Investigating the Applicability of Mobile IP and Cellular IP for Roaming in Smart Environments

Keara Barrett, Ray Carroll and Dr. Sven van der Meer
Telecommunications Software & Systems Group,
Waterford IT, Ireland
{kbarrett, rcarroll, vdmeer}@tssg.org

Abstract

Increased research and development in the field of ubiquitous computing, and in particular smart spaces, has heightened the need for a comprehensive mobility solution. Existing mobility protocols are often categorised as either macro or micro mobility but few, if any, bridge the divide between the two. Mobile IP is at present the IETF proposed standard for delivery of IP packets to mobile devices. However, as a macro mobility protocol, it does not adequately support data delivery to mobile devices that regularly roam within local networks. Cellular IP, a more recent development in mobility, falls under the banner of micro mobility and as such delivers a number of benefits that a macro mobility protocol alone could not. This paper describes a complete mobility architecture accomplished by integrating Mobile IP with Cellular IP and continues by addressing the suitability of this integration for supporting roaming in smart environments.

Keywords: Smart environments, smart spaces, macro mobility, micro mobility, Mobile IP, Cellular IP

1 Introduction

The Ubiquitous Computing paradigm has rapidly emerged in the last number of years as a significant field of research. The notion of computers all around us, embedded in walls, furniture, clothing and various aspects of physicality has captured the imagination of the research community. Within ubiquitous computing the concept of smart spaces is also widely discussed. The National Institute of Standards and Technology (NIST) Smart Space Laboratory (www.nist.gov/smartspace/) defines smart spaces as "*…environments with embedded computers, information appliances, and multi-modal sensors allowing people to perform tasks efficiently by offering unprecedented levels of access to information and assistance from computers*" These spaces are typically delimited by a physical space, i.e. a certain room or building may be an individual smart space.

The entire concept of ubiquitous computing revolves around the ability of users to be mobile while seamlessly retaining 'always on' access to information and services. The revolution in computer mobility that is anticipated in the computing research community can be compared to that of the telecommunications world. Computer mobility will be as simple as picking up a mobile device and moving as is the case today with mobile phones. As smart spaces are expected to be widespread, users must be able to move between them quickly, easily and as often as is required. However, in current networking standards such as TCP/IP, mobility is limited and involves the clumsy breaking and re-establishment of connections. Hence new mechanisms and standards that allow users to roam seamlessly between smart spaces and their administrative domains are essential for the success of this new computing paradigm.

In terms of mobility, there are two main types that must be considered. These are Micro and Macro mobility. *Macro Mobility* is concerned with the movement of users/devices at a large scale, between wide area wireless networks. On the other hand *Micro Mobility* deals with mobility on a local level, such as within a wireless network. Cellular IP is a micro mobility while the Mobile Internet Protocol (Mobile IP) falls under the banner of macro mobility.

2 Overview

2.1 Mobile IP

2.1.1 MIPv4

Mobile IP first came to light in the early nineties when IBM submitted a draft of the standard to the Internet Engineering Task Force (IETF). This draft was accepted as a Request For Comment (Perkins, 1996-RFC 2002) and has been the topic of much research over the last number of years. The protocol is designed to allow transparent mobility of users while minimising the impact of mobility on current internet standards. In today's IP environment any node that moves from its own

network (*Home Network*) to some other network (*Foreign Network*) will be assigned a new IP address. Any communicating nodes (*Correspondent Nodes*), however, would continue to transmit to the original home IP address (*Home Address*) without realising that the node had moved and this address was now obsolete. Furthermore, TCP (Transport Control Protocol) relies on IP addresses to establish and maintain connections. So in order for communication with a new IP address to continue, the session would need to be restarted with the new IP address.

Mobile IP is an enhancement of TCP/IP since it uses the existing protocols to send its messages. The key concept is that each mobile node (MN – 'Mobile Host' in Cellular IP) has two IP addresses. The original home IP address of the node is retained and a new address (*Care-of Address*) is assigned to the mobile node while away from its home network. The correspondent node (CN) can continue to transmit to the home address but the data is forwarded from the home network to the care-of address. In this way the correspondent node is not aware that the node has moved. Similarly the mobile node will continue to receive packets as if it were still attached to its home network. The principle is very similar to that of *call forwarding* in the telecommunications industry (e.g. a phone call to someone's home can be forwarded to his or her mobile phone, office etc).

To facilitate this, Mobile IP introduces three major components: the Home Agent (HA), the Foreign Agent (FA) and the Care-of Address (CoA). As can be seen in Figure 1 the home/foreign agent is located in the home/foreign network and operates as a router. Mobility agents (home/foreign) advertise their presence on a network using special messages called *Agent Advertisements*. These messages are broadcast or multicast at regular intervals. From the agent advertisement it receives, the mobile node can determine if it is on the home or a foreign network. When a mobile node moves to a foreign network it acquires a care-of address in one of two ways. The CoA may be obtained from a particular field of the agent advertisement and is known as a '*foreign agent care-of address*'. This is actually the address of the foreign agent that the mobile node is registered with and not the mobile node itself. This way more than one mobile node can share the same care-of address, as data from the home agent is only tunneled as far as the foreign agent who then determines which mobile node the data is destined for and sends it to this node. Alternatively the care-of address can be assigned directly to the mobile node using some external means, such as the Dynamic Host Configuration Protocol (DHCP). This type is known as a '*co-located care-of address*'. This address is uniquely addressable so data can be forwarded directly to the mobile node.

The purpose of the home agent is to intercept all incoming data destined for the mobile node's home address and forward this data to the mobile node's care-of address. So once a care-of address has been assigned, the mobile node must then register this address with the home agent. This is done by sending a *Registration Request* message to the home agent who then replies with a *Registration Reply* accepting or denying the request. Once the mobile node has been registered communication between the correspondent and the mobile node can occur. The correspondent node sends packets to the home address as normal but the home agent (aware that the MN is away from the home network and has a CoA) intercepts these packets using the Address Resolution Protocol (ARP).

The home agent then *tunnels* these packets to the care-of address. Tunneling means that a new IP header is attached to the original IP packet using the IP in IP tunneling technique (Perkins, 1996 - RFC1853). The new header uses the care-of address as the destination address. Since the original packet is encapsulated within a new IP header its source and destination addresses have no effect on the routing of the packet until it reaches the care-of address.

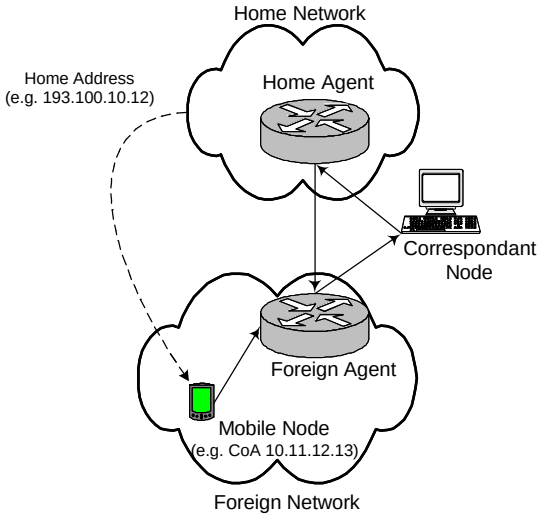

Figure 1 – Mobile IP (v4)

At the (foreign agent) care-of address the outer IP header is striped off by the foreign agent and the inner destination address (home address) is compared to the entries in the foreign agents *visitor list*. If the packets destination address has an entry in the visitor list (mobile node is registered with that foreign agent) the decapsulated packet is sent

to that mobile node. In the case of a co-located care-of address the encapsulated packet is sent straight to the mobile node where it is decapsulated by the node itself.

In response to the correspondent node, the mobile node sends packets using the correspondent node address as the destination and its own home address as the source. This packet is not tunneled but instead sent straight to the correspondent node via normal routing means. As these packets use the MN home address as their source, the correspondent node will continue to transmit to the home address as it knows nothing of the mobile nodes new loaction.

2.1.2 Problems with MIPv4

2.1.2.1 Triangular Routing

Triangular routing is the situation where all traffic from the correspondent node to the mobile node is routed via the home agent (see Figure 1). This method of routing increases the traffic on the network as the packets are first routed to the home agent and from here they are tunneled to the mobile node. In particular this increases the load on the home agent.

2.1.2.2 Ingress Filtering

Ingress Filtering (Fergesun & Senie, 2000) involves routers dropping packets that do not have a source IP address consistent with the network address of the network it is being sent from. This presents a major problem to the operation of Mobile IP. As was described in section 2.1.1, a mobile node attached to a foreign network sends packets using its home address as the packet source. Hence the packet source will have a different network prefix to the foreign network address. Routers in the foreign network that employ ingress filtering will drop this packet.

2.1.3 Mobile IPv6

Mobile IPv6 (Perkins, Johnson & Arkko, 2003) was designed based on the experiences gained with Mobile IPv4 and as such resolves many of the problems identified with the previous version. The key advantage in MIPv6 is that it is based on the new IPv6 protocol. IPv6 addresses many of the shortcomings of the older IP protocol (namely the limited address space) and any modifications to Mobile IP can be made prior to the rollout of IPv6. Hence these changes can be better incorporated into the new IP protocol.
The basic principle of MIPv6 is the same as that of MIPv4 but there have been some notable changes.

2.1.3.1 Address Auto Configuration

The most noticeable difference in MIPv6 is the lack of any foreign agent. Due to the larger address space and the address auto configuration feature of IPv6 the need for a foreign agent has been removed. The mobile node can now obtain a care-of address from a DHCPv6 server or by extracting the network prefix from router advertisements and adding a unique interface identifier to it. Hence the mobile node is uniquely addressable and data can be forwarded directly to it.

2.1.3.2 Route Optimisation

As mentioned before, one of the main problems with MIPv4 is triangular routing (see 2.1.2.1). The recommended solution to this problem is termed route optimisation. Initially the correspondent node (CN) will send packets to the mobile nodes home address. The home agent will then tunnel these packets to the mobile node as is normal in MIPv4. However, by receiving a tunneled packet the mobile node can reason that the correspondent node is unaware of its changed location (if the packet is tunneled then the CN is still transmitting to the home address). In this case the mobile node sends a *binding update* to the correspondent node. A binding contains the mobile nodes home address along with the care-of address it is currently using and is stored in a *binding cache*. The update informs the CN of the mobile nodes care-of address so it can now send packets directly to the mobile node without tunneling through the home agent.

2.1.3.3 Routing Headers

The location of the mobile node must remain transparent to the CNs upper layer protocols in order to maintain connections. This requires that packets retain the MNs home IP address as their destination address. However the packet must be routed to the mobile nodes care of address. This problem was solved in Mobile IPv4 using tunneling, but most packets transmitted using MIPv6 take a different approach. In the case described above (2.1.3.2) where the CN is transmitting directly to the care-of address, an IPv6 *Routing Header* is attached to the packet and uses the care-of address as the destination. This header uses less bytes than IP-in-IP encapsulation thus reducing the overhead of packet delivery.

2.1.3.4 Ingress Filter Bypass

MIPv6 uses a mechanism called the Home Address Destination Option to bypass the problems previously identified with ingress filtering. In this

mechanism the mobile node sends packets with both the care-of address and the home address. Using the care-of address the packet can pass ingress filters as it appears to have a correct IP address. When the packet arrives at its destination the home address is then used in order to maintain transparency of the mobile nodes location.

2.2 Cellular IP

Cellular IP, which can be used as an extension of Mobile IP, incorporates two caches that store information about the current location of mobile hosts. These caches are called the route cache and the paging cache and they both operate in primarily the same way. By using two caches, the location tracking of idle and active hosts can be monitored at different levels of granularity, reducing the overhead of tracking mobile hosts, which is a desirable trait when dealing with smart environments that contains many computing devices. A Cellular IP network is subdivided to cater for frequent roaming. Splitting the Cellular IP network into paging areas, in addition to varying the level of tracking for idle and active hosts, allows Cellular IP to deal with frequent roaming in a proficient manner. When applying the Cellular IP protocol, updates detailing the location of a mobile host are sent when requested or when necessary and not every time a mobile host changes location. This makes Cellular IP suitable for local mobility management.

Mobile hosts that are roaming in a Cellular IP network listen for beacon signals that are transmitted by Base Stations. These signals allow the mobile host to identify the nearest Base Station, which route IP packets inside the Cellular IP network and communication with mobile hosts through a wireless interface. When the mobile host transmits a packet it is passed to the Base Station via a wireless interface, which subsequently relays the packet to the Gateway node via hop-by-hop shortest path algorithm. All packets are relayed to the Gateway node (A Base Station that has at least one interface connected to a wired network) irrespective of the destination address. Finally the Gateway makes the decision to either forward the traffic to another mobile host in the Cellular IP network or to transmit the packet outside the cellular network.

As the packets are forwarded to the Gateway, Route Caches on the path to the Gateway are updated. Route Caches are held on Base Stations in the Cellular IP network and contain mappings between active mobile host IP addresses and the neighbour Base Station from which packets from the active mobile host arrived. Active mobile hosts are those that are at present transmitting or receiving IP packets. Packets destined for active mobile node are delivered using the reversed chain of cached mappings. As active mobile hosts roam, the route caches are updated using route update packets and so the reversed chain of mappings constantly point to the present location of the active mobile host.

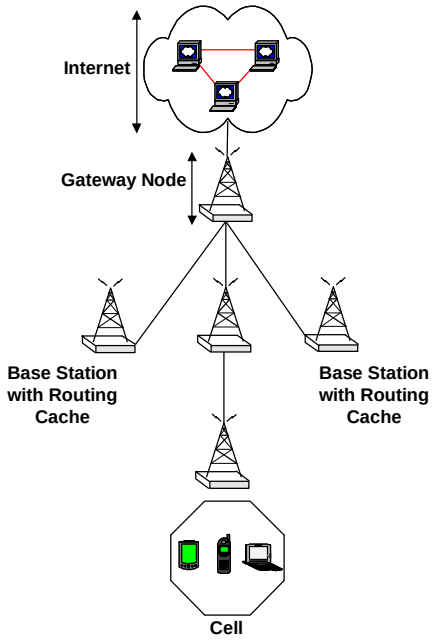

Figure 2 - Cellular IP

Although idle host (hosts that are not transmitting or receiving IP packets) do not have entries in a route cache they are tracked using a separate cache system called a paging cache. In this way packets destined for idle nodes are delivered successfully. Paging caches operate in fundamentally the same way as route caches although they have some distinct differences. Paging caches hold entries for both active and idle hosts, the timeout value for mappings in paging caches is longer than in route caches and they do not reside on every base station as is the case with route caches. The use of two caches is advantageous. With the increasing number of mobile devices existing within a network, the paging cache could potentially have a colossal number of mappings as it holds mappings for both active and idle hosts. However at any one time the percentage of active mobile devices will be relatively small and the majority of downlink packets will be destined for active devices. Therefore a search of the route cache would normally find the mapping for the appropriate mobile host since it only holds mappings for active host. This reduces processing requirements and speeds up the lookup procedure.

When an IP packet is destined for an idle mobile node, no entry will be present in the route cache so

the paging cache will be used to forward the packet. However in some cases a base station may not have a paging cache so the packet is broadcasted to all downlink neighbours and on the wireless interface. A base station that has a paging cache searches for a mapping. If a mapping is found the packet is transmitted to the mobile node or to the next hop base station, otherwise the packet is deleted. When the mobile host receives the packet, a route update packet is sent via the shortest path to the gateway. This packet creates a mapping in the all route caches on the path to the gateway and the host is now considered an active host, hence the remainder of the packets will be routed using the route cache.

2.2.1 Paging Areas

Cellular IP attempts to reduce network congestion and power consumption while supporting better scalability by permitting regular IP packets to refresh the caches and hence minimises the number of control packets that must be sent. (Campbell et al 2002) Network congestion is further reduced by means of paging areas. Within a Cellular IP network, cells are grouped together to form a Paging Area. Every Base Station within a Paging Area transmits the relevant Paging Area Identifier in its beacon signal. It is possible for a mobile host to recognise which Paging Area it is in and to observe when it roams into a new Paging Area based on the Paging Identifier it receives in the nearest base stations beacon signal. As idle mobile nodes are allowed to roam between cells within a paging area without transmitting location update packets network congestion is reduce. However a paging update must be transmitted when the idle mobile node roams into a new Paging Area. This is necessary in order to update the paging caches with the new location of the mobile node. Active mobile nodes in contrast are required to transmit route-update packets when they transverse cell and paging area borders. Although regular packets can refresh the route cache, i.e. reset the timeout value of a mapping, they cannot update the route cache, i.e. change the mappings in the route-cache. Therefore it is compulsory to send a route-update packet when an active host roams between paging areas.

When a mobile host roams into a new cell within the same or a different paging area a handoff occurs. A handoff is the automatic switch between base stations so that a new base station is assigned responsibility to send and receive packets from a mobile host. Cellular IP has two alternative handoff mechanisms entitled hard handoff and semi-soft handoff. Hard handoff is a straightforward method that trades off packet loss in exchange for minimising control signals. With hard handoff the mobile host abolishes all connections with the old Base Station and then establishes a new connection with the Base Station in the new cell. In this way the mobile host is not associated with any Base Station for a period of time and packets will be lost for this duration. This duration and hence the packet loss is proportional to the return distance from the mobile host to the gateway and to the packet rate. Semi-soft handoff on the other hand takes advantage of the fact that the mobile host can simultaneously receive packets from both the new and old base stations during handoff, so the mobile host has a connection with both Base Stations. In this way there is no packet loss and the mobile host receive packets without interruption (Ghassemian 2002). If the Cellular IP network is been used by services that are sensitive to packet loss then the semi-soft handoff will be used.

It is essential in smart environments to allow mobile hosts to roam seamlessly between areas to facilitate the continuous accessibility to services. Cellular IP allows for roaming within a local area and does so with a nominal number of control signals, keeping network traffic to a minimum. Cellular IP uses two caches and by doing so a larger number of devices can exist without putting an extreme processing load on the system. However Cellular IP is not apt for global roaming so it most be used in conjunction with a macro management protocol such as Mobile IP.

3 Analysis

3.1 Integrating Mobile IP and Cellular IP

With the advent of smart environments computing devices will be embedded into everyday arbitrary objects and as a result the number of computing devices will escalate significantly. These devices should communicate in a non-intrusive manner to assist a user and they will have to maintain their usefulness as they roam from area to area. This means that effective roaming mechanisms must be applied. As delineated in section 2.1, Mobile IP can control mobile devices roaming in a wide area and it enables the devices to operate adequately as they roam between administrative domains. While Mobile IP is an established macro mobility protocol that is at present an IETF proposed standard, it does have limitations in its ability to manage sizeable numbers of frequently roaming mobile nodes. These limitations restrict Mobile IP from becoming the unique holistic solution to mobility. Mobile IP does not support fast and seamless handoffs, which is crucial within a local

network where large numbers of devices migrate frequently. The overhead of the signalling traffic generated when using Mobile and the QoS issues that arise from acquiring a new CoA each time a node migrates, hamper Mobile IP from providing a complete mobility solution. (Jun-Zhao Sun 2000)

Cellular IP in contrast is a micro-management protocol that effectively manages mobile nodes as they roam within a local network (domain). Cellular IP supports vast numbers of frequently roaming nodes, with low-latency handoffs, decreased network congestion and effective routing algorithms. However, it is not apt for wide area mobility since the mapping entries and the route lookup procedures increase rapidly with increase in mobile population. Cellular IP and Mobile IP may be inter-worked to accomplish local and wide area mobility, whilst maintaining a distinct separation between areas governed by the different mobility protocols. This separation allows for global roaming while eliminating the need to update the home agent each time the mobile node roams within a local network. This is vital as when cells and spaces become smaller and more widespread node migration frequency and user population will increase (Valko 1999). Figure 4 and the steps outlined below describe how Mobile and Cellular IP inter-work to accomplish local and wide area mobility.

3.1.1 Cellular and Mobile IP Integration Example

The most apt way to outline the integration of Mobile and Cellular IP is through example. The following sequence of events occurs when a correspondent node wants to send a packet to a mobile node that is currently residing on a foreign cellular IP network.

1. The correspondent node wishes to send an IP packet to the mobile node, so the IP packet is sent over the internet using regular IP networking. The packet that is transmitted will use the MNs home address (11.12.13.8) as the destination address and the CNs address (18.19.20.1) as the source address.
2. When the packet arrives at the home network the home agent intercepts the packet and at this point Mobile IP takes control of routing.
3. The HA encapsulates the packet into another IP packet, using the MNs Care of Address (14.15.16.8) as the destination address and the HA external interface address (11.12.13.1) as the source address.
4. When the packet reaches the foreign network on which the MN is located, the border router of the foreign network forwards the packet to the gateway (14.15.16.3) of the appropriate Cellular IP network.
5. Now Cellular IP routing mechanisms take over. The reversed chain of cached mappings are utilised to forward the packet to the MN.
6. The gateway searches its route cache to discover the next hop downlink Base Station (14.15.16.4). (Note: If no mapping exists in the route cache this implies that the MN is idle and consequently the paging cache is exploited. See section 2.2).

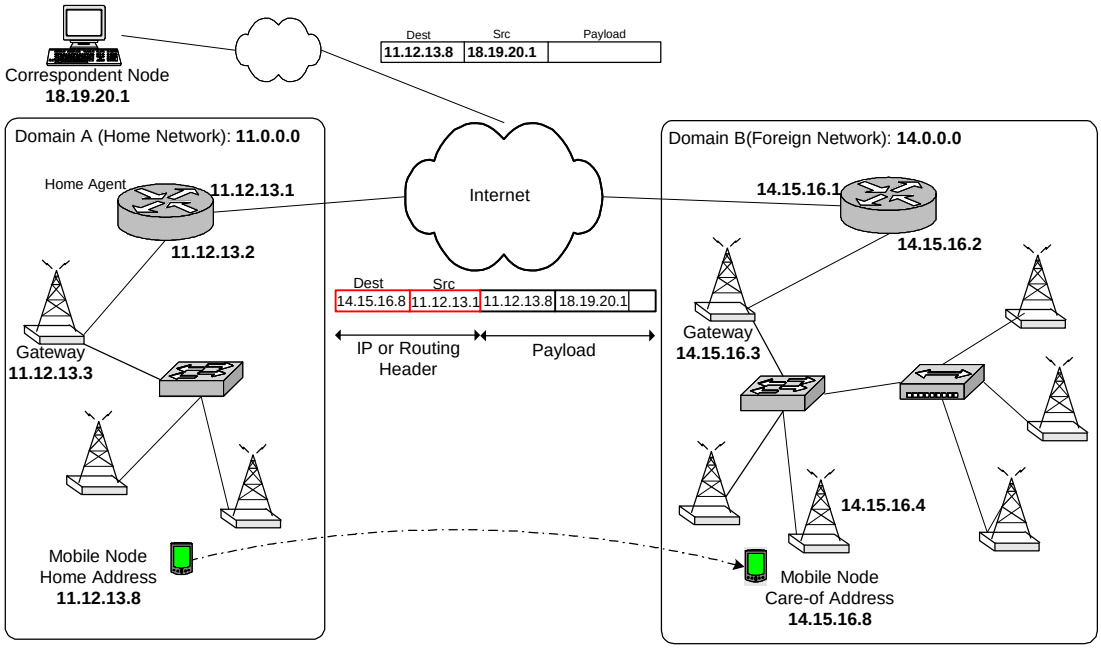

Figure 3 - Mobile and Cellular IP Integration Example

7. When the Base Station that has a wireless interface to the MN is reached, the Base Station forwards the packet to the MN across the wireless interface.
8. The MN then decapsulates the packet and extracts the original packet sent by the CN.
9. The MN realises that the packet is the first it has received from the CN since it roamed into the foreign network because it is an IP-in-IP encapsulated packet. Therefore the MN generates and sends a binding update to the CN. The binding update updates the CN binding cache, i.e. a mapping between the MNs CoA and the MNs home address is created in the CNs binding cache.
10. If the MN wishes to send a reply to the CN, the packet will have the MNs CoA (14.15.16.8) as the source address and the CNs address (18.19.20.1) as the destination address.
11. The reply packet will then be send across the wireless interface to the Base Station (14.15.16.4) and then directly to the Cellular IP gateway via the shortest path. The Cellular IP gateway subsequently makes the decision to forward the packet outside the Cellular IP network.
12. The packet is then forwarded to the CN using regular IP routing.
13. The CN can now use the CoA that is stored in its binding caches to address packet directly the MNs CoA. This is accomplished using routing headers instead of encapsulating the packet, which diminishes the number of additional bits required.

3.2 Mobile/Cellular IP and Smart Spaces

The integration of Mobile and Cellular IP forms a mobility architecture with similar characteristics to the roaming requirements identified in smart environments.

A very basic hierarchy can be identified in smart spaces in which an administrative domain contains one or more smart spaces. (E.G. a college may contain canteen, library, lecture hall smart spaces etc) Also a smart space will typically contain one or more cells. When considering smart spaces there are three types of roaming that may be identified. Firstly there is the situation where mobile nodes move between cells within a space. This can be described as intra-space roaming. Secondly, roaming may occur between separate and distinct smart spaces within the one administrative domain. This may be termed *intra*-domain roaming. Finally, roaming between administrative domains is also considered. This is termed *inter*-domain roaming.

A similar hierarchy to the one described above can be identified in Cellular IP. The Cellular IP network contains paging areas, which, as described in section 2.2.1, are a grouping of one or more cells. Smart spaces, which are delimited by physical space also contain cells, e.g. a lecture hall may be an individual smart space offering lecture hall services that are specific to that space. In practical terms a large lecture hall may require more than one cell to cover the entire room. So a Cellular IP paging area (with its paging area id) could not only facilitate routing and handoffs within smart spaces (between cells) but could also provide a method of uniquely identifying individual spaces. Similarly the Cellular IP network, as the overall administrative domain, could provide routing and handoffs between smart spaces. Thus Cellular IP essentially performs the intra-domain roaming that is required by smart spaces. Mobile IP on the other hand deals with inter-domain roaming. Through Mobile IPs routing operation, carried out by the home agent, care-of address, etc, mobile nodes can move between domains.

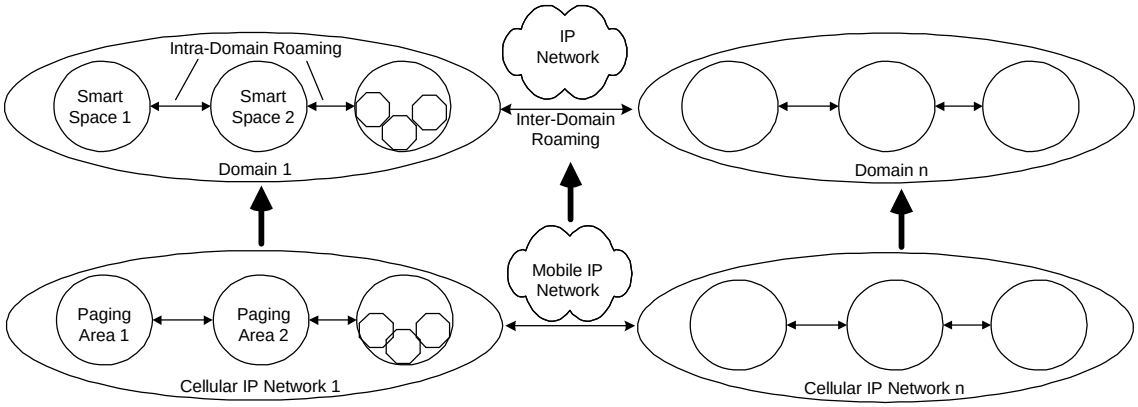

Figure 4 – Mapping of Mobile/Cellular IP to Smart Space concepts.

Clearly there is a considerable overlap between Mobile/Cellular IP and Smart Spaces (see Figure 4). Cellular IP in particular appears to be an extremely valuable protocol in facilitating the micro mobility requirements of smart spaces.

4 Conclusion

Mobile IP is an extremely versatile protocol in providing mobility across wide area networks. However, it does not present a complete mobility solution due to its ineptness in managing large volumes of frequently moving mobile devices. Similarly Cellular IP has its own niche in facilitating mobility within local access networks. However this too falls short of a complete mobility solution as scalability issues prohibit its use across wide area networks. It is widely accepted that both macro and micro mobility protocols are required to achieve a holistic mobility architecture. As Mobile IP is a macro mobility protocol and Cellular IP is a micro mobility protocol, integrating these will produce such an architecture.

Cellular IP and its concepts map readily to the key concepts identified in smart spaces. Roaming between paging areas as detailed in Cellular IP fulfills many of the requirements of smart space roaming. Furthermore, Mobile IPs ability to support roaming across domains satisfies the need for inter-domain roaming identified in smart spaces. The analysis of Mobile and Cellular IP (section 3) has shown that the two protocols in combination have a lot of potential for smart environments.

The M-Zones programme, funded by the Higher Educational Authority in conjunction with WIT, CIT and TCD, is aimed at investigating the management issues of smart spaces. At present implementation, testing and evaluation of various architectures for smart environments is underway. The mobility architecture outlined in this paper will be further evaluated in its use as a platform for the development and testing of smart space software and systems.

References

Campbell A., Gomez J., Kim S., Turanyi Z., Wan CY, & Valko, A, '*Comparison of IP Micro-Mobility Protocols'*, IEEE Wireless Communication Magazine, Vol. 9, No.1, February 2002.

Campbell, A., Gomez, J., Wan, C-Y., Kim, S., Turanyi, Z., & Valko, A., 2000, 'Cellular IP', Internet Draft, draft-ietf-mobileip-cellularip-00.txt, Work in Progress.

Ghassemian Mona, Aghvami A. H. 2002, *'Comparing different handoff schemes in IP based Micro-Mobility Protocols'*, IST 2002, Thessaloniki, Greece.

Ferguson, P. & Senie, D., 2000, 'Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing', IETF RFC 2827.

National Institute of Standards and Technology Smart Space Laboratory, Available www.nist.gov/smartspace/

Perkins, C., 1996, 'IP Mobility Support', IETF RFC 2002.

Perkins, C., 1996, 'IP Encapsulation within IP', IETF RFC 2003.

Perkins, C., 2002, 'Mobility Support for IPv4', 2002, IETF RFC 3344.

Perkins, C., Johnson, D. & Arkko, J., 2003, 'Mobility Support in IPv6', Internet Draft, Work in Progress.

Jun-Zhao Sun, Howie Douglas, Jaakko Sauvola 2000, '*Mobility management techniques for the next generation wireless networks'* Wireless and Mobile Communications Conference, Beijing 2001

Shelby, Z., Gatzounas, D., Campbell, A. & Wan, CY, 2000, 'Cellular IPv6', Internet Draft, draft-shelby-seamoby-cellularipv6-00.txt, Work in Progress.

Valko, A. G., 1999, '*Cellular IP – A New Approach to Internet Host Mobility'*, ACM Computer Communication Review, Vol. 29, Issue 1, January 1999.

Xinming He, Shun Jiang, Xiaojing Zheng 2000, *'Secure Mobile IP and Cellular IP'* [Online] Available: http://netweb.usc.edu/~xinming/papers/859_mobile_ip.pdf [2003 April 15]