

Mobile IP - deployment after a decade

Kishore Ramachandran
kishore@winlab.rutgers.edu

Abstract—It has been over a decade since Mobility support for IPv4 was proposed and standardized by the IETF. The challenges of maintaining active sessions for mobile users without modifying existing correspondent hosts or the scalable nature of Internet routing were met by associating separate IP addresses for routing and end-point identification. This approach resulted in a per-packet overhead of a certain number of header bytes as well as suboptimal routing – a packet destined for a mobile user needed to always visit the home network before being sent to the actual location. Optimizations for routing as well as header compression techniques were proposed and standardized subsequently.

The adoption of this standard, however, has been much slower than was previously expected even though commercial routers have been shipping with support for over half a decade. Additionally, the seeming lack of applications, poor handoff performance, suboptimal routing, signalling overheads and security issues have raised questions about whether Mobile IP will ever see widespread adoption. In this paper, we take the position that in spite of its limitations and slow uptake, Mobile IP will see widespread commercial deployment in the near future. The primary basis of our argument is the adoption, and subsequent use, of Mobile IP in the cellular service provider community.

I. INTRODUCTION

Lack of support for host mobility in IPv4, the rapid growth of the Internet and the rapid proliferation of powerful portable devices were the primary reasons behind the proposal and subsequent standardization of the Mobile IP (MIP) protocol ([19], [22]). The main design goal was to prevent the disruption of active application sessions for a mobile user traversing multiple, heterogeneous networks while not requiring changes to existing routers and hosts on the Internet.

However, even though it has been over a decade since it was first proposed, the adoption of Mobile IP seems to be not as prevalent as was previously predicted. This is certainly the case for networks which rely on IEEE 802.11 [14] where most laptops and desktops do not use this technology. To add to this, the seeming lack of motivating applications, poor handoff performance, sub-optimal routing, signalling overheads and security

considerations have led to a questions being asked over the future of MIP.

In this paper, we argue that in spite of its slow adoption over the last decade and in spite of its limitations, Mobile IP will be one of the core technologies adopted by wireless Internet service providers. We base this argument on the fact that networks with the largest base of mobile wireless customers, namely those belonging to the major cellphone service providers have already deployed Mobile IP in their networks. Additionally, with these providers pushing towards replacing their non-IP backbone infrastructure with IP, we expect this technology to be even more prevalent in the future till it is eventually replaced by its IPv6 version. The main factors influencing the deployment of Mobile IP in cellular networks are:

- 1) the ability for providers to closely control, monitor and optimize the service provided to customers even when they are in another provider's network,
- 2) the lack of standardized alternatives,
- 3) the ability to architect away the disadvantages,
- 4) inter-operability with other service providers,
- 5) the growing demand for data applications (as opposed to voice) and Internet connectivity,
- 6) support for incremental deployment,
- 7) the general shift towards a common IP backbone with all applications, including voice riding on top of this network.

The following sections elaborate on these issues in a bid to convince the reader that the benefits of MIP outweigh its disadvantages and that MIP as a technology is here to stay. In section II, we provide an overview of the basic MIP protocol, followed by a discussion on deployment issues in section III. Section IV looks at the security issues affecting deployment and in section V, we address counter claims and arguments. Finally, we conclude in section VI.

II. MOBILE IP - OVERVIEW

A fundamental problem that needed to be addressed while attempting to achieve the design goal was the dual purpose nature of an IPv4 address – it serves both as

an *end-point identifier* and a *routing directive*. Above the network layer, the IP address serves to uniquely identify the host but **at** the network layer, the IP address also serves to identify the network to which the host belongs. In other words, applications require the IP address to remain the same irrespective of host location (or mobility) whereas Internet routing requires the IP address to change when the host moves from one network to another. A possible solution to this conundrum would be to keep the same IP address as a host moves across networks and propagate host-specific routes to aid routing. However, this would break the hierarchical nature of Internet routing and compromise scalability by causing an unbounded growth in the size of routing tables.

The solution proposed by MIP involves splitting the dual roles of an IP address into two independent entities. Two IP addresses are associated with each mobile:

- one to denote the point of network attachment referred to as the *care-of-address* and
- a second one that remains the same across network boundaries referred to as the *home address*.

The home address of the mobile is allocated from the *home* network's address space. Networks on the Internet, other than the home network, to which the mobile is allowed to attach to are known as *foreign* networks. The care-of-address is allocated from the address space of these networks.

To support the two-tier addressing format without requiring modifications to end-hosts and routers on the Internet, MIP introduces two architectural components – the *home agent* (HA) and the *foreign agent* (FA). Together, these two entities ensure that the mobile can maintain its home address as it moves across networks while maintaining connectivity with the rest of the Internet.

A mobile expects to receive periodic advertisements from both types of agents and deduces that it has moved out of its home network when it stops receiving advertisements from its home agent. In a foreign network, the mobile listens for advertisements from foreign agents. If it does not hear any advertisements for a certain period of time, it tries to explicitly determine the presence of these agents. If one is found, the care-of-address is the IP address of the foreign agent. Alternatively, if no foreign agent exists and if the mobile can obtain a temporary IP address from the foreign network (for e.g. using DHCP [3]), the temporary address can be used as the care-of-address.

At this point, the mobile proceeds to convey its current

network location to its home agent (via its foreign agent if one exists). On receiving this message, the home agent knows that the mobile is no longer in its home network. It creates a mapping between the home address of the mobile and its care-of-address and also sends a proxy ARP to the default router indicating that all packets for the home address should be sent to the home agent. Packets from hosts communicating with the mobile (referred to as *correspondent hosts*) are addressed to the home address of a mobile. The home agent intercepts these packets and forwards them to the care-of-address. It achieves this by *tunnelling* incoming IP packets to the care-of-address.¹ On receiving a packet from the home agent, the foreign agent (if it exists) strips off the extra IP header and forwards the packet to the mobile. Alternatively, if the foreign agent does not exist, the mobile strips off the extra IP header on packets arriving from the home agent before they reach the higher layers.

Thus, the home agent is responsible for keeping track of the mobiles and forwarding packets to their current network location. For this purpose, it maintains a registry of mappings between the home address and care-of-address of all mobiles. The foreign agent is responsible for intercepting packets from the home agent, stripping off the extra IP header and forwarding the packet to the appropriate mobile.

III. DEPLOYMENT ISSUES

As stated in section I, the primary driver for the deployment of Mobile IP is the cellular service provider community. The primary reasons why they pushed for and eventually deployed Mobile IP, inspite of its limitations are described in the following subsections.

Before we proceed to understand these factors, we would like to briefly touch upon the issue of the lack of (or slow) adoption of Mobile IP in the past. In our opinion, the primary reason was the lack of adequate wireless technologies that could support existing Internet applications for mobile users. Wide-area wireless providers were previously focussing on voice and it was not until 1999 that broadband data technologies were standardized for both wide area wireless [7] and local area wireless networks [14]. Thus even though MIP was proposed in 1995, it was not until after 1999 that local-area high speed wireless data links were available and

¹It appends another IP header to the incoming packet with the source IP set to that of the home agent and the destination IP set to the care-of-address.

not until 2003 [20] that providers started deploying wide-area high-speed wireless data links. Without such links, it was infeasible to support Internet applications for mobile users and hence MIP was never really used.

A. Ability to control and optimize service provided

An important factor in favor of MIP is that it provides service providers with a technique to route their customers' traffic to their own network regardless of where the mobile is roaming. Thus, it is possible to maintain control over a majority of the network paths that customer traffic will see. This implies that the same user experience can be provided to customers regardless of whether they are within the service provider's network or not. Customer profiles and preferences can be accessed in the same way that they were accessed when the customer was in the home network. Providers can leverage each other's cellular infrastructure in areas where their own infrastructure is lagging or non-existent and have customer data routed to their own networks with minimal additional deployment (home and foreign agents) of Internet infrastructure.

We also expect that MIP simplifies the SLAs with other service providers – provider A has to just route provider B's traffic via its foreign agent to provider B's home network.

B. Lack of standardized alternatives

Although a number of alternative approaches have been proposed ([21], [28], [27], [16], [15]), none of these have been standardized. Moreover, only MIP is supported by commercial routers [2].

C. Minimizing limitations through “clever” engineering

Poor performance during handoff in the form of increased latency and packet loss is often cited as a drawback of Mobile IP. Similarly, increased signalling overhead in the presence of large numbers of mobile stations and frequent handoffs is another limitation.

To overcome these issues, cellular service providers limit the number of network layer handoffs by engineering the network such that these events are very infrequent. Each HA or FA serves a large number of cell sites (upto a thousand) and hence a very large number of mobile users. In this way, although lower layer handoffs are taking place, there are very few instances of network layer handoffs. Thus, signalling overhead as well as occurrences of packet loss and increased round-trip latency are reduced.

D. Inter-operability

If competing service providers adopt a particular standard and if peering arrangements with these providers is unavoidable (as in the case of cellular networks), inter-operability is an important factor when considering the adoption of any protocol (and subsequent implementation). Currently most major cellular service providers support MIP ([30], [13], [26]) furthering the need for others to comply.

E. Demand for Internet connectivity

With the phenomenal growth of the Internet and the arrival of powerful handheld PCs ([10], [9]), it was only a matter of time before cellphone providers started offering wireless data services for these customers. Additionally, the last few years have seen a host of multimedia applications ([29], [25]) being offered by cellphone providers. Arguments in favor of deploying MIP are:

- 1) wide-area wireless speeds are still not high enough to support very fast transfers (in seconds) and
- 2) customers are unlikely to tolerate poor performance due to mobility for multimedia applications.

F. Incremental deployment path

The design and architecture of MIP inherently support an incremental deployment path, which is a strong advantage for cellphone providers with pre-deployed networks.

G. Architectural direction towards all-IP backbone

In the longer term, we expect cellular providers to start phasing out their non-IP infrastructure for the following reasons:

- 1) **Ease of maintenance (operational)** - currently, the system architecture for cellular networks includes a host of protocols between layers 2 and 3 that make management and debugging quite cumbersome. An all-IP network is expected to ease these tasks by replacing these protocols with IP.
- 2) **Reduction of protocol overhead** - another advantage would be a reduction in protocol overhead if IP manages to replace all these protocols with a cleaner design.
- 3) **Reduction in delays** - not only are there various protocols between layers 2 and 3, there also are corresponding network components that could potentially be replaced by a single network component. This design will thus cut delays corresponding to the traversal of these multiple component paths.

- 4) **Reduction in costs** - due to the reasons above, overall operational costs are expected to be cut by a large enough factor so as to motivate this direction.

IV. SECURITY CONSIDERATIONS

So far, we have looked at some of the major factors that influenced cellular providers to adopt Mobile IP. In this section, we look at the implications of this decision from the perspective of security.

The basic security provided by Mobile IP is in the form of user authentication based on the MD5 message-digest function [24] using a shared secret between the home agent and the mobile. Given that cellular providers have contracts with specific equipment manufacturers, we expect that it is not too difficult to store the key for each provider inside each cellphone in a memory location that is inaccessible from the end-user. The same scheme using secret key cryptography is also proposed between home agents and correspondent hosts on the Internet and clearly in this case, this approach does not scale.

The initial draft proposed the use of *nonces* and *timestamps* to protect against replay attacks. However, since these were relatively weak forms of protection from the point of view of an FA, a challenge-response mechanism was introduced by [23] for mobile node authentication by the FA. The authors of [12] also provide a requirements specification for Authentication, Authorization and Accounting (AAA) services that aid in providing MIP service.

These forms of authentication seem weak relative to other mechanisms that perform similar functions on the Internet. However, from a deployment perspective, given that cellular networks exercise tight control over both the network elements and the end-user, these mechanisms suffice for the moment. We expect that stronger mechanisms will be needed by cellular networks in the future with more powerful end-hosts with potentially more freedom [5].

V. COUNTER ARGUMENT

In the following subsections, we attempt to address the claims which argue the opposite position, namely that Mobile IP will never be successfully deployed.

A. Application sessions are short-lived

The first half of this argument is that most application sessions are short-lived. For e.g. HTTP sessions involve a query and a response and the duration between these two events is usually quite small. Thus, unless the IP address

changes in this short interval, there is no real justification for the deployment of Mobile IP. The second half of this argument is that even if the IP address does change in this short interval, users can “refresh” the webpage and get content with the new IP address.

In our opinion, this argument is flawed because it is based on the underlying assumption that very short-lived applications such as web browsing are going to be far more popular than longer-lived multimedia applications such as audio song or music video downloads. The recent past has shown this to be untrue – multimedia applications form the fastest growing segment of the market. In Korea, with over 25 million customers and Japan, with over 20 million customers, the successful adoption of 3G cellular technology is attributed to multimedia (from an applications perspective) ([20], [1]). We expect users to be far more intolerant of breaks in connectivity with these applications. We also expect the trend to continue, with regards to the increasing popularity of multimedia applications due to increased wide-area wireless broadband capabilities ([7], [8], [11]) and the availability of cell-phones capable of handling such speeds ([6], [4]). Unlike previous IP networks, we expect mobility to be a first-class citizen with the ultimate “application pull” coming through the deployment of Voice over IP (VoIP) on top of these networks.

Additionally, this argument focuses only on the applications and fails to take into account the deployment advantages (outlined in section III) that Mobile IP gives to service providers.

B. Sub-optimal network-layer routing

The primary flaw in the MIP architecture is that of triangular routing – packets traverse a sub-optimal (potentially longer) forward path from the correspondent hosts to the mobile since they have to always go through the home agent. This problem is exacerbated when,

- two mobiles are communicating with each other and
- some network administrators prefer symmetric paths (for ease of debugging) and hence force packets from the mobile to traverse the home network on the return path as well.

The Route optimization extension to Mobile IP [18] attempts to solve this problem. It provides for optimized communications with mobile nodes by proposing the modification of other Internet hosts and routers². It

²Note that in the case of two mobiles communicating with each other, no modifications are required of other Internet hosts or routers. The home agents of the respective mobiles inform their foreign agents, which then proceed to communicate directly.

proposes that foreign agents, correspondent hosts and Internet routers maintain a cache storing the mapping between the home address and the care-of-address of destination mobiles. This cache is populated by the home agent after the first packet traverses through the home network. A stale entry in the cache results in a notification from the older foreign agent stating that the entry is invalid. The correspondent host (or the foreign agent or the Internet router) then goes back to sending the packets to the home agent, which in turn sends an update to the cache. The older foreign agent knows that the mobile has moved since these extensions also allow for communication between foreign agents while the mobile moves from one foreign network to another.

It can be argued that the benefits of these extensions can only be derived if all communicating entities, namely the home and foreign agents as well as correspondent hosts and participating routers implement these extensions. In 3G networks, given the tight control exercised by service providers over their networks, we expect that at least all home agents, foreign agents and routers within these networks will implement these extensions. Thus, the ill-effects of triangular routing can be minimized if not completely eliminated. Further, although routing is sub-optimal, we argue that unless applications are adversely affected, there is no real cause for concern. If the delays introduced are a small fraction of the overall delay and they do not negatively impact application performance, it is a tradeoff that service providers will be willing to make.

C. Home Agents could be performance bottlenecks

The home agent could potentially be a bottleneck as well as the single point of failure. However, organizations can provide for redundancy among home agents as described in [17]. By linking together two or more home agents behind an ethernet switch, a Virtual Home Agent (VHA) can be formed. One physical home agent serves as the primary whereas the other serves as the secondary or backup. Both physical home agents share the same “virtual” IP and MAC addresses. Note that the secondary home agent will have to be updated with all the registrations received by the primary (from mobile users).

D. Signalling Overhead

Each time the mobile moves from one network to another, there is signalling overhead between the mobile, the foreign agent and the home agent. Additionally, if route optimization is used, the home agent needs to

update the caches of the correspondent hosts, routers or foreign agents on the Internet.

However, as stated earlier, the signalling overhead can be reduced by limiting the number of times a mobile moves from one IP network to another.

E. Handoff Latency

Similarly, the occurrence of poor handoff latencies can also be reduced by architecting the network so as to reduce the frequency of handoffs.

F. Security Issues

We accept the criticism that security is weak in current deployments. Known solutions [5] proposed to potential denial-of-service (DoS) attacks include,

- separating voice and data traffic so as to protect voice from malicious data traffic,
- over-provisioning the network to deal with such short-term anomalies and
- limiting the number of channels for data traffic.

VI. CONCLUSIONS

When the topic of Mobile IP is broached, skepticism about its future is the first reaction that comes to people’s minds. However, this is far from the truth – cellular networks have embraced this technology and deployed it across their networks. They have managed to leverage an aspect of this technology for their benefit, which for long was thought of as its weakness – that of routing all packets from/to a mobile via the home network. By doing so, these tightly controlled networks have managed to maintain control over data traffic from their customers regardless of whether the mobile is in their network or in another provider’s network. By engineering the network to reduce handoffs and signalling overheads, these networks have also managed to hide the limitations of Mobile IP. After a decade of relative anonymity, Mobile IP has finally risen to be part of the core technologies that support a truly mobile Internet.

VII. ACKNOWLEDGEMENTS

I am grateful to Praveen Atreya from Verizon Wireless for patiently answering all my questions on this topic. I would also like to thank Ivan Seskar and Dr. Sanjoy Paul (previously with Lucent Technologies) for their opinions on to this matter.

REFERENCES

- [1] 3g in japan - FAQ. <http://www.eurotechnology.com/3G/index.html>.
- [2] Inc. Cisco Systems. Cisco IOS mobile ip support. <http://www.cisco.com/>.
- [3] R. Droms. "dynamic host configuration protocol". Internet RFC 1541, October 1993.
- [4] LG Electronics. LG VX8000 phone. <http://www.mobiledia.com/phones/lg/vx8000.html>.
- [5] W. Enck, P. Traynor, P. McDaniel, and T. L. Porta. Exploiting open functionality in sms-capable cellular networks. In *ACM Computer and Communications Security CCS'05*, November 2005.
- [6] Wikipedia The Free Encyclopedia. 1xEV-DO phones. http://en.wikipedia.org/wiki/EV-DO#EV-DO_Phones.
- [7] Wikipedia The Free Encyclopedia. Evolution-data optimized. <http://en.wikipedia.org/wiki/Evolution-Data.Optimized>.
- [8] Wikipedia The Free Encyclopedia. High-speed downlink packet access. http://en.wikipedia.org/wiki/High-Speed_Downlink_Packet_Access.
- [9] Wikipedia The Free Encyclopedia. PDAs. http://en.wikipedia.org/wiki/Personal_digital_assistant.
- [10] Wikipedia The Free Encyclopedia. Pocket PCs. http://en.wikipedia.org/wiki/Pocket_PC.
- [11] E. Esteves, P. J. Black, and M. I. Gurelli. Link adaptation techniques for high-speed packet data in third generation cellular systems. In *European Wireless Conference*. Qualcomm, Inc., 2002.
- [12] S. Glass, T. Hiller, S. Jacobs, and C. Perkins. Mobile ip authentication, authorization, and accounting requirements. Internet RFC 2977, October 2000.
- [13] Inc. Hewlett Packard. HP enables vodafone UK billing for mobile IP services. <http://www.hp.com/hpinfo/newsroom/press/2001/010524a.html>, May 2001.
- [14] IEEE. *Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. "IEEE-SA Standards Board", 445 Hoes Lane, Piscataway NJ, USA, August 1999.
- [15] J. Ioannidis, D. Duchamp, and G. Q. Maguire Jr. "ip-based protocols for mobile internetworking". In *Proc. ACM SIGCOMM*, pages 235–245, 1991.
- [16] J. Ioannidis and G. Q. Maguire Jr. "the design and implementation of a mobile internetworking architecture". In *Proc. Winter USENIX*, pages 491–502, January 1993.
- [17] isoc.org. Network design with mobile IP. In *11th Annual Internet Society Conference*, Stockholm, Sweden, June 2001.
- [18] D. B. Johnson, C. Perkins, and A. Myles. Route optimization in Mobile IP. IETF Internet-Draft v12, March 2000.
- [19] David B. Johnson. Scalable support for transparent mobile host internetworking. *Wirel. Netw.*, 1(3):311–321, 1995.
- [20] Nortel Networks. M. Morell. Wireless market survey - nortel networks. <http://www.educause.edu/ir/library/powerpoint/nmd0408.pps>, February 2004.
- [21] A. Misra, S. Das, A. Dutta, A. Mcauley, and S. K. Das. Idmp-based fast handoffs and paging in IP-based cellular networks. In *3GWireless*, May 2001.
- [22] C. Perkins. IP mobility support. Internet RFC 2002, October 1996.
- [23] C. Perkins and P. Calhoun. Mobile ipv4 challenge/response extensions. Internet RFC 3012, November 2000.
- [24] R. L. Rivest. The MD5 message-digest algorithm. Internet RFC 1321, April 1992.
- [25] Sprint. Picture messaging. <http://pictures.sprintpcs.com/serviceoptions.do>.
- [26] Sprint. Sprint offers wireless connectivity for businesses. http://www2.sprint.com/mr/news_dtl.do?id=1809.
- [27] Fumio Teraoka and Mario Tokoro. Host migration transparency in ip networks: the vip approach. *SIGCOMM Comput. Commun. Rev.*, 23(1):45–65, 1993.
- [28] Fumio Teraoka, Yasuhiko Yokore, and Mario Tokoro. A network architecture providing host migration transparency. In *SIGCOMM '91: Proceedings of the conference on Communications architecture & protocols*, pages 209–220, New York, NY, USA, 1991. ACM Press.
- [29] Verizon Wireless. Picture and video messaging. http://getitnow.vzwshop.com/index.aspx?id=messaging_pixflix.
- [30] Verizon Wireless. Verizon wireless launches internet access for pocket PC. <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/02-21-2001/0001432273&EDATE=>.