Journal of Information & Communication Technology
Vol. 3, No. 1, (Spring 2009) 36-49

Terminal Mobility In 3G and Beyond 3G Networks: Mobile Terminal and IPv6 Factors

Nazrul Nifkuzyaire Bin Zainudin*
Rahmat Budiarto *
School of Computer Sciences

Khurram Ghaniz*
School of Management,Universiti Sains Malaysia

ABSTRACT

The convergence of mobile phones with PDAs has give birth to smart phones as well as mobile terminals. The integration between cellular based operator systems such as GPRS/UMTS with Wireless LAN is known as Operator wireless LAN (OWLAN).Two giant companies in telecommunication industry Nokia and Ericsson both has their own Operator Wireless LAN solutions to offer to their targeted customers. This paper will suggest new OWLAN solution to fix with IPV6 network, WLAN, WWAN, and VLAN and also to support 3G and Beyond 3G devices. This paper also proposes new conceptual framework and protocol to facilitate mobility management in IPv6 network .We will also review IPv6 role for voice application powered by 3G and beyond 3G.

INSPEC Classification : B6250, C0230, C 3370, C 5640, C5670

Keywords : OWLAN, VLAN, Handoff Management, Hi^3, HDE, AOB, MMN, MMB3G, MT,WRS,Fast handoff,Dos,IPsec,SPINAT,HIT,HIP,I^3,,HI^3.,VoIPv6, QoS.

1. INTRODUCTION

Mobility management refers to terminal mobility, which includes two major complementary operations one: handoff management and the other location management (Sun J and Sauvola J. 2002). Handoff management maintains the active connections for roaming mobile terminals as they change their point of attachment to the network while location management tracks the Mobile Terminals for successful information delivery (A. H. Zahran, B. Liang, and A. Saleh, 2006). Terminal mobility is the only form of mobility currently supported for wireless system including dominating 2G, 3G and initial phase of the 3G+ also referred as B3G or 4G.Terminal mobility in 3G and beyond networks refers to the combination of wireless LAN solutions of modest authentication and roaming capability with mobile operator's SIM based subscriber management functions and roaming infrastructure.

Terminal mobility in 3G and beyond 3G networks is the promising step towards IP-network architecture. In the current defined OWLAN system architecture see figure 1 the WLAN

* The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (BIZTEK) or School of Computer Sciences and Universiti Sains Malaysia.

*Nazrul Nifkuzyaire Bin Zainudin : rmastech@yahoo.com
*Rahmat Budiarto : rahmat@cs.usm.my
*Khurram Ghaniz : bhailoogpk2000@yahoo.com

© JICT is published by the Institute of Business and Technology (BIZTEK).
Ibrahim Hydri Road, Korangi Creek, Karachi-75190, Pakistan.

access is authenticated and charged using GSM SIM. Currently, most OWLAN service provider use Radius protocol (C. Rigney, S. Willens, A. Rubens, and W. Simpson. 2000). Radius allows the existing PPP based authentication, authorization and accounting infrastructure to be used to control LAN access in addition to PPP access. Instead of using Radius for public WLAN (A. Acharya, C. Bisdikian, A. Misra, and Y.-B. Ko, 2003), we think of introducing new protocol and framework to suite public WLan environment in IPV6 network.

Seamless access to modern office tools or databases is essential for mobile professional workers. But using mobile to remotely access office networks is usually limited by transmission capacity of cellular networks. Seamless roaming and handover management between GSM/UMTS and Wireless LAN can settle this problem but a proper network protocol must be used at a proper network. Mobile IPv6 is a protocol specification developed by Internet Engineering Task Force to address the mobility of individual nodes. Mobile IPv6 takes this wireless access networks one step further by providing mobile nodes the ability to roam across wireless IP subnets without loss of network-layer connectivity. Mobile IPv6 is widely deployed in IP-based networks nowadays. Due to security holes, mobile IPv6 is now competing with Host identity protocol (R. Moskowitz and P. Nikander. 2003).

We are facing the integration of heterogeneous networks such as WWAN and WLAN, where vertical handoff is required. The heterogeneous co-existence of access technologies with largely different characteristics results in handoff asymmetry that differs from the traditional intra-network handoff (horizontal handoff) problem (A. H. Zahran, B. Liang, and A. Saleh, 2006).

During handover (IEICE TRANS. COMMUN., 2006), there is a period when the Mobile Node is unable to send or receive packets both due to link switching delay and IP protocol operations. This ``handover latency" (Srikant Sharma, Ningning Zhu, Ningning Zhu, 2004) resulting from standard Mobile IPv6 procedures, namely movement detection, new Care of Address configuration and Binding Update.Thus we for enhanced Ipv6.

In section 2, we summarize the related works (J. McNair, I. Akyildiz, and M. Bender, 2000), (Raihan Al-Ekram and Sagar Naik. 2002), (Srikant Sharma, Ningning Zhu, Ningning Zhu, 2004), (Andrei Gurtov, Anthony D. Joseph. 2004), (P. Nikander, J. Arkko, and B. Ohlman. 2004), (Gonzalo Camarillo; Miguel-Angel Garcia-Martin). In section 3 we explain Operator Wireless LAN system architecture. In section 4, we recommend IPv6 total mobility and its mobile components. In section we introduce Handoff Decision Engine (HDE) conceptually. In section 6, we discuss security in terminal mobility and outline current problems and solutions. In section 7 we explain Ipv6 roles in seamless mobility handover using VoIP.

2. BACKGROUND AND RELATED WORKS

Some works on vertical handoff have been reported in the literature. In (ROBERTO BATTITI, RENATO LO CIGNO, MARCO CONTI (editors) (2004)) a roaming scheme that considered the relative bandwidth of WLAN and GPRS was proposed. No information on how to obtain the available bandwidth is given. In (J. McNair, I. Akyildiz, and M. Bender, 2000) a detailed vertical handoff signaling procedure was presented. Recently a project team introduces a framework to analyst Vertical handoff algorithm in location-aware heterogeneous wireless network .The system architecture enable mobile node to wake a hotspot interface and prepare for approaching vertical handoff.

Researchers believe if the host is a mobile node, triangle routing problem occurs, since mobile IPv4 allows mobile to roam transparently in any network. In this situation mobile node must notify transfer information to its own home agent and correspond node in IPv6 network (Dae Sun Kim, Choong Seon Hong, Tatsuya Suda, 2006).Mobile IPv6 protocol can handle this problem since it support terminal mobility and also provides mobility independent of radio technology. Raihan Al- Ekram et al. (Raihan Al-Ekram and Sagar Naik. 2002) claimed that Mobile IPv6 handles mobility of individual nodes; it ignores the mobility of the entire network. Thus they proposed new framework and protocol operation to suite their mobility model. They also proposed a way to extend mobile IPv6 to enable network mobility and mobility inside mobility.

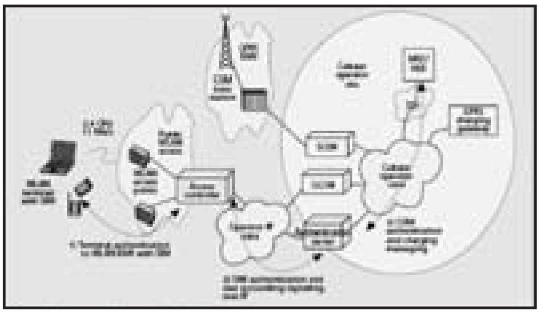
In the near future, the mobility and multi-homing features will coexist in the majority of small devices, e.g., terminals, PDAs, etc. In other word, mobile networking now is towards mobile host with multiple interfaces e.g. WLAN and UMTS. An IP address own by a typical mobile node represents both a host's identity and the host topological location led to ownership issue thus trustworthiness must now be proved through explicit cryptographic mechanisms. Recently, an efficient and secure protocol known as Host Identity Indirection Infrastructure (Hi3) emerges (P. Nikander, J. Arkko, and B. Ohlman. 2004). The proliferation of 802.B ROBERTO BATTITI, RENATO LO CIGNO, MARCO CONTI (editors) (2004)) (WIFI) based WLAN technology, the benefit of high STREAMIX connectivity as well the aggressiveness of IPv6 deployment in this country may convince investors such as Microsoft, Nokia, and Ericsson to deploy their OWLAN solutions in our country.

BridgePort Networks has vigorously participated in and led the development of the MobileVoIP handover requirements being finalized at both the 3GPP and 3GPP2 organizations. A number of handover control methods were evaluated. They ranged from methods that placed handover control in the handset versus the network. An alternative methods incorporated a single call leg versus two call legs. After debate, the industry has settled upon similar approaches in both the GSM and CDMA realms. 3GPP is working to adopt the IMS Control Model (ICM) MobileVoIP handover method, and 3GPP2 has adopted the Call Transfer Model (CTM) MobileVoIP handover method. Both standards anchor control for MobileVoIP handover in IMS network (Gonzalo Camarillo; Miguel-Angel Garcia-Martin) elements and establish multiple call legs during the handover process.

3. OPERATOR WLAN SYSTEM ARCHITECTURE

The OWLAN system architecture, depicted in Fig. 1, consists of the public LAN access network and the cellular operator site, which communicate over the IP backbone. The OWLAN have four entities: authentication server, access controller, access point, and mobile terminal (Fig. 1).The system architecture resembles a GPRS network.

Figure 1:
An overview of OWLAN system authentication (taken from (Juha Ala-Luarila, Jouni Mikonen, Jyri Rinnemaa, 2001))



The operator WLAN approach decreases the load of the cellular core by transporting only control signaling data to the cellular core. To enable packets access directly to the IP backbone and later use public or private services, the access control is needed sort of as the router. The subscriber authentication start off at public WLAN access point using GSM SIM to gets an IP address from the access controller, and initiates the network authentication by sending a dedicated authentication request to the access controller (1). The access controller relays the authentication request to the server (2) which implements the gateway between the access network and the GSM signaling network. The authentication server queries the GSM home location register (HLR) for the authentication data and performs user authentication using this information (3)

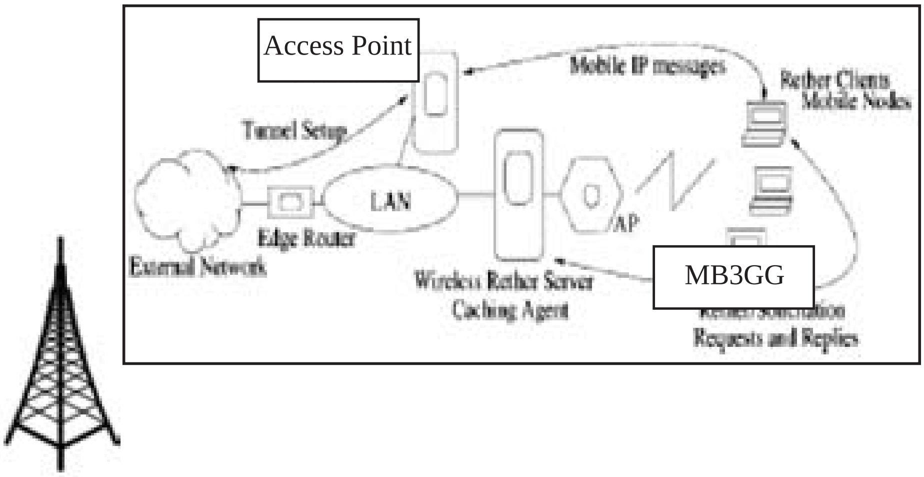
4. IPV6 ENHANCE TERMINAL MOBILITY

To facilitate mobility management in IPv6 Internet, we propose a conceptual framework and protocol operation by extending the Mobile IPv6 specification. The main idea is that, a typical mobile terminal in home network can act as mobile router in foreign network itself.

4.1.1 Mobility Model and Components

We extend the mobility model described in(Raihan Al-Ekram and Sagar Naik. 2002) to form the model for IPv6 terminal Mobility. In our model, a mobile network can consist of any number of nodes and beyond 3G routers inside it. The proposed solution is backward-compatible with existing PWLAN deployments. Figure 2 shows the components that comprise this model, and the following are the descriptions of those components.

Figure 2
Mobility Model and Components



4.1.2 Mobile Moving Network (MMN)

MMN is a network with two modes namely infrastructure (or access point) mode and ad-hoc (or peer-to-peer)mode, connected to the Internet by a single Beyond 3G router **(MB3GG),** which dynamically changes its point of attachment in the Internet. Thus its reachability in the IP topology is also changing dynamically. (i.e in a moving train).We integrated our MMN with wireless rether in order to provide QoS with roaming support. Whenever a mobile node in MN migrates to a new wireless subnet, it registers with the

Wireless rether server **(WRS)** responsible for the new subnet by sending a rether registration request to the well-known MAC address. Wireless Rether employs a centralized software token passing protocol to avoid collisions on the wireless channel.The token is distributed across wireless nodes in an exclusive fashion by a central node called wireless Rether server (Srikant Sharma, Ningning Zhu, Ningning Zhu, 2004).

4.1.3 Mobile Beyond 3G Gateway (MB3GG)

It is beyond 3G router which acts as border for the mobile multiple network **(MMN),** which attaches the (MMN) to the rest of the Internet. The **(MB3GG)** has at least two interfaces. The first interface is attached to the home agent if the mobile network is at (local network), or it is attached to cache agent (WRS) if the mobile network is away from home network. The beyond 3G router maintains the Internet connectivity for the mobile network and routes packets between the mobile network and the fixed internet via Public wireless Access point that serves as bridges between wired and wireless network. Multiple mobile terminals (MTs) is attached to this border router. They communicate among them using special case of mobile ad-hoc MOHAN (IEICE TRANS. COMMUN., 2006).

4.1.4. Mobile terminal (MT)

"Two-player games implemented in mobile terminals are an example of peer-to-peer services. If there is nostatic addressing (at the user layer), the users who want to play a game together would need to meet via a network resident server. This could mean that new games could not be introduced into new mobile terminals, before making sure that the deployed servers (if any) meet the specific requirements of the game in question.Mobile IPv6 can be used as a solution to this problem. The dynamic address being assigned by the GGSN is used as the Mobile IPv6 co-located care-of address.By registering this address with a home agent, a mapping of the dynamic address to a more static home address is created. This allows the mobile node to be reached with the home address, and also via a DNS name, since the home address can be registered with the DNS" (Nokia White paper 2001).

5. CONCEPTUAL FRAMEWORK COMPONENT

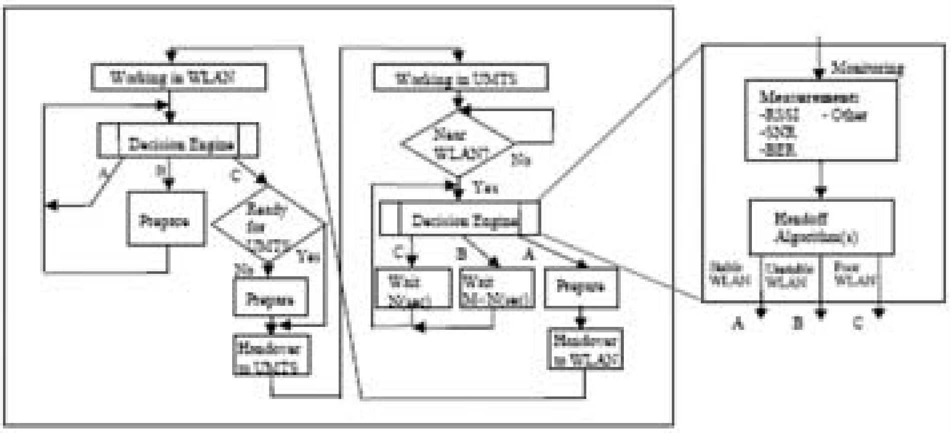
Our conceptual framework consists of AOB method and handoff decision engine to facilitate terminal mobility (mobility management) in heterogeneous network. Secondly, we introduce combination of Host identity protocol with I3 can cope with DoS attack.

AOB is a method to minimize the route discovery cost. The ABO method achieves this goal on the basis of packet overhearing. Packet overhearing is helpful to reduce route discovery cost, however, in current IEEE 802.11 MAC design; frames that are not targeted to the node will be discarded. If a node needs to receive packets that are not targeted to it, it is essential to set the node's network interface into promiscuous mode. In this mode, the MAC address filtering function that discards frames not targeted to the node is disabled. The drawback of using promiscuous mode is that, once it is set, all frames that can be correctly received will be passed to the upper layer and the node may eventually be drowned by overheard packets (IEICE TRANS. COMMUN., 2006).

5.1 Handoff Decision Engine

Handover management which is a part of terminal mobility consisting horizontal and vertical handoff. Horizontal handoff means handoff within the same wireless access network technology, and vertical handoff means handoff among heterogeneous wireless access network technologies. We can use handover decision engine (HDE) [6] to determine when to change between cellular system and WLAN. The engine can monitor handover between WLAN and UMTS as depicted in figure 3.

Figure 3:
Vertical handoff procedures between WLAN and UMTS (taken from K. Pahlavan et al., (2001))



We assume that WLAN hotspots implement loosely coupled connection with the 3G network using WLAN gateways. These gateways perform several tasks including serving as Mobile-IP agents and possibly providing QoS in the form of multiple service classes defined within the WLAN.

6. OVERVIEW OF MOBILE SECURITY

Mobile terminals need smart application to check for network security. We started off by introducing Hi3 protocol for our MMN above. This protocol check for security at IP-layer since its predecessor mobile IPv6 have build-in security which is IPsec still vulnerable to DOS attack. In addition, many of the current security protocols open a direct venue for CPU exhaustion denial-of-service attacks by sending in garbage. Finally, there is the desire to limit the possibilities for traffic analysis even by legitimate parties. Information about the current IP addresses (and therefore the location) of important units should not be visible to parties that are not involved in direct communication with them.

6.1.1. Host Identity Indirection Infrastructure

Networking architecture for mobile host is Hi^3. It is combination of Internet Indirection Infrastructure (i^3) and the Host Identity Protocol (HIP) forming the Host Identity Indirection Infrastructure. For future internet application Hi^3 is importance for secure mobility and multi-homing. Multi-homing refers to a situation where an end-point has several parallel communication paths that it can use (Pekka Nikander, Jukka Ylitalo, and Jorma Wall. 2003). Usually multi-homing is a result of either the host having several network interfaces (end-host multi-homing) or due to a network between the host and the rest of the network having unneeded paths (site multi-homing). Hi^3 were introduced to overcome Internet Protocol design which ignore address agility or IP-layer security (like IPsec and Mobile IP) and are not fully integrate, hence sometime doesn't interact well. Hi^3 uses the IPsec-aware NAT and SPINAT.

6.1.2. Internet Indirections Infrastructure (i^3)

Hi^3 suggest using i^3 to relay HIP handshake packets, thus serving as a control plane. I^3

was proposed to easy operation of services. as an alternative of clearly sending a packet to a destination, each packet is associated with a destination identifier; this identifier is then used by the infrastructure to deliver the packet. As an example, a host R may insert a trigger (id,R) in the i^3 infrastructure to receive all packets that have the destination identifier id. I^3 provide usual support for mobility. When a host changes its address, the host needs only to update its trigger. When the host changes its address from R1 to R2, it updates its trigger from (id,R1) to (id,R2). As a result, all packets with the identifier id are properly forwarded to the new address and this change is completely visible to the sender. The advantages i^3 are better DoS shield, support for simultaneous mobility and higher fault-tolerance when using Distributed Hash Table (DHT) with data replication. The shortcomings of using i^3 are dependence on an extensive infrastructure, server scalability, and use of UDP and lack of traffic encryption. Although i^3 could perform on both UDP and TCP, only UDP is support because maintaining much TCP connection between servers is difficult. As a cost some i^3 features maybe disable in the wide area, because UDP packets often do not traverse through firewall (even though not all) and Network Address Translation (NAT) devices. Basic i^3 did not support data encryption and lack of privacy for control packets- so when public infrastructure is used, i^3's wide-ranging infrastructure requirements bring other serious security issues including the possibility of malicious or mischievous i^3 nodes that do not forward correctly and a lack of trust of random i^3 severs from end points.

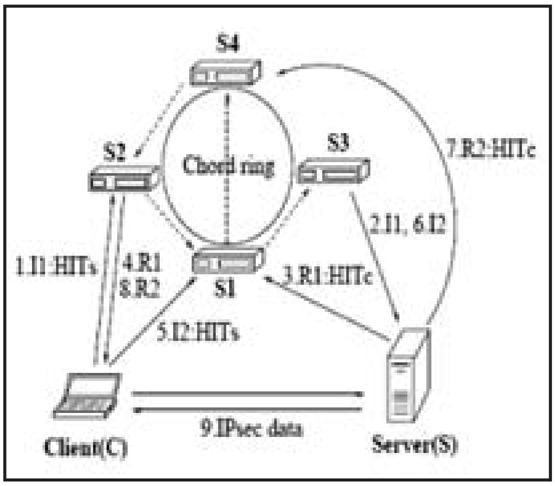
6.1.3. SPI multiplexed NAT

As a result of introducing IP-address-independent end-point identifiers, the connectivity trouble created by NATs becomes easier to deal with. Both the HITs in HIP and the trigger identifiers in i^3 are such address-independent identifiers. Nevertheless, utilizing the identifiers for NAT traversal in an architecturally clean way requires that the NATs become aware of the identifiers. SPI multiplexed NAT (SPINAT), as proposed by Ylitalo (J. Ylitalo and P. Nikander. (2004), is an approach to establish a state for HITs during a HIP base or mobility exchange. The association at the SPINAT device consists of a HIT pair, IP address pair, and ESP SPI pair. The base or mobility exchange packets are routed based on the HITs in the HIP header. Once the state at the SPINAT device has been established, the device identifies connections using the SPI value and the destination IP address in the ESP-protected data packet headers. With a SPINAT-like approach it becomes possible to connect several IP realms into a single network where the upper layer identifiers are used to route packets between the realms.

6.1.4. Integrating HIP and i^3

By combination of HIP and i^3 could overcome problem that arise from both protocol and infrastructure. The advantages of using i^3 as control plane (to establish Bindings between Mobile Node, Home Agent and Foreign Agent) for HIP in Hi^3 include protection from DoS attacks, solving the double jump problem, and providing an initial rendezvous service. By hiding parties' IP addresses until the HIP handshake partially authenticates them Hi3 provides additional protection against DoS attacks. Although some DoS protection could be provided by a HIP rendezvous server, the client's IP address is revealed to a server in the first control packet. Simultaneous mobility of both hosts in i^3 is supported by sending update control packets via i^3 when end-to-end connectivity is lost (Andrei Gurtov, 2004). Hi^3 inherits the challenges of the extensive i^3 infrastructure, including trust, accountability, and cost issues.

Figure 4:
setup of HIP connections in Hi^3. Taken from (Andrei Gurtov, 2004)



The client C sends an I1 packet to the address of a random i3 server it happens to have, S2 in this case. The public trigger for the server's S HIT (HITs) is stored in S1 server, and the packet is forwarded from S2 to S1 via Chord. The client obtains the correct i^3 server for future contacts to the recipient server, S1. For security, the server S also registers a private trigger that happens to reside on server S3. Therefore, S1 forwards I packets to S3 that in turn delivers them to S. A similar procedure is followed by S to send an R1 reply packet to C. C first contacts S1 that informs it on the correct location of C's public trigger, S4. From S4 packets are forwarded to C's private trigger on S2. The consequent I2-R2 exchange occurs in a similar manner, except that packets are sent straight to i3 servers keeping the public triggers, S1 and S4 respectively. When the base HIP exchange is completed, further communication occurs directly between C and S using IPsec payload (Andrei Gurtov, Anthony D. Joseph. 2004).

7. VOIP TECHNOLOGY FOR PROFESSIONAL WORKERS

VOIP networks are becoming an important part of the office and home network with many brands now producing reasonably priced VoIP equipment and phones. Software phones have also become much more flexible with support of many codecs (compressor/decompressors) available to perform video as well as voice data encoding compatible with standard computer equipment such as soundcards and webcams. With the recent spread of wireless network coverage around the world, it is now possible to buy 802.11b wireless SIP phones, enabling users to roam freely within a wireless network such as within a company. Other mobile technologies such as Mobile-IPv6 have also been developed enabling users to roam different IPv6 supported networks while maintaining the same "home location" IP address.

7.1.1 Overview of VoIP

Voice over IP (VoIP), also known as IP telephony, is the delivery of voice information over Internet Protocol (IP) packet switched networks. This means sending voice information in digital form in discrete packets instead in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP is that it can avoid the costs charged by ordinary telephone service by utilizing fixed charge IP network services such as broadband.

7.1.2 VoIP Servers

There are many different servers available both commercially and as open source. SIP Express Router (SER) supports only SIP clients and services. SER has inbuilt support for IPv6 as well as IPv4 and can listen on ports under both protocols simultaneously, giving the advantages of IPv6 such as mobility and removing the need for network address translation (NAT) (SIP Express Router).

Other packages available include Vovida Open Communication Application Library (VOCAL) which also supports both IPv4 and IPv6. VOCAL is an open source software package that enables a network to support VoIP. It is a complete system which comprises everything from user agent to call control and operations service support.

7.1.3 VoIP Clients

As with the server technology the more popular clients, software and hardware, mainly support the IPv4 protocol with support for IPv6. Some examples of commercially available clients include Windows Messenger for windows, SJPhone for Linux and Windows but none of these being open source (SJLabs SJPhone). KPhone and LinPhone are 2 excellent open sources software packages for Linux, both providing an easy to use Graphical user interface to enable an easy setup (KPhone). LinPhone is the only client found capable of supporting IPv6 without requiring any patching. The main problem is that the interface does not supply a long field enough to enter a full IPv6 address. Therefore, hostnames of IPv6 machines have to be used (LinPhone).

Typically most of the actual VoIP systems take advantage of the fact that users will accept low quality, stability issues and interoperability problems, in view of the fact that the system is free, with hardly any hardware costs if they own a PC and allows for just one access line where users can both simultaneously surf and talk. However this is not the view taken by professional VoIP developers.

Professional developers' main aims are to resolve the stability and interoperability problems of the system, as well as keeping the quality of audio at a quality level equal or better to that offered by the traditional telephone.

Interoperability issues are usually solved within VoIP system with the use of gate keepers and gateways. Gate keepers primarily store the addresses of all the users in which the gate keeper is in charge for. When one VoIP application wishes to contact another they must first contact the gate keeper who either usually returns the current address of the recipient or sets up a connection with the recipient and the calling applications.

Gateways are used to allow different types of VoIP application or possible other telephony application to interconnect with one other and this solves a lot of the interoperability issues.

The majority of VoIP system also actively monitors the quality of the audio during calls, such that, if a number of packets are being lost which results in a prolonged outage, the sending system is usually signaled to increase or change compression codec to reduce the congestion on the wire and to try and remove any future outages. On the other hand if there hasn't been a lost packet after a high number of received packets, then this usually means the network has some spare capacity. Therefore the receiving system may signal the sending system to change codec to improve the voice quality actively utilizing spare bandwidth.

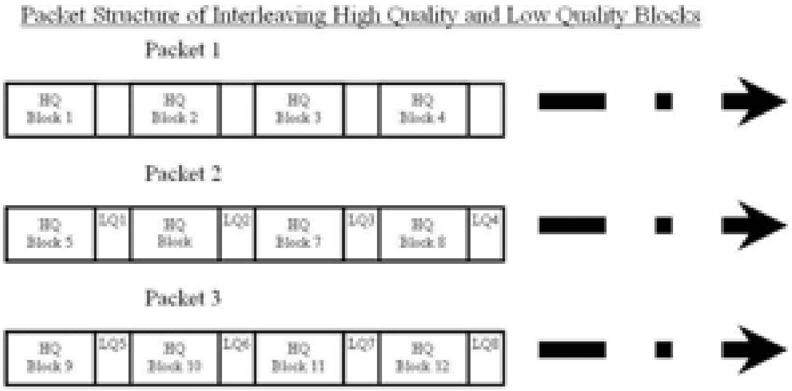
Some VoIP system allow for full mobility such that instead of simply allowing for mobile terminals as such within the Mobile Phone system, where users can use their phone whilst on the move, some VoIP systems, don't assign each terminal an address but assign each user an address to allow user roaming. This means users can both be mobile whist within a call, and also have the aspect of mobility in terms of moving from device to device. An example of this would be when an employee leaves home there contacting device would switch from their home phone to their mobile and then to their office phone when they arrive at work, this allows the user to maximize on the resources at hand since possibly at work or at home there may be extra bandwidth available in which will allow for improved quality or other services to be provided such as video.

To cope with data lost

There are a number of different approaches which could be implemented to try and cope with lost packets during transmission. Unfortunately, the most intuitive solution such as using a reliable protocol such as TCP which resends packets until the packet arrives successfully is not possible due to the temporal characteristic of this real time application.

A technique which could be implemented which tries to avoid data loss rather than to attempt to cope with its after effects is to transmit two copies of each audio block in separate packets. One such method which implements this technique is to within each packet, transmit four consecutive high quality audio blocks with interleaved a lower quality smaller copy of the blocks sent in the previous packet. This way if one packet is lost, there will be a lower quality copy of the audio within the next packet to fall back on. Diagram 1 below Figure 5 illustrates the packet structure.

Figure 5:
Pakcket Structure of Interleaving High Quality and Low Quality Blocks



The main advantage of this method is that when the occasional packet is lost as long as the next consecutive packet arrives, then the system can utilize the lower quality copy of the data within the next incoming packet reducing the chance of an audio outage.

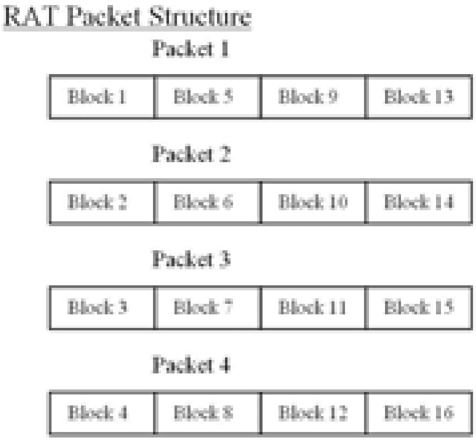
This method has a number of disadvantages specifically if consecutive packets are lost, then both high quality and low quality copies of the data will be lost resulting in an outage of audio where the receiving system has lacked audio blocks to play.

In order to implement this method successfully, requires adequate buffering of incoming packets on the receiving system, such that, audio blocks are available which can be played, while the application waits for the next packet to arrive with the replacement blocks within. This extra buffering adds extra delay. However, it is usually a normal practice to have extra buffering on the receiving system as a jitter buffer, to allow the system to re-sort out of order incoming packets, so packets are not classed as lost if they simply arrive out of order.

Another method of coping with data loss is to try and split the possible loss over time, such that for example if 100ms of sound was lost within a lost packet it would be better to have that loss split over 400ms such that four consecutive blocks of 25 ms are not lost. This helps to maintain the flow of voice exiting the system with just small blocks missing. This can be more easily ignored by the user than longer outages which can result in having to repeat words which can break up the flow of the user's conversation which can be very annoying.

This method has been taken from the Robust Audio Tools (RAT) within the MBONE multicasting tools developed at University College London (The Robust Audio Tool). Sixteen audio blocks are placed into four packets in packet order rather than block chronological order, this makes sure blocks within packets are not in consecutive ordering. The order of the blocks within the packets is important since this helps for the splitting of the outage of audio due to lost packets over time. The ordering of blocks consists of placing block one within packet one, block two in packet two, block three in packet three, block four in packet four, block five in packet one and so on and so forth. Figure 6 helps illustrate more clearly this ordering of blocks within packets.

Figure 6:
block order within packets used within the Robust Audio Tools developed at UCL.



RAT Packet Structure

Packet 1

Block 1	Block 5	Block 9	Block 13

Packet 2

Block 2	Block 6	Block 10	Block 14

Packet 3

Block 3	Block 7	Block 11	Block 15

Packet 4

Block 4	Block 8	Block 12	Block 16

The main advantage of this method is that the audio outage caused by a lost packet is split over time, for example if packet two was lost although four blocks of data would have been lost it would not be four consecutive blocks. The loss of the four blocks contained within the lost packet would be spread evenly over sixteen times the size of a block, this would help make the audio loss a little less noticeable.

8. DEVELOPING VOIPV6 APPLICATION

The main reason for developing a VoIPv6 application is that with little modification, the application should run on a Pocket PC PDA running the IPv6 stack. The benefit of this is that when combined with a wireless 802.11 network infrastructure running IPv6 and with a wireless card, the application could become mobile. This would make roaming possible as long as the devices remain within the area covered by the wireless network. This would allow users to make free voice calls to other users on the network, allowing for a greater level of interaction between mobile users.

9. DISCUSSION

Mobile terminals and Ipv6 factors are undeniable two important parts of discussion in terminal mobility management. In this paper, we aimed for quality of service indirectly via integration between fast handoff with wireless rather (Srikant Sharma, Ningning Zhu, Ningning Zhu, 2004),second via IPv6 enhanced mobility which takes advantage of mobile router(beyond 3G router) and specialized mobile ad-hoc (MOHAN). In addition we recommend of using ABO method so that mobile nodes can still surfing without Access points.

If we use existing mobile IP protocol for mobile network and the egress interface of the MB3GG follows MIPv6 operation, the packets from a CN to the MB3GG are successfully delivered but the packets destined to the nodes behind the MB3GG are dropped at the HA since binding cache in the HA has no information about the nodes behind the MR. To support the network mobility, the binding cache in Mobile IP must have information about the mobile network prefix of the MR's ingress interface.Note that MB3GG refer to mobile router.A mobile terminal which support beyond 3g system can act as mobile router and attach to many interface thus improve terminal mombility as a whole.

If a mobile terminal in MMN try to access to wired network via access points it will first locate the mobile agent.The mobile IP specification specifies two mechanisms for MA discovery, namely, MA advertisement and MA solicitation.Advertisement soliciting, caching and replaying can all be done in a way completely transparent to mobile IP. The caching agent need not be an independent host on the wired network. The caching and replay module may be run on the MA machine itself (Pekka Nikander, Jukka Ylitalo, and Jorma Wall. 2003) The only requirement is that the host participating in caching and replaying should set its network interface in the AOB mode.

Currently, mobile VOIP is synonymous with 'voice over WiFi' i.e. voice calls made over a WiFi network. Although the WiFi network is growing fast, the world is far from being a 100% WiFi enabled space. This means, mobile VOIP suffers from the physical limitations of being near a WiFi hotspot.

The requirement of being near a WiFi hotspot plus the high cost of Mobile WiFi handsets means that mobile WiFi is currently a niche technology. It's initial deployment is expected to be in the enterprise or within hotspots.

The real potential of mobile VOIP lies in the use of dual mode handsets. Dual mode handsets support the seamless handover between a cellular (in practise 3G and beyond) network and a WiFi network. The technologies used in this space are currently being defined for example - Unlicensed Mobile Access (UMA) and the Mobile Integrated Go-to-Market Network IP Telephony Experience (MobileIGNITE) alliance[Predictably, the incumbents such as mobile operators are reluctant to support mobile VOIP because it's a threat to their existing business (mobile voice calls). However, companies from outside the existing value chain are keen to promote mobile VOIP. Most notably fixed line operators and handset manufacturers However, the biggest barriers to the uptake of mobile VOIP are the pricing for IP traffic. I believe that the technology will really take off only when cheap, 'unlimited use' IP traffic becomes possible. Thus, as with so many services in the mobile data industry, the barriers are not technological but commercial. There is no doubt that mobile VOIP will have a part to play in the evolution of mobility in general. Its eventual success and role will depend on a range of technical and commercial factors some of which are outlined above. However, its real significance lies in the fact that it will put a downward pressure on voice call prices (which is still the mainstay of income For mobile operators).

If cheap unlimited use bandwidth becomes a possibility then the market may well take off in other directions. For example - it could be possible to make voice calls from a 3G network through an IP client on the phone without going through a dual mode handset etc. The success of such schemes depends on low costs for IP traffic. However, note that the technology exists even today to make this possible.Ironically, the mobile network itself is shifting to an IP core with technologies like IMS.When that happens, it should be possible to make end to end VOIP calls.

10. CONCLUSION

"The increasing amount of roaming data users and broadband Internet services has created a strong demand for public high-speed IP access with sufficient roaming capability. Wireless LAN systems offer high bandwidth but only modest IP roaming capability and global user management features. The designed architecture using by Nokia and Ericsson today exploits GSM authentication, SIM-based user management, and billing mechanisms, and combines them with public WLAN access. With the presented solution cellular operators can rapidly enter the growing broadband access market and utilize their existing subscriber management and roaming agreements. The OWLAN system allows cellular subscribers to use the same SIM and user identity for WLAN access. This gives the cellular operator a major competitive advantage over ISP operators, who have neither a large mobile customer base nor a cellular kind of roaming service" [12]. In this paper we recommended an OWLAN solution. We introduced a mobility model which can be attached to OWLAN .We also discussed the security issues in mobility and suggested that our OWLAN should use Hi3 protocol instead of using mobile IPv6 or HIP protocol which currently deployed
greatly world-wide. At the end or this paper we touch on Ipv6 role for voice application.

REFERENCES

Sun J and Sauvola J. (2002). Mobility and mobility management: a conceptual framework. Proc. 10th IEEE International Conference on Networks, Singapore, 205 - 210.

A. H. Zahran, B. Liang, and A. Saleh, (2006). Signal threshold adaptation for vertical handoff in heterogeneous wireless networks. ACM/Spring Mobile Networks and Applications (MONET), Special Issue on Soft Radio Enabled Heterogeneous Networks, vol. 11, no. 4, pp. 625-640, (extended version of IFIP Networking 2005 paper).

C. Rigney, S. Willens, A. Rubens, and W. Simpson. (2000). Remote Authentication Dial In User Service (RADIUS). RFC 2865, IETF Network Working Group, June.

A. Acharya, C. Bisdikian, A. Misra, and Y.-B. Ko, (2003). ts-PWLAN: A value-add system for providing tiered wireless services in public hot-spots. Proc. IEEE ICC 2003, vol.1, pp.193-197, Anchorage, Alaska, USA.

R. Moskowitz and P. Nikander. (2003). Host Identity Protocol Architecture. Internet Draft, work in progress.

ROBERTO BATTITI, RENATO LO CIGNO, MARCO CONTI (editors) (2004). Wireless On-Demand Network Systems Proceedings of WONS2004 Lecture Notes in Computer Science LNCS2928, 327-341.

J. McNair, I. Akyildiz, and M. Bender, (2000). An Inter-System Handoff Technique for the IMT-2000 System. Proc. IEEE INFOCOM 2000.

Dae Sun Kim, Choong Seon Hong, Tatsuya Suda, (2006). A Terminal Mobility Management Architecture for IPv4 and IPv6 Environments. Proceedings of 1th IEEE BcN2006, Vancouver,Canada,pp. 123-132.

Raihan Al-Ekram and Sagar Naik. (2002). IPv6 Total Mobility: An Extension of Mobile IPv6 to Support Mobility of Arbitrary Combinations of Nodes and Networks on the Internet 2002 International Conference on Wireless Networks (ICWN 2002); Las Vegas, USA, 24 - 27.

P. Nikander, J. Arkko, and B. Ohlman. (2004). Host Identity Indirection Infrastructure (Hi3). In Proc. Of The Second Swedish National Computer NetworkingWorkshop 2004 (SNCNW2004).

ROBERTO BATTITI, RENATO LO CIGNO, MARCO CONTI (editors) (2004). Wireless

On-Demand Network Systems Proceedings of WONS2004 Lecture Notes in Computer Science LNCS2928, Springer 327-341.

Juha Ala-Luarila, Jouni Mikonen, Jyri Rinnemaa, (2001). Wireless LAN access network architecture for mobile operators",IEEE Communications Magazine,vol 39(11), 82 89.

Srikant Sharma, Ningning Zhu, Ningning Zhu, (2004). Low-Latency Mobile IP Handoff forInfrastructure-Mode Wireless LANs, IEEE Journal on Selected Areas in Communication, Special issue on All IP Wireless Networks.

IEICE TRANS. COMMUN., (2006). VOL. 89-B (4).

Nokia White paper (2001). Introducing mobile IPv6 in 2G and 3G mobile networks.

K. Pahlavan et al., (2001). Handoff in Hybrid Mobile Data Networks, IEEE Pers. Commun..

Pekka Nikander, Jukka Ylitalo, and Jorma Wall. (2003). Integrating Security, Mobility, and Multi-homing in a HIP Way. Ericsson Research NomadicLab.

Andrei Gurtov, Anthony D. Joseph. (2004). Friends or Rivals: Insights from Integrating HIP and i3.Helsinki Institute for Information Technology.

J. Ylitalo and P. Nikander. (2004). BLIND: A complete identity protection framework for end-points. In Proc. Of the Twelfth International Workshop on Security Protocols.

SIP Express Router - http://www.iptel.org/ser

SJLabs SJPhone - http://www.sjlabs.com/

KPhone - http://www.wirlab.net/kphone/index.html

LinPhone - http://www.linphone.org

The Robust Audio Tool, URL http://wwwmice.cs.ucl.ac.uk/multimedia/software/rat/ the SIM application toolkit; stage 2. http://www.3gpp.org.

Gonzalo Camarillo; Miguel-Angel Garcia-Martin, "The 3G IP Multimedia Subsystem (IMS)", John Wiley & Sons, Ltd. pp. 6-12.