Integration of GSM technology with IPv6 Architecture

1SAMIR N. AJANI, 2PRATIMA L. PATEL
1Department of Computer Technology, SDMP, Nagpur, India
2Department of Computer Science & Engineering, GHRCE, Nagpur, India
Samir.ajani@gmail.com, pratima2011.patel@gmail.com

ABSTRACT

Consumers are demanding world-wide cellular access to the internet. This requires a global standard and effective means of accessing the internet from wireless devices. Integrating the two successful domains, viz., cellular networks and the Internet, provide anytime, anywhere access in third generation (3G) cellular networks. In this paper a hierarchical architecture for integration of cellular network (GSM) and Mobile IPv6 as mobility management is proposed. GSM is the most widely used cellular network and Mobile IP allows transparent routing of IP datagram in the Internet to the Mobile node irrespective of its physical location. Mobile IP provides an elegant solution for inter-domain, or macro-mobility management, but does not perform well for micro-mobility or intra-domain management. The transition of IPv4 to IPv6 is studied and its improvements are incorporated in the proposed architecture. The proposed hierarchical architecture improves the performance of Mobile IP in GSM networks in terms of fast intra-domain hand-offs.

Keywords - GSM; Mobile IPv6; IPv6 addressing scheme, neighbour discovery

1. INTRODUCTION

There are two major trends emerging in the world of telecommunications: an increase in the usage of mobile wireless devices, and an increase in usage of the internet. For example, the total number of Global System for Mobile Communications (GSM) subscribers has recently surpassed 110 million world wide. This, coupled with the high growth in IP data traffic, is leading the cellular industry to consider ways of combining these trends into one worldwide service. However, two major problems are holding up the development of wireless internet access. The Internet Protocol (IP) is the basic building block on which all Internet protocols are built. With the high growth in IP data traffic, combining the trends into one worldwide service is a research focus. The third generation (3G) networks intend to make the Internet mobile – accessible anytime and anywhere, providing complete access to time-sensitive data, regardless of the physical location. 3G cellular network architectures are being developed worldwide. The two bodies working towards 3G standards, 3GPP and 3GPP2, have introduced IP-based core network architectures. Though IP-based networks form part of 3G networks, there is still no agreement on any particular mobility management scheme. Mobile IP extends IP to support computing on the move and it is gaining wide acceptability. Most of the Internet traffic uses TCP (Transmission Control Protocol) connections. A TCP connection is defined by the combination of IP address and port number of both end-points of the communication. If one of these four number changes, the communication is disrupted and has to be reestablished. If a mobile node connects through a different access point to the network, it needs a new IP address. Mobile IP [1][1][3] addresses the challenges of moving a node to a different connection point without changing its IP address, by assigning the mobile node with two different IP addresses. Mobile IP being an extension of IP for mobile networks, it is well suited for the mobility management.

GSM (Global System for Mobile Communication) is the most successful digital mobile telecommunications system with over 100 million users in more than 130 countries using the GSM network. In GSM, system architectures and protocols, used for user-network signaling and global roaming are identical all over the world and hence enable worldwide development, manufacturing and marketing of products. There are usually three types of mobility encountered in IP based cellular networks- micro-mobility, macro-mobility and global mobility. Their definitions are as follows:

Micro-mobility: It is the movement of an MN (Mobile Node) within or across different BSs (Base Stations) within a subnet and occurs very rapidly. It is currently managed by using link-layer support.

Macro-mobility (intra-domain mobility): It is the movement of an MN across different subnets within a single domain or region, and occurs relatively less frequently.

Global mobility (inter-domain mobility): It is the movement of an MN among different administrative domains or geographical regions. Mobile IP works well in macro-mobility and global mobility environment. But it introduces significant latency when used in a cellular environment as handoffs occur frequently and registration messages may travel large distances before packet redirection occurs. Hence extending the powerful nature of Mobile IP for micro-mobility is the motivation for this paper. Many schemes like Cellular IP [4], HAWAII [9], MIP [4], Tele MIP [7] and GSM.IP [4] have been proposed as micro-mobility protocols. In this paper, we propose a hierarchical architecture that integrates GSM as a cellular network and Mobile IP as the mobility manager. The proposed architecture is different from these schemes in that it takes into consideration the addressing scheme for Mobile IPv6.
The rest of the paper is organized as follows. Section 2 discusses IP and IPv6. Section 3 describes about how GSM and IPv6 addressing schemes works. We present the proposed architecture with its advantages and analytical comparisons in Section 4. Conclusions are drawn in the last section.

2. MOBILE IP

Mobile IP can be thought of as the cooperation of three major subsystems. First, there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the Internet. Second, once the mobile computer knows the IP address at its new attachment point, it registers with an agent representing it at its home network. Lastly, mobile IP defines simple mechanisms to deliver datagrams to the mobile node when it is away from its home network. Mobile IP, through the use of sockets in the networking layer, supports application running on mobile devices. The logic behind choosing the network layer is to allow the mobility related issues to be treated as routing problem. It assigns two different IP addresses to the MN. One is the home address, which is static and does not change. It is therefore used to identify the TCP connection. The second IP address is called the care-of-address (CoA). It changes depending on the network to which the node is currently attached. If the mobile user moves away from its home network, the Home agent (HA) forwards the packet from the home address to the CoA. Home agent is a specially designated server that intercepts and forwards packets for absent subscribers. When away from home, the mobile unit sends its location information to its home agent via the Internet control message protocol (ICMPv6). This is called binding update.

2.1. Terminology

Before getting into more details, it is a good idea to frame the discussion by setting some terminology, adapted from the mobile IP specification [1][2]. Mobile IP introduces the following new functional entities:

- **Mobile node** - A host or router that changes its point of attachment from one network or subnetwork to another, without changing its IP address. A mobile node can continue to communicate with other Internet nodes at any location using its (constant) IP address.

- **Home agent** - A router on a mobile node’s home network which delivers datagrams to departed mobile nodes, and maintains current location information for each.

- **Foreign agent** - A router on a mobile node’s visited network which cooperates with the home agent to complete the delivery of datagrams to the mobile node while it is away from home.

- **Agent advertisement** - Foreign agents advertise their presence by using a special message, which is constructed by attaching a special extension to a router advertisement [1][2], as described in the next section.

- **Care-of address** - The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. There are two different types of care-of address: a foreign agent care-of address is an address of a foreign agent with which the mobile node is registered; a collocated care-of address is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

- **Correspondent node** - A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

- **Foreign network** - Any network other than the mobile node’s home network.

- **Home address** - An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

- **Home network** - A network, possibly virtual, having a network prefix matching that of a mobile node’s home address.

- **Link** - A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

- **Link-layer address** - The address used to identify an endpoint of some communication over a physical link. Typically, the link-layer address is an interface’s media access control (MAC) address.

- **Mobility agent** - Either a home agent or a foreign agent.

- **Mobility binding** - The association of a home address with a care-of address, along with the remaining lifetime of that association.

- **Mobility security association** - A collection of security contexts between a pair of nodes which may be applied to mobile IP protocol messages exchanged between them.

- **Node** - A host or a router datagram and then forwards it along to its ultimate destination.

- **Virtual network** - A network with no physical instantiation beyond its router (with a physical network interface on another network). The router (e.g., a home agent) generally advertises reachability to the virtual network using conventional routing protocols.

- **Visited network** - A network other than a mobile node’s home network to which the mobile node is currently connected.

- **Visitor list** - The list of mobile nodes visiting a foreign agent.
3. MOBILE IPv6

Mobile IPv6 [3], [6], is an evolutionary process and tries to eliminate the difficulties faced in IPv4. Much of its developments have been influenced by lessons learned in the existing Internet. As a technology it promises a number of advances such as larger address space (128 bits) which can support 128 addresses and enables hierarchical routing infrastructure, flexible addressing scheme, more efficient packet forwarding, inherent support for secure communications with IPsec, ability for differentiated services (QoS), better support for mobility and ease of management. The operation of Mobile IPv6 [10] is shown in Fig. 1 and can be summarized as follows: If the mobile node is in a Home network, it acts like any fixed host or router when connected to its home link. If it is in a foreign network, a mobile node determines its current location and acquires its care-of address using Neighbor Discovery Protocol and address autoconfiguration. A mobile node uses IPv6-defined address autoconfiguration to acquire a collocated care-of address on the foreign link either by stateless autoconfiguration or by stateful address configuration like DHCPv6. The mobile node notifies its care-of-address to its home agent via ICMPv6 by binding.

Update. The mobile node also sends binding update of its care-of-address to selected correspondent nodes, assuming it can do so securely. Packets sent by correspondents that are ignorant of the mobile node’s care-of address are routed first to mobile node’s home network, where the home agent tunnels them to the care-of address. Packets sent by correspondents that know the mobile node’s care-of address are sent directly to the mobile node using an IPv6 Routing Header, which specifies the mobile node’s care-of address as an intermediate destination. In the reverse direction, packets sent by a mobile node are routed directly to their destination using no special mechanisms. In Mobile IPv6, extension headers are used to allow the sending of packets to the mobile node’s care-of address directly by cashing the binding of a mobile node’s home address with its care-of address. The mobile node attached to a foreign network now uses its care-of address as a source address when sending packets. The mobile node’s home address is carried in a Destination Options header, which means the session control information is piggybacked onto the same packet [10][3].

![Fig (1) Working of Mobile IPv6](image)

3.1. Performance Evaluation

We used the standard metrics for protocol evaluation in our tests. We measured round-trip time in nanoseconds (ns) for TCP, throughput in megabits per second (Mbps) for both TCP and UDP protocols, socket creation time in ns for stream (TCP) and datagram (UDP) sockets. We also measured connection time for an application to tunnels them to the care,

which specifies the mobile node’s care-of address space (128 bits) which can support 128 addresses and enables

better support for mobility and ease of management. The operation of Mobile IPv6 [10] is shown in Fig. 1 and can be summarized as follows: If the mobile node is in a Home network, it acts like any fixed host or router when connected to its home link. If it is in a foreign network, a mobile node determines its current location and acquires its care-of address using Neighbor Discovery Protocol and address autoconfiguration. A mobile node uses IPv6-defined address autoconfiguration to acquire a collocated care-of address on the foreign link either by stateless autoconfiguration or by stateful address configuration like DHCPv6. The mobile node notifies its care-of-address to its home agent via ICMPv6 by binding.

Update. The mobile node also sends binding update of its care-of-address to selected correspondent nodes, assuming it can do so securely. Packets sent by correspondents that are ignorant of the mobile node’s care-of address are routed first to mobile node’s home network, where the home agent tunnels them to the care-of address. Packets sent by correspondents that know the mobile node’s care-of address are sent directly to the mobile node using an IPv6 Routing Header, which specifies the mobile node’s care-of address as an intermediate destination. In the reverse direction, packets sent by a mobile node are routed directly to their destination using no special mechanisms. In Mobile IPv6, extension headers are used to allow the sending of packets to the mobile node’s care-of address directly by cashing the binding of a mobile node’s home address with its care-of address. The mobile node attached to a foreign network now uses its care-of address as a source address when sending packets. The mobile node’s home address is carried in a Destination Options header, which means the session control information is piggybacked onto the same packet [10][3].

![Fig (1) Working of Mobile IPv6](image)

3.1. Performance Evaluation

We used the standard metrics for protocol evaluation in our tests. We measured round-trip time in nanoseconds (ns) for TCP, throughput in megabits per second (Mbps) for both TCP and UDP protocols, socket creation time in ns for stream (TCP) and datagram (UDP) sockets. We also measured connection time for an application to establish TCP connection in ns. Finally, we measured the percentage of CPU utilization for all the measurement tests and number of connections that can be established per second. Maximum efforts are taken to minimize the number of processes running while the testing applications are run to give better access to the resources for the testing applications. But owing to the pre-emptive nature of the operating systems that are being tested, we cannot guarantee exclusive access of the resources for the testing applications. However, the experiments are repeated to get consistent measurements. The test for each metric is carried out for 30 times for any given payload size and the average is taken. The entire experiment was conducted for around 2000 times initially to check for the consistency of the values obtained for all iterations and found that a sample size of 30 is sufficient to get a consistent average. Moreover, we are interested in the performance of the IPv6 stack as perceived by the end users and hence exclusive access to resources is not mandatory. As far as test-beds II and III are concerned, they are isolated from other networks to avoid the unwanted traffic caused by other systems on the network.

4. INTEGRATING GSM AND MOBILE IPv6

In order to understand the integrated architecture, let us first discuss how GSM will work in conjunction with IPv6 addressing scheme [11][3].

4.1. Gsm Architecture

The GSM architecture is shown in Fig. 2. The architecture is divided into sub-systems like mobile station, base station subsystem and network subsystem. The different components in Fig. 2 are explained as below.
By using the Subscriber Identity Module (SIM) card with a GSM terminal, the user is able to receive and make calls from that terminal. Each mobile terminal has been assigned a 15-digit International Mobile Subscriber Identity (IMSI) using the SIM card. Each ME (mobile equipment) is also assigned a unique 15-digit International Mobile Equipment Identity (IMEI) at the time of manufacture. The Base Transceiver Station (BTS) contains the radio transceivers for a cell and implements radio-link protocols to interface with the mobile station. The mobile equipment and the BTS are connected through a Um interface. The Base Station Controller (BSC) manages one or more BTSs. It performs radio-channel setup, frequency hopping, and handovers. There is an interface between BTS and BSC. The BSC connects the mobile station with mobile services switching center (MSC). The MSC is the most important component of Network Subsystem. Its functions are to provide services related to registration, authentication, location updating, handovers, and call routing. Call routing is achieved by using the home location register (HLR) and visitor location register (VLR) along with the MSC. HLR contains the registration information of subscribers and their present location. The HLR is a database and could be implemented as a distributed database. The VLR associated to each MSC is a very dynamic database which stores all important information needed for the MS users currently in the Location Area (LA) that is associated to the MSC. Security and authentication are achieved by the use of equipment identity register (EIR) and the authentication center (AuC). EIR is a database, which stores all the valid mobile equipment information, such as IMEI for each mobile station on the network. The secret key for each user's SIM card is stored in the AuC database. This key is used for authentication and encryption. There is an A interface between base station subsystem and network subsystem.

### 4.2. IPv6 Addressing Scheme

IPv6 addresses are assigned to interfaces, not to nodes, as in OSI (Open System Interconnection), so each interface of any node needs at least one unicast address. A node can therefore be identified by the address of any of its interfaces. An IPv6 address has 128 bits, or 16 bytes. The address is divided into eight, 16-bit hexadecimal blocks, separated by colons. For example:

```
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

A typical IPv6 address consists of three parts – the global routing prefix, the subnet ID, and the interface ID, as shown in Fig. 3.

![IPv6 address structure](image)

**Fig (3) IPv6 address structure**

The global routing prefix is used to identify a special address, such as multi-cast, or an address range assigned to a site. A subnet ID is used to identify an interface within a site. The subnet ID may also be referred to as subnet prefix or simply “subnet”. A subnet ID is associated with one link. Multiplesubnet IDs may be assigned to one link. An interface ID is used to identify an interface on a link and needs to be unique on that link. Addresses in the prefix range 001 to 111 should use a 64-bit interface identifier that follows the EUI-64 (ExtendedUnique Identifier) format (except for multicast addresses with the prefix 1111 1111). The notation for prefixes has been specified as:

An IPv6 unicast address uniquely identifies an interface on a IPv6 node. A packet sent to a unicast address is delivered to the interface identified by that address. Aggregatable global unicast addresses are identified by binary prefix 001. The format of global-scope IPv6 unicast address is as shown in Fig. 4.

![Global Scope IPv6 Unicast Address](image)

**Fig. (4) Global Scope IPv6 Unicast Address**

TLA ID (Top-Level Aggregation Identifier): The TLA ID identifies the highest level in the routing hierarchy. TLA IDs are administered by the Internet Assigned Numbers Authority (IANA) and allocated to local Internet...
registries that in turn allocate individual TLA IDs to large, long haul ISPs. Res (Reserved): Bits that are reserved for future use in expanding the size of either the TLA ID or the NLA ID (defined next). NLA ID (Next-Level Aggregation Identifier): The NLA ID allows an ISP to create multiple levels of addressing hierarchy within its network to both organize addressing and routing for downstream ISPs and identify organization sites. SLA ID (Site-Level Aggregation Identifier): The SLA ID is used by an individual organization to identify subnets within itself.

Interface ID — It indicates the interface on a specific subnet. The size of this field is 64 bits. The interface ID in IPv6 is equivalent to the node ID or host ID in IPv4.

4.3. Local-Use IPv6 Unicast Addresses

There are two types of local-use unicast addresses defined: Link-Local and Site-Local addresses. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Link-local unicast addresses have the hexadecimal prefix Link-Local addresses have the format shown in Fig. (5).

![Fig. (5) Link-Local IPv6 Unicast Address](image)

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present. Routers must not forward any packets with link-local source or destination addresses to other links. Site-local unicast addresses have hexadecimal prefix FECA::/10. Site-Local addresses have the format shown in Fig (6).

![Fig. (6) Site-Local IPv6 Unicast Address](image)

Site-Local addresses have the format shown in Fig. Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. Although a subnet ID may be up to 54 bits long, it is expected that globally-connected sites will use the same subnet IDs for site-local and global prefixes. Routers must not forward any packets with site-local source or destination addresses outside of the site.

4.4. Neighbor Discovery

Neighbor Discovery and stateless autoconfiguration in IPv6. The IPv6 protocols known collectively as Neighbor Discovery (ND) [12] replace a number of IPv4 protocols that offer some autoconfiguration facilities. ND defines new functionality as well. In general, ND performs three major functions: First, it provides address resolution service, updating and expanding IPv4’s address resolution protocol (ARP), to determine layer 2 addresses of nodes on the same link. Second, it allows hosts to discover what neighboring routers are present and provides a mechanism for obtaining certain configuration information from them. Third, it defines Neighbor Unreachability Detection (NUD), a mechanism that determines when a neighbor becomes unreachable. If the neighbor is a router, the node invokes a reconfiguration procedure to find an alternate router. ND is implemented within the Internet Control Message Protocol (ICMP), making all services independent of link technologies. ND defines two main pairs of messages. Neighbor solicitation (NS) and neighbor advertisement (NA) messages are used to determine the link-layer addresses of neighbors, as well as to verify that a neighbor is reachable. Router solicitation (RS) and router advertisement (RA) messages are used to locate and obtain information from routers. During ND, a node first forms its link-local address by appending its 64-bit interface ID (mostly a MAC in EUI-64 format). It also does DAD (Duplicate Address Detection) Check to ensure that the newly formed address is not already in use by another node on the attached link.

5. HIERARCHICAL ARCHITECTURE

The architecture shown in Fig. 7 is hierarchical and makes use of link-local Unicast address for communicating in a region under one BSC and site-local Unicast address for communicating in a region under one MSC. The mobile node acquires its unicast addresses by using its IMSI of SIM card. Interface ID. The SIM card or IMSI number of the mobile device is a 15-digit number. In order to use this SIM as interface identifier, it is assumed that this number is converted into IEEE EUI-64 format for mobile interfaces. Let us call the converted format as SIM-EUI 64. Each roaming mobile node digits two care-of-addresses, one link-local address to move in a region under particular BSC and one Site-local address to move in a region under one MSC. For the Home agent and the correspondent node, the care-of-address of the mobile node would be the IP address of MSC. Each BSC keeps a database of all the nodes in their domain; the node registers with them. The BSC maintains and manipulates the tuple <Home address, Link-Local Address, Site-Local Address> as and when a node registers or leaves. The Home address is same as the global Unicast address. This database at the base station does not differentiate whether the mobile terminals registered in it are its own subscribers or roamers. The BSC send updates to MSC each time a particular mode enters or leaves its domain. A MSC contains list of subscribers.
in its HLR and roamers in its VLRs. It also maintains the table of tuple <HomeAddress, Site Local Address, Corresponding BSC ID> for all mobile nodes in its region.

6. ADVANTAGES OF THIS SCHEME
Whenever the mobile node moves from one BSC to another BSC under the same MSC, it changes link-local care-of-address, but retains the same site-local care-of-address and hence it need not have to send the binding update to its homeagent each time it changes its BSC. The MSC handles this hand-off as it handles for normal hand-off in cellular networks. So MSC handles the intra-domain mobility. Whenever the mobile node changes its MSC, then it sends the binding update to its home agent with the care-of address as the new MSC's IP address. This way, the mobile node does not have to send the binding updates each time it changes its point of attachment. As the number of binding updates to home-agent is reduced, the latency is decreased. Consider this case. MN1 and MN2 are both roamers, but both are roamers under the same BSC. Inconventional Mobile IP, the routing of packets from MN1 to MN2 will be from the subnet of MN1 to home agent of MN1, from home agent of MN1 to home agent of MN2, from home agent of MN2 to subnet of MN2 (which is same as that of MN1) and then communication is established. This increases latency. Using the proposed architecture, the communication between MN1 and MN2 is established in one go only, due to the database in BSC. It is consistent with the GSM architecture. All the entities in GSM are used with few modifications. As the GSM subscribers now use SIM card, they can still use the SIM card with slight modification to adapt to this IP based architecture, as it achieves the address using SIM card number.

7. ANALYTICAL COMPARISON
Analytical comparisons of different architectures in terms of number of location updates is shown in Table 1. M is the total number of MSCs, HN is Home Network, FN is Foreign Network, P is number of mobiles visiting “N” BSCs one by one, N being the total number of BSCs and R is number of BSCs under one MSC. It is seen that the proposed architecture achieves same efficiency in terms of location updates as that of TeleMIP, but our proposed architecture takes into consideration Mobile IP version 6 and does not make use of separate Mobile Agents (MA) and DHCP servers, which helps in decreased implementation cost compared to TeleMIP. It is seen that the high latency during location update can be reduced if there are more BSCs under each MSC. Reducing this latency makes it possible for real-time data to be communicated over wireless channels.

8. CONCLUSIONS
Mobile IP in general and Mobile IPv6 in detail are studied. An architecture to integrate GSM and Mobile IPv6 is proposed which can improve the performance of Mobile IP in micromobility environments. The proposed architecture is compared with other architectures. It is observed that the latency can be minimized using this architecture, as the binding updates are not sent to the home agent (and correspondent nodes) each time the MN changes its point of attachment.

9. REFERENCES
[10] Daniel G. Waddington and Fangzhe Chang, Bell Research Laboratories “Realizing the Transition to IPv6”.