BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN (P): 2348-0513, ISSN (E): 2454-471X,
Vol. 4, Issue 3, Mar 2016, 35-52

PERFORMANCE EVALUATION OF MOBILE INTERNET PROTOCOL VERSION 6

SHERIF KAMEL HUSSEIN

Department of Communications and Electronics, October University for Modern Sciences and Arts [MSA], Giza, Egypt

ABSTRACT

Nowadays a lot of computing devices are available in the market. These devices are supporting wireless and mobile technology. Mobile IPV6 is an enhanced version that was designed to be a natural outgrowth of Mobile IPV4. As reliance on Internet and web-based services increases, so do customer expectations for availability, reliability, and responsiveness of the services, especially in the Mobile IPv6 network environment. In this paper, the advantages of IPv6 for mobility are given and the Mobile IPv6 protocol is overviewed. Then the paper introduces some issues about Route optimization security and Quality of service (QoS) requirement of packet streams between Mobile Node (MN) and Correspondent Node (CN) or between MN and Home Agent (HA).

KEYWORDS: Mobile IPv6, Triangle routing, Route optimization, Quality of service, Security

INTRODUCTION

Internet is now becoming its own victim of its own great success because the intrinsic limitation of the current internet protocol version 4. Among the problems that IPv4 had to face, the most serious one is that the addresses of IPv4 will be exhausted in the near future based on the current developing speed of the Internet.

IPv6 is the new version of IP and born out of the great success of IPv4. The huge address space of IPv6 will meet the requirements for rapid development of Internet easily. Mobility, security and QoS are now integrated in IPv6. It is considered that IPv6 is the important foundation stone for building the mobile information society and the future Internet.

As we know, IPv4 does not provide any support for mobility. In the current IPv4 Internet, each computer is assigned a fixed IP address that is belonged to a network. If the computer changed the attachment point to a different network, the packets sent to it will be routed the former network and will be discarded because of the absence of the destination. Moreover, the mobile computing equipments such as the embedded devices, multi-purposed handset will require the mobility support in IP.

It is an important milestone for mobile computing because of the naissance of the IPv6. The main features of IPv6 that are important for the future growth of mobile wireless network are as follows: sufficient number of IP address; mandated security header implementation; destination options for efficient rerouting; address auto configuration; avoidance of the ingress filtering penalty; error recovery without soft-state bottleneck [1].

The design of Mobile IP support in IPv6 (Mobile IPv6) represents a natural combination of the experiences gained from the development of Mobile IP support in IPv4 (Mobile IPv4) together with the opportunities provided by the design and deployment of a new version of IP itself (IPv6) and the new protocol features offered by IPv6. In mobile IPv6 three operation entities are defined: mobile node (MN), correspondent node (CN), home agent (HA); four new IPv6 destination options are defined: binding update option, binding acknowledgement, binding request and home address option; two

ICMP message are defined for 'Dynamic Home Agent Address Discovery': ICMP home agent address discovery request message and ICMP home agent address discovery reply message; two new IPv6 options for 'Neighbor Discovery': advertisement interval option and home agent information option [2,3].

MOBILE IPv6 PROTOCOL

Mobile Ipv6 Terminology [4]

Mobile Node (MN): A node that can move from its home network to another foreign network .

Corresponding Node (CN): A mobile or a stationary node that communicates or corresponds with the MN by sending or receiving packets to or from MN.

Home Network (HN): The unique network that administers the MN.

Foreign Network (FN): Another network to which the MN is currently attached instead of its HN.

Home address (H@): An unchangeable IP address assigned to MN within its home network.

Home Agent (HA): A router on a mobile Node's home network. While the MN is away from home, the HA intercepts packets on the home network destine to the MN's address, encapsulates them, and tunnels them to the MN's registers CoA.

Access Router: Offers connectivity to the mobile node at its new point of attachment to the Internet.

Binding: It is an association between mobile node home address and its new care of address on the foreign network.

Binding Update: Is the update for the binding information including home address and Care of Address (CoA).

Care-of-Address (CoA): An IP address associated with a MN while visiting a foreign network; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of-addresses that a MN may have at a time, the one registered with the MN's Home Agent is called its primary CoA.

Mobility Anchor Point (MAP): New Mobile IPv6 node or new Mobility Agent, in a network visited, to act as a HA in order to handle binding update procedures locally. The MAP can be located at any level of routers; a MAP is not required on each subnet.

Regional Care-of-Address (RCoA): An address on the MAP's subnet, obtained by the MN which moves into a new network. The RCoA is the address that the MN will use to inform its HA and CNs about its current location.

On-link CoA (LCoA): The LCoA is based on the prefix advertised by its default router.

Route Optimization (RO): Improves data transmission rates between the CN and the MN. With RO, the MN and CN communicate directly with each other and bypass the HA. RO is especially beneficial when the MN and CN are in the same network.

Resource Reservations Protocol (RSVP): Is a set of communication rules that allows channels or paths on the Internet to be reserved for the multicast transmission of video and other high bandwidth message[4].

End-to-End: The End-to-End principle was originally articulated as a question of where best to put the state associated with functions in a communication system.

Flow: A sequence of packets in some way corrected and that therefore must be treated coherently by the IP layer. Packet belong to the same flow in the basis of parameters like the source address, the destination address, the QoS, the accounting, the authentication and the security. A flow can contain several TCP connections.

Flow Directions: Regarding the effects suffered by a traffic flow when it is send from the MN to the CN or vice versa . When the MN is sending packets to the CN and a handover starts, it stops immediately while searching for a new Access Point (AP), those packets are buffered at L2 by the wireless drivers. Only after the MIPv6 handover is finished, the packets flow correctly to the CN. In the case that the CN is the source of the flow the handover behaves differently. The CN sends packet constantly, when the handover starts, all those packets are lost because they are sent to incorrect AR. The CN realizes of the new location of the MN and sends the packets to the correct address.

QoS: Under a QoS environment, as stated above, there are other parameters which highlight the level of provide QoS. Those parameters are the One Way Delay (OWD) and the Inter Packet Delay Variation (IPDV).

Latency of Handovers: Is the time between the last moment where the Mobile Node can receive and send packets through the Old Access Router (OAR) and the first moment where it can receive and send packets through the New Access Router (NAR). Thus, this is the time during which the Mobile Node can neither receive, nor send IP traffic. That time is used to express the Handoff performances.

Movement Detection: Mobile Nodes use IPv6 Router Advertisements and Neighbor is covery methods to detect when they have moved to or attached to a new network.

L2 Handover: Movement of a MN's point of Layer 2 (L2) connection from one wireless access point to another.

L3 Handover: Movement of a MN between ARs which involves changing the on-link care-of address at Layer 3 (L3).

L2 Trigger: Information from L2 that informs L3 of particular events before and after L2 handover.

Multihoming: More than one IP network interface can be assigned to a single endpoint.

2.2 Mobile IPv6 Overview and Operation [5,6]

The main goal of using Mobile IP protocol is to keep the physical connection to the internet while roaming from one network to another. When the mobile node is attached to a foreign network , it will addressed by the Care-Of-Address in addition to its original home address taken at its home network. Binding update will associate the home address of the mobile node to the care-of address. These features allow the mobile node to always be addressable at its home addresses. A mobile node typically acquires its care-of address through stateless or stateful (e.g., DHCPv6) Address Auto configuration, according to the methods of IPv6 Neighbor Discovery or other methods such as static pre-assignment by the owner or manager of a particular foreign link.

In Mobile IPv6, when the node is transferred from the home network to the foreign network it will register its care-of- address with the home agent router existing in the home network The home agent will intercept all IPV6 packets addressed to the mobile node and tunnel all of them to the mobile node care-of-address. Home agent will tunnel the packets using IPV6 encapsulation with the outer IPV6 header addressed to MN care-of-address.

It is possible that while a mobile node is away from home, some nodes on its home link may be reconfigured, such that the router that was operating as the mobile node's home agent is replaced by a different router serving this role. In this case, the mobile node may not know the IP address of its own home agent. Mobile IPv6 provides a mechanism, known as "dynamic home agent address discovery", that allows a mobile node to dynamically discover the IP address of a home agent on its home link with which it may register its care-of address while away from home.

Mobile IPv6 also defines one additional IPv6 destination option. By including the Home Address option in each packet, the sending mobile node can communicate its home address to the correspondent node receiving this packet, allowing the use of the care-of address to be transparent above the Mobile IPv6 support level (e.g., at the transport layer).

With IPv6, a mobile node can inform each of its corresponding nodes of its care-of address. This avoids the phenomenon of triangle routing. The Optimization functionality allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent, and thus eliminates the problem of "triangle routing" present in the base Mobile IPv4 protocol. Since the population of the future Internet is expected to largely be composed of wireless mobile nodes, any such widespread improvement in routing efficiency may have a substantial effect on the continued scalability of the Internet. Figure 1 shows the Basic operations in MIPv6.

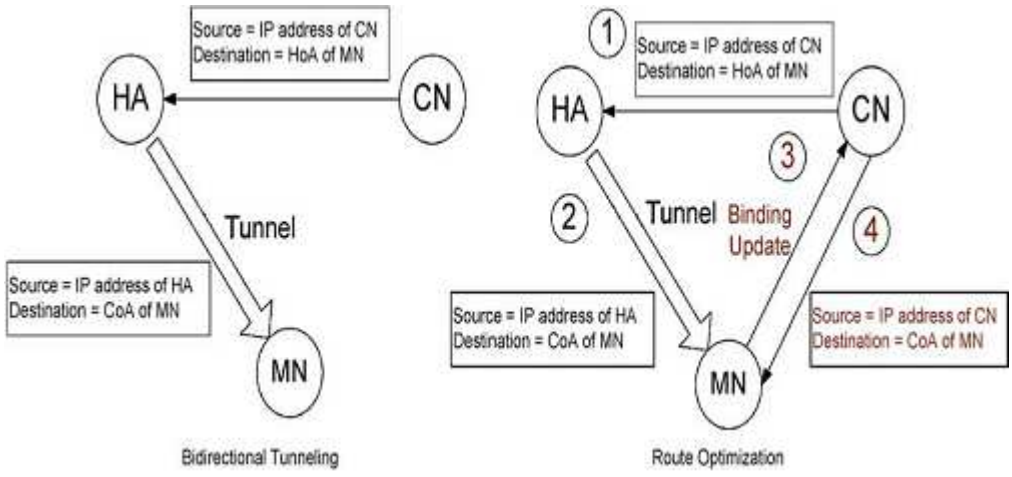


Figure 1: The Basic operations in MIPv6

HANDOVER

Overview

Mobile IPv6 already offers a handover procedure, which is recognized to have sufficient in certain circumstances that makes it unsuitable for real-time applications. The purpose of studying handover is to define a solution that reduces handover latency, so that Mobile IPv6 is a better candidate for handling mobility for mobile nodes hosting real-time applications. Additional signaling procedures and optimizations may be proposed to be used in addition to the basic handover procedure specified in Mobile IPv6.

Fast Handover is a kind of handover operation that minimizes or eliminates latency for establishing new communications paths to the mobile node at the new access router. Smooth Handover is a kind of handover operation that minimizes data loss during the time that the mobile node is establishing its link to the new access point. Moreover, Seamless Handover a handover that is both fast and smooth.

Generally, handovers are considered to fall into one of two classifications: Network-Controlled, whereby some entity in the serving domain directs the establishment of a new link between the mobile node at some point of attachment determined by the network elements. Mobile-Controlled, whereby the mobile node is responsible for determining its new point of attachment and carries out the necessary protocol for making the determination as well as establishing the link at the new attachment point.

An important issue to consider when supporting real-time applications like VoIP in mobile networks is the capability to provide smooth handoffs. A critical requirement for smooth handoffs is to minimize packet loss as a mobile node (MN) transitions between network links [7].

Handover Schemes

MIPv6 Handover Performance Analysis

In MIPv6, when in local subnet, MN communicates normally with other nodes; when moving to a new subnet, MN will disconnect with previous access router (PAR), then connects with a new access router (NAR). This procedure is called mobile handover, which includes link-layer procedure and network-layer procedure. The network-layer handover procedure is initiated only after the link-layer handover procedure comes to end. And the network-layer handover process includes Movement Detection, care-of address configuration, Duplicate Address Detection and Binding Update.

DL2 denotes the link-layer delay, which is different because of using different devices. Movement Detection (MD) procedure is to determine whether or not it moves to a new subnet, the delay of MD is marked DMD. In MIPv6 the value of DMD is 0.5-1.5s.

After completing MD, MN configures its New Care-of Address (NCoA), and this delay is marked DNCoA. If using stateful address auto-configuration, the value of DNCoA equals to the time of configuring DHCP server. If using stateless address auto-configuration, MN generates a NCoA through adding its interface ID to the router prefix information, and the delay of this way can be ignored. Before assigning the address to an interface MN should run Duplicate Address Detection (DAD) procedure to verify the uniqueness of the NCoA. DDAD which denote the delay of DAD procedure is a higher percentage of the whole delay of MIPv6.Through the Binding Update (BU)procedure, MN registers its temporary location to its Home Agent(HA) in its home network and Correspondent Node(CN) every time it moves, which brings a lot of signaling messages, and increases network load. DBUHA/CN denotes the delay of BU.

Figure 2 shows that DMIPv6= DL2+DMD+DNCoA+DDAD+DBUHA /CN, DMIPv6 denotes the whole delay of MIPv6, among which DMD, DDAD, and DBUHA/CN can be optimized. Because of long delay of handover in MIPv6, MN can not receive packets when in handover procedure, and the ratio of data loss is high.

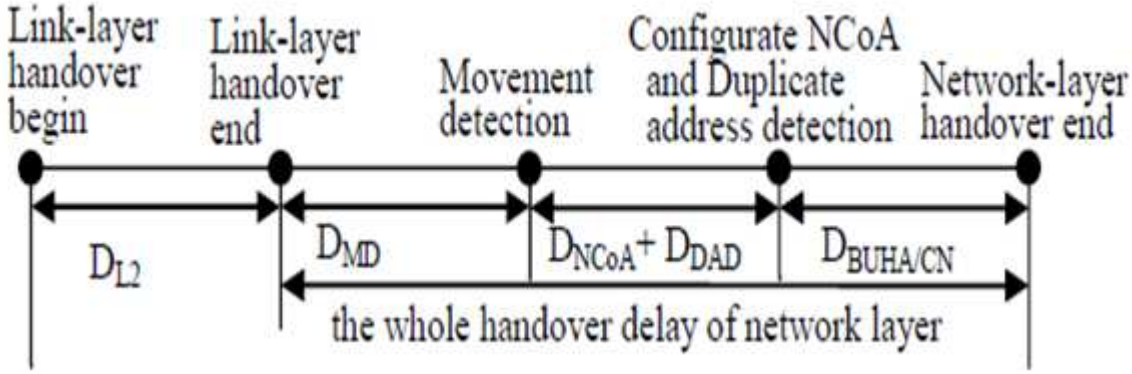


Figure 2: Handover delay of MIPv6

FMIPv6 Handover Performance Analyses

IETF standardized Fast Handover for Mobile IPv6 (FMIPv6) for supporting IPv6 mobility in 2005[8,9]. In FMIPv6, before moving to a NAR, MN generates its NCoA which can be used in the region of NAR through signaling messages. If MN hasn't generated its NCoA after connecting to the NAR, it should establish a tunnel from the PAR to the NAR to forward packets.

FMIPv6 technology can be divided into predictive handover and reactive handover. When connecting with PAR, MN receives FBACK message, which is called predictive handover. When disconnecting with PAR, MN hasn't received FBACK message, which is called reactive handover. Figure 3 shows the procedure of predictive handover.

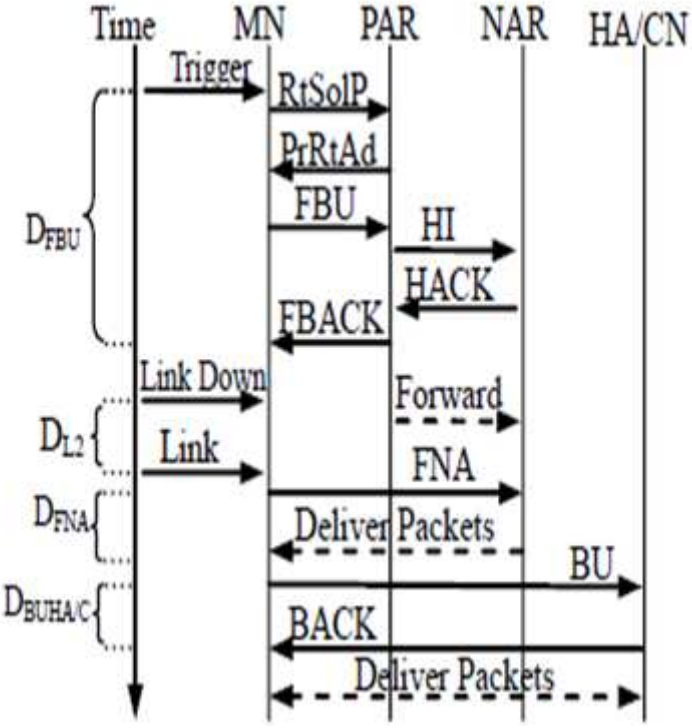


Figure 3: Predictive Handover Procedure

In predictive handover, MN communicates in the region of PAR before handover. When detecting a new network, MN sends a Router Solicitation for Proxy (RtSolPr)to the PAR, the PAR will responds to MN a Proxy Router

Advertisement (PrRtAdv) message including the information of the NAR's network premix and IP address. Then MN generates an NCoA and sends a Fast Binding Update(FBU) message to the PAR, the PAR immediately sends a Handover Initiate (HI) message with MN's NCoA to the NAR. The NAR verifies that the NCoA can be used on the NAR's link, and responds to PAR a Handover Acknowledge (HACK) message. Then PAR sends a Fast Binding Acknowledgement (FBACK) message to MN, and begins forwarding packets to the NAR by bidirectional tunnel between PAR and NAR. In this paper, DFBU denotes the time from MN's beginning to detect the NAR to this moment. Since then MN disconnects with PAR, and can not receive packets. Link-layer handover begins.

After moving to the region of NAR, MN sends a Fast Neighbor Advertisement (FNA) message to NAR asking for packets. Then NAR starts to forward buffering packets to MN, and then the communication between MN and CN is restored. DFNA denoting the above time. Finally, MN sends BU message to HA and CN, then HA and MN responds to MN by Binding Acknowledgement (BACK),the whole handover procedure comes to end. Therefore DFMIPv6= DFBU+DL2+ DFNA+ DBUHA/CN, DFMIPv6 denotes the whole delay of FMIPv6.

HMIPv6 Handover Performance Analyses

In MIPv6 and FMIPv6, when MN far from its HA and moving through more subnets, frequent handover brings more signaling messages, and increases delay. IETF standards Hierarchical Mobile IPv6 (HMIPv6) protocol [8,10], which using local registration mechanism to update binding update procedure, reduce the number and delay of MN's registration to HA and CN.

HMIPv6 uses a local anchor point called Mobility Anchor Point (MAP). The MAP's function is equal to the local agents of foreign network; it deals with MN's intra-domain movement. The domain managed by MAP can be divided into several subnets. Figure 4 shows the system architecture of HMIPv6.

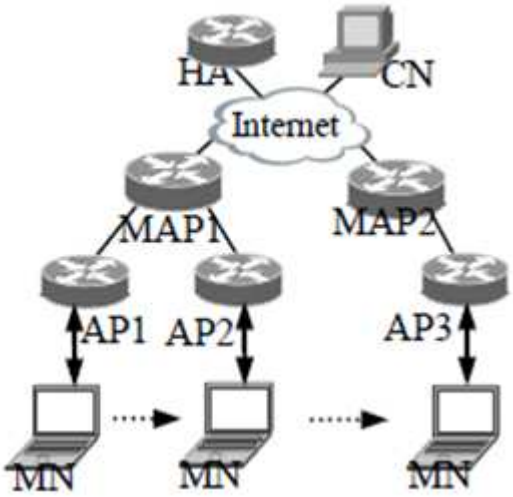


Figure 4: System Architecture of HMIPv6

In HMIPv6, MN obtains Regional Care-of Address (RCoA) from MAP and uses RCoA to communicate with HA and CN; MN also obtains Link Care-of Address (LCoA) from access router and communicates with MAP using LCoA. When moving in a MAP's intra-domain, MN only registers LCoA to MAP. DLBU denoting the delay of this registration, and needn't send BU message to HA and CN because of RCoA having no change. This intra-domain handover is very fast, so DIHMIPv6= DFBU+DL2+ DFNA+ DBUHA/CN, DIHMIPv6 denotes the whole delay of intra-domain HMIPv6.

Seamless Handover Scheme for Mobile IPv6

Seamless Handover for Mobile IPv6 (S-MIPv6), enables an MN performing a new CoA, and then to register to HA and CNs before the MN leaves from the original subnet. There are two modes in this scheme, a soft mode and hard mode, respectively. The soft mode routine presents fairly good performance for most applications. If any application needs extremely performance on minor (even zero) packet loss, it appeal to the hard mode routine. An infrastructure, which contains the neighboring information of mapping between AP and AR, is required. The Cross-layer Address Resolution (CAR) is used to support MN in anticipating the next associated subnet In the original Mobile IP, handover mechanism works with Home Agent (HA) closely. In this scheme, CNs move to new subnet first and then notified HA. The operation of binding update is no different to other service hence they could be handle in the same time. It is no necessary to process HA updating before other handover procedure [11].

Low-Latency Mobile IP Handover Based on Active Scan Link Layer Assisted EMIPv6 [12]

This scheme has the advantage of FMIPv6 and uses an active-scan L2 scheme to help FMIPv6 to reduce the handover latency. The active-scan scheme can monitor the channel status in the background, decides whether the handover is needed and is able to promptly trigger upper layer protocol to initialize the handover procedure. By the background monitor, it reduces the handover latency that the potential and scan phase may cause. Besides, the AP can collect the necessary information that FMIPv6 needs to assist the handover initialization. This helps FMIPv6 to initialize the handover promptly and avoids unnecessary latency. Finally, a modification of FMIPv6 should be proposed. It makes the OAR builds the tunnel before the L2 handover procedure just like the original FMIPv6 does, but the OAR can keep forwarding packets to the MN in its link instead of to the NAR. This can solve the early-start problem in FMIPv6 and can let FMIPv6 get benefit from predictive handover.

3.4.5.1 Active-Scan Link Layer Assistance

The active-scan link layer aims to bypass the most time-consumption phases in the L2 handover procedure and provides prompt information for upper layer. Hence, it monitors the channels it may operate in to bypass the potential phase, and triggers the upper layer as soon as possible while the handover is needed. Nevertheless, monitoring the channels may cause unnecessary packet loss or delay the packet transmission. To avoid the packet loss and unnecessary delay, the monitor procedure must be low enough, i.e. the monitored channels must be as less as possible. This scheme also provides a Selective Channel Probing scheme. In addition, the scheme can actively probe the channels without waiting for the potential phase detecting the needed handover. This different handover style eliminates potential phase and reduces the L2 handover delay.

3.4.5.2 Selective Channel Probing

Selective Channel Probing is a good scheme for reducing the L2 handover delay, especially in an arranged network, it can reduce about 30% to 60% handover delay compared with the IEEE 802.11 handover.

MIPv6 SECURITY

Overview

In MIPv6, there are two possible modes for communications between the MN and a CN. One mode is called bidirectional tunneling. This mode is based on using both forward tunneling and reverse tunneling which are applied on the packets transferred from CN to MN and from MN to CN respectively. The other mode " Route Optimization" (RO)

requires the binding information to be saved at the correspondent node .Route optimization will eliminate the inefficient triangle routing and bidirectional MN–HA tunneling as shown in Fig. 1. On receiving a tunneled packet from its HA, MN knows that CN that sent the packet is unaware of its current CoA. MN may choose to inform CN its new CoA using a Binding Update (BU) message, thereby allow CN to send subsequent packets directly to MN. Unfortunately, unauthenticated or malicious BU messages provide intruders an easy means to launch various types of attacks . Therefore, RO security is of paramount importance for MIPv6 to meet its basic security requirements [13].

Mobile IPv6 Security Threats

Mobile IPV6 route optimization is built into IPv6 protocol rather than added as an extension to the protocol as in MIPv4. As the route optimization improves the efficiency and eliminate the triangle routing problem but, still increasing the number of binding updates sent by MN to its CoA and that definitely will lead to an increase in the security risk and will open the door for many types of attacks.

False Binding Update Attacks

Spoofed Binding Updates may be sent to both the correspondent nodes and the home agents. By spoofing, the attacker can redirect all the traffic to itself or to any other node and prevent the original node from receiving the traffic destined to it.

Man-in-the-Middle Attack

It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Denial-of-Service Attack

In this type of attack a single person or group of people are concerted to prevent an internet site or service from functioning efficiently .This attack could be done by sending a large amount of unwanted traffic to overwhelm the resources of the network. First the attacker will join a heavy data stream site and establish connection with it.Then the attacker will send the binding update to the correspondent node to redirect the subsequent data traffic to the attacker new location that of arbitrary point.This node then wll be bombed with a large unnecessary traffic.

Mobile IPv6 Security Mechanisms

Mobile IPv6 provides a number of security features. The various security issues within MIPv6 include security of IPv6 routing header, home address option and privacy extensions for stateless address auto configuration. In IPv6 initially IPSec authentication header protocol is used for authenticating binding messages but this approach has many problems. To overcome these problems other methods have been developed based on using IPSec ESP [Encapsulation Security Payload) between the mobile node and the home agent and home agent Return Routability (RR) between mobile node and correspondent node.

IPSec

Internet Protocol Security (IPsec) is a protocol suite used to secure the internet protocol by establishing mutual authentication between agents and also negotiating the cryptographic keys [14].The main problem of IPSec is the key

distribution switch called Internet Key Exchange (IKE).IPSec is chosen to be used for authenticating the binding messages between MN and CN.

Return Routability Procedure (RRP)

This method is developed to authenticate the communication between the Mobile Node and the correspondent node. In this procedure the tokens are exchanged between MN and CN. MN uses the tokens to verify the data in its binding update message to the CN. Return Routability Procedure (RRP) protects against Denial of Service Attacks (DoS) in which the attacker is using the victim's addsress as its care-of-address but at the same time (RRP) not able to defend against the attackers that already able to monitor the path between MN and CN.

Cryptographically Generated Addresses (CGA)

In this technique a one way hash function is used to cryptographically generate an address .It a method for binding a public key to an IPv6 address.Discovery Protocol. This method is based on the idea that apart of the IPv6 address is derived somehow from the public key of the node. The length of the IPv6 address is 128 bits. It consists of a 64-bit network prefix and a 64-bit interface identifier. The network prefix is used for routing in the network and a specific node in a link is identified with the interface identifier, which must be of course unique in the link. The advantage of this method is that no certificate is needed to convince another node in the network that the address is used by the owner of the public key that is included in the packet [14,15].

A Robust Secured Mobile IPv6 Mechanism for Multimedia Convergence Services[16]

With the current status of the Mobile IPv6 Security Mechanisms there are still a lot of security flaws to be addressed. This security mechanism for Mobile IPv6 uses IPSec ESP in the tunnel mode between MN and the home agent . CGA method should be used in parallel with Return Routability for better security.In addtition to that if the messages are encrypted, no one in the foreign network will be able to break the security of the protocol.

Providing Efficient Secured Mobile IPv6 by SAG and Robust Header Compression[17]

Wireless networks encounter more technological challenges such as bandwidth, handoff latency and security problems This Scheme propose a new methodology to solve these problems. Security Access Gateway (SAG) is first proposed to solve the security issue by offering high calculating power for the encryption.Second the Robust Header Compression (RoHC) is used to increase the utilization of the bandwidth.

ESS-FH: Enhanced Security Scheme for fast Handover in Hierarchical Mobile IPv6[18]

This scheme achieves the superior performance in terms of handover latency .However, without being secured F-HMIPV6 is vulnerable to various security threats. ESS-FH achieves the strong key exchange for enhanced security policy. In This scheme FMIPv6 improves the handover latency through link layer (L2) triggers and bi-directional tunneling between access routers (ARs).HMIPv6 optimizes the signaling overhead by adopting a local home agent (HA) called Mobility Anchor Point (MAP).Each MN negotiate a secret key with MAP whenever moving to MAP domain .For this negotiation, the public key cryptography is applied in conjunction with CGA. Based on the secret key ,ESS-FH achieves a seamless integration between the fast handover and local binding update .Moreover it allows MN to continually execute the fast handover even between different MAP

Domains.

QUALITY OF SERVICE (QOS) FOR MOBILE IPV6

QoS Overview

As the Mobile Node changes its point of attachment with the Internet, the intermediate network domains traversed by its packets may change. So it is required to keep the performance of QoS running at a desirable level .

In [19] a new IPv6 option called "QoS Object" has been introduced and included as Hop by Hop optioned or a destination option in the IPv6 packets which are carrying the binding updates and the acknowledgements. Upon that a certain QoS procedures will be triggered at the intermediate network domain.

QoS Object is included, depending on the context, either as a Destination Option or as a Hop-by-Hop Option along with the packets carrying Binding Update and Binding Acknowledgment options. The basic idea is to include QoS Object as a Hop-by-Hop option along with the binding message that travels in the same direction (HA to MN, CN to MN or MN to CN) as that of MN's QoS-sensitive packet stream. As this packet traverses different network domains in the end to end path, the QoS Object is examined at these network domains to program QoS support for the MN's data packets.

As we know, there are essentially two types of QoS available:

Resource reservation (integrated services): According to the application's QoS required and based on the bandwidth management policy the network resources will be apportioned .RSVP provides the mechanisms to do this [20].

Prioritization (differentiated services): Network traffic and resources will be classified according to the management policy criteria by giving a preferential treatment to the applications identified by more demanding requirements [21].

There are two other methods to characterize the type of the QoS::

Per Flow: It is used with a single data stream between source and destination and identified by the following 5 – Tuples (transport protocol, source address, source port number, destination address, and destination port number).

Per Aggregate: applied on 2 or more flows which have something in common.

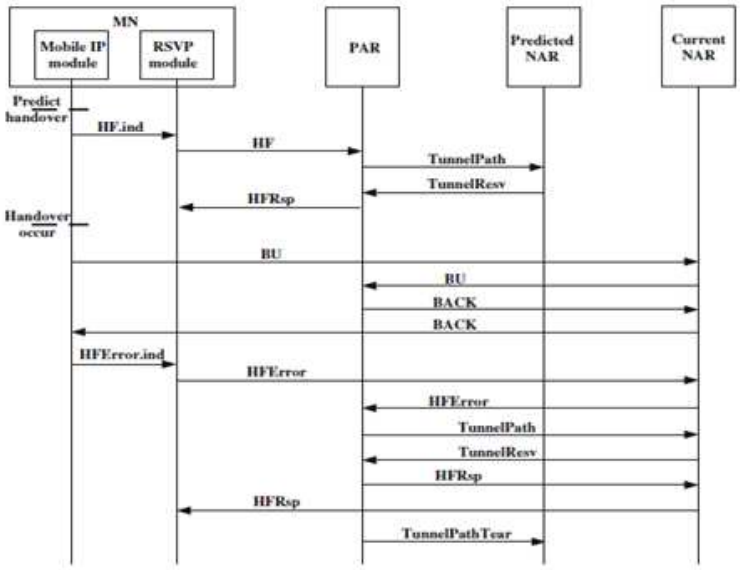
DiffServ possesses excellent scaling properties from the perspective of the network, but there is not a highly accurate service response to every clients application, so an application may not be aware whether a particular service state is being delivered to the application. Moreover, the lack of end-to-end signaling facilities makes such an approach one that cannot operate in isolation within any environment. What appears to be required within the DiffServ service model is both resource availability signaling from the core of the network to the DiffServ boundary and some form of signaling from the boundary to the client application. So the existing signaling will be extended such as Binding Update, Binding Acknowledge, Binding Request to build a response model for Mobile IPv6 in DiffServ environment.

Recent QoS Schemes in Mobile IPv6

Fast RSVP: Efficient RSVP Mobility Support for Mobile IPv6 [22]

In this scheme the handover process with QoS is divided into two stages. The first stage is to setup the resource reservation neighbor tunnel. The second stage is for the resource reservation on the optimized route. As illustrated in figure 5 the mobile node at first communicates with CN and initialize the resource reservation neighbor tuner which was already

setup ahead of the handover. When MN becomes stable in the new subnet it will start the resource reservation process on the optimized route.



HF.ind: Handover Forecast.ind
HF: Handover Forecast
HFRsp: Handover Forecast Response
HF Error.ind: Handover Forecast Error.ind
HF Error: Handover Forecast Error

Figure 5: Message Flowchart of Resource Reservation Neighbor Tunnel setup when Handover Prediction Fails

The implementation of Fast RSVP needs to modify two modules at different layers: mobile IP module and RSVP module. By adding some primitives between them, we let the two modules work together to help the mobile node hand over with QoS guarantees, to avoid resource wasting due to the triangular routes, advanced reservations and duplicate reservations, and to distinguish reservation requests from different types of sessions thus reducing the rate of the handover session forced termination rate. In fast RSVP two flag bits will be added in the common header of the RSVP protocol to indicate the bidirectional reservation and advanced reservation as shown in figure 6.

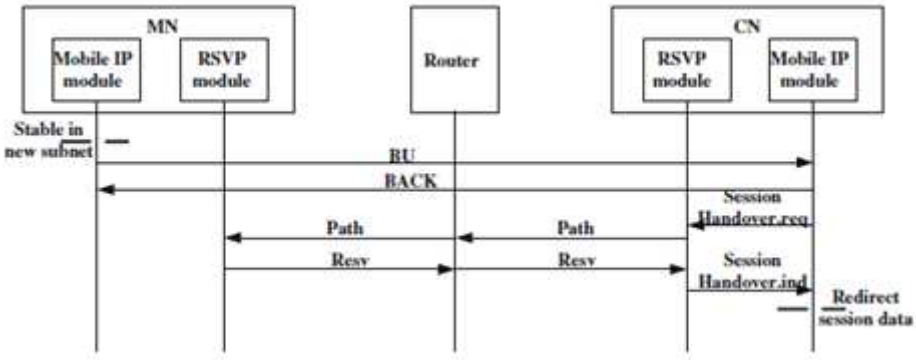


Figure 6: Message Flowchart of Resource Reservation on the Optimized Route

If the endpoint of a session requires to set up a bidirectional reservation, it can set the “B” flag bit in the common header of the Path or Tunnel Path message. When the other endpoint receives the Path or Tunnel Path message with the “B” flag bit set, in addition to replying with a Resv or Tunnel Resv message, it will also reply with a separate Path or

Tunnel Path message with the same SENDER_TSPEC, thereby completing the bidirectional reservation for the session.

If the "A" flag bit in the common header of the Tunnel Path or Tunnel Resv message is set, it means that the resources reserved for the session in advance can be temporarily borrowed by sessions with low priorities. When routers receive the Tunnel Resv or Tunnel Path message with the "A" flag bit set, they will mark the resources in the "advanced reservation state" and resources in this state can be temporarily borrowed by other sessions with low priorities. These resources return to the "normal reservation state" when the routers receive the Tunnel State Change message, after the mobile node indeed hands over to the predicted subnet.

In order to better mark the multimedia sessions in mobile environments, Fast RSVP imports a new object MSESSION to replace the SESSION object in the ordinary RSVP protocol. Compared with the SESSION object, MSESSION adds a "home address" field in the object, and it is defined as:

<MSESSION> ::= <Home Address><Dest Address>.

<Protocol I d><Flags><Dest Port>.

The "Home Address" field is filled with the MN's home address and its value is invariable, so we can utilize it to label the mobile node. The "Dest Address" field contains the MN's care-of address but this address might change after the MN hands over to another subnet. In a mobile environment, the RSVP router should label a multimedia session based on the content of MSESSION and set up the corresponding Path State and Resv State accordingly.

An Enhanced Scheme To Support QoS in MIPv6 Based Networks Using DiffServ [23]

This scheme aims to utilize the basic building blocks in Diffserv-MIPv6. Therefore, this will minimize the packet losses and handover latency in this scheme. Figure 7 represents the proposed architecture where (ER) is the Edge Router, (CR) is the Core Router and (BB) is the bandwidth Broker to optimize the existing resources. In addition to that the Access Router (AR) is connected to one or more base stations to provide the connectivity to MIPv6 nodes.

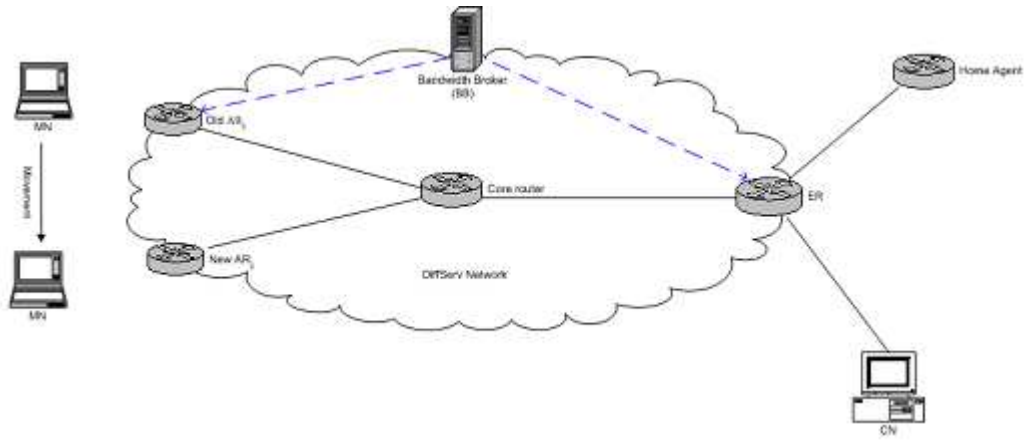


Figure 7: DiffServ Support within Mobile IPv6 Network

COMPARISON BETWEEN MOBILE IPV4 AND MOBILE IPV6

In MIPV6 the packets sent to MN will be tunneled using an IPV6 routing header rather than IP encapsulation, whereas Mobile IPv4 must use encapsulation for all packets. The use of a routing header requires less additional header bytes to be added to the packet, reducing the overhead of Mobile IP packet delivery.

In MIPv6 there will be no need to deploy foreign agents as in MIPv4. Mobile IPv6, mobile nodes make use of the enhanced features of IPv6, such as neighbor discovery and address auto configuration.

"Route Optimization" procedure is built in as a fundamental part of Mobile IPv6, rather than being added on as an optional set of extensions in MIPv4.This allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent, and thus eliminates the problem of "triangle routing" present in the base Mobile IPv4 protocol.

While a mobile node is away form home, its home agent intercepts any packets for the mobile node that arrive at the home network, using IPv6 neighbor discovery rather than ARP as is used in Mobile IPv4.

Mobile IPv6 uses destination options which allow all Mobile IPv6 control traffic to be piggybacked on any existing IPv6 packets, whereas Mobile IPv4 and its route optimization extension needs separate UDP packets for each control message.

Mobile IPv6 allows mobile nodes and Mobile IP to coexist efficiently with routers that perform "ingress filtering". A mobile node now uses its care-of-address as the source address in the IP header of packets it sends, allowing the packets to pass normally through ingress filtering routers. The mobile node carries its home address in a home address destination option, allowing the use of the care-of-address in the packet to be transparent above the IP layer.

Mobile IPv6 utilizes IP Security (IPsec) for al security requirements (sender authentication, data integrity protection, and replay protection) for binding updates (which serve the role of both registration and route optimization in Mobile IPv4), whereas Mobile IPv4 relies on its own security mechanisms for these functions, based on statically configured "mobility security associations".

Although Mobile IPv6 enables wide-area mobility to be implemented at the IP level, it does not have functions characteristic of wireless access networks such as high-speed handover or paging function.

A key design point of Mobile IPv4 [9] was to support host mobility in networks without mandating changes to every existing IPv4 node while Mobile IPv6 includes explicit support for host mobility.

Mobile IPv6 and Mobile IPv4 with routing optimization [10] could in theory support mobile networks similarly as in Mobile IPv4. However, although mentioned in the Mobile IPv4 specification, the current specifications of Mobile IPv4 with routing optimization and Mobile IPv6 don't mention them anymore. Mobile IPv6 can not be used without major changes if we want to provide optimal mobility support to networks. Particularly, Mobile IPv6 doesn't scale to the size of the mobile network.

Mobile IP still acts as an "open-door" for hackers of all kinds, there is no strong authentication of the visiting user, no data privacy and no data integrity protection between the MN and its home network.

CONCLUSIONS AND FUTURE WORK

The fast Internet evolution together with the enormous growth in the number of users of wireless technologies has resulted in a strong convergence trend towards the usage of IP as the common network protocol for both fixed and mobile networks.

In this paper, the advantages of IPv6 for supporting mobility have been described and the Mobile IPv6 protocol is overviewed. Also the paper has introduced the handover that is composed of fast handover and smooth handover. Security design, plus the assumptions and the starting point of security designs in MIPv6 are first elaborated in details. Then the security threats in MIPv6 and the classification of the attacks against routing optimization are analyzed. Finally the quality of service protocols used with MIPv6 are introduced. Also a recent schemes for Handover, security, and Quality of Service in Mobile IPv6 are discussed in this paper and a final comparison between Mobile IPv4 and Mobile IPv6 has been introduced.

In the next paper a proposed route optimization scheme in MIPv6 that verifies the required level of security and quality of service will be introduced.

REFERENCES

1. Charles E. Perkins, "*Mobile IPv6 and Cellular Telephony"*, 2000 International Conference on Communication Technology Proceedings.
2. Byungjoo Park, Sunguk Lee, Haniph Latchman, "*A Fast Neighbor Discovery and DAD Scheme for Fast Handover in Mobile IPv6 Networks*", Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), 2006 IEEE.
3. Christophe Jelger ,Thomas Noel, "*Proactive Address Auto configuration and Prefix Continuity in IPv6 Hybrid Ad Hoc Networks"*, 2005 IEEE.
4. Sherif Kamel Hussein, Iman Saroit Ismail, S. H. Ahmed ,(2006),"*Triangle Routing Problem in Mobile IP"*, INFOS 2006, 25-27 March, Proceedings of the Fourth International Conference on Informatics and Systems, Conference Hall, Cairo University, Cairo, Egypt.
5. D. Johnson and C. Perkins, *"Mobility Support in IPv6"*, Internet Draft, Internet Engineering Task Force. Draft-ietf-mobileip-ipv6-12.txt. April 2000.
6. Tsuguo kato, Ryaichi takechi, Hideak Ono. "A Study on Mobile IPV6 Based Mobility Management Architectture", Fujitsu Sci.,Tech.J,37,1,PP65-71,June 2001.
7. Mo Lin-Li, *"Research on Mobile IPv6 Technology and Handover Performance Optimization*", American Journal of Engineering and Technology Research, Vol. 11, No.9, 2011.
8. H. Soliman, C. Catelluccia, et al., "*Hierarchical Mobile IPv6 Mobility Management (HMIPv6)"*, RFC4140, August 2005.
9. Mohamed Alnas, Irfan Awan, R.D.W. Holton, *"Performance Evaluation of Fast Handover in Mobile IPv6 Based on Link-Layer Information"*, The Journal of Systems and Software 83 (2010) 1644–1650.
10. Hee Young Jung, Seok Joo Koh, Hesham Soliman, Karim E1-Malki. *"Fast Handover for Hierarchical MIPv6 (F-HMIPv6)"*, Draft-jung-mobileip-fastho-hmipv6-04.txt. Jun 2004.
11. Wei-Ming Chen, Wally Chen, Han-Chieh Chao, "*An efficient mobile IPv6 handover scheme"*, Telecommun Syst. (2009) 42: 293–304.

12. Ming Chun Hsia, Chunhung Righard Lin, "*Low Latency Mobile IP Handover Based on Active scan Link Layer Assisted FMIPv6"*, Journal of Information Science and Engineering, 25, 235-250 (2009).

13. Shalini Punithavathani, Dr. K.Sankaranarayanan, A. BrammaSakthi, *"Comparative Story of Secured Optimized Route in MIPV6"*, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008.

14. Timo Koskiahde, Tampere University of Technology, 8306500, "*Security protocols, Security in Mobile IPv6"*, 18.4.2002.

15. Andre Encarnacao, Greg Bayer, "*Mobile IPv6 Binding Update - Return Routability Procedure"*, March 2008.

16. Yvette E. Gelogo1, Ronnie D. Caytiles1, Byungjoo Park, "*A Robust Secured Mobile IPv6 Mechanism for Multimedia Convergence Services*", International Journal of Multimedia and Ubiquitous Engineering Vol. 6, No. 4, October, 2011.

17. Tin-Yu Wu, Han-Chieh Chao, and Chi-Hsiang Lo, "*Providing Efficient Secured Mobile IPv6 by SAG and Robust Header Compression"*, Journal of Information Processing Systems, Vol.5, No.3, September 2009.

18. Ilsun You, Jong-Hyouk LEE, Kouichi Sakurai, Yoshiaki HORI, "*ESS-FH: Enhanced Security Scheme for fast Handover in Hierarchical Mobile IPv6"*. IEICE TRANS. INF.& syst., Vol. E(3-D, NO.5 May 2010.

19. H. Chaskar, R. Koodli. "*A Framework for QoS Support in Mobile IPv6*", draft-chaskar-mobileip-qos-00.txt, November 2000.

20. IETF *"Integrated Services"* working group. See http://www.ietf.org/html-charters/ intserv-charter.html.

21. IETF "*Differentiated Services*" working group. See http://www.ietf.org/html-charters/diffserv-charter.html.

22. Yi Sun, Yucheng Zhang, Yilin Song, Eryk Dutkiewicz, "*Fast RSVP: Efficient RSVP Mobility Support for Mobile IPv6*", Wireless Pers Commun (2011) 60:769–807.

23. Loay Faisal Ibrahim, Aisha-Hassan A. H., Farhat Anwar, Othman O. Khalifa, Omer Mahmoud, Rashid A. Saeed, Shihab A. Hameed and Jamal I. Daoud, "*An Enhanced Scheme To Support QoS in MIPv6 Based Networks Using DiffServ*", Australian Journal of Basic and Applied Sciences, 5(6): 447-455, 2011.

AUTHOR

Sherif kamel Hussein Hassan Ratib has Graduated from the faculty of engineering in 1989 Communications and Electronics Department, Helwan University. He received his Diploma, MSc,and Doctorate in Computer Science - Major Information Technology and Networking from Cairo University in Egypt. He is currently Associate Professor in Electrical

and Communication Engineering department at October University for Modern Sciences and Arts, He has worked internationally in the area of Networking, Control and Automation. He joined many private and governmental universities inside and outside Egypt for almost 15 years .He shared in the development of many industrial courses .His research interest is GSM Based Control and Macro mobility based on Mobile IP.