Comparative Stury of Secured Optimized Route in MIPV6

. Shalini Punithavathani[1],Dr.K.Sankaranarayanan[2] ,A. BrammaSakthi[3]

1. Registrar, AnnaUniversity Tirunelveli **2.**Dean of Electrical Sciences V.L.B.Janakiammal College of Engineering and Technology **C**oimbatore, **3**.Lecturer,G.U.Pope College Of Engineering,Tirunelveli.

Summary
The current Internet is based on an architecture created decades ago. Today however, the use of mobile devices and wireless networks present new challenges for Route Optimization of location management and security. Therefore many alternative solutions have been engineered. This paper introduces and compares three mobility implementing protocols, each from a different layer. The purpose of the comparison is to determine which protocol would be best suited for mobility. The chosen protocols are Mobile IPv6(MIPv6), Host Identity Payload (HIP), and MIPv4 .There is really no straightforward solution to the choice of protocol for mobility. On the contrary, approaches used in different layers often complement rather than exclude each other.

Key words:
MIPv6, HIP, MIP, mobility comparison

1. Introduction

The Internet's current addressing scheme follows the design decisions made in the 1970's. Back then, the Internet was a quite static network, and all hosts were connected to it through one specific interface. Any computer could be easily identified with its unique IP address. The location directly identified the node in the network. Many things have changed since then, including computer networks.

The main revolution has been the deployment of mobile devices. With wireless interfaces giving ease of use, these devices have become increasingly popular. The underlying Internet, however, does not support the needed features and architectural structures for mobility. Because of that, the existing general mobility support solutions in the IP world have tried to hide the dynamic change of IP addresses from the higher layer protocols Another major change concerns security: Today's Internet is accessible for practically anyone, and this unfortunately opens a chance for misuse as well. Both individuals and businesses use the Internet for sending and receiving important messages, and these transactions must be properly secured. Therefore, when considering choices for mobility, security issues have to be taken into account.

The purpose of this paper is to find some benefits and drawbacks when using one of the protocol mentioned above as a place for mobility. To accomplish this, an overview of the three protocols with a short description of their functioning is given, and a comparison of the layers is done through the protocols.

From this section, input the body of your manuscript according to the constitution that you had. For detailed information for authors, please refer to [1].

2. Problem Definition

As discussed above, there is a need for change from address orientation to host orientation. This means that the original situation of using only well-known single persistent IP addresses is no longer a viable solution. A setup of this kind was valid in the early days of the Internet, when four issues were considered invariants[9]:

- An address received was the address sent,
- Addresses were stationary (non-mobile),
- Source and destination were reversible, and
- All hosts knew to which address they should send packets to reach the wanted host.

According to Henderson, these assumptions cause four fundamental problems in the network layer[3].

The first concerns **Addressing,** As IP routing and addressing are hierarchically defined for scalability, the mobile hosts usually have a topologically incorrect interface address when they attach to a new network.

Secondly, when changing network, the mobile host may become unreachable to the rest of the network unless the new address is somehow mediated to other nodes **(location management).**

The third problem is related to **session management,** as the current transport protocols use the IP address as part of the connection identifier, the change of address breaks active connections.

Finally, the mobile hosts must be able to authenticate themselves to their peers upon moving and maintain or re-establish network level **security associations**.

The main issue to be resolved in the current Internet addressing scheme is the separation of the concepts *address* and *identifier*. Currently the devices connected to the network are identified by their IP addresses. When the

Manuscript received November 5, 2008
Manuscript revised November 20, 2008

mobile device moves between networks, its IP address changes and so does its identifier. The device has two choices to continue the ongoing communication with its peer. The new identifier is mediated to the peer or alternatively the device makes itself reachable via the original identifier. A host cannot in the truest sense "own" a location name because bits can be duplicated. Therefore, the identifiers must also be based on some cryptographic method.

3. Current Mobility Solutions

In this section a solution for mobility is presented for each of the three protocols discussed above. In Section 3.1, Mobile IPv6 is presented. An overview of HIP is given in Section 3.2.

3.1 Mobile IPV6

Mobile Internet Protocol version 6 (MIPv6) is a network layer protocol, and it is the current Internet Engineering Task Force (IETF) proposal for a standard for the mobility problem. The protocol relies on IPv6[2], which was designed from the start to support mobility. MIPv6 enables a mobile device to maintain its IPv6 address and transport layer connections while its point of attachment to the network changes. Although MIPv6 has come a long way, it is still under ongoing development by the IETF Mobile IP Working Group. The protocol is documented in the Internet draft Mobility Support in IPv6[4], and the following chapters sum up the protocols operation.

3.1.1 Architecture

Each Mobile Node (MN) is identified by its Home Address (HoA). The address is given by a Home Agent (HA), which is a router supporting mobility services in the nodes home network. For discovering a HA, MN uses Dynamic Home Agent Address Discovery protocol.
If MN operates in its home network, conventional mechanisms are used to route packets addressed to it. When the node moves to another network, it acquires a new address called a Care-of Address (CoA) through either stateless or stateful automatic Address Auto configuration. The mobile node then informs the Home Agent of its current address. The association between MN's Home Address and Care-of Address is known as a "binding" for the node. Using this information, the Home Agent forwards any packets addressed to MN into the new location. This registration procedure is called a binding update (BU). MIPv6 enables nodes to cache these address bindings into HA's binding cache[4].
Any node communicating with MN is known as a corresponding node (CN). CN may itself be a stationary or a mobile node. In a basic situation, all traffic between MN and CN are tunneled through the Home Agent. Figure 1 illustrates this situation.

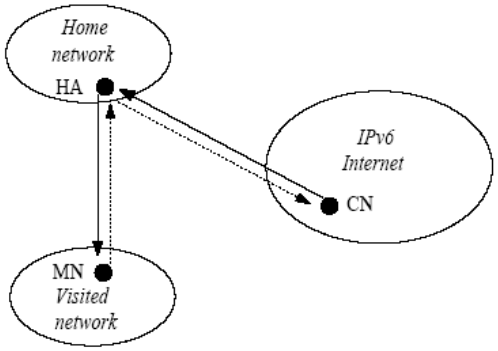


Fig. 1 Tunneling traffic between the MN and CN

In Figure 1, data sent by MN to CN is illustrated with a dotted line and the opposite transmission made by CN with a solid line. All traffic goes through HA; this mode of communication is known as bidirectional or reverse tunneling. IPv6 encapsulation is used in the tunneling. The nice thing about this mode is that CN does not require to support Mobile IPv6 at all.
Even so, bidirectional tunneling is not always efficient, especially if the MN is close to CN, and therefore communicating through the Home Agent creates an unnecessarily long path. MIPv6 offers a solution for this sort of situation through route optimization: Only the first packet is tunneled through HA. Then MN can register its current location by sending its current binding information to a CN (a BU message).
After this, the packets from CN can be routed directly to the Care-of Address of MN with the help of CN's home address in the routing header. Similarly, MN sends all packets to CN directly, using the Home Address destination option. Route optimization is presented in Figure 2.

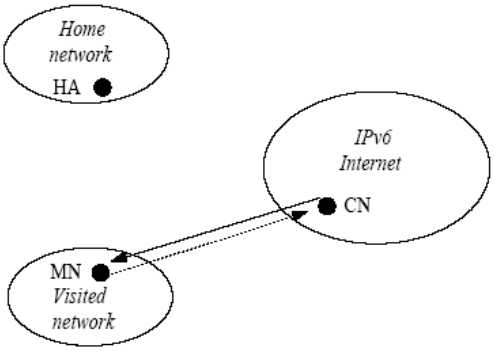


Fig. 2 Route optimization for traffic between MN and CN

As previously, the data sent by MN to CN is marked with a dotted line, and the traffic from CN to MN is marked with a solid line in Figure 2. The shortest communication path is used when packets are routed directly to MN's Care-of Address. This also eliminates congestion around HA[4].

3.1.2 Security

Binding updates are one of the key factors in the functioning of MIPv6. Therefore, the binding messages must be authenticated and protected against replay attacks to prevent malicious nodes from corrupting the binding caches with invalid addresses[4].
Before using any binding updates, the Mobile Node must register to the Home Agent. This is done in order to create an IPsec Security Association (SA) between the two entities. If manual keying is used, SA is pre-installed. Internet Key Exchange (IKE) can also be used, if it is supported by both parties.
When the Security Association is created, it is used to authenticate the binding update messages between MN and HA. To achieve this goal, MIPv6 uses the IPsec framework[1], either Authentication Header (AH) or Encapsulated Security Payload (ESP) can be used with a non-null authentication algorithm.
When authenticating the binding update between MN and CN, a return routability procedure is used instead of SA. The procedure uses cryptographic tokens in verification. Basically, CN sends test messages as a challenge, and MN responses. After this, MN constructs from random data and data gathered from the procedure a binding management key, Kbm, that is used in the binding procedure. The Binding Updates are then protected against replay as the messages used have sequence number, and with a Message Authentication Code (MAC), tampered messages can be detected.
The MACs are created with RSA algorithm[1].

3.2 HIP

Host Identity Protocol[9] is a proposal to separate identifier from locator at the network layer of the TCP/IP stack. It is a new name space of public keys. It is a protocol for discovering and authenticating bindings between public keys and IP addresses[5,6,7]. HIP introduces a new Host Identity layer (layer 3.5) between the IP layer (layer 3) and the upper layers. In HIP, upper layer sockets are bound to Host Identities (HI) instead of IP addresses. In addition, the binding of these host identities to IP addresses is done *dynamically*. The purpose of HI is to support trust between systems, enhance mobility, and greatly reduce the DoS attacks.
A great advantage in this mobility solution is that the hosts can easily have both the current IPv4 and the new IPv6 addresses. Furthermore, there is no need to change the current
routing methods. Multi-homing, NAT-traversal, anonymity, and avoiding Man in the Middle (MitM) - attacks are other features the HIP has to offer[8].

3.2.1 Architecture

HIP is similar to MIPv6 in the sense that the main goal for both of them is to make mobility transparent to the applications. In HIP, the hosts are identified with public keys, not IP addresses. A typical host identity is a public cryptographic key of an asymmetric key-pair. Each host will have at least one HI that can either be public or anonymous.
The HIs can be different in sizes depending on the used public key method. Therefore, the HI is represented via its 128 bit (SHA-1) hash, called Host Identity Tag (HIT), or 32 bit Local Scope Identity (LSI). The HIT identifies the public key that can validate the packet authentication, and HITs should be unique in the whole IP universe. They are stored in some public address directory (e.g. DNS) with the exception of anonymous identities.
LSIs are 32 bit localized representations of a HI. Each host selects its communicating partners LSI, and the value must be random. Even so, collisions between different LSIs may easily occur, and therefore they should only be used in local scope according to local policies. The main reason for LSIs is to make the use of HIP possible with existing protocols such as IPv4. The LSI's advantage over HIT is its size; On the other hand, the LSI's disadvantage is its local scope.
One of HIP's features is authentication during connection establishment. To achieve this, the HIP-protocol (or Host Layer Protocol) is used. However, normal packets cannot be used, and so HIP presents a new packet structure: The transport layer packet (e.g. TCP) must be enclosed with a HIP header, which contains the HIT[6]. Figure 3 illustrates the situation. For simplicity, any extension headers are omitted from the figure.

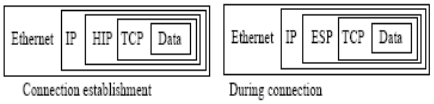


Fig. 3 The HIP packet structure

HIP packets are only needed to establish an authenticated connection.
As mentioned above, the HIP protocol is used to authenticate the connection. In addition to authentication, the procedure establishes Security Associations for a secure connection with IPsec ESP. The HIP-protocol uses a four-way handshake with Diffie-Hellman key exchange. The entity that wants to establish a connection is referred

to as initiator and the other party as responder. Before the actual exchange takes place, the initiator has fetched the responders IP address, HI, and HIT from an address directory (e.g. DNS).

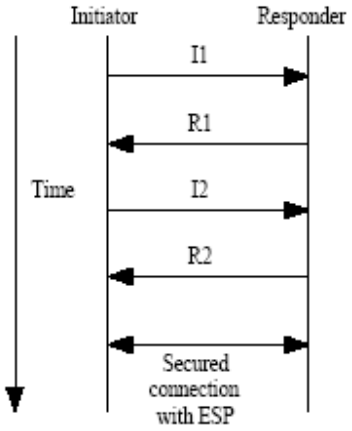


Fig. 4 The HIP exchange

Figure 4 illustrates the exchange, and the four packets used in it are explained below.

I1 packet is sent by the initiator to see if the responder speaks HIP. The packet contains the HITs of the both parties.

R1 packet is sent back as a reply by the responder. As the responder cannot yet trust the initiator, it initiates a three-way cookie exchange. Packet R1 holds the responders public Diffie-Hellman key, HI, and information about the supported ESP modes as well as a challenge. The impact of a DoS attack is minimized as the responder is the one giving the challenge.

I2 packet contains the initiators public Diffie-Hellman key and a computed response to the challenge. The computation makes the DoS attack unprofitable for the initiator. The ESP options are also sent with the packet.

R2 packet completes the handshake. The responder sends it if the initiators response to the challenge was correct. After the sending of the R2 packet, the ESP encrypted datagrams (see figures 3 and 4) can be used to secure the whole connection.

During the secured connection, mobility in HIP is quite straightforward. As HIs are used to identify the mobile node instead of IP addresses, the *location* of the node is not bound to the *identifier*. Therefore only a simple signalling protocol (the HIP protocol discussed above) is needed to take care of the dynamic binding between the node's IP address and HI. When one of the communicating peers changes location, it simply sends a HIP readdress (REA) packet through the secured ESP channel. The SAs are bound to the HITs and not to addresses, and thus the connection continues uninterrupted.

However, if the responder changes location before the connection has been properly established or if both of the peers change location at the same time (the double jump problem), a *rendezvous server* is needed. It is a packet forwarding agent which simply temporarily forwards the initial HIP packet to the responder. All further packets are handled normally between the initiator and responder.

3.2.2 Security

The HIP security is quite good. Firstly, as discussed in the previous section, the connection establishment is well authenticated with the help of IPsec. During this procedure, the Security Associations needed for a secure ESP connection are obtained. Secondly, the HIP identifiers are public keys, and therefore they can be used to authenticate the HIP packets as well as to protect them from most Man-in-the- Middle attacks [5].

In addition using public keys as identifiers means that no explicit Public Key Infrastructure (PKI) is needed. Thirdly, the impact of DoS attacks is decreased as the *responder* is the one giving the challenge and deciding its difficulty. If DoS attacks are attempted using multiple I1 packets, the responder can to some extent reuse the R1 packets. Finally, HIP supports anonymity as HITs can be anonymous. This is appealing for many users but on a governmental level it can be seen as a threat.

There are also a number of MitM attacks that can be used against HIP. The resolution to most of these attacks is to use secure and authenticated connections. In addition, the HIs can be fetched from a signed DNS zone so that these signed HIs are used to validate the HIP packets.

4. Performance Analysis

The key issues to consider are security, signalling and other functional overhead, and the effects on both applications and over all architecture. As all of the three protocols are quite new, the security considerations were taken into account from the start. For example, IPsec can be used together with all of them. Even so, the return routability procedure used by MIPv6[10] .It has a simple and fast solution to the key distribution system, which is one of the biggest issues with MIPv6. In addition, HIP unlike MIPv6 enables location changes that do not break ESP secured connections. The cryptographic nature of HIP namespace also increases support for security.

Cryptographic methods used in HIP, however, require heavy computations. This may present efficiency problems at least for mobile devices with Limited CPU power. HIP work with current IPv4 and future IPv6 networks but

MIPv6 relies only on IPv6[3]. Furthermore, MIPv6 requires changes to routers whereas the other solutions do not. In the following section I conclude my view for the best location for mobility in the Internet architecture.

Table 1: Mobile IPv4,IPv6 and HIP Key features

Key Features	Mobile IPv4	Mobile IPv6	HIP
Addressing	32bits	128bits	Depends On public Keys(SHA-1,128bits)
Architecture	Nodes:CN,MN, HA	Nodes: MN, CN,HA	Randevouz Point needed
Security	NO	IPSec	Diffie-Hellman exchange for initial connection, IPSec
Usability	Only for IPv4	Only for IPv6	High, can use any lower layer protocols
Mobility	Binding Updates Between nodes	Binding Updates Between Nodes+ Optimizat-ion	Randevouz point needed e.g: DNS UPDATE method
Handover performance	low	Better than HIP	low
Sec (MitM)	No	BU, Return Routabilit y	IPsec, DNSSEC
Sec (DOS)	No	BU, Return Routabilit y	Reacha--bility check
Bandwidth	More	Less	less

Packet delivery means a sampled measure, expressed as a percentage ratio of the number of IP packets inter route core IP nodes on the inter route IP network.

Average percentage of packet delivery is calculated using the formula,

$$T_{av} = \frac{\Sigma_i R_i}{\Sigma_i S_i} * 100$$

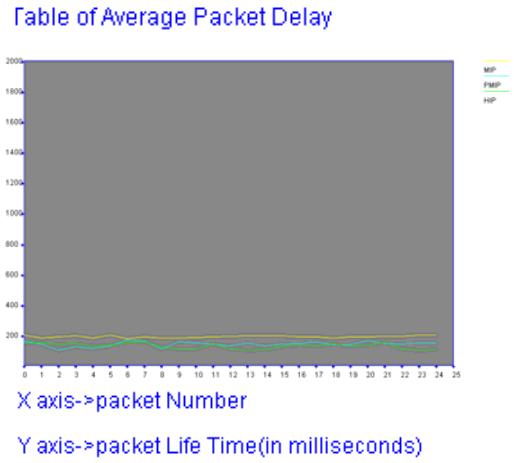
T_{av} –the average percentage packet Delivery.

R_i – the total number of IP packet Received.

S_i – the total number of IP packets Sent.

Comparison of registration times for MIPv4,MIPv6 and HIP for with data packet flows is presented below:

	Basic Scheme	Return Routability	HIP
delay	190	141	129
% of Improvement		34.0	47.0



5. Conclusion and Future Work

Mobility and security have been an active research area in recent years because the current Internet architecture has been insecure and originally designed to be very static. In this project , we first discussed the backgrounds in MIPv6 and HIP security design. The assumptions and starting point of the security designs in MIPv6 and HIP are first elaborated in detail. Next we analyzed the security threats in MIPv6, and HIP. Classified the attacks against Routing Optimization into two kinds. Attacks of the first kind try to exploit the spoofed Binding Update messages to achieve attackers_ purpose (e.g., redirecting the traffic). The second kind of attacks tries to attack the Binding Update protocol itself, and prevent the protocol participants from correctly completing the protocol .Next we compared the security in Mobile IPv4,MIPv6 and HIP. HIP seems to be a good solutions for mobility it solves many security, mobility, and multihoming issues at the same time. The difference is small and most likely to be insignificant in real life. Future work of this paper is HIP have to add a new layer to a well established Internet architecture which increases data traffic and implementation complexity [3]. HIP and MIPv6 suffered

from undesired end-to-end latency when readdressing is rapid [3]. To sum it up, each protocol or layer has its benefits and drawbacks.
It is an interesting topic for future research.

References

[1] Comer, Douglas E., Internetworking with TCP/IP VolI: Principles, Protocols and Architecture, Fourth Edition, Prentice Hall, 2000, 750 p.
[2] Deering, S., Hinden, R., Internet Protocol, Version 6 (IPv6) specification, *RFC 2460, IETF IP Version 6 Working Group*, December 1998, ftp://ftp.rfceditor. org/in-notes/rfc2460.txt
[3] Henderson, T., R., Ahrenholz, J., M., Kim, J., H., Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming In. *IEEE Wireless Communications and Networking*, pp. 2120-2125, 16-20 March 2003, vol.3
[4] Johnson, D., Perkins, C., Arkko. J., Mobility Support in IPv6, *Internet draft, version 24, IETF Mobile IP Working Group*, June 2003, http://www.ietf.org/internetdrafts/ draft-ietf-mobileip-ipv6-24.txt
[5] Moskowitz, R., Host Identity Payload Architecture, *Internet draft, version 2, IETF*, February 2001, http://homebase.htt-consult.com/ hip/draftmoskowitz-hip-arch-02.txt
[6] Moskowitz, R., Host Identity Payload and Protocol, *Internet draft, version 5, IETF*, October 2001, http://homebase.htt-consult.com/_hip/draftmoskowitz-hip-05.txt
[7] Moskowitz, R., Host Identity Payload Implementation, *Internet draft, version 1, IETF*, February 2001, http://homebase.htt-consult.com/ _hip/draftmoskowitz-hip-impl-01.txt
[8]Nieminen,K.,Tietoturvaprotokollat, 3.4.2003, *Presentation in course 8306500 Tietoturvaprotokollat in Tampere University of Technology* http://www.tml.hut.fi/pnr/publications/Opodis02-Ylitalo-et-al.pdf
[9] Nikander, P., IPCN 2001, From Address Orientation to Host Orientation http://www.tml.hut.fi/ pnr/presentations/IPCN2001slides
[10] Ylitalo, J., Jokela, P., Wall, J., Nikander, P., Endpoint Identifiers in Secure Multi-homed Mobility