Chapter 3
Mobile IPv6:
Mobility Management and Security Aspects

Tayo Arulogun
Ladoke Akintola University of Technology, Nigeria

Ahmad AlSa'deh
University of Potsdam, Germany

Christoph Meinel
University of Potsdam, Germany

ABSTRACT

Mobile Internet Protocol (MIP) enables a mobile node to be recognized via a single IP address while the node moves between different networks. MIP attains the connectivity to nodes everywhere without user intervention. One general improvement in Mobile IPv6 (MIPv6) compared to MIPv4 is the enhanced security. However, there are areas still susceptible to various kinds of attacks. Security approaches for the MIPv6 are still in progress and there are few unsolved concerns and problems. This chapter focuses on MIPv6 security considerations, potential threats, and possible defense mechanisms. The authors discuss and analyze in detail the MIPv6 mobility management and security approaches with respect to the efficiency and complexity and bring forward some constructive recommendations.

INTRODUCTION

Mobile devices will undoubtedly dominate the population of the future Internet due to reduced cost, enhanced portability, increased capabilities, pervasive computing, etc. This dominance of mobile devices has made researches in mobility and security of IPv6 to be a hot area.

MIPv6 allows Mobile Nodes (MN) to move within the Internet while maintaining reachability without disruption to active sessions, using a permanent Home Address (HoA). MIPv6 was designed to serve as the basic mobility management method in the IP-based wireless networks (Perkins, Johnson, & Arkko, 2011) but some shortcomings, such as prolonged handover latency

DOI: 10.4018/978-1-4666-4514-1.ch003

and security vulnerabilities which reduce the quality of users experience and trust. Research in MIPv6 is very active due to these shortcomings and more importantly due to the current Internet architecture being insecure and originally designed to be relatively static.

The theme of this chapter is to bring to focus the current and anticipated positions of security solutions in MIPv6 and to project what can be done further to enhance the security in this important domain. Through this chapter, we set the following objectives to be achieved: (1) to identify and analyze the anatomy of MIPv6 protocol and its mode of operations, (2) to review with purpose to bring out security designs and implementations in MIPv6, and (3) to gather and bring to the focus of the readers new suggestions or modifications to MIPv6. We conclude with the summary and findings presented in the chapter.

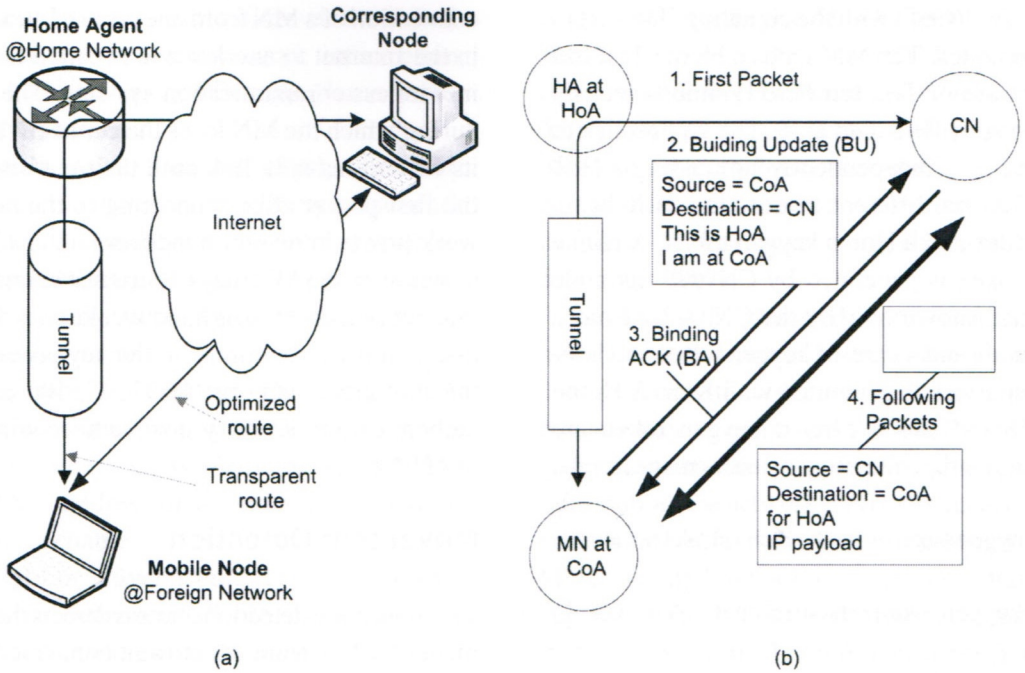
MIPV6 DESIGN

MIPv6 is network-layer mobility protocol-based on IPv6 and standardized by the Internet Engineering Task Force (IETF) via the Request for Comments (RFC) number 6275. Its design was based on the MIPv4 and offers more enhancements as summarized in (Perkins et al., 2011). One of the main differences between MIPv4 and MIPv6 is that, in the latter, MN can perform mobility signaling directly with mobile and non-mobile Correspondent Nodes (CN) (Aura & Roe, 2006). The architecture of MIPv6, Figure 1(a), allows MN to move within the Internet while maintaining reachability without noticeable disruption to active sessions, using a permanent Home Address (HoA) and Care of Address (CoA) for communication with a CN. MIPv6 operates using multiple IPv6 extension headers: the *Mobility Option Header*, the *Destination Option Header*, the *Type 2 Routing Header (RH2)* and Internet Control Message Protocol for IPv6 (ICMPv6) messages for signaling. These headers are used to send packets to and from the MN at its CoA, to CN as if HoA is the source and the destination of these packets respectively. When a MN moves away from its home location to a foreign network, it registers with its HA. To register, the MN sends a packet from its CoA to the HA with the *Destination Option Header* containing the HoA of the MN and a *Mobility Option Header* with a *Type 5 Binding Update (BU)* message. HA confirms this BU by sending a packet to the CoA of the MN that contains an *RH2* that lists the HoA of the MN and contains a *Mobility Option Header* with a *Type 6 Binding Acknowledgment* (BA) message. The MIPv6 mobility can be blue printed via *Transparent* mode or *Route Optimization* (RO) mode as shown in Figure 1(a).

In *Transparent* mode, HA is a router at the home network, acts as the MN's trusted agent and link to the CoA. The HA intercepts packets sent by CN to the HoA and forwards them to the CoA over IPv6 tunnel. When the mobile wants to send packets to CN, it sends them to the HA over the reverse tunnel. The HA decapsulates the packets and forwards them to the CN. When MN moves to a new location, it tells HA its new CoA by sending a BU message. The BU message causes the HA to update the IP-in-IP tunnel in such a way that the tunneled packets are routed to and from the new CoA. The binding update and the subsequent BA are authenticated using a preconfigured IP security (IPsec) security association between the MN and the HA.

In Figure 1(b), RO uses the BU and BA messages. When MN changes its current address, it sends BUs to its CN to notify about its new location. The BU contains the MN's HoA and CoA. CN acknowledges the BU with a BA and stores the location information in the binding cache, which is the routing table that describes how packets destined to HoA should be sent to the CoA. RO protocol eliminates the triangle routing between the MN, HA and the CN that is inherent in the transparent route mode. This enables a more efficient routing of data to and from the MN and

Figure 1. MIPv6 architecture: (a) mobility route, (b) route optimization (Aura & Roe, 2006)



the removal of possible congestion at the home network because MN may communicate with several CN.

Unauthorized binding update protocol implemented as described in RO would create BU spoofing, security vulnerability that could lead to session hijacking, Denial of Service (DoS) and packet flooding attacks (Bombing Attack). Unauthorized location information updates make it possible for an attacker to steal address to deceive CN about the MN's location and, thus, redirect packets intended for MN to an erroneous destination. The simple and unauthorized BU procedure was based on the need to make MIPv6 simpler, efficient and transparent to higher level protocols. The risk of this vulnerability is reduced with the Stateless Address Auto-configuration (Thomson, Narten, & Jinmei, 2007) based on Privacy Extension (Narten, Draves, & Krishnan, 2007) or Cryptographically Generated Address (CGA) (Aura, 2005) because the attacker needs to know both MN and CN IP addresses. Moreover RO is optional and can be disabled by either the MN or the CN.

The Return-Routability protocol (RR) was proposed to secure binding updates from MNs to CNs.

The Return-Routability (RR) Protocol

Return-Routability (RR) protocol was design and standardized to authorize a BU for RO. RR protocol enables the CN to verify that the MN is indeed reachable at its claimed CoA, as well as at its HoA (Perkins et al., 2011). Successful usage of RR implies that there is indeed a node at each of the claimed addresses and CN can accept BU from MN and direct MN's data traffic to its claimed CoA. This is done by testing whether packets addressed to the two claimed addresses are routed to the MN. The MN can pass the test only if it is able to supply proof that it received certain data sent by CN to the claimed addresses. These data from CN are combined by the MN into a binding management key (K_{bm}) (Perkins et al., 2011).

RR procedure consists of Home Test (HoT) and Care-of Test (CoT) with the signaling flows from the three nodes. The MN sends a Home Test Init (HoTI), Care-of Test Init (CoTI) simultaneously to CN to start HoT, and CoT. The CN replies to both messages independently by sending a HoT and a CoT via different routes. The HoT has a nonce index and a Home keygen token. A Home keygen token is generated by CN with its node key (Kcn), known only by the CN. A CoT has a nonce index and a care-of keygen token. A Care-of keygen token is generated with Kcn. A Home keygen token and a care-of keygen token are calculated by the following formulas respectively.

Home keygen token= hash (Kcn | HoA | nonce | 0)

Care-of keygen token = hash (Kcn | CoA | nonce | 1)

The Home keygen token received by the MN is used for proving that the MN is indeed at the HoA. And Care-of keygen token received by the MN is used for proving that the MN is indeed at the CoA. Each nonce index allows CN to easily find the nonce which was used during generation of keygen token. The MN which has a Home keygen token and a Care-of keygen token can create a binding management key (K_{bm}) to substantiate that the MN stays at the HoA and CoA concurrently.

K_{bm} = hash (Home keygen token | Care-of keygen token)

The tunnel between the MN and the HA is protected by IPsec's Encapsulated Security Payload (ESP), which makes it impossible for the outsiders to learn the contents of a HoT. Therefore RR is secure from malicious attacks. The RR procedure was designed with the objective to provide a level of security that compares to that of today's non-mobile Internet (Nikander, Arkko, Aura, Montenegro, & Nordmark, 2005).

Prior to MN receiving the first packet from CN at CoA in the MIPv6 mobility blueprint, two other processes must precede the BU process namely Movement Detection (MD); and Address Configuration (AC). The process of transferring the connection of a MN from one point of attachment in the Internet to another one is called handover in wireless communication systems. The period during which the MN loses the connectivity with its current network link until the time it receives the first packet after connecting to the new network link is known as handover latency. During a handover, the MN may experience connectivity interruption due to long handover latency. Further discussion will continue on the key processes in the mobility blueprint: MD, AC, BU and BU authentication, security goals and requirements of MIPv6 design.

Movement Detection

The movement detection process detects the movement of a MN from the current connected router and eventual connection to an appropriate new access router via router discovery process. Router discovery process is the method that allows MN to automatically discover the identity of local routers on the current link, and learn important details of the routers. MIPv6 uses Neighbor Discovery for IPv6 (Narten, Nordmark, Simpson, & Soliman, 2007) for router discovery process as specified in (Perkins et al., 2011). IPv6 nodes on the same link can discover each other's presence, determine each other's link-layer addresses, find routers, and maintain reachability information about the paths to active neighbors with Neighbor Discovery for IPv6 specifications.

Neighbor Discovery for IPv6 (Narten et al., 2007) and Stateless Address Auto-Configuration (SLAAC) for IPv6 (Thomson et al., 2007) are collectively called Neighbor Discovery Protocol (NDP). NDP is used for router, address prefix and parameter discoveries, address auto-configuration, address resolution, Duplicate Address Detection (DAD), Neighbor Unreachability Detection (NUD), next-hop determination and redirect. NDP defines the following additional ICMPv6 messages (Conta, Deering, & Gupta, 2006) so as to perform its functionalities:

1. **Router Solicitation (RS), type 133:** RS is sent by IPv6 host to discover the default router and to learn network information, such as prefixes and Domain Name Server (DNS) address.
2. **Router Advertisement (RA), type 134:** The router that receives a RS message sends back a RA message (solicited router advertisement). Also, RA is sent by IPv6 routers periodically (unsolicited multicast router advertisements).
3. **Neighbor Solicitation (NS), type 135:** NS is used to resolve the neighbor nodes IPv6 address to its Media Access Control (MAC) address or to verify if the node is still reachable.
4. **Neighbor Advertisement (NA), type 136:** NA is a response to NS. NA message include the MAC address of the node.
5. **Redirect message, type 137:** Used by router to inform other nodes of a better first-hop toward a destination.

Generically, MN movement detection in MIPv6-based mobility uses *Neighbor Unreachability Detection* to detect when the default router is no longer bi-directionally reachable, in which case the mobile node must discover a new default router usually on a new link (Perkins et al., 2011) using RS and RA messages.

Address Configuration

Address Configuration (AC) is the method employed by MN in acquiring a CoA using SLAAC in conjunction with network prefix advertised by the new access router and the confirmation of the CoA uniqueness using DAD procedure. AC also relies on NDP ICMPv6 messages for effective implementation. MIPv6 supports both stateful and stateless address autoconfiguration, such as address configuration with Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (Droms et al., 2003) server and SLAAC mechanisms respectively. With SLAAC of NDP, hosts on a link can automatically configure link-local addresses for themselves. Global network addresses can be obtained by combining the interface identifier part with address prefixes advertised by routers located in the network segment (Thomson, Narten, & Jinmei, 2007).

SLAAC is the preferred address configuration method for MN because of its lightweight address configuration that supports plug-and-play IP connectivity as compared to DHCPv6. SLAAC generates the address by combining two pieces of information: the network prefix, obtained from the routers located in the network segment to which MN is attached and link-local address obtained by appending an interface identifier to the link-local prefix (FE80:: /10). The interface identifier could be obtained from the MN's network interface. Also, the interface identifier can be generated by Privacy Extension (Narten, Draves & Krishnan, 2007) mechanism to make it more difficult for eavesdroppers and other information collectors or by using Cryptographically Generated Addresses (CGA) (Aura, 2005) to make it more secure. Using CGA ensures IP address authentication for MN. Before assigning the new link-local address to its interface, MN must verify that the address is unique. This is accomplished by sending an NS message targeted to the new address. If reply is received then the address is a duplicate and the process is terminated after three failed attempts. When no reply is received to the NS message, the MN now has a valid CoA for mobility activities. The likelihood of this process being terminated due to failed DAD procedure is very small unless the MN is under attack from malicious node. This attack is basic to MIPv6 as inherited from IPv6 and SEcure Neighbor Discovery (SEND) (Arkko, Kempf, Zill, & Nikander, 2005) was proposed to counteract the attack.

Security Goal and Requirements of MIPv6 Design

The security goal in designing MIPv6 was simply to make it, at least, as secure as IPv6 with minimal signaling among the communicating nodes (Aura & Roe, 2006). To achieve this goal, the following design and security assumptions were made by MIPv6 working group for the architecture and security design of MIPv6.

MIPv6 Design Assumptions

The MIPv6 design relies heavily on the following assumptions:

1. The routing prefixes available to a MN are determined by its current location, and therefore the MN must change its IP address as it moves.
2. The routing infrastructures deliver packets to their intended destinations as identified by the destination address.
3. The design of MIPv6 is to follow the end-to-end principle, to duly notice the differences in trust relationships between the nodes, and not to make the security any worse than IPv4 is today.
4. The end-to-end principle is applied by restricting mobility related state primarily to the HA, and CN.

MIPv6 Security Assumptions

The following MIPv6 security assumptions were made:

1. Pre-established security association between a MN and HA: MN and HA know each other, and can thus have a pre-established strong security association to reliably authenticate exchanged messages between them using IPsec's ESP to set up a secure tunnel between MN and HA.
2. No pre-established security association between MN and a random CN: It is expected that MIPv6 will be used on a global basis between nodes belonging to different administrative domains, hence building a global Public Key Infrastructure (PKI) to authenticate any MN and random CN would be very complex and demanding task. It may be possible to have global PKI or its semblance in the nearest future.

With these goals and assumptions, infrastructure-less security protocols, such as RR and SEND were specified and further standardized for MIPv6 (Perkins et al., 2011) along with traditional security protocol such as IPsec (Arkko, Devarapall, & Dupont, 2004; Devarapalli & Dupont, 2007) and Internet Key Exchange (IKE) (Kaufman, Hoffman, Nir, & Eronen, 2010). These security protocols are discussed under Security threats and counteract proposals of this chapter. The stated goal of MIPv6 using the design and security assumptions were achieved with the final MIPv6 standard specification. However, standard MIPv6 still surfer from some mobility and security issues, such as long handover latency in homogeneous and heterogeneous networks, DoS, Address stealing, etc. These issues are not only peculiar to MIPv6 alone but to IPv6 and MIPv4.

There have been various suggestions, and some IETF standardized alternative mobility management solutions engineered for MIPv6 with couple of security management protocols and algorithms. We will discuss it in more details in the next section.

MIPV6 MOBILITY MANAGEMENTS AND SECURITY ISSUES

A number of extensions and security suggestions for enhancing the mobility management and security of MIPv6 are discussed in the following sections.

MIPv6 Mobility Management

Mobility management is the planning and control of transparent MN movement from its home network to foreign networks with the aim of optimizing the handover latencies by reducing signaling overhead, reducing packet loss, and reducing location updates, for efficient and effectiveness IP-based communication with any CN in the Internet. Maintaining connections during movement is the basic necessity that has given rise to MIPv6. MIPv6 provides the optimal packet routing but requires high signaling cost and long handover latency. Due to this inadequacy, IETF currently standardized four enhancements to MIPv6 namely: Hierarchical MIPv6 (HMIPv6) (Soliman, Castelluccia, ElMalki & Bellier, 2008), Fast Handovers for MIPv6 (FMIPv6) (Koodli, 2009), Proxy MIPv6 (PMIPv6) (Gundavelli, Leung, Devarapalli, Chowdhury, & Patil, 2008), and Proxy-Based Fast Handovers for Mobile IPv6 (PFMIPv6) (Yokota, Chowdhury, Koodli, Pati, & Xia, 2010).

MIPv6, HMIPv6 and FMIPv6 are host-based mobility management protocols while PMIPv6 and PFMIPv6 are network-based mobility management protocol. Host-based mobility management rely mainly on MN for the mobility related signaling while Network-based mobility management do not require MN's participation in any mobility-related signaling.

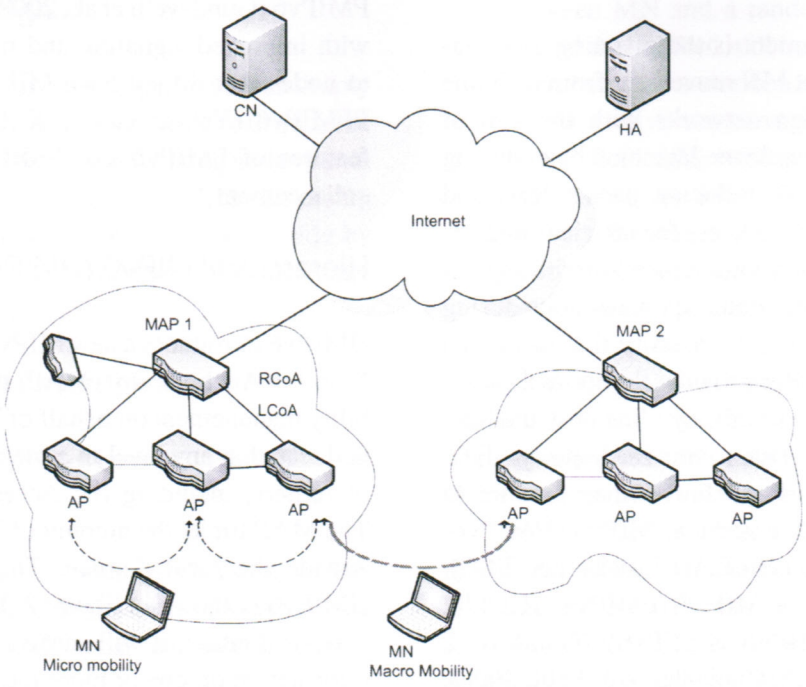
HMIPv6 (Soliman et al., 2008) allows MN to signal its local handovers to a Mobility Anchor Point (MAP) located somewhere nearby the MN. In this way, HMIPv6 avoids high latency signaling to the MN's HA and CN. FMIPv6 (Koodli, 2009) aims at reducing handover latencies by proactively executing the configuration of the MN interface for the link to the target access router while the MN is still connected to the link on the current serving access router. FMIPv6 also exploit packets forwarding by the serving access router to the target access router during the critical phase of the handover and buffering of these packets at the target access router until the MN attaches to it. PMIPv6 (Gundavelli et al., 2008) extends MIPv6 with improved signaling and mobility supports to nodes that do not have MIPv6 functionality. PFMIPv6 (Yokota et al., 2010) combines the features of FMIPv6 and PMIPv6 for mobility enhancement.

Hierarchical MIPv6 (HMIPv6)

HMIPv6 introduces a new MIPv6 node known as Mobility Anchor Point (MAP) that provides mobility management on behalf of MN. MAP could be located at any level in a hierarchical network of routers, including the Access Router (AR). The MAP limits the amount of MIPv6 signaling outside the local domain. The architecture of HMIPv6 is shown in Figure 2. When MN enters a MAP domain, it will receive RAs containing information on one or more local MAPs.

The On-Link CoA (LCoA), in Figure 2, is configured on the MN's interface based on the prefix advertised by the current link default router. This is equivalent to the CoA of MIPv6, and Regional CoA (RCoA) is analogous to the HoA in the case of MIPv6. A local BU is sent by the MN to the MAP to create a mapping between an address on the MAP's subnet called RCoA and LCoA (Soliman et al., 2008). This is because the RCoA remains the same when a MN moves within the domain of the MAP, but the LCoA changes and hence a BU is required to be sent to MAP. HA and CN only receives BU when MN moves to another MAP domain hence, MN creates a new RCoA and new LCoA binding in the new MAP domain. Acting as a local HA, the MAP will receive all packets on behalf of the MN it is serving and will encapsulate and forward them directly to the MN's current address. If MN changes its current address within a local MAP domain (LCoA), it only needs to register the new address with the MAP. Hence, only the RCoA needs to be registered with correspondent nodes and the HA. The RCoA does not change as long

Figure 2. HMIPv6 architecture



as the MN moves within a MAP domain. In HMIPv6, MN hides its LCoA from its CN and its HA by using its RCoA in the source field of the packets that it sends. As a result, the location tracking of MN by its CN, HA or adversaries is difficult because only RCoA is known and not its LCoA. The rest of the mobility procedure remains the same as in MIPv6 with RO being utilized.

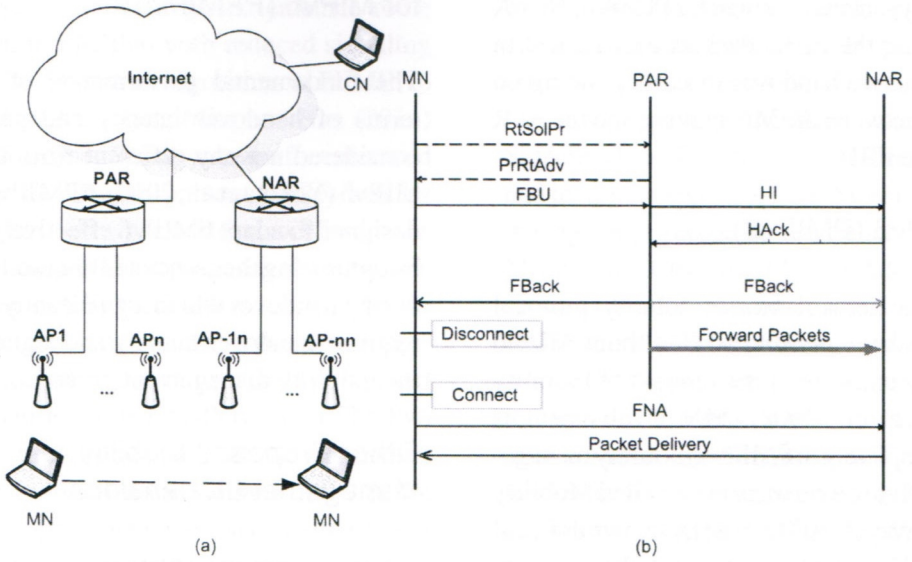
Fast Handover for MIPv6 (FMIPv6)

Fast handover mobility management for Mobile IPv6 was proposed to reduce the handover latency by initiating and executing some of the time-consuming handover processes such as Router Discovery, Address Configuration, and Duplicate Address Detection while MN is still present on the current link with the help of timely generated link Layer-trigger (Koodli, 2009). The architecture of FMIPv6 is shown in Figure 3(a). A MN in its home network has address know as Previous CoA (PCoA) and is connected to the access router known as the Previous Access Router (PAR). On moving to the new network, it connects with a New Access Router (NAR) and acquires a New CoA (NCoA) and packet destined to MN from CN during the movement are tunneled by PAR to NAR. FMIPv6 uses Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) for fast handover as shown in Figure 3(b) to obtain details of suitable NAR. There are three modes of initiating FMIPv6 namely; predictive, reactive and network modes.

Predictive Handovers

In predictive mode, the MN anticipates a change of network link and initiates handover by sending an RtSolPr message to the PAR to indicate that it wants to perform a fast handover. PAR sends this message to NAR, if it has not the details of NAR. The PAR replies MN with a PrRtAdv that provides the MN with tuple about the new link for accelerated movement detection. The received

Figure 3. FMIPv6 structure and operation sequence



tuple (access point ID (AP-ID), AR-Info) contains an AR's layer two (L2) and IP addresses, and the prefix valid on the interface to which the Access Point (identified by AP-ID) is attached. This is the tuple that the MN would receive when it moves to a new access point with AP-ID. MN also forms an NCoA while it is still connected to PAR. MN sends a Fast Binding Update (FBU) to the PAR using this NCoA and receives a Fast Binding Acknowledgement (FBack) to indicate success. A tunnel between the PCoA and the NCoA is created when PAR sends a Handover Initiation (HI) message to NAR and it replies with a Handover Acknowledgement (HAck). After the tunneling phase is over, packet forwarding starts. PAR begins tunneling packets arriving for PCoA to NCoA. The tunnel remains active until the MN completes the Binding Update with its CN. Forwarding support for PCoA is provided through a reverse tunnel between the MN and the PAR since CN's have to be updated with a Binding Cache entry that has the NCoA. MN sends a Fast Neighbor Advertisement (FNA), to start the packet flow from NAR to itself.

Network Initiated Handover

If the PAR detects low link quality on MN link or topologically better NAR or believe that MN should move to better link served by another NAR, it will send an unsolicited PrRtAdv to the MN containing the information with which the MN can connect to the new network. Apart from the absence of the initial RtSolPr message, the message exchanges are the same as in Figure 3(b). MN must only be able to connect to the network specified in the PrRtAdv message by configuring a CoA for itself and issuing a FBU to the PAR.

Reactive Handover

Reactive handover mode is used when a node suddenly loses its connection with its current PAR or current Access Point (AP) during the fast handover procedure. Therefore, MN does not get an FBack for the FBU from the PAR, or the MN could not send the FBU to the PAR before the movement. Once the MN is in NAR's link, a FBU is sent and is usually encapsulated in the FNA. The NAR

forwards the FBU to the PAR and the PAR starts the tunneling packets destined for PCoA to NCoA after receiving the FBU. Packets may be lost in FMIPv6 Reactive handover mode depending on the interval between the MN moving and the PAR receiving the FBU.

Proxy MIPv6 (PMIPv6)

PMIPv6 is a network-based mobility protocol that aims to keep MN with or without MIPv6 functionality unaware of the process of mobility (Gundavelli et al., 2008). MN involvement is removed completely in PMIPv6 mobility management by involving a network node called Mobility Access Gateway (MAG) and a HA known as Local Mobility Anchor (LMA) in the signaling process creating a Proxy Mobile IPv6 Domain (Gundavelli et al., 2008). LMA in PMIPv6 domain serves as an anchor point for the MN possible home addresses and manages MN's binding state. MAG is an access router that tracks the MN's movement to and from the access link and informs the LMA regarding this movement. LMA has an address configured on its interface known as the LMA Address (LMAA). It is the endpoint of the bi-directional tunnel between it and the MAG. Proxy CoA (PCoA) forms the other end of this bi-directional tunnel. This address is configured on the outer interface of the MAG and this serves as the CoA of the MN and is used in the binding cache entry for the MN. A prefix advertised by the MAG in the PMIPv6 domain for MN is known as the Mobile Node-Home Network Prefix (MN-HNP). The MN always configures its address from this prefix that is anchored at the LMA. The address used by the MN for communication is the Mobile Node Home Address (MN-HoA). The LMA is aware of the MN-HNP and not the exact MN-HoA that is configured on the MN. The MN can use this address at all attachment points in the PMIPv6 domain (Gundavelli et al., 2008). PMIPv6 stands a good chance as the mobility management protocol of choice for use in next generation IP-based heterogeneous networks.

Proxy-Based Fast-Handovers for MIPv6 (PFMIPv6)

The fundamental performance of PMIPv6 in terms of handover latency and packet loss is considered not any different from that of basic MIPv6 (Yokota et al., 2010). PFMIPv6 protocol is designed to adapt FMIPv6 effectively in PMIPv6 by optimizing the associated data and control flow during handover which significantly improve the required handover latency and signaling cost of the mobility management protocol.

Other Proposed Mobility Management Extensions

While the experimentation and standardization of the four Mobility Management Extensions; HMIPv6, FMIPv6, PMIPv6, and PFMIPv6 were ongoing there, were a number of proposals on the extension of MIPv6. Most of these proposals suggest enhancements to optimize the operations and security while others try to amalgamate some of these mobility management protocols.

Jung, Soliman, Koh and Lee (2005), proposed Fast Handover for Hierarchical MIPv6 (F-HMIPv6) that optimally combines HMIPv6 and FMIPv6 using the structures of HMIPv6 and the FMIPv6 signaling messages for handover support with the aim of shortening the handover latency in ARs within the same MAP domain. Yoo, Tolentino, Park, Chang and Kim (2009), proposed a scheme for Efficient Fast Hierarchical Mobile IPv6 (ESFMHIPv6) to overcome ineffectiveness of the simple combination of FMIPv6 and HMIPv6 using dual buffer for storing beacon message and control factor for assigning a beacon message time interval to supporting a fast handover effectively. Ryu and Mun (2005) proposed a Tentative and Early Binding Update (TEBU) scheme for FMIPv6 that ensures that NCoA is registered to HA before layer 2 trigger signal with possible 21% lower handover latency than FMIPv6. Ryu and Mun (2007) further proposed an enhancement to TEBU scheme to include implementation of RR

procedure before layer 2 trigger signal. Na, Ryu, Lee, and Mun (2010), proposed enhance route optimization in PMIPv6 with reduced signaling cost using the prediction algorithm in PFMIPv6 protocol. Choi, Kim, Lee, Min, and Han (2011) proposed a Smart Buffering scheme for enhanced handover in PMIPv6 to prevent packet loss by proactively buffering packets that will be lost in current serving MAG. It proposes network-side handover prediction mechanism, and an MAG discovery mechanism to achieve the buffering.

Shih, Kuo, Huang, and Chen (2011) proposed the combination of F-HMIPv6 and PFMIPv6 protocols to provide seamless handover scheme for PMIPv6 in hierarchical architecture with the introduction of two new messages called Local Proxy Binding Update and Local Proxy Binding Acknowledge where Local Proxy Binding is sent to the MAP rather than the HA during handover. Simulation results showed that this proposed scheme avoided packet loss during a handover and ensure ordered packet sequence while the handover latency is effectively reduced by up to 23% and 22% compared with PMIPv6 and FHMIPv6 in predictive and reactive modes respectively. Most of the above described proposals introduce more signaling load, or security threats or implementation and interoperability challenges.

A summary of six MIPv6-based Mobility Management extensions based on analysis of various mobility schemes is shown in Table 1. It is based on Key infrastructure used, Optimization for movement detection/address configuration, Signaling load, Packet loss, Handover performance and location privacy of MN. Most of the mobility management protocols are either optimized for Movement Detection (MD) or Address Configuration (AC) and in some cases such as MIPv6, HMIPv6 and FHMIPv6 that are optimized for both AC and MD operation as shown in Table 1 so as to improve the overall handover performance. In terms of total signaling load, MIPv6 still has the minimum mobility signaling load between MN, key infrastructure such as HA, MAP, LMA, MAG, etc; and CN when compared to other protocols. Nevertheless, MIPv6 with its very good signaling load comes at high latency that increases the signaling cost resulting in high packet loss as compared to other protocols.

Other Special Mobility Management Protocol

There are some special mobility management protocols, such as Network Mobility (NEMO) Basic Support Protocol and Mobile Ad-Hoc Network

Table 1. Summary of mobility management extensions

Mobility Protocol	Class	Address of MN	Key Infrastructure	Optimized for MD/AC	Signaling Load	Reduced Packet Loss	Overall Handover Latency
MIPv6	Host	CoA; HoA	HA	MD; AC	Very Good	Poor	Fair
H MIPv6	Host	LCoA	HA; MAP	MD; AC	Good+	Good	Good
F MIPv6	Host	CoA	HA; AR	AC	Fair	Very good*	Good
P MIPv6	Network	HoA	LMA; MAG	AC	Good	Fair	Fair+
PFMIPv6	Network	LCoA	HA; AR	AC	Good	Very good	Very good
F-HMIPv6**	Host	LCoA	HA; AR; MAP	MD; AC	Good	Good	Very good

* Packet loss will be higher in reactive mode.** FHMIPv6 is IETF draft,+ Slight improvement

(MANET). NEMO basic support is described briefly because of its importance and its similarity to MIPv6 mobility management.

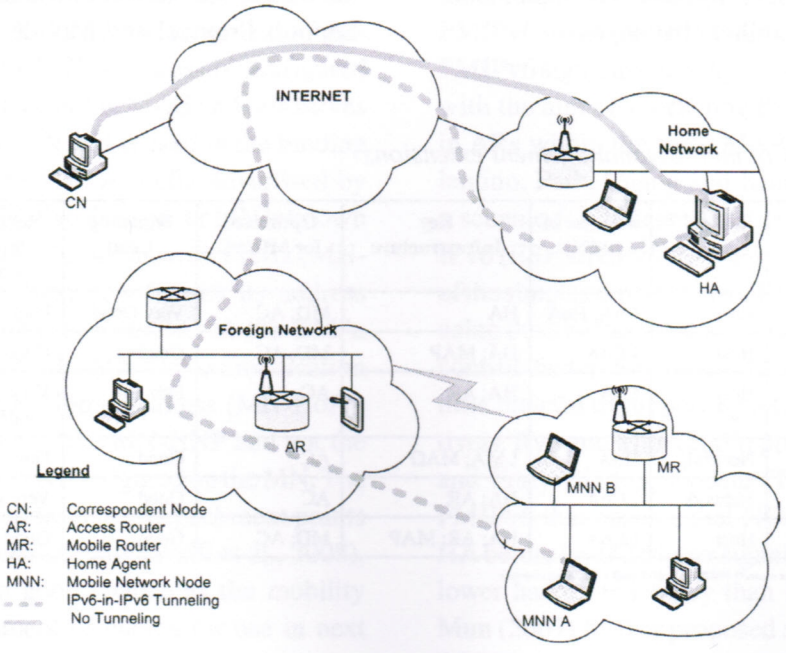
Network Mobility (NEMO) Basic Support Protocol

NEMO basic support is a special extension of MIPv6 with the main goal of supporting mobility of a whole network as against an MN that allows session continuity for every node in the Mobile Network as the network moves. It enables Mobile Networks to attach to different points in the Internet with the reachability of every node in the Mobile Network. The nodes can be static or mobile node and are called Mobile Network Node (MNN). The Mobile Router (MR), which connects the network to the Internet, runs the NEMO basic support protocol with its Home Agent. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network (Devarapalli, Wakikawa, Petrescu, & Thubert, 2005). NEMO has adopted the methods used for host mobility support in Mobile IP and has extended them in the simplest way possible to achieve its goals (Ernst, 2007). NEMO is designed as in Figure 4 such that each MR has a HA, and use bi-directional tunneling between the MR and HA to preserve session continuity while the MR moves. The MR acquires a CoA at its attachment point much like what is done for mobile hosts. There are NEMO basic supports variants, such as PMIPv6 and MIPv6 based NEMO management.

POTENTIAL SOURCES OF SECURITY CONCERNS IN MIPV6

Security concerns and possible threats are not usually unanticipated in a new protocol design and more particularly in its implementation. There is no exception to MIPv6 with the following five categories of sources of security and privacy concerns; Binding Updates to Home Agents, Binding Updates to Correspondent Nodes, Dynamic Home Agent Address Discovery, Mobile Prefix Discovery, and Payload Packets (Perkins

Figure 4. Architecture of NEMO basic support protocol



et al., 2011). These security issues could lead to security threats, such as connection interception attack, connection redirect attack, replay attack, reflection attack, forced non-optimized routing of packets, ICMPv6 message based attacks, etc. These security issues, threat and mitigation methods are discussed in more details as follows:

1. **Binding Updates to Home Agents:** To prevent an attacker from spoofing the BU from MN to HA, the MN and the HA MUST use an IPsec Security Association (SA) to protect the integrity and authenticity of the Binding Updates and Acknowledgements (Perkins et al., 2011). Both the mobile nodes and the home agents must support the Encapsulating Security Payload (ESP) header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity, and optional anti-replay protection. AH protocol of IPsec is also useful to secure MN-HA route.
2. **Binding Updates to Correspondent Nodes:** The links between CN-MN and CN-HA are vulnerable to attacks, hence the integrity and authenticity of the Binding Update messages to CN needs to be protected by using a keyed-hash algorithm rather than infrastructure based method due to absence of prior mutual relationship of MN to CN unlike as existed between HA to MN. The following are the components of binding update messages to CN that may need protective handling; Node Keys, Nonces, Cookies and Tokens, Cryptographic Functions, Authorizing Binding Management Messages, Updating Node Keys and Nonces, Handling Interruptions to Return Routability.
3. **Dynamic Home Agent Address Discovery:** Dynamic Home Agent Address Discovery (DHAAD), allows a MN to discover the address of a preferred HA on the home link. Dynamic home agent address discovery has been designed for use in deployments where security is not needed (Perkins et al., 2011) because the procedure involves Anycast address and it is not possible to establish IPsec security association with Anycast address. Another possible reason for absence of security in DHAAD is that there is the assumed trust relationship between MN and HA. However, DHAAD could suffer from security threats because the trust relationship may not be there, hence the signaling is neither authenticated nor its integrity protected and prone to attack from malicious host on the home link.
4. **Mobile Prefix Discovery:** The HA can send an unsolicited ICMPv6 prefix reply message to the MN when network renumbering event occurs or the MN send an ICMPv6 prefix solicitation message to the HA for the same event. The reply message contain subnet prefix for the MN home link. An attacker can spoof the unsolicited mobile prefix reply message, causing MN to update its home subnet prefix to that of the attacker. An attacker could also eavesdrop to the ICMPv6 prefix reply message to discover topology of the home network, which could be used for future attacks.
5. **Payload Packets:** Mobile IPv6 introduces the Home Address destination option and a new routing header type 2, and uses tunneling headers in the payload packets. The Home Address destination option could be used to direct response traffic toward a node whose IP address appears in the option. In this case, ingress filtering would not be effective against the fake "return address". The protocol must protect against potential new threats involving the use of these mechanisms in payload packets using Home Address destination option. Payload packets exchanges with MN are also exposed to similar threats as that of regular IPv6 traffic.

MIPv6 Security Threats

The following security threats are possible from the earlier discussed sources of MIPv6 security concerns such as connection interception attack, connection redirect attack, replay attack, reflection attack, forced non-optimized routing of packets, ICMPv6 message attacks.

Connection Interception and Redirect Attack

An attacker could determine the MN's home address through MIPv6 mobile prefix solicitation and reply DHAAD, or through the home address option in payload packets. At some point in an ongoing session between an MN and a CN, the attacker can send a BU to the CN using the acquired HoA and a malicious CoA with purpose of tampering with the CN binding cache. The CN would believe that the MN has moved to a new CoA. CN updates the entry for the MN in its binding cache. The packet stream for the ongoing session from the CN to the MN is now diverted to the specified malicious CoA. This attack is known as Traffic Redirection. If the CoA specified is the address of the attacker, then this attack is known as Traffic Hijacking. It is also possible for the attacker to send a BU to the MN, supposedly from the CN, and hence insert himself as a man in the middle (MitM) for traffic between the two. The attacker in MitM must be located in the same link as the MN or the CN.

Replay Attack

Replay attacks are possible for route optimization as with any signaling protocol. An attacker can record authenticated or non-authenticated Binding Update messages, and resend it when the MN has moved to a different CoA, thereby disrupting the ongoing MN's traffic with CN. The attacker can record BU only if the attacker is on the same link with MN.

Inducing Unnecessary Binding Updates

An attacker can induce the MN to initiate binding update protocols with a large number of CN at the same time. If the correspondent addresses are real addresses of existing IP nodes, then most instances of the binding update protocol might even complete successfully. The entries created in the Binding Cache are correct but useless. In this way, the attacker can induce the MN to execute the binding update protocol unnecessarily, which can drain the mobile's resources, thereby causing DoS. A CN can also be attacked in a similar way by using it as target node. The attacker sends spoofed IP packets to a large number of mobiles, with the target node's address as the source address. These mobiles will initiate the binding update protocol with the target node. Again, most of the binding update protocol executions will complete successfully. By inducing a large number of unnecessary binding updates, the attacker is able to consume the target node's resources (Nikander et al., 2005).

Forced Non-Optimized Routing of Packets

A variant of the Inducing Unnecessary Binding Updates attack is Forced Non-optimized Routing of Packets. The attacker can prevent a CN from using route optimization by filling its Binding Cache with unnecessary entries so that most entries for real mobiles are dropped. Any successful DoS attack against a MN or CN can also prevent the processing of binding updates. The target of this DoS attack may respond by stopping route optimization for all or some communication. Obviously, an attacker can exploit this fallback mechanism and force the target to use the less efficient home agent-based routing. The attacker only needs to mount a noticeable DoS attack against the MN or CN so as to default to non-optimized routing.

Flooding Attack

By sending spoofed binding updates, an attacker could redirect data traffic to an arbitrary IP address. This could be used to overburden an arbitrary Internet address with an excessive volume of packets. The attacker could also target a network by redirecting the data to one or more IP addresses within the network. There are two main variations of flooding: basic flooding and return-to-home flooding. In basic flooding, the attacker starts the download of heavy data stream from CN which is a server, after performing TCP handshake it sends a forge BU involving victim address as CoA. Once the BU is accepted by CN a huge amount of unsolicited data traffic are transmitted to the victim to degrade its performance as well as to waste its bandwidth. Thus while the BU is authenticated, the MN (attacker) is not at the claimed CoA. The attacker also sends spoofed acknowledgement for the ongoing communication to CN to ensure that the data flood to the victim's node continues. In return-to-home flooding, a variation of the basic flooding attack would target the HoA or the home network instead of the CoA or a visited network. The attacker would claim to be MN with the HoA equal to the target address. While claiming to be away from home, the attacker would start downloading a data stream. The attacker would then send a binding update cancellation from the Binding Cache or just allow the cache entry to expire. Either would redirect the data stream to the home network. As when flooding a CoA in basic flooding, the attacker can keep the stream alive and even increase the data rate by spoofing acknowledgements as in basic flooding.

Rogue HA

It is possible for an attacker on the same subnet as the HA of MN to pretend to be the HA while the MN is in foreign network; intercepts the BUs from the MN and its destined traffic which originates from other CNs. Camouflaging the HA's identity can lead to drastic effects, which open the door for various MitM attacks, and DoS attacks with spoofed addresses or Home Agent Address Discovery messages.

Space-Time Shift Attack

This attack is possible in MIPv6, if an attacker can eavesdrop the return routability state of the network at the time when the HoT and CoT messages were sent out, thereby having access to the binding cache entry and K_{bm}. It after that moves to a safer place and starts an attack from there or the attacker waits for a better point in time to start attack.

Security Threats Counteract Proposals

The identified MIPv6 security threats and the possible counteract methods are described in Table 2. Some threats' severity such as traffic redirection, traffic hijacking are classified as moderate because the effect of the threat will affect the target only. If the threat affects the whole network, then it is classified as high severity. A very high threat severity is one that can affect any node in the Internet, open more threats or affects the whole Internet. Some of the counteract methods will not eradicate the threats but will mitigate the effect because the threat is still possible and the threat can reduce performance such as QoS. For example, basic flooding attack is still possible but the attacker is also affected by his attack based on the counteract methods.

A number of security solutions are specified for MIPv6 in RFC6275 (Perkins et al. 2011), RFC4877 (Devarapalli & Dupont, 2007) and RFC3971 (Arkko et al., 2005) for securing MIPv6 signals to make it secure as the regular IPv6 protocol. Perkins et al. (2011) specifies the use of RR procedure for securing BU/BA between MN and CN while (Arkko et al., 2005) specifies SEND for securing address configuration of MN. IPsec with IKEv2 was specified for establishing security association to secure traffics on MN-HA route,

Table 2. MIPv6 security threats and counteracts methods

Threat	Severity	Target	Counteract Methods	Solution Type	Comment
Traffic Redirection	Moderate	MN	Securing ICMPv6 message type 144-147.	Mitigation	
Traffic Hijacking	Moderate	MN; CN	Same as above. Authenticate BU from MN-AH, MN-CN routes.	Eradication on MN-HA route; Mitigation on MN-CN route	
Man-in-the-Middle	High	MN; CN; HA	Same as above. Security Association between MN and HA using IPsec.	Mitigation	DoS is possible
Replay attacks	Moderate	MN; CN	Sequence number for BU freshness, time stamping, Nonces.	Eradication	
Inducing Unnecessary Binding Updates	High	MN; CN	Selective BU processing, disable route optimization	Mitigation	QoS degrades
Forced Non-optimized Routing of Packets	High	MN; CN	Same as above	Mitigation	QoS degrades
Basic Flooding	Very High	Any node in the Internet	Verification of CoA location, TCP reset	Mitigation	Attacker is also affected
Return-to-Home Flooding	Very High	MN at HoA, HA, any home network nodes	Verification of CoA and HoA locations, TCP reset	Mitigation	Attacker is also affected
Rogue HA	Very High	MN, CN	Securing ICMPv6 message with SEND, DNSsec	Mitigation	DoS, MitM
Space-time shift attacks	Moderate	MN, CN	Refreshing CoA registration regularly	Eradication	

HA prefix discovery procedure as described in RFC4877. No security association was specified for DHAAD procedure. CN-MN route was not recommended for IPsec based security because there is presently no way to globally manage the required pre-shared keys in IPsec security association or Public Key Infrastructure (PKI) to validate authenticity of various CNs and MNs. Protection of payload routing mechanism for home address destination option and type 2 routing header against misuse is also important.

Secure Neighbor Discovery (SEND)

Neighbor Discovery Protocol (NDP) (Narten et al., 2007; Thomson et al., 2007) introduces security vulnerabilities in router discovery, prefix discovery, and address auto-configuration mechanisms that could affect the IPv6 network address resolution, Duplicate Address Detection (DAD), Router Advertisement (RA), and address configuration. SEcure Neighbor Discovery (SEND) (Arkko et al., 2005) protocol is a response to security vulnerabilities in NDP; these vulnerabilities are documented inIPv6 Neighbor Discovery (ND) Trust Models and Threats (Nikander, Kempf, & Nordmark, 2004). Proof of address ownership, message protection and router authorization mechanism were the three enhancement features recommended by SEND to secure NDP. To realize these enhancements, SEND comes with four new options and two new ICMPv6 discovery messages. The options are *CGA*, *RSA Signature*, *Timestamp*, and *Nonce* while the ICMPv6 messages are *Certificate Path Solicitation* and *Certificate Path Advertisement* for the router authorization mechanism. The options and the messages are described as follows: