

Comparison and Analysis of IP and IKEv2 Mobility Extensions

Chandani Haresh
Helsinki University of Technology
Department of Computer Sciences and Engineering
Haresh.Chandani@hut.fi

Abstract

Tremendous growth in hand held devices that use data services have revolutionized the information society; further more integration of wireless, cellular, and fixed network using internet services has provide promising computing platform; key issues in such heterogeneous environment are transparent mobility and security.

Internet Key Exchange version 2 (IKEv2) is being designed by MOBIKE working group within Internet Engineering task force (IETF) as a security protocol for mobile nodes. This paper present mobility solution that includes mobile IPv4 (MIPv4) and mobile IPv6 (MIPv6), and explains IKEv2 mobility extension for securing them.

KEYWORDS: Mobility, MIPv4, MIPv6, IKEv2.

1 Introduction

Internet solution has been developed long before cellular and wireless networks exists integration of these networks have bring a need of seamless mobility where a node can change its point of attachment without loosing the connection.

Mobile IP is one of the promising solutions that provide inter-network mobility. In an IP network each node is assigned and recognized by an IP address, and when a node changes its point of attachment, it is assigned a new IP address; the existing connection becomes invalid and requires rebuilding. Mobile IP solves the mobility problem by correlating the static home address with the dynamic care-of-address (CoA) [2].

Mobile nodes require security features to ensure proper operation. When a node acquires a new IP address, it requires authentication with new assigned IP address and Internet key exchange version 2 (IKEv2) provides a way to secure end to end connection by establishing security associations (SA) between entities. SAs are the one way rules for two communicating peers that define the security parameter for a connection that includes security protocol, cryptographic algorithm, keys used for algorithm, and SAs life time [6].

For a mobile node, It is impractical in many situation to establish SA manually; the device might be too slow for re-keying or it might requires some credential that requires user interaction [13]. IKEv2 mobility extension provides mobility support that allows mobile host a way to keep existing IKE SAs and IPsec SAs without re-keying and also authenticating those changes [13].

In section 2, mobility solutions that include MIPv4 and

MIPv6 are discussed; continuing in chapter 3, I will discuss about IKEv2 protocol and its mobility extension that is used for securing mobile node end to end connection. In chapter 4, I will present brief comparison and analysis of mobility protocols, chapter 5 concludes this paper.

2 IP mobility

Mobile IP (MIP) is standardized by IETF. It provides transparency to the higher layers and network layer mobility where a node can change its point of attachment from one subnet to another subnet.

2.1 Mobility requirements.

- Transparent mobility.
- Availability of services or data.
- Efficient delivery of data without any loss.
- End to end security.

2.2 Overview of Mobile IPv4

In IPv4 network, the node is represented by its IP address that identifies its point of attachment to the network. In MIPv4, mobility is created with help of two IP addresses, home address or fixed address, and care-of-address (CoA). Home Address refers to the static home network address of Mobile Node (MN) that is used for identification, where as CoA is temporary address assigned in foreign network (FN) used for routing. CoA represents mobile node's current point of attachment to the Internet [2]. In home network of mobile node, a Home Agent (HA) is used. HA keeps dynamic mapping between the home address and CoA.

MN determines its movement by listening to the agent advertisement [2]. When the MN moves in a foreign network, it acquires a new temporary CoA from FA by listening to ICMP router advertisements which are sent periodically or by sending route solicitation request. Notification messages called Binding Updates (BU) are sent for registration of new care-of-address. The foreign agent registers the CoA with the home agent.

MN can also obtain the CoA by contacting Dynamic Host Configuration Protocol (DHCP) server; this care-of-address is called co-located care-of-address [10]. MN registers this care-of-address directly to HA.

2.2.1 Routing

In MIPv4 mobility is transparent to the Correspondent node (CN) and is achieved by triangular routing. CN does not need to know the mobile node's current location and sends the data packet as usual to the mobile's home address. When a packet for mobile node arrives at home network, the HA intercepts the packet and determines the CoA, and tunnels the packets towards node's CoA.

Tunneling is done by encapsulating using IP within IP protocol [5]. HA adds the IP tunnel header which contains the CoA as the destination in the IP packet. The tunnel header contains a mark that defines that the next header is again IP header. At the destination the packet is de-capsulated; the original packet is recovered with CN as source and MN as destination. The packet is then forwarded to the MN.

When a mobile node wants to send the packet to the correspondent node, it uses standard IP routing mechanism and sends the packet directly to the correspondent node [2]. MN uses its home address as source address might suffer from ingress filtering [12]. Firewall on foreign network might discard the packets of mobile node, because address used by MN is not topologically correct.

Reverse tunneling extension [8], is defined to overcome this problem, where a reverse tunnel is established. A mobile node tunnels the packets back to HA that removes the outer IP header from the packet and forward the packets to the correspondent node [8]. MIPv4 solves mobility by triangular routing which is not efficient, where packets from the CN pass through HA to the MN. Route optimization is defined for MIP that allows CN to send the packets directly to MN. Route optimization is achieved by sending mobile node's current care-of-address to the CN. HA sends the binding updates to the CN [4].

The routing scenario for MIPv4 is shown in the figure 1.

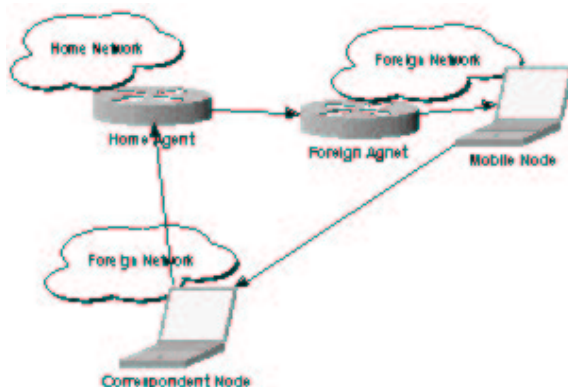


Figure 1: Routing in MIPv4 [1].

2.2.2 Security

Security is open issue in MIPv4.

In MIPv4, the CN might suffer from the router's ingress filtering. Foreign network protected by firewall may reject the packets when MN sends the packet directly to the CN using its home address as source address [10]. Ingress filtering can be avoided by using reverse tunnelling.

In MIPv4 majority of risk is associated with the authentication of the mobile node. Registration information i.e. Binding Updates (BU) and acknowledgement must be authenticated to make sure that entities are the ones who claim to be. Otherwise malicious node can impersonate as mobile node by sending bogus care-of-address to the home agent that makes the actual node unavailable. Malicious node can gain access to the mobile node's traffic, what is called that remote redirection [9].

In Mobile IP, mobility is achieved by triangular routing that is vulnerable to single point of failure. All the packets from MN are passes through HA, and in case of HA failure, all the desired traffic for the mobile nodes using that HA will be interrupted.

2.2.3 Summary

MIPv4 is designed to provide mobility support in an IPv4 network. Mobility is transparent to the transport and higher level protocols [2]. Mobility is achieved by triangular routing which brings higher latency, extra overhead, and load to the network.

Route optimization extension is defined to achieve better performance. Reverse tunneling extension can be used to avoid ingress filtering.

Majority of security risk is associated with MN registration information. MN must be authenticated. Internet Key Exchange (IKE) Protocol can be used to provide better security services.

2.3 Overview of Mobile IPv6

Mobile IPv6 is designed to provide mobility support for IPv6 nodes. MIPv6 is enhanced version of MIPv4 with security and performance consideration; it allows transparent routing of IP packets. MIPv6 has similar mobility concepts as in MIPv4.

In MIPv6, the node can be identified by its home address regardless of its current point-of-attachment. When visiting in a foreign network, Care of address (CoA) is assigned. CoA is generated using IPv6 stateless address auto-configuration by adding network prefix with a mobile node interface identifier or by using statefull address configuration provided by DHCP or PPPv6 server. Thus, a Foreign Agent is not needed in MIPv6 [12].

2.3.1 Routing

In MIPv6, CoA can also be used to identify the node when node is in foreign network. Mobile Node sends CoA to HA for registration. When a correspondent node sends packets to the mobile node, HA intercepts the packets and tunnels the traffics towards mobile nodes care of address [3].

In MIPv6, corresponding node (CN) can dynamically learn the mobile nodes CoA and store it to its cache locally. When a CN want to send a packet to the mobile node, it checks the cache for an entry. If the address is found, it directly sends the packet to the mobile node eliminating the triangular routing.

In MIPv6, the mobile node also keep track of CN to whom its communicating, so when it changes its point of attachment and get new IP address, it sends BU to the HA also to the CNs [3]. If no cache entry is found in the correspondent node, CN send the packet normally through mobile home agent [3]. Routing scenario for MIPv6 is shown in Figure2.

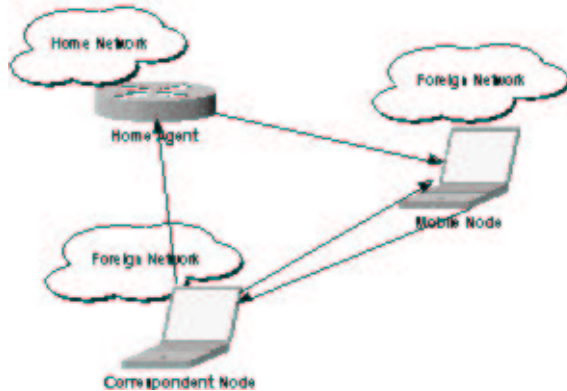


Figure 2: Routing in MIPv6 [1].

2.3.2 Security

In the MIPv6 protocol, the security features are integrated and provided as an extension to header. Information that is sent between mobile node and home agents is protected by IPsec AH and ESP protocols. IP security is applied to the binding updates and acknowledgement [12].

MIPv6 eliminates the reverse tunneling. In MIPv6, MN uses home address in a packet with Home address destination option. MN uses its care-of-address as source address in IP header and sends the packet directly to the CN, so it passes through firewall [9].

2.3.3 Summary

MIPv6 provides mobility for IPv6 network with better security and performance. MIPv6 eliminates triangular routing. Route optimization is the part of the protocol. In MIPv6 corresponding node learns mobile node's CoA dynamically and sends the packet directly to mobile node using IPv6 routing header. Binding Updates (BU) and acknowledgement packets are authenticated using IPsec AH and ESP [1]. MIPv6 uses address configuration protocol i.e. neighbor discovery or stateless address auto configuration to acquire CoA, thus FA are not used [3].

3 IKEv2 mobility

Internet Key Exchange (IKE) version 2 is part of IPsec. It is used for authentication, and establishing and maintaining security association (SAs) [6]. IPsec provides network layer security service for each IP datagram. These security services include confidentiality, integrity, access control, and origin authentication [6].

SAs are binding agreement between the two peer entities. When node changes its point of attachment it is assigned

a new IP address, and thus existing SAs becomes invalid and need to be re-established by rekeying. IKEv2 provides framework to securing end to end connection but lacks the address management capability for mobile environment.

To cope with challenge of mobility, SAs must need to be highly configurable. New version of IKEv2 mobility extension will enable entities to keep existing IKE and IPsec SAs without fully rekeying and also authenticating changes by the host [4].

Next in this paper, I will IKEv2 base protocol and its mobility extension.

3.1 IKEv2 Overview

IKEv2 is the key management protocol for negotiating protocols and algorithms to create SAs and generate authentication information [6]. It allows using symmetric and asymmetric cryptographic techniques [6]. Authentication header (AH) and Encapsulated Security Protocol (ESP) can be used as traffic security protocol for establishing SAs [6]. SAs are uniquely identified by Security Parameter Index SPI, destination IP, and an identifier for traffic security protocol. Security Policy Database (SPD) is used for managing policies in the form of SAs [6].

IKEv2 establishes security association in two phases. Each phase consists of message pairs; messages are in form of request and response, initiator need to re-transmit the request if it did not get response within timeout interval [6].

Phase 1 negotiation is mandatory to create SAs, it consist of four messages, which are in form of two pairs. First pair of message is

```
IKE_SA_INIT ->
<- IKE_SA_INIT
```

Using these messages, peer entities negotiate cryptographic algorithms, send nonces, and make Diffie Hellman Exchange. Results is creation of IKE SA that is secure but not authenticated [6].

Second pair of message is

```
IKE_AUTH ->
<- IKE_AUTH
```

Using these messages peer entities authenticate previously exchanged messages, exchange identities and certificates, and establishes a CHILD SA. Authentication method can be based on pre-shared keys or using of signature algorithm [?]ref6).

Phase 2 negotiation is optional. It is used to create additional CHILD SA, and it consist single pair of message that can be initiated by either side.

```
CREATE_CHILD_SA ->
<- CREATE_CHILD_SA
```

This exchange create child SA i.e. IPSEC SA. It is used when one SA already exists, and there is change in security policy or SA expiration. This exchange is cryptographically protected as it is initiated after first negotiation [6].

IKEv2 defines INFORMTIONAL message for sending control information.

INFORMATIONAL —>
 <— INFORMATIONAL

It is used for sending the control information about SAs when some error occurs or there is change in configuration. Also, it is used to notify half open connection. These messages are sent after initial exchange, and thus they are protected with negotiated keys [6].

3.2 Mobility extension to IKEv2

IKEv2 mobility extension is being designed by MOBIKE working group within IETF to support mobility features for IKEv2 [?].

IKEv2 provides security features but lacks the support for efficient mobility. When mobile node is roaming and IP address changes, exiting SAs becomes invalid. One possible solution is rekeying of all IPsec and IKE SAs.

To provide seamless mobility in most of cases, it is impractical to use an option of rekeying, as the node might be too slow to rekey the SAs or it might require user interaction [13]. Mobility supports needs updating IKEv2 SA and IPsec SA end points without rekeying, and to authenticate those changes [13].

IKEv2 mobility and multi-homing protocol (MOBIKE) [13] defines mobility support for IKEv2. It uses IKEv2 notify payload to send address updates, and to detect dead-peer for return routability check. Notify messages are separately defined for IPv4 and IPv6.

When the addresses are changed, IKE SAs are updated with new address, and IPsec SAs are created using IKE SAs updates [14].

MOBIKE protocol also defines DISCONNECT_NOTIFY message that is used to inform the other nodes for how long the peer assumes to be disconnected. The other node might allow disconnection or do not allow and send delete notification for IKE SA [13].

3.3 Summary

IKEv2 provides end to end secure connection by establishing SAs, which are bindings between the entities. It lacks the address management support for mobile nodes. That gap is being filled by MOBIKE protocol that provides mobility extension to basic IKEv2 protocol and allows to configure and to authenticate SAs without re-keying.

4 Comparison

MIPv4 and MIPv6 have similar mobility concepts. There are implementation changes that affect the performance and security factors. In mobile IPv6, security and mobility features are integrated where as in IPv4 mobility is implemented as an extension to the protocol. This might cause the scalability problem in MIPv4, as there might be some nodes that may not support mobility.

MIPv6 has exhaustive pool of routable address space and thus it eliminates the need of NAT which brings performance and security issues [3].

MIPv6 eliminates need of triangular routing and thus increases the performance and eliminates chance of single point of failure. MIPv6 eliminates need of FA, the CoA generated by stateless or statefull auto configuration [9].

MIPv6 provides better performance, scalability, and security features. IKEv2 can be used with both MIPv4 and MIPv6 to provide strong cryptographic security services. It negotiates security services and authenticates peers by establishing SAs. IKEv2 mobility extension can be used to manage SAs effectively.

5 Conclusion

Mobility does not work without security. Mobile IP defines security features but thinking about the security of mobile IP itself does not consider all aspects. Connections from one mobile node to another node must be made secure. IKEv2 provides security services by establishing SAs that includes connectionless integrity, data origin authentication, confidentiality, and anti-replay service. IKEv2 lacks address management capability for mobile environment. Mobility extension to IKEv2 protocol is being developed by MOBIKE working group within IETF, and it provides the lacking mobility support to IKE.

MIPv6 and IKEv2 mobility extension provides seamless mobility solution with security features that fits well for mobile environment.

References

- [1] Alan Halachimi, Eric Smiley. IP Mobility: An Investigative Comparison Between IPv4 and IPv6. Duke University, Spring 2002. www.disp.duke.edu/esmiley/cps214mobilityfinal.doc
- [2] Charles Perkins. IP Mobility Support for IPv4. RFC 3344, IETF Network Working Group, August 2002. <http://www.ietf.org/rfc/rfc3344.txt>
- [3] D. Johnson, C. Perkins, J. Arkko. IP Mobility Support for IPv6. Internet draft, version 21, IETF Mobile IP Working Group, February 2003. <http://www.ietf.org/internetdrafts/draft-ietf-mobileip-ipv6-21.txt>
- [4] Charles Perkins, David B. Johnson. Route Optimization in Mobile IP. Internet draft, version 11, IETF Mobile IP Working Group, September 2001. <http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-mobileip-optim-11.txt>
- [5] C Perkins. IP Encapsulation within IP IETF's RFC 2003, October 1996 <http://www.ietf.org/rfc/rfc2003.txt>
- [6] Charlie Kaufman, Editor Internet Key Exchange (IKEv2) Protocol IETF Internet Draft Published on March 22, 2004 expires on September 2004 <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-13.txt>

- [7] Francis Dupont. Address Management for IKE version 2 IETF Internet Draft February 2003. <http://www.ietf.org/internet-drafts/draft-dupont-ikev2-addrmgmt-04.txt>
- [8] G. Montenegro : Reverse Tunneling for Mobile IP revised RFC 2003: Netowrk working group. Jan 2001 <http://rfc.sunsite.dk/rfc/rfc3024.html>
- [9] John W. Mark, Weihua Zhuang: Wireless Communication and Networking. Center of wireless communication Department of Electrical and computer engineering. University of Waterloo Canada Book: Published by Prentice Hall, 2003
- [10] Jochen Schiller: Mobile Communication 2nd Edition. Book published by Addison-Wesley, 2003.
- [11] R. Droms. Dynamic Host Configuration Protocol. RFC 1541, IETF Dynamic Host Configuration Working Group, March 1997. <http://www.ietf.org/rfc/rfc1541.txt>
- [12] Salem itani: Use of IPsec in Mobile IP Term Paper. The American university of Beirut, MAY 21, 2001 http://ganges.cs.tcd.ie/htewari/papers/ipsec_itani.pdf
- [13] T. Kivinen. Design of the MOBIKE protocol IETF Internet Draft Published on February 24, 2004 expires August 24, 2004 <http://www.ietf.org/internet-drafts/draft-kivinen-mobike-design-00.txt>
- [14] T. Kivinen MOBIKE protocol IETF Internet Draft Published on February 24, 2004 expires August 24, 2004 <http://www.ietf.org/internet-drafts/draft-kivinen-mobike-protocol-00.txt>