identifier and locator to support node mobility. In the application layer, a target node can be specified by its identifier in addition to the conventional model in which the target node is specified by the locator. When the application specifies a target node, the identifier sub layer maps the identifier to the corresponding locator, and then the delivery sublayer "embeds" the identifier in the locator. In conventional networks the IP address has two semantics associated with it, one is the identification and the other is location. LINA introduces two entitles in the network layer to support *node mobility*, the interface locator (uniquely identifies the nodes current port) and node identifier (signifies the identify of the node). *Location management* is done by DNS and a mapping agent (MA). LIN6 defines two types of network address. The LIN6 generalized ID (formed by concatenating LIN6 prefix and LIN6 ID) and LIN6 address (network prefix and LIN6 ID). LIN6 generalized ID is formed by concatenating LIN6 prefix and LIN6 ID and is used at transport layer to identify the connection. The LIN6 address is formed by concatenating network prefix and LIN6 ID and is used for routing packets over the network. Figure 9 shows the how communication between LIN6 nodes is done.

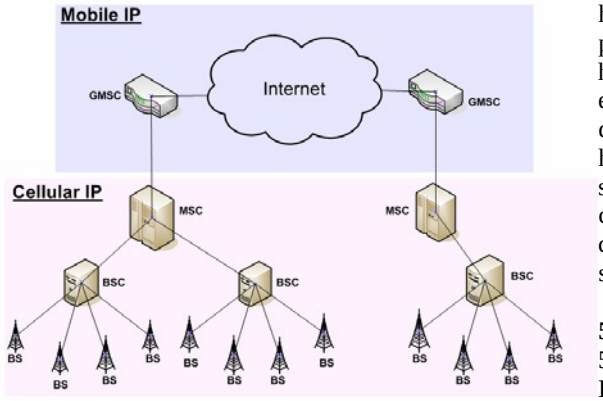

Figure 9 : MIP & CIP Integration Architecture

It uses IPSec for *security*. In the sending node, IPSec is processed as follows. When the packet is passed from the transport layer, the source and the destination address fields in the IPv6 header contain LIN6 generalized IDs. The security association is decided by using the destination LIN6 generalized ID, and then IPsec calculation is executed. After that, the source and the destination LIN6 generalized IDs are converted to LIN6 addresses. In the receiving node, IPsec is processed as follows. Upon packet reception, the source and the destination address fields of IPv6 header contain LIN6 addresses. First, these LIN6 addresses are converted to LIN6 generalized IDs. The security association is decided by using the destination LIN6 generalized ID, and then IPsec calculation is executed.

5.4.4 Cellular IP

Cellular IP [21], is an internet host mobility protocol that takes an alternative approach to that found in mobile telecommunications (e.g. General Packet Radio Service) and in IP Networking (Mobile IP). Cellular IP represents a new mobile host protocol that is optimized to provide access to a Mobile IP enabled internet in support of fast moving wireless hosts. The universal component of cellular IP network is a base station which serves as a wireless access point but at the same time routes IP packets and integrates cellular control functionality traditionally found in Mobile Switching Center (MSC) and Base Station Controllers (BSC). The cellular IP network is connected via gateway router. Mobility between gateways (i.e. Cellular IP access networks) is managed by Mobile IP while mobility within access networks is handled by Cellular IP. The *location management* and *handoff management* support are integrated with routing. To minimize control messages, regular data packets transmitted by mobile hosts are used to establish host location information. Uplink packets are routed from mobile to the gateway on hop-by-hop basis. The path taken by these packets is cached in the base-station. To route downlink packets, that are address to a mobile host, take is the same as the path used by recent packets transmitted by the host. When the mobile host has no data to transmit then it periodically sends empty IP packets to the gateway to maintain its downlink routing state. To perform handoff a mobile host has to tune its radio to the new base station and send a route-update packet. This creates routing cache mapping on route to the gateway hence configuring the downlink route to the new base station.

5.5 Link Layer Solutions

5.5.1 Inter Access Point Protocol (802.11F)

IEEE 802.11F [22] or Inter-Access Point Protocol, is a recommendation that describes an optimal extension to IEEE 802.11 to enable wireless access-points to communicate among multi-vendor systems. Briefly, IAPP is a set of functionalities and protocol used by an AP to communicate with other AP's on a common distribution system (DS). It is part of a communication system comprising of Access Points (AP's), Mobile Stations (STA's), Arbitrarily connected DS and Remote Authentication Dial In User Service (RADIUS) servers. Radius provide two functions, mapping of Basic Service Set (BSS) Identification (BSSID) of an AP to its IP address on the DS and distribution of keys to the AP's to allow the encryption of the communication between the AP's. The basic functions of IAPP are to facilitate

certain maintenance of Extended Service Set (ESS), support the mobility of STA's, enable AP's to enforce the requirement of a single association for each STA at a given time and enable proactive caching for fast hand-off.

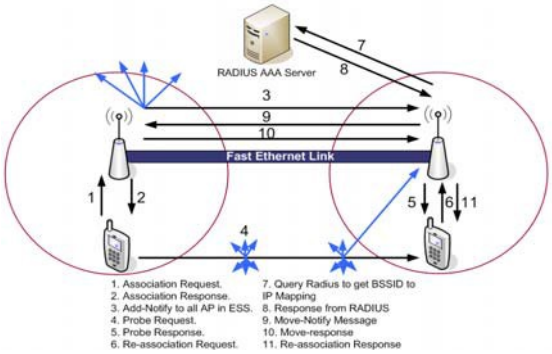

Figure 10 : Working of IAPP

The Working of IAPP is demonstrated in Figure-10. Mobility management requirements fulfilled by IAPP are *handover management, security and layer specific performance enhancement*. In addition to these it also provides a mean for access point communication and proactive context cashing for fast handovers. It provides 802.11i (WPA2) based security and also provide secure way for inter access point communication within a single Extended Service Ser (ESS).

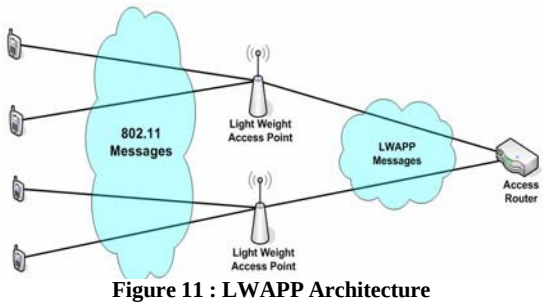

Figure 11 : LWAPP Architecture

5.5.2 Light Weight Access Point Protocol (LWAPP)

LWAPP [23] is a protocol designed to make communications between access points and wireless switches automatic. This protocol allows a router or switch to interoperably control and manage a collection of wireless access points. Inorder to move some of the loading due to Wi-Fi processes and function complexity to the centralized wireless switches or routers.

LWAPP is a protocol that defines how lightweight access points communicate with Access Routers (AR). It assumes a network configuration that consists of multiple APs connected either via layer 2 (Ethernet), or layer 3 (IP) to an AR. The APs can be considered as remote RF interfaces, being controlled by the AR. The AP forwards all 802.11 frames received from mobile stations (STA) to the AR for processing via the LWAPP protocol. Similarly, packets from authorized mobiles are forwarded by the AP to the AR via this protocol, if the protocol works on layer 3. These forwarding operations between APs and ARs are accomplished according to a LWAPP transport layer specification which defines how to tunnel 802.11 frames in 802.3 (Ethernet) frames or IP packets in UDP packets. The Lightweight Access Point (LWAPP) protocol is said to fulfill the *handoff management, security and layer specific performance improvement at the link layer*. As discussed above, there are two major components of LWAPP, wireless LAN controller and lightweight access points. The real-time frame exchange and certain real-time portion of MAC management are accomplished by access points and other management tasks like authentication, security management, and handoff management are handled by the wireless LAN controllers. LWAPP provides cellular like fast handoffs which makes it's a excellent protocol to support mobile application such as voice over WLAN. The performance enhancement is achieved by transferring the intelligence to a centralized wireless LAN controller and making the access points lightweight. Within a LAN the mobile station does not have to re-authenticate itself as far as it is moving within the range of Wireless LAN Controller.

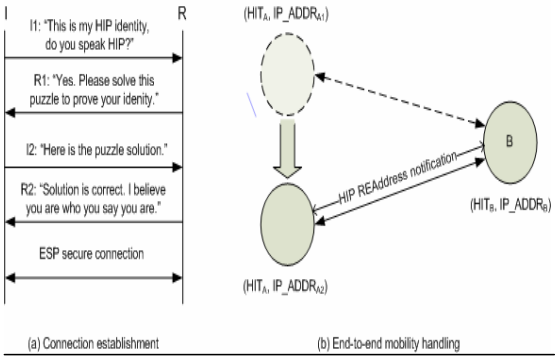

Figure 12 : Working of HIP

5.6 New Layer Solutions

5.6.1 Host Identity Protocol

HIP [24] handles mobility by introducing a thin layer of additional resolution between the network and transport layers, decoupling transport sockets from network level addresses. Instead of binding to the IP addresses, HIP enabled applications bind to 128-bit Host Identity Tags (HIT), a global identifier generated by hashing a public key. In order for HITs to be globally reachable, some kind of infrastructural support (*location management*) is required to be able to map HITs to routable network level addresses. At present several mechanisms including DNS,

distributed hash tables, and rendezvous servers are being investigated as a means to provide this mapping. However, once both hosts engaged in end-to-end communication are aware of each others HIT, no further infrastructural support is required unless both hosts change network location simultaneously with no prior notification. Due to the decoupling between network and transport layers, HIP enables applications on the mobile node to continue communication oblivious to changes in available network addresses and also provides a mechanism to directly signal a change in network address to the correspondent node. An authentication process proceeds each HIP communication session. HIP uses a four-way key exchange to verify the identity of the hosts, termed Initiator (I) and Responder (R).

Mobility management solution by adding a new layer appears to be quite useful in term of fulfilling mobility requirements. HIP can provide *location management, handoff management, security and multi-homing*. HIP decouples the transport from the internetworking layer, and binds the transport associations to the Host Identities and keep internetworking layer addresses for routing. Therefore, HIP can provide for a degree of internetworking mobility and multi-homing. HIP mobility includes IP address changes to either party. Thus, a system is considered mobile if its IP address can change dynamically. HIP links IP addresses together, when multiple IP addresses correspond to the same Host Identity, and if one address becomes unusable, or a more preferred address becomes available, existing transport associations can easily be moved to another address.

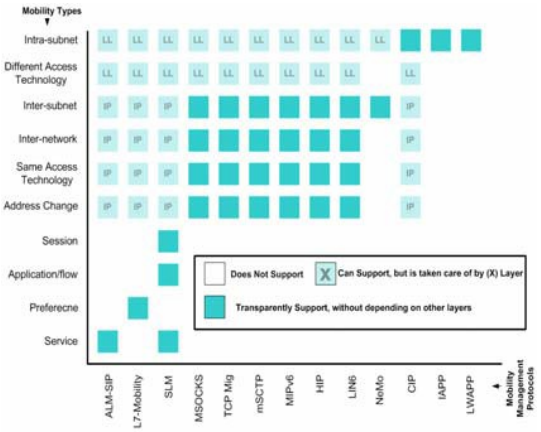

Figure 13 : Mobility Management protocols and their support for mobility types

6 Proposed Mobility Enabled Protocol Stack

Our proposed mobility enabled protocol stack, naming mechanism and wireless network architecture for the future wireless systems is shown in Fig. 14. In this architecture we demonstrate how we can use IAPP (Link layer solution), LWAPP (Link layer solution), 802.11 (Link layer solution), MIPv6 (Network layer solution), HIP (A new layer solution), SLM (Session layer solution) and FreezeTCP together in-order to support the entire mobility requirement (Fig-X) and to support all mobility types (figure-X). Generally, it is not recommended that the above mentioned protocols should co-exist with their full implementations. The reason is that they have different endpoint objects [1] and many mobility requirements will be redundant if they co-exist. Therefore, in our solution we propose to use an And-Based Co-existence (ABC) mechanism, as described in section 1.

In this proposed scheme, we propose a new end-host design, an enhancement of the naming service (e.g. DNS) to include End-Point Identities (EPID) [1] and new network architecture. We believe that in the future wireless networks end-host will have multiple interfaces and can have multiple server/client applications running on it. There may be cases in which we are just aware of the application name/id but do not have information about the device on which the application resides and the network it may be located in. Moreover, the mobile users might want to move application/session/flows between different devices in a Personal Area Network (PAN). Keeping these future mobility requirements in mind, we have proposed an end host design with three levels of identities i.e. interface identity, host identity and application identity. These identities have many to one and one to many relationships respectively. Interface identities are Care-of-Address (MobileIPv6) which a device gets in the visited network. A device identity is a Host Identify Tag (HIT) as defined in Host Identity Protocol (HIP) [Ref]. Mobile Object (MO) identity is EPID [1]. Another advantage of such architecture is that there is no tight binding of IP layer, transport layer and application layer as shown in (Figure-1). The naming system (e.g. DNS) is modified to have another mapping of Application ID (AID) to the IP address. The proposed naming system looks like, IP Address (could be multiple, as a device could have multiple interfaces): HIT (Theoretically/logically should be only One): Application ID (Could be multiple as device can have multiple applications running on it). In this case if a user only knows the application/service he/she needs to access and have no information about the location (IP) of the service and device its resides on (HIT), still the user can query the DNS with the AID to get corresponding HIT and IP address information. In our network architecture we propose to have lightweight access points with which mobile devices will directly communicate through 802.11 interface. The lightweight access point and access router will communicate using LWAPP [Ref] based messages. Inter heterogeneous access routers communication will be done by using 802.11F (IAPP) and this

protocol can also support proactive caching for fast mobile host handoffs.

The working of this proposed architecture is shows in the figure X, with the help of three mobility scenarios. First, movement of the mobile device within the same LWAPP administered domain. Second, movement of mobile device within two or more different LWAPP administered domains. Finally, the movement of mobile objects from one device to another within a Personal Area Network (PAN). In the case of (1), the mobile device is moving between the lightweight AP's within the administrative range of single LWAPP enabled access router. In this case as all the management operations including handover management is handled by the same Access Router (AR) so we do not have to make any changes to the end point (mobile device). (we have to associate Link Layer function)

In the case of (2), the mobile device is moving between two different LWAPP administrative domains. Now the mobile device will acquire a new address (CoA) from the new access router. IAPP will initiate a fast handoff (3) as discussed in section 5.5.1. Finally when the handover is complete the mobile node needs to update its CoA with in DNS, HA and CN (in case of router optimization). In the case of (6), where the mobile object (MO) moves from one device to another, the application needs to update its corresponding HIT and IP address in the naming system. HIP and MIP integration architecture is explained in HarMoNy [27]. The transport protocol which we plan to use is FreezeTCP[28], it is a connection migration scheme that's lets the MH 'freeze' or stop an existing TCP connection during handoff by advertising a zero window size to the CN, and unfreezes the connection after handoff. This technique is suitable for our architecture as it's a mobility aware scheme and reduces packet loss during the handoff process. Moreover this technique is specific to transport later and can work with other higher or lowers layers techniques. In our proposed architecture the vertical handoff can be achieved using any context aware vertical handoff application layer solutions [2][28].

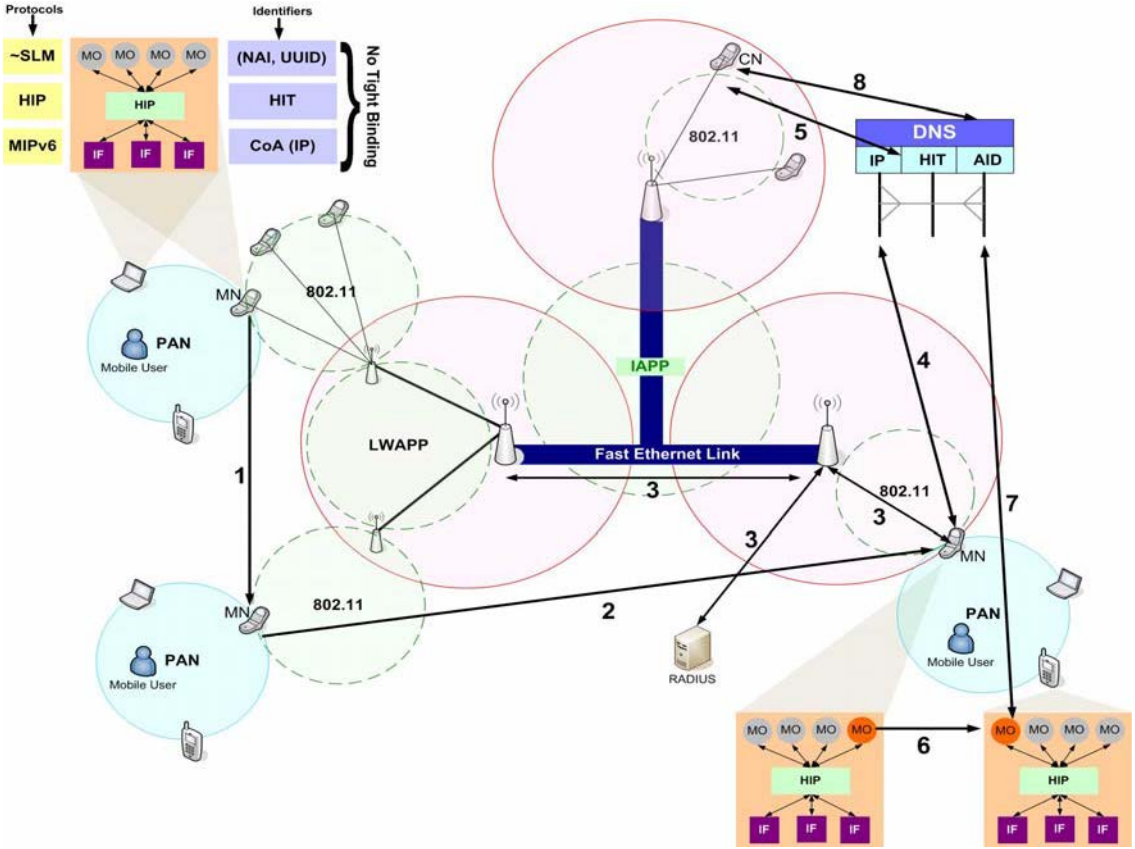

Figure 14 : A Proposed Mobility Management Architecture based on the AND-Based Co-Existence (ABC) Concept, for Future Wireless Networks

7 Conclusion

In this paper we are trying to emphasize on the concept of distribution of the mobility management tasks to all layers of the OSI protocol stack. We introduced a notion of "Mobility Enabled Protocol Stack" instead of mobility management solution on a

specific layer. In order to distribute the mobility management tasks to all OSI layers, in this paper we discuss these layers according to the mobility management requirements, their responsibilities in case of mobility, mobility types that can affect them and mobility types that they can support. We describe current proposed protocols for mobility management on different OSI layers. In addition to this, we have also pointed out the mobility management requirements that these protocols can fulfill and mobility types that they can support. As all these protocols are specific to a mobility solution on a particular layer, therefore they inherit limitations enforced by the dependency of that layer on other layers. Keeping this in mind, we propose And-Based Co-existence of mobility management solutions on different layers, to be the ideal solutions to materialize the concept of "Mobility Enabled Protocol Stack" for future wireless networks. We also propose a novel mobility enabled protocol stack that's based on our proposed notion of And-Based Co-existence. In our technique we also eliminate the dependencies of different OSI layers on each other to introduce flexibility and hot-swapping of interfaces and mobile objects on a single device. Our proposed technique fulfills all the mobility types and requirements and open up new horizon to a new area of Co-existence.

We identified two types of co-existence techniques And-Based and Or-Based. Although in this paper we proposed a solution based on the And-Based co-existence concept, but still we are not ignoring Or-Based co-existence. In future work, we plan to study Or-based co-existence in more detail, while thinking of redundancy as an opportunity not a threat for mobility management. The vision of our research is to make a hot-swappable mobility management stack that can be modified, changed and moved according to the network and user context.

8 REFERENCES

[1] Ismailov, Y. Holler, J. Herborn, S. Seneviratne, A. Internet Mobility: An Approach to Mobile End-System Design. *IEEE International conference on Mobile Communication and Learning Technologies*, (April. 2006), pp. 124-124.

[2] Balasubramaniam, S. Pfeifer, T. Indulska, J, Active Node suppoprting Context-aware Vertical Handover in Pervasive Computing Enviournment with Redundant Positioning, *IEEE International symposium on Wireless Pervasive Computing (ISWPC) 2006, Phuket, Thailand*, (January 2006)

[3] Yuan Chen, Lemin Li. A Fair Packet Dropping Algorithm Considering Channel Condition in Diff-Serv Wireless Networks. *The Fourth International Conference on Computer and Information Technology (CIT'04),* (June 2004) pp. 554-559.

[4] Wesley M. Eddy, At What Layer Does Mobility Belongs?, *IEEE Communication Magazine*, (Oct 2004). pp 155-159

[5] C. Perkins. *IP Mobility Support for IPv4*, January 2002. RFC 3220.

[6] Ian F. Akyildiz, Xie. J, Mohanty. S, A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems, *IEEE Wireless Communications, (August 2004).* pp. 16-28.

[7] Schulzrinne. H, Wadlund. E, Application-Layer Mobility Using SIP. *Mobile Computing and Communication Review*, (July 2000) Volume1, Number 2

[8] Fi. X, Hogrere. D, Narayanan. S, Soltwisch. R, QoS and Security in 4G Network. *First Annual Global Mobile Congress*. (Oct 2004).

[9] Tourrilhes. J, L7-Mobility: A framework for handling mobility at the application layer, *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, (2004), pp. 1246-1251. Vol.2

[10] Landfeldt. B, Larsson. T, Ismailov. Y, Seneviratne. A, SLM, A Framework for Session Layer Mobility Management, *In the Proc. IEEE ICCCN* (Oct 1999).

[11] Maltz. D, Bhagwat. P, MSOCKS: An architecture for Transport Layer Mobility, *In the Proc. INFOCOM* (1998)

[12] Snoeren. A, Balakrishnan. H, An End-to-End Approach to Host Mobility, *In the Proc., of MobiCom* (2000)

[13] L. Ong, J. Yoakum, An Introduction to the Stream Control Transmission Protocol (SCTP), *RFC 3758*, (May 2002)

[14] Stream Control Transmission Protocol (SCTP) dynamic address reconfiguration. *IETF Internet draft, Mar 2003*

[15] M. Riegel and M. Tuexen. Mobile SCTP. *IETF Internet Draft; draft-riegel-tuexen-mobile-sctp-*02.txt, Feb. 2003.

[16] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6. *RFC 3775*, June 2004

[17] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, Network Mobility (NeMo) Basic Support Protocol. *IETF RFC 3963*, (Jan 2005) [18] NeMo Working Group: http://www.ietf.org/html.charters/nemo-charter.html

[19] Ferguson P, Senie. D, "Network ingress Filtering: Dafeating Denial of Service Attack which employ IP source Address Spoofing", *IETF RFC 2267*, (Jan 1998)

[20] Ishiyama. M, Kunishi. M, Teraoka. F, An Analysis of Mobility Handling in LIN6, *International Symposium on Wireless Personal Multimedia Communication* (2001)

[21] A. G. Valko, A. T. Campbell, J. Gomez,

"Cellular IP - A Local Mobility Protocol," *IEEE 13th Annual Computer Communications Workshop, Oxford, Mississippi*, (October 1998).

[22] Chun. C, Shin. Kang, An Enhanced Inter-Access Point Protocol for Uniform Intra and Inter-subnet Handoffs. *IEEE Transactions on Mobile Computing*, Vol. 4, (August 2005).

[23] Zhaohui Cheng, Manos Nistazakis and Richard Comley. "*Security Analysis of LWAPP*", IWWST-2004, London, UK, (April 2004)

[24] R. Moskowitz, P. Nikander, Host Identity Protocol (HIP) Architecture, *IETF RFC 4423*, (May 2006)

[25] Perena. E, Sivaraman. V, Seneviratne. A Survey on network mobility support, ACM SIGMOBILE Mobile Computing and Communications Review, Volume 8, Issue 2 (April 2004), pp. 7-19.

[26] Xiaoming Fu, Dieter Hogrefe, Deguang Le, A Review of Mobility Support Paradigms for the Internet, IEEE Communications Surveys and Tutorials, Volume 8, No. 1, First Quarter, IEEE, ISSN 1553-877X, (2006).

[27] Herborn. S, Haslett. L, Boreli. R, Seneviratne, HarMoNy – HIP Mobile Networks. *VTC 2006*.

[28] T. Goff, J. Moronski, D. S. Phatak, V. Gupta, "Freeze-TCP: a true end-to-end enhancement mechanism for mobile environments", *IEEE INFOCOMM, Tel Aviv, Isreal. Pp 1537-1545*, (March 2000)

[29] Vidales. P, Baliosian. J etl. *Autonomic System for Mobility Support in 4G Networks*, IEEE Journal on Selected Areas in Communications. Vo1 23. pp 2288-2304.

[30] R. Koodli, Fast Handovers for Mobile IPv6, *IETF RFC 4068*, (July 2005)

[31] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, Hierarchical Mobile IPv6 Mobility Management (HMIPv6), *IETF RFC 4140*, (August 2005)