Mobile IP Latency

Elizabeth Abreu, Betty (Chung-Yin) Koo, Albert Tsai, Kapil Datt, and Quang Pham
Graduate Students from George Mason University

Abstract – The advancements in new mobile networking technologies such as PDA's, cell phones and 4G networks utilizing WiFi access points have become integrated in our every day lives; keeping users connected to a network has become a necessity. This is where Mobile IP comes into play. Mobile IP is a standard communications protocol that allows a device to have a single permanent IP address and have the capability to move from one network to another without changing it. Mobile IP is designed to support uninterrupted connectivity of mobile computers as they roam from place to place. It provides scalable node mobility within networks, and allows devices to maintain transport and higher-layer connections while in a mobile state. It can be realized without requiring host-specific routes throughout specific static routes.

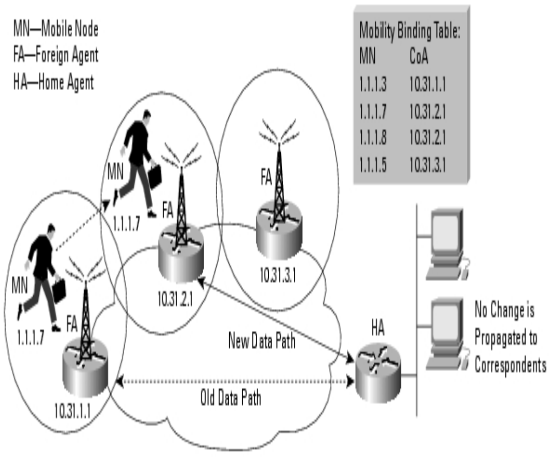
One of the largest challenges of Mobile IP is issue of latency. With the extra overhead of providing consistent communication, and the inherent nature of mobile wireless networks, latency will be considerably larger than that of fixed networks. This paper is intended to go over what Mobile IP is, including its architecture and how it works. In the latency section we will talk about why reducing latency is important. We will follow with a solution and a developed system model our team believes is the best one to reduce latency in the link layer level that consists of Ghost Mobile IP architecture with a separate proposed Geographic Routing Algorithm. We will conclude with how Mobile IP can change the nearby future.

1.0 Introduction

As technology progresses, achieving global connectivity becomes almost a necessity for the business users on the go. However, the requirement for data connectivity solutions for mobile users is very different than the ordinary fixed dialup or stationary wired LAN users. In IP networks, a device is reachable through routing by its stationary IP address that is assigned on the network. Once the device roams away from its home network and is no longer reachable using the normal IP routing, it is terminated.

With such demand in the near future, Mobile IP, a new technology primarily defined in RFC 3220, was integrated by Cisco IOS. "Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, which allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks." [1]

Mobile IP consists of three components: mobile node (MN), home agent (HA) and foreign agent (FA) [1]; and there are two IP addresses for each mobile node in mobile IP: a permanent address, used by higher-level protocols, on its home network, and a care-of address (CoA) which signifies the node's actual location within a network and its subnets, on another network.[2]



The Movement is Transparent to All Other Devices

In a cellular network, a mobile node connects to a fixed base station. As the mobile moves, its connection needs to be handed off from one base station to another base station. Typically, the strength of radio signal that the mobile node or the base station hears is used for this purpose. This is known as a link layer handoff performance of such handoff schemes can be improved by using position information which will be discussed further. Since the mobile node needs to perform this handoff function in order to get uninterrupted service, it should be as smooth as possible, in order not to disrupt the Internet or other real time services and applications with possible packet losses. Mobile data networking and mobile computers require Mobile IP to preserve connectivity and properly route information while roaming over foreign networks. It is a fundamental technology used to maintain the hand shake to an IP network freely and dynamically as the device is free to roam packet switching networks. The Global Positioning System (GPS) is used to give an exact location to a receiver any where in the entire world. After extensive research, we have come up with a design requirement which necessitates the integration of a positioning system. GPS will be used in order for a mobile device to determine their position (longitude, latitude, and altitude) by retrieving information from the satellites.

The location information provided by GPS can be used at different layers of the protocol stack. The proliferation of wireless networks and high-speed internet access has led to massive deployment of IEEE 802.11b access points and embedded network cards in mobile devices. Wireless Local Area Networks provide connection speeds of 1-11Mbps [1] and 1-55Mbps [2] and represent a potential option for replacing or complimenting 3G cellular networks. The application of position information provided by GPS in ad hoc wireless networks, cellular networks and in sensor networks, has been researched to be the main solution focus of this study. A routing scheme that uses position information of the destination for making routing decisions is discussed. This paper consists of a definition of Mobile IP and associated components, the inherent problems and issues of the technology, definition of systems and applications supported by optimizing the Mobile IP handoff, and proposed solutions.

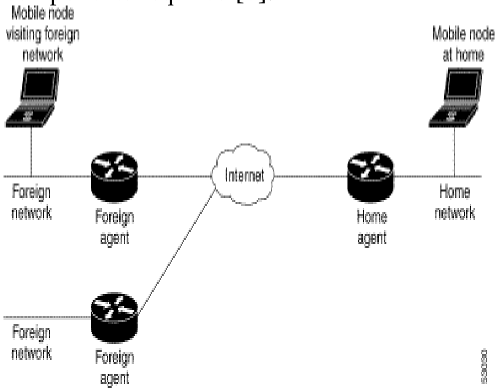
1.1 Mobile IP Architecture

Mobile IP enables users to maintain the same IP address while remaining connected, and while roaming between IP networks. Mobile IP is based on the Internet protocol. Any media that can support IP can support Mobile IP, therefore making mobile IP scalable for the Internet. Scalability is possible because only participating components need to be Mobile IP aware. The components are the mobile node and the endpoints of the tunnel. Mobile IP makes it possible for the mobility of a user to be transparent to all executing applications.

Mobility is enabled by link layer technologies. The problem lies when the data crosses the network or different link layers. Mobility functions of Mobile IP are performed at the network layer instead of the physical layer. This allows the mobile device to span across different types of wireless and wire line networks, while maintaining connections and allowing the active session to remain open.

Mobile IP consists of the following three components: Mobile Node, Home Agent, and a Foreign Agent. The mobile node consists of devices such as a cell phone, PDA, laptop with networking capabilities. The home agent consists of a router on the home network serving as the anchor point of communication with the mobile node. A tunnel is established between the home agent and a reachable point for the mobile node in the network. Packets are tunneled from a device on the Internet known as the Correspondence Node, to the roaming mobile node. An association is maintained between the home IP address of the mobile node and the home agent. The third component mentioned above is the foreign agent. The foreign agent is a router that functions as the point of attachment for the mobile node when it roams to a foreign network. Packets are delivered from the home agent to the mobile node.

The diagram below illustrates the topology of a mobile IP network and the components required [8]:



The following scenario shows how a datagram moves from one point to another point within the Mobile IP framework:

1. Normal IP routing occurs if the mobile node is located on its home network.

The Internet host sends a datagram to the mobile node by using the mobile node's home address. If the mobile node is not on its home network, the home agent receives a datagram.

2. If the mobile node is not located in the home network, if it's located on a foreign network, the home agent forwards the datagram to the foreign agent. The home agent encapsulates the datagram in an outer datagram so that the foreign agent's IP address appears in the outer IP header.
3. The foreign agent then delivers the datagram to the mobile node.
4. Normal IP routing procedures are used to send datagrams from the mobile node to the Internet host. The packets are delivered to the foreign agent if the mobile node is located on a foreign network. The datagram is then forwarded to the Internet host.

Mobile IP has 3 main phases: Agent Discovery, Registration and Tunneling. During Agent Discovery, the mobile node discovers its home and foreign agents. The home and foreign agents "advertise" their services on the network using ICMP IRDP (Router Discovery Protocol). The mobile node determines if these services are connected to its home network or foreign network by using the agent advertisement messages. The IRDP service carries a mobile IP extension, which specifies the following: whether an agent is a Home or foreign agent, its care-of address, and the types of services provided (reverse tunneling, generic routing encapsulation (GRE)).

The 2nd phase, Registration, informs the home agent about the current location of the mobile node. It begins when the Mobile Node has detected that the agent has moved outside of its home network. The mobile node listens for mobility agents advertising their presence. These advertisements help the mobile node determine when the mobile node moves to another subnet. "When a mobile node determines that the mobile node has moved its location, the mobile node uses the new foreign agent to forward a registration message to the home agent. The mobile node uses the same process when the mobile node moves from one foreign network to another foreign network" [10]. The mobile node sends a Registration Request message to the foreign network, which include the permanent IP address of the mobile host and the IP address of its home agent. In turn, the foreign agent sends a Registration Request containing the permanent IP address of the mobile node and IP address of the foreign agent to the home agent. Once the home agent receives the Registration Request, the home agent will update the mobility binding by associating the care-of address of the mobile node with its home address. The home agent sends an acknowledgement to the foreign agent. The foreign agents then updates its visitor list by inserting the entry for the mobile node, thus sending a reply to the mobile node.

The 3rd phase is tunneling. Tunneling occurs when the home agent sets up a shared tunnel to the care-of address in order to route packets to the Mobile Node as they roam the network. The care-of address identifies the current location of the mobile node on the foreign network. It ensures packets are forwarded using conventional IP routing to the mobile node's current location in foreign network. Packets are sent by the mobile node, using its home IP address, maintains the appearance that it's always on its home network. The movements of the mobile node while it's roaming on the foreign networks are transparent to the correspondent node. More information about tunneling will be discussed later in this document.

1.2 Mobile IP addressing schemes

Mobile IP addressing scheme consists of a Mobile IP Registration Request and Mobile IP Registration Reply. Previously stated, the goal of Mobile IP (MIP) is to be able to flow from one access router to another. Needless to say, the home IP address will always be identified on the network. As for information about the new location, the mobile node combined with the care-of address identifies its current location. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. The mobile node at the receiving end examines the datagram and forwards the datagrams to the mobile node.

Mobile IP defines a set of new control messages, sent with UDP, Registration Request and Registration Reply. The IP packet consists of the IP source and destination addresses, followed by the UDP source and destination ports, followed by the Mobile IP fields. Mobile IP packets can be either registration request or registration reply. [13]

Type

1 signifies a registration request.

S-Simultaneous bindings. Mobile mode is requesting that the home agent retain its prior mobility bindings

B-Broadcast datagrams. When set, the mobile node requests that the home agent tunnel to it any broadcast datagrams that it receives on the home network.

D-Decapsulation by mobile node. When set, the mobile nodes will itself decapsulate datagrams which are sent to the care-of address. In other words, the mobile node is using a co-located care-of address.

M-Minimal encapsulation. When set, the mobile node requests that its home agent use minimal encapsulation for datagrams tunneled to the mobile node.

G-GRE encapsulation. When set, the mobile node requests that its home agent use GRE encapsulation for datagrams tunneled to the mobile node.

V-The mobile node requests that its mobility agent use Van Jacobson header compression over its link with the mobile node.

T-When set, the mobile node asks its home agent to accept a reverse tunnel from the care-of address. Mobile nodes using a foreign agent care-of address ask the foreign agent to reverse-tunnel its packets.

Rsv-Reserved bit, set to zero.

Lifetime-The number of seconds remaining before the registration expires.

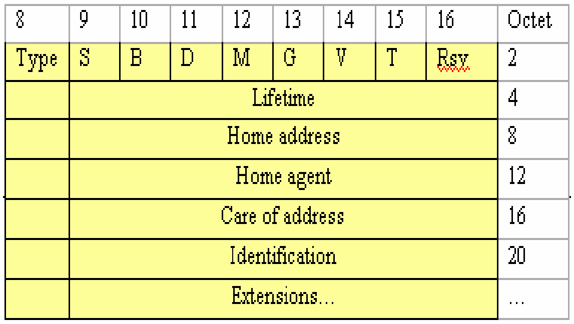
Home address-IP address of the mobile node.

Home agent-IP address of the mobile node's home agent.

Care-of address-IP address for the end of the tunnel.

Identification-A 64-bit number, constructed by the mobile node, used for matching registration requests with registration replies, and for protecting against replay attacks of registration messages.

Extensions - The fixed portion of the registration request is followed by one or more of the extensions listed in Section 3.5 of RFC2002. The Mobile-Home Authentication Extension must be included in all registration requests.



8	9	10	11	12	13	14	15	16	Octet
Type	S	B	D	M	G	V	T	Rsv	2
	Lifetime								4
	Home address								8
	Home agent								12
	Care of address								16
	Identification								20
	Extensions…								…

Mobile IP reply message scheme

1.2.1 MIP Registration Reply Message Scheme

Type

3 indicates a registration reply.

Code

A value indicating the result of the Registration Request. Values may be as follows:

Registration successful:

0 Registration accepted.

1-Registration accepted, but simultaneous mobility bindings unsupported.

Registration denied by the foreign agent:

64-Reason unspecified.

65-Administratively prohibited.

66-Insufficient resources.

67-Mobile node failed authentication.

68-Home agent failed authentication.

69-Requested Lifetime too long.

70-Poorly formed Request.

71-Poorly formed Reply.

72-Requested encapsulation unavailable

73-Requested Van Jacobson compression unavailable.

Service denied by the foreign agent:

74-Requested reverse tunnel unavailable.

75-Reverse tunnel is mandatory and T bit not set.

76-Mobile node too distant.

Registration denied by the home agent:

80-Home network unreachable (ICMP error received).

81-Home agent host unreachable (ICMP error received).

82-Home agent port unreachable (IMCP error received).

88-Home agent unreachable (other ICMP error received).

Service denied by the home agent:

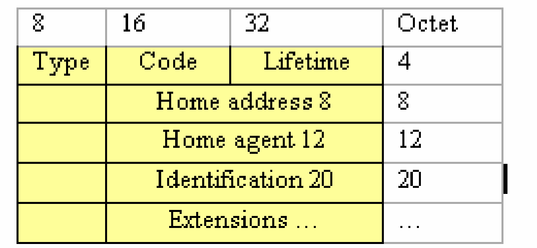
137-Requested verse tunnel unavailable.

138-Reverse tunnel is mandatory and T bit not set.

139-Requested encapsulation unavailable.

Lifetime

If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration expires. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and are ignored on reception. [13]



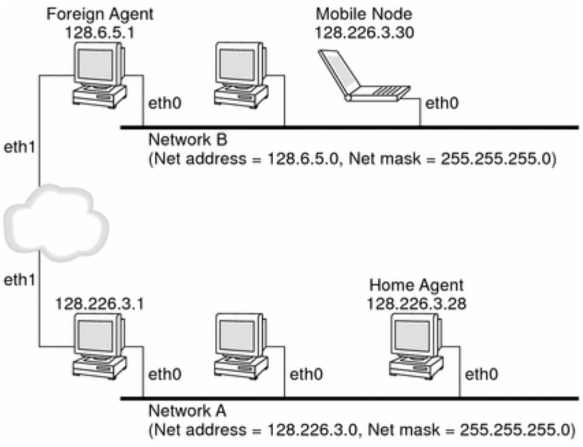
8	16	32	Octet
Type	Code	Lifetime	4
	Home address 8		8
	Home agent 12		12
	Identification 20		20
	Extensions ...		...

Mobile IP Registration Reply Message structure

1.3 Mobile IP Routing and Tunneling

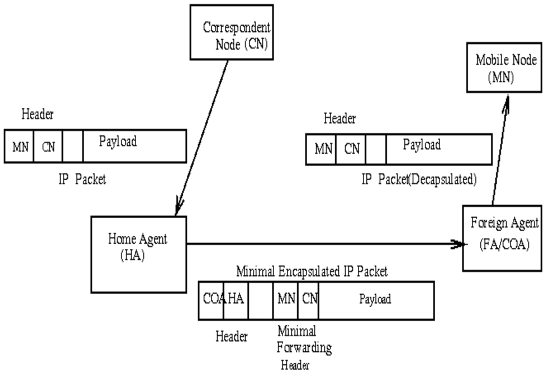
As mentioned earlier, mobile IP (MIP) allows the mobile node to use two IP addresses, a fixed home address and a care-of address. The home address identifies the mobile node regardless of where the mobile node is attached. The care-of address provides information about the current point of attachment of the mobile node, and changes at each new point of attachment. Mobile IP registers the care-of address with a home agent. Communication activities and sessions are not disrupted when the user changes the computer's point of attachment. The network is updated with the new location of the mobile node.

The home agent redirects datagrams to the care-of address. A new IP header is constructed that contains the care-of address of the mobile node as the destination IP address. The new header encapsulates the original IP datagram. The datagram is de-encapsulated once it arrives at the care-of address. The illustration below shows a mobile node that resides on its home network (network A), before the mobile node moves to the foreign network (netwoon

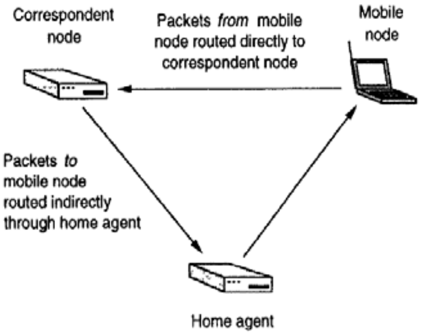


With mobile IP, encapsulation is carried out by placing the original datagram inside another IP envelope. Several fields in the outer IP header are duplicated from the inner IP header. A Minimal Encapsulation Scheme has been defined, as mentioned earlier in the header section, to prevent the waste of space that occurs. Instead of inserting a new header, the original header is modified to reflect the care-of address. A minimal forwarding header is inserted to the header and then stores the original source and destination address. Therefore, the home agent's address becomes the source address, and the care-of address of the mobile node becomes the destination address. Using the Minimal Encapsulation Scheme, the foreign agent restores the fields in the forwarding header to the IP header. The forwarding header is then removed.

The figure below illustrates the Minimal Encapsulation Scheme [9]:

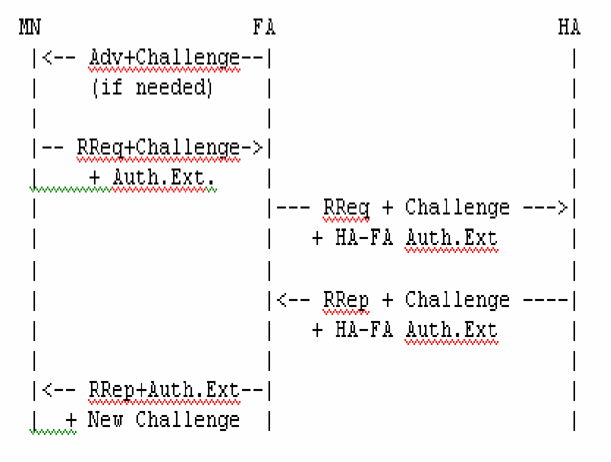


Mobile IP architecture uses "triangular routing". With triangular routing, packets being sent from the mobile node must first be routed to the mobile node's home subnet. The home agent then forwards the packets to the mobile node at its current location. Packets from the mobile node follow a direct path to a Correspondent Node (CN) such as an internet host. Packets from the CN are rerouted via the mobile node's home network to its point of attachment in the foreign network. The packets are then forwarded to the mobile node's current location. For example, suppose the mobile node and CN are located in the same network, but not in the home network of the mobile node. Messages will experience unnecessary delay since they have to be first routed to the home agent that resides on the home network. Triangular routing adds to the latency problem with mobile IP by creating many unnecessary path traversals. As the number of mobile nodes increases, it can significantly increase the latency problem during the location update process. Route optimization is highly essential for supporting real time communications in any future mobile IP enhanced network infrastructure as we will discuss further.


Correspondent node
Packets *from* mobile node routed directly to correspondent node
Mobile node
Packets *to* mobile node routed indirectly through home agent
Home agent

This diagram illustrates Triangle Routing [12]:

1.4 Handshaking



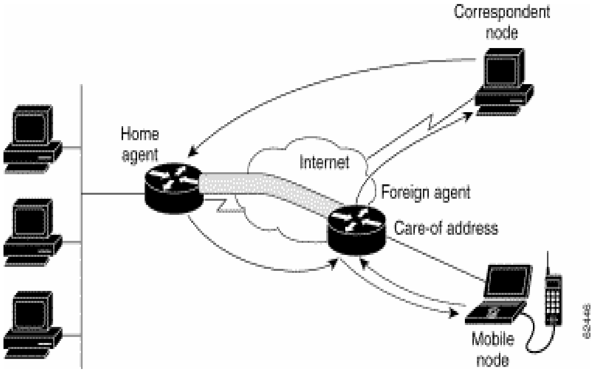
```
MN                  FA                        HA
 |<-- Adv+Challenge--|                         |
 |    (if needed)    |                         |
 |                   |                         |
 |-- RReq+Challenge->|                         |
 |    + Auth.Ext.    |                         |
 |                   |--- RReq + Challenge --->|
 |                   |    + HA-FA Auth.Ext     |
 |                   |                         |
 |                   |<-- RRep + Challenge ----|
 |                   |    + HA-FA Auth.Ext     |
 |                   |                         |
 |<-- RRep+Auth.Ext--|                         |
 |  + New Challenge  |                         |
```

Figure 2: FA Challenge Messaging with MN-FA Authentication [3]

1. The FA broadcasts a challenge value in an agent advertisement produced after receiving an agent solicitation from the MN (not shown in the diagram).
2. The MN creates a registration request including the advertised challenge value in the challenge extension, along with a Mobile-Foreign authentication extension for security.
3. The FA sends the registration request to the HA specified by the MN.
4. The FA receives a registration reply with the appropriate indications for authorizing connectivity for the MN.
5. The FA sends the registration reply to the MN, possibly along with a new challenge value to be used by the MN in its next registration request message. If the reply contains the code value HA_BAD_AAA_AUTH, the FA takes actions indicated for rejected registrations. If the HA allows the registration, it will work as a proxy of the MN. [3]

In order to successfully implement Mobile IP, we must have a routing mechanism for transporting packets to and from the Mobile Node as it roams across different networks. To achieve this, Mobile IP utilizes a Tunneling technique. The Mobile Node sends packets using its home IP address, thus maintaining the appearance to other nodes that it is always in its home network. The reality is the mobile node is roaming, perhaps continuously, and its movements are transparent to other peer nodes that communicate with it. Data packets addressed to the Mobile node are always routed to its home network, and it is there that the home agent of the mobile node will intercept it and use tunneling to forward packets to it.

Tunneling basically has two primary functions. One is the encryption of data packets at the home agent. The other is the decryption of data packets at the mobile node. The following diagram [1] shows how a typical mobile node sends data packets to the foreign agent, where it gets routed to their final destination at its corresponding node.



However, this does not reflect the true IP network source for the data—instead it reflects the home network of the Mobile Node. Because the packets show the home network as their source inside a foreign network, an access control list on routers in the network called ingress filtering drops the packets instead of forwarding them. This is where a feature called reverse tunneling comes in where it solves this problem by having the Foreign Agent tunnel packets back to the Home Agent when it receives them from the Mobile Node.

Tunnel MTU discovery is a mechanism for a tunnel encapsulation, such as the Home Agent, to participate in path MTU discovery to avoid any packet fragmentation in the routing path between a Correspondent Node and Mobile Node. For packets destined to the Mobile Node, the Home Agent maintains the MTU of the tunnel to the care-of address and informs the Correspondent Node of the reduced packet size. This improves routing efficiency by avoiding fragmentation and reassembly at the tunnel endpoints to ensure that packets reach the Mobile Node.

1.5 RFC – IPv6

IPv6 shreds a new light in the world of Mobile IP. Mobile IPv6 promises to stabilize the connectivity to the internet as the increase in mobility from one access router to another.

However, Mobile IPv6 does not eliminate or improve handoff latency; therefore, utilizing mobile IP in time sensitive application is still a major problem. In RFC 4068, IPv6 procedure such as movement detection, new Care of Address configuration and binding IP are the causes of handoff latency. [16]

In RFC 3583, the cause of latency exists when a mobile node utilizing mobile IP is switching in between one access router to the next. In other words, as a mobile node travels from one access router to another access router packets may not know where to travel to. In addition, the packets belonging to Mobile nodes on-going session may start using a new care-of-address after handover. Hence, they may not be recognized by some forwarding functions in the nodes. This could changes a session ID in midst of a connection. [14]

According to RFC 4260, one way to reduce latency is to predict or constantly respond to handover. This will be discussed further as we define our problem and solution. This allows IP connectivity to be restored at the new point of sooner than would otherwise be possible. In addition, by tunneling data between the old and new access routers, it is possible to provide IP connectivity in advance of actual Mobile IP registration with the home agent or correspondent node. This allows real-time services to be reestablished without waiting for such Mobile IP registration to complete. Because Mobile IP registration involves time-consuming internet round-trips, the Mobile IPv6 fast handover can provide for a smaller interruption in real-time services than an ordinary Mobile IP handover. When the mobile node roams from one subnet to the next, the corresponding FA starts to transmit mobile IP advertisements to the mobile node. The mobile IP software that runs on the mobile node then intercepts these advertisements and sends a registration request to the newly discovered FA. An IP-over-IP tunnel is established between the HA and the FA after authentication. Starting from this point, the HA acts as a proxy for the mobile node to intercept. The HA transmits all the packets over the tunnel. HA is the start of the tunnel which does the encapsulation. [4] The FA is the end of the tunnel and is responsible for de-encapsulating the packets coming fro

r
c r
s h
A h
ag t
its o
to t e

wh is more lo n ba
order t supp b e en

re nds of appli ons. For time
sensitive app s su as file
g
ort g e in n ity d n a y

1

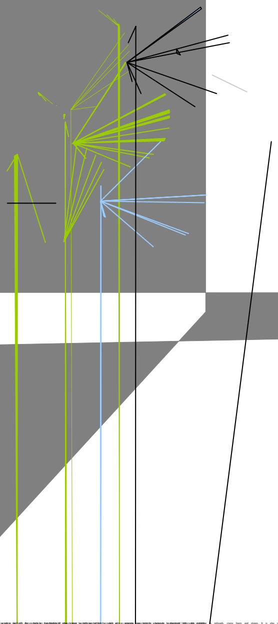
could have pr oun
v d q v no

dden ch

a user edits a fil

use problems for hte use

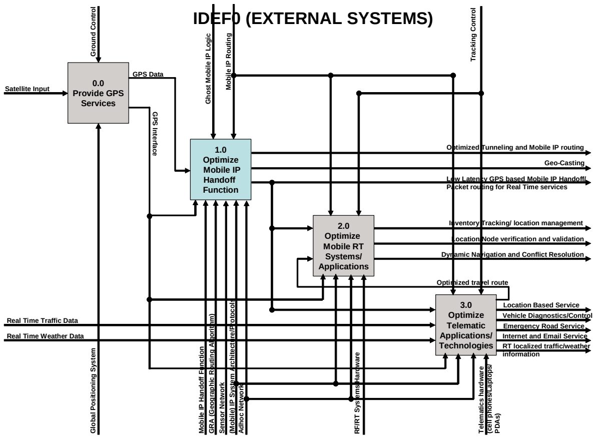
r s



T

External Systems (IDEF0)

Interfaces to our sub system are defined in the figure below (IDEF0), “1.0 Optimize Mobile IP Handoff function” is to be considered as the focus of this paper. The other functions are stand alone systems and are to be viewed as either their own entity or application systems. This model was designed to define the external interfaces to our solution and to discuss why optimizing the Mobile IP handoff function is so important. Although gear towards a general solution, the outputs of the systems who might level achievable objectives applications.


IDEF0 (EXTERNAL SYSTEMS)
Ground Control
Ghost Mobile IP Logic
Mobile IP Routing
Tracking Control
Satellite Input
0.0 Provide GPS Services
GPS Data
GPS Interface
1.0 Optimize Mobile IP Handoff Function
Optimized Tunneling and Mobile IP routing
Geo-Casting
Low Latency GPS based Mobile IP Handoff/ Packet routing for Real Time services
2.0 Optimize Mobile RT Systems/ Applications
Inventory Tracking/ location management
Location Node verification and validation
Dynamic Navigation and Conflict Resolution
Optimized travel route
3.0 Optimize Telematic Applications/ Technologies
Location Based Service
Vehicle Diagnostics/Control
Emergency Road Service
Internet and Email Service
RT localized traffic/weather information
Real Time Traffic Data
Real Time Weather Data
Global Positioning System
Mobile IP Handoff Function
GRA (Geographic Routing Algorithm)
Sensor Network
(Mobile) IP System Architecture/Protocols
Adhoc Network
RF/RT Systems Hardware
Telematics hardware (cell phones/Laptops/ PDAs)

IDEF0 0.0 Provide Global Positioning System Services

Research has shown that a location based Mobility management mechanism is needed for the optimization of the handoff. For this reason, we have added a GPS solution as a modular system needed to provide scalable applications discussed further. Markets for GPS applications have be at approximately $10 Billion since the year 2002. It has been a system which is increasing less expensive to provide services and applications to outside technologies. “0.0 Provide GPS Services” is a stand alone external system which interfaces with the Mobile IP handoff subsystem. The need for GPS data as an input is vital to optimize the handoff as seen in many researched solutions. As shown in the diagram, above, the GPS satellites provide the input to the system needed to provide GPS coordinates for the mobile device, and other network entities which will be discussed further. Ground control is critical for the GPS interface to each external system since terrestrial links are mostly leveraged by enterprise network implementations.

IEDF0 1.0 Optimize the Mobile IP Handoff function

At different communication layers there are several components that contribute to the overall delay of packet stream delivery during the Mobile IP handoff function. As the mobile device moves from one cell to another it experiences delays at various layers. A layer 2 handoff shown (in the figure below) as Δ1, is the initial stage in which the mobile decides to connect to a different access point after listening to a new signal beacon and in some technologies such as CDMA, been known as soft-handoff techniques.

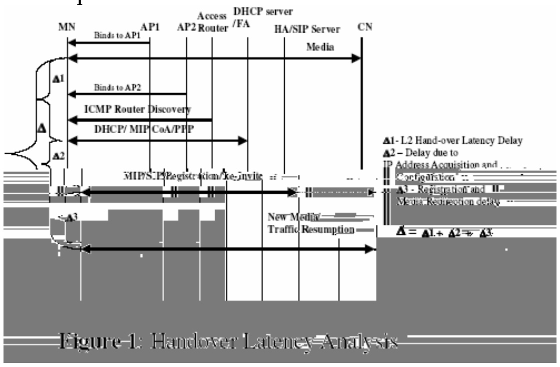

MN
AP1
AP2
Access Router
DHCP server /FA
HA/SIP Server
CN
Binds to AP1
Media
Δ1
Binds to AP2
ICMP Router Discovery
Δ
DHCP/ MIP CoA/PPP
Δ2
MIP/SIP Registration/Re-invite
Δ3
New Media/ Traffic Resumption
Δ1 - L2 Hand-over Latency Delay
Δ2 – Delay due to IP Address Acquisition and Configuration
Δ3 - Registration and Media Redirection delay
Δ = Δ1 + Δ2 + Δ3

Figure 1: Handover Latency Analysis

“If the base stations in the adjacent or nearby cells belong to the same subnet; the delay due to L2 handoff will take into account the beacon interval from an Access Point.” Beacon interval delay is a configurable parameter and is typically set for good performance at around 100ms refer to Multilayered handoff figure. After the layer2 handoff is complete and the mobile connects to the adjacent Access Point, it needs to determine which subnet it has handed off too. Listening to the ICMP router, FA, or any other server advertisements, the device determines whether it is on a foreign or home segment. Depending on its previous registration, the client configures itself with a new IP address or FA (Foreign Agent) CoA (Care-of-Address). This function is known as IP address discovery phase and is mostly denoted as Δ2. Existing IP address discovery process can be either stateful, or stateless. A stateful IP address assignment involves a server (such as a DHCP server/relay agent, PPP server or MIP server) which keeps a state of all the IP addresses assigned. An IP address is determined by using its subnet prefix advertisement from the router and the link local prefix. Depending on the type of mobility management hierarchy, the client is reconfigured either with a new IP address or FA COA, and will send either a SIP Re-invite, a MIP register or a MIP update so that packet switching can be forwarded to the mobile's new location. "Thus delay incurred between the IP address discovery (client's reconfiguration) and the arrival of new media is denoted as Δ3." This factor depends upon "the number of signaling messages traversed between MH, CH and Home Agent, distance between the mobile and the correspondent host" in the original Mobile IP architecture. Figure 1 (above) shows details of the original Mobile IP handoff function and the latency associated at each step.

As it has been proven, the reasoning behind the redesign or optimization of this sub-function can be viewed in the external systems diagram (IDEF0). The need for a GPS data input, is explained further, as we break the system down functionally further below into subsystems. Externally, there is also a need for a GPS interface as a systematic component to 1.0. In order to control the system, a Ghost Mobile IP logic must be introduced as a control, as well as the generic Mobile IP routing control mechanism must me introduced to the system. As seen as external outputs, an "optimized tunneling technology" as well as a re- defined multicast logic called "Geo-casting," are both known mechanisms which may be introduced into other application systems. These outputs can be considered valuable to other geographical information broadcasting applications. An example would be a local law enforcement agency using a GPS based mapping GUI to address a geographic area by selecting a region on the electronic map to send out a local emergency area broadcast message. The voice or data message will be sent to any device capable of receiving it within the "Geo- caste" or GPS defined survey area. The major impact output is the "low latency GPS based Mobile IP handoff and packet routing for real time services" function (of IDEF0). This is the major input needed for the application systems addressed.

IDEF0 2.0 Optimize Mobile Real Time Systems and Applications

The purpose of this function is to group any real time application systems into a functional system related to Mobile IP and the need for the optimal GPS-IP handoff. As explained, the major dwell time of the IP address acquisition, reconfiguring, registration, and overall hand off time for a Mobile IP session causes a major bottleneck specifically for real time applications and at higher speed mobility. The convergence of Mobile VoIP has stirred a great deal of interest in the integration of GPS. VoIP as a stand alone system, is continuing to evolve on its own, but already has sparked interests of large corporations as predicting millions of dollars in savings costs for telecommunications services. Mobile communications is the next big step in VoIP convergence. Integration of RFid (or RF tagging) and real time monitoring services implementing GPS have been long sought after from retail giants such as Wal-Mart, who have began deploying and implementing such technologies for their distribution networks. Being able to track expensive or mission critical inventory at each node and mapping critical travel paths are the wave of the future. Mobile IP and GPS are the cornerstones of these markets. The information can range from tracking a fugitive to location of hiding groups, to helicopter and general aviation navigation, surveillance, and conflict resolution using on-board pseudo radar applications and GPS systems. These navigational aides may originate from feedback of telematic systems as shown in the IDEF0 diagram. This data is sent from sensor systems to the ground base stations. From the base station, whether it is to an automobile or a helicopter, the data is routed by Mobile IP.

IDEF0 3.0 Optimize Telematic Applications and Technologies

Telematics aims at collecting and processing useful information about transportation conditions and travel options in order to allow people to take full advantage of the transportation system. Vehicle users need to be informed about the possible road conditions, estimated travel times, open routes, emergency broadcasts, traffic congestion and weather conditions to where they are headed. An on board GPS navigation system is not enough to produce this type of information. Localized information is fused with GPS data by using sensor networks. Cheap, small sensors scattered around the environment collect data with their magnetic, temperature, light, acoustic, and other sensors. Vehicle users may want uninterrupted Internet service provisioning they can connect to the Internet. The low latency handoff will assist Mobile IP data transfer and allow these applications and technologies to evolve. There are numerous applications as shown in the diagram as outputs.

3.0 Solutions and Further Analysis

There are numerous solutions to the problems defined in the above sections. The solutions to these outstanding problems span a wide spectrum from specific routing algorithms to sensor networks. For this reason, the solution presented here is a hybrid of two such solutions. The hybrid consists of a Ghost Mobile IP architecture with a separately proposed GRA (Geographic Routing Algorithm). The integration of the two has been done the same way the external system was defined, using an IDEF model mechanism. For this reason, we present IDEF1 (the solution system) here. The following section for further research displays an alternate architecture which does not involve sensor networks.

IDEF1 1.1 Implement Ghost Mobile IP

In order to improve the performance of Mobile IP and the handoff function, we must implement a derivation of it called Ghost Mobile IP. This is done by complimenting the system with two new entities: a ghost Mobile Host (g-MH) and a ghost Foreign Agent (g-FA) to Mobile IP logic. In order to balance the handoff mechanism for high speed mobility, Ghost Mobile IP creates an adaptation of the TCP stack and context transfer among inter-domain and intra-domain handoffs, in order to enhance the performance of TCP. It incorporates network awareness and a location management function integration of Layer-2 and Layer-3 protocols. “Speed of the mobile node and trajectory determination become important factors. Trajectory prediction and predictive algorithms for mobility in wireless networks have been investigated in different cellular and micro-cellular infrastructures.” A predictive-distance based location management algorithm is used to calculate a user’s location based on previous values of position and velocity. These predictable models involve dynamic programming and stochastic control which allow surrounding cells to act as shadows where packets are forwarded to depending upon network and mobility conditions.

The Ghost Mobile IP routing protocol determines speed and trajectories using GPS (Geographical Positioning System) as an input, as seen in the IDEF1 figure. GPS information is also investigated in Ad hoc networks [10] where GPS information is used to improve the performance of Distance Vector protocols. A Location Aided routing (LAR) acts as a routing subsystem of the Ad hoc network (as seen in IDEF1) component. The combination of Mobile IP and GPS has been proven to derive great improvements during handoff and registration and henceforth “its utilization is highly recommended.” “The majority of mobile networking protocols require registration to keep the home network aware of mobility. The Home Location Register (HLR) and the home agent structure are used in Mobile IP.” [15]

Ghost Mobile IP is a dynamic Mobile IP impl

Implement Geographical Routing Algorithm" function as seen in IDEF1. The g-MN acts as a "virtual" repeater, capable of registering and allocating resources in a predictive matter. The g-MN speeds up handoff and augments the performance of Mobile IP.

The g-MN "is capable of replicating the registration request, handling the creation of the tunnel, and replicating Authentication and Authorization information from the MN and acts on behalf of the MN before it is in the range of the new FA. The g-FA is created in the neighborhood of the FA. Its main role is to advertise the FA presence
from a neighbor FA. A g-FA acts on behalf of LFA2 (Leaf Foreign Agent), so any MN can include that FA as a potential place for handoff when in LFA1 range. Once the MN has moved to the vicinity of LFA2 (coming from LFA1), registration has already been done, and resources have been allocated for the MN." The HA or HFA (hierarchical Foreign Agent) will initiate a new tunnel or trunk channel towards the MN new location and data is forwarded. Once the mobile has acknowledged a registration message, the g-FA updates the information of available FAs in the MN and handoff decisions can be executed with less overhead. The g-MN will buffer the incoming traffic from the Correspondent Host (CH) intended for MN that could have been lost during handoff. The g- MN and g-FA allocate bandwidth resources much more efficiently at each access point. Again, the use of a Kalman Filter, which is based on a function of time, was originally part of the Ghost Mobile IP system. This is replaced by the input (as seen in IDEF1) and use of a geographically predicted algorithm, which integrates sub functions of 1.1 to produce the output of an optimal Ghost Mobile IP packet route.

On average, the Ghost Mobile IP design reported a 30 to 50% increase TCP average throughput. At 40 m/s, it has been observed that TCP registered almost 20 million packets transferred during a Ghost Mobile IP simulation. In the non-Ghost Mobile IP run, about 14 million packets arrived from the FTP server. For 80 m/s, it was observed that more than 10 million packets arrived to the mobile node using the Ghost Mobile IP architecture, while about 6 million made it during the original Mobile IP case. Experiments performed on over 40 m/s through 80 m/s have been shown as an improvement of approximately 1.5 times (average) according to Ghost Mobile IP studies. This, however, does not take in to account the introduced GRA which is explained below. The "geographically predicted trajectory" input is an enhancement to Ghost Mobile IP which, in a systematic viewpoint, is used mainly for location management and routing architecture.

IEDF1 1.2 Implement Geographical Routing Algorithm (GRA)

"The Geographical Routing Algorithm (GRA) [8] is an asynchronous, real-time distributed and scalable algorithm for ad hoc routing with incomplete knowledge of network topology." The GPS interface component (as seen in IDEF1) allows each node to obtain its geographical position from the GPS data input and has the capabilities to determine the position of the destination node. "When a node has a packet for a destination, it chooses from the nodes it knows about the one which is closest to the destination, and sends the packet on its way to that node. Along the path, a node may know of an even closer node to the destination. The packet then gets redirected to that node. On its way to that node, it may get redirected again, and so on until it reaches the destination. The routing table consists of a subset of all nodes in the network, their positions (with GPS time-stamps), and corresponding next hop neighbors. Initially, nodes know about neighbors only and later other nodes get added to the routing table until the tables are "complete", i.e. routing to any node can be accomplished using the tables.
The GRA consists of the following protocols (as seen in IDEF1):

1. Location Advertisement Protocol: Each node will periodically broadcast route advertisement packets. A route advertisement packet consists of an Ethernet header and a geographic header. When a node receives a route advertisement it will check its routing table and update it if necessary and it will not re-broadcast this packet.
2. Geographical Routing Protocol: When a node receives data packet it will first check the final destination, if the final destination is a neighbor it will forward the packet, else it will check its routing table, find the closest geographic neighbor to this destination and then forward the packet to that neighbor.
3. Route Discovery Protocol:

•Each node knows its position and can find position of destinations.
• Each node knows neighbors and learns a few extra nodes.

"In real networks, however, since GPS position has some error, and network topology is dynamic, information is never precise and complete." For this reason, Geo-casting is provided as an output to function 1.2 (in IDEF1). Ghost Mobile IP logic is an input to the sub system which includes the two additional entities discussed previously, as well as the shadow mechanism in the routing and tunneling of packets. These combined produce an output of a "geographically predicted trajectory" which is associated with a function of time. After re processing, the "optimal geographic packet route is produced and fed into the final sub function. A major problem arises in providing real-time services due to frequent handoffs resulting from mobility [2].

Geo-casting, shown as an output (in IDEF1), adds functionality to Ghost Mobile IP as it's input and acts during each handoff , when the mobile registers to its home agent. The HA keeps track of the mobile user's current access point in the network by using GPS data at each access point integrated with the Ghost Mobile IP location advertisement messages. Each access point contains a GPS device so it knows its location. Ghost Mobile IP messages are used in order to send this location information to other access points. Each access point updates its table, the entries of which include the IP address and [redacted] Mobile IP messages are broadcasted periodically and during an

to the OSI model.

functional architecture, inputs, controls, sub systems, and protocols that make up the system. The provisioning of the function is done by the tunneling mechanism of Ghost Mobile IP, the GRA predicted trajectory, and the geo-casting controls and is dependant on functions 1.1 and 1.2. The final product is the "low latency GPS based, optimal Mobile IP handoff and packet routing for real time applications."

3.1 Related Works and alternative solutions

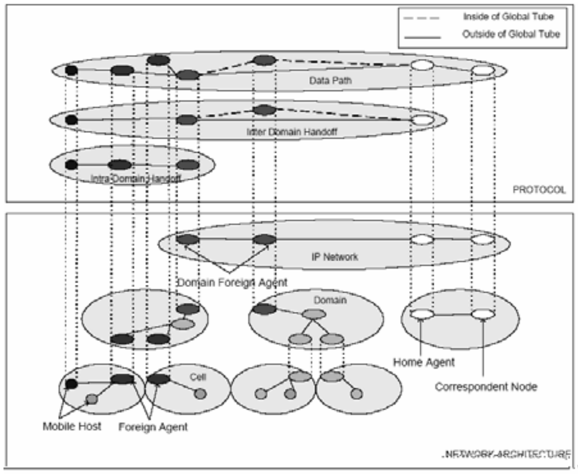


Figure 1 [17]

As seen in the above alternative network architecture, many solutions do not implement a sensor network. There are many approaches to the addressed Mobile IP handoff latency problem, not all necessarily relating to Location based Mobility management. However, the above solution defines one which "proposes a fast, intra-domain and inter-domain handoff scheme (network hand-off solution)using the location of routers to meet the delay and packet loss requirements of real-time services." It does not include the GRA (Geographich Routing algorithm) discussed in the above , but uses GPS to provide for location of routers and defining domain boundaries for mobile nodes.

4.0 Summary

Mobile IP is still implemented rarely, partly because there's little need for it and partly because present implementations waste bandwidth and requires at least two precious IP addresses per user. However, mobile IP is expected to become more important as wireless networks and IPv6 become ubiquitous. Cellular vendors are pushing it hard, as a way to allow seamless roaming between third-generation (3G) and (4G) networks and higher-bandwidth hot spots based on Bluetooth or Wi-Fi (802.11b). [2]

Mobile IP will allow an employee to unplug a handheld computer from its Ethernet cable, and then continue to download a file or conduct a Voice over IP (VoIP) conversation while the connectivity is transferred, first to the office's Wireless LAN (WLAN), then to an outside cellular network, and finally to a home DSL line. [2] As discussed in the application section above, there are countless applications and modular evolutionary technologies which would one day change our lives in a profound way. As of now Mobile IP is a technology in an evolutionary life cycle, but will one day be as prominent as all IP networks. It is the cornerstone of having data and voice services everywhere you go, and accessible anytime.