TOKEN BASED SECURITY IN MIPV6, HMIPv6 AND IN DYNAMIC MAP MANAGEMENT HMIPv6

M. N. Doja¹ and Ravish Saggar²

¹Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India, E-mail: ndoja@yahoo.com
²Research Scholar, Singhania University, Faculty, Banarsidas Chandiwala Institute of Information Technology, New Delhi, India, E-mail: ravishsaggar@rediffmail.com

ABSTRACT

Mobile Internet Protocol (MIP) is a standard protocol defined by Internet Engineering Task Force (IETF) that allows mobile devices to maintain a permanent IP address irrespective of their roaming between networks. In this paper we present the working and issues related with various MIP versions and their solutions. In addition, we have proposed a token based solution for authenticating the Mobile Node reaching any foreign network and securing the Binding Update messages sent by MN to Home Agent (HA) and Correspondent Node (CN) when it moves from one network to another network.

Keywords: Mobile IP, MIPv4, MIPv6, HMIPv6, Stateless Address Auto-configuration, Route Optimization, Neighbor Discovery, Triangular Routing, Ingress Filtering, Double Crossing, Issues with Mobile IP, Binding Update, Mobility Anchor Point, Public Key Encryption, security attacks.

1. INTRODUCTION

Recent years have seen a tremendous growth in wireless devices such as laptops, cell-phones, notebooks etc. because of which Mobility Management in the wireless domain has become a challenging issue. Frequent change in network requires a new IP address and the packets to get routed to it. IETF defined a set of rules for this mobility under IPv4 called Mobile Internet Protocol version 4 (MIPv4) which allows mobile devices to be associated with one permanent IP address while they freely move from one network to another network. In every foreign network they get a new IP address called Care-of Address. There are certain issues with MIPv4 like double crossing, ingress filtering and triangular routing but the main problem is - IPv4 is about to get exhausted. The central Internet Assigned Numbers Authority (IANA) pool of IPv4 was depleted on January 31, 2011. Regional Internet Registries (RIRs) are also going to deplete soon with first RIR to get exhausted on December 3, 2012 [1]. Vint Cerf, recently Commissioner for the Broadband Commission for Digital Development and the “father of the Internet”, selected the 32-bit system in 1977 because he thought a pool of 4.3 billion possible IP addresses would be enough. With the depletion of IPv4 addresses, the next batch of addresses that will be available from IANA will be IPv6 addresses, which use the 128-bit addressing scheme and have more than 340 undecillion possible addresses [2].
Host, only a Local Binding Update message is sent to MAP which solves Update Latency and Signal Overloading issues up to some extent. In this paper Dynamic MAP management for HMIPv6 scheme is presented which will solve the signal latency without compromising the efficiency event if load increases at MAP. In this there will be multilayer MAP, Super and Sub MAP. If load increases at Super MAP some load will be transferred to Sub MAP and when load goes down Sub MAP load be taken back by Super MAP. So the fall in efficiency due to heavy load will not happen.

In both MIPv6 and Dynamic HMIPv6, Stateless Address Auto-configuration and Binding Update messages play a very important role. Hence this paper is proposing a token based scheme for resolving security issues in them. The propose scheme will make sure that only authenticated nodes will be able to obtain temporary IP address and send Binding Update messages.

This paper starts with a brief introduction about various MIPs and ICMP messages.

2. MOBILE INTERNET PROTOCOL VERSION 4 (MIPv4)

Every Mobile Node (MN) is associated with a network called Home Network where it has a permanent IP address called Home Address. A Home Agent (HA) which is a network node generally a router which has the function of acquiring all the data that is sent to the MN when the MN is outside its Home Network. When a MN moves to network other than home network then it is said to be on a Foreign Network. Since IPv4 supports only Stateful Address Auto-configuration a DHCP server on that network provides a temporary IP address to that MN called Care-of Address (CoA). This IP address changes depending on the node's point of attachment. Foreign Agent (FA) which is a network node generally a router on the foreign network. After receiving CoA, MN registers its CoA with FA and announces its Home Address and Home Agent's address to FA. FA after registering MN registers with HA by sending a message. HA in return sends a Registration Reply message informing whether it accepts registration or not. This allows the HA on home network to know exactly where the MN is located and therefore will be able to know where to send packets. If MN is unable to find a FA on foreign network then it, itself, acts as FA and then its temporary address is called Co-located Care-of Address. Each time MN changes network it gets another CoA, registers with a FA there which in turn registers with HA.

In MIPv4 addresses and routers are maintained and managed with the help of ARP and ICMPv4 messages. Correspondent Node (CN) is any node which wants to send data to MN. CN doesn't know CoA in MIPv4, it only knows Home Address i.e. permanent IP address of node. So it sends the packet with Home Address of node. Registered Home Agent receives that packet and transfers it to MN's current address where either MN directly receives it or FA receives and relays it to MN. A tunnel is set up by the HA to the CoA of node to route packet to MN which is called Tunneling. Each time CN sends packet to MN it follows the same path - from CN to HA, HA to FA, FA to MN.

3. ISSUES WITH MIPV4

There are certain issues with MIPv4

3.1. Ingress Filtering

Ingress Filtering is a technique performed by the firewall of some systems to make sure that the packets are actually from the network that they claim to be. In this technique those packets whose IP address differs from the network that the device is in are rejected. In MIPv4 the MN sends packets with Home Address while it being in foreign network and hence those packets get rejected by systems which perform Ingress Filtering. The solution to it is Reverse Tunneling. In Reverse Tunneling FA after receiving packet from MN transfers it to HA, it in turn relays it to CN.

3.2. Double Crossing

Even if CN and MN are on the same network still whenever CN wants to send a packet to MN it will follow the same path - from CN to HA, HA to FA, FA to MN i.e. the packet crosses the internet twice. Though, the transmission would have been faster and reliable if packet travels directly from CN to MN.

3.3. Triangular Routing

Since CN is unaware of the CoA of MN it always sends packet to Home Address of MN which relays it to FA which further relays it to MN. Hence a packet from CN to MN always gets routed from this triangular path.
Though, the transmission would have been more faster and reliable if CN knows the CoA of MN and directed the packets directly to MN's present address.

4. MOBILE INTERNET PROTOCOL VERSION 6 (MIPV6)

Main features of MIPv6 are:

4.1. Stateless Address Auto-Configuration

In IPv6, a node can configure its own IP address with the help of Internet Control Message Protocol version 6 (ICMPv6) messages. Unlike in IPv4, where a DHCP sever provides MN with a temporary IP address, it is called stateless because no one other than the node itself manages its address, therefore no need to manage state.

4.2. Neighbor Discovery Protocol

In MIPv6, MN can automatically locate routers in the network with the use of two ICMPv6 messages - Router Solicitation and Router Advertisement.

MN, after reaching Foreign Network, multicasts Router Solicitation message on the network. Corresponding Routers on that network responds by sending Router Advertisement message. Routers which are ready to become agents append Agent Advertisement message to the Router Advertisement message.

Stateless Address Auto-configuration takes place with the help of ICMPv6 Address Resolution messages - Neighbor Solicitation and Neighbor Advertisement.

Neighbor Solicitation message is sent by MN to request link layer address of neighbor, or to verify that a neighbor is still reachable and also for duplicate address detection. Neighbor Advertisement is response to Neighbor Solicitation by a node telling its link layer address. A node may also send unsolicited Neighbor Advertisement message to announce a link-layer address change.

4.3. Route Optimization

This allows a CN to send messages directly to the MN's CoA and for MN to send messages to CN using its current temporary IP address i.e. CoA, bypassing the HA. Hence it solves Ingress Filtering, Double Crossing and Triangular Routing problem.

5. WORKING OF MIPV6

For first packet from CN to MN working of MIPv6 is same as MIPv4. CN only knows Home Address of MN, it sends the packet with destination address as Home Address of MN. Since MN is not there HA receives it and forwards it to MN's CoA.

But once MN knows that CN wants to communicate with it, it sends a Binding Update (BU) message to CN which contains its present IP address. CN after knowing the current location of MN sends the packet directly to MN with destination address on packet as CoA of MN. MN also sends packet directly to CN by using source address as CoA hence resolving Ingress Filtering problem.

6. ISSUES WITH MIPV6

There are certain issues with MIPv6:

6.1. Update Latency

The MN is obliged to send a Binding Update message to its HA and CN each time it changes point of attachment. If HA or CN are at large distance from MN and MN is changing location frequently than update latency occurs.

6.2. Signaling Overhead

End-to-end path establishment is necessary for transmission and due to which BU and BA are waited for. Signals and packets get lost during waiting.

6.3. No Location Privacy

There is no location privacy in MIPv6 since the change in temporary local address as the MN moves exposes the MN's location to CN and potentially to eavesdroppers.

7. HIERARCHICAL MOBILE INTERNET PROTOCOL VERSION 6 (HMIPv6)

HMIPv6 proposes multi-level Hierarchical Network architecture. In HMIPv6 a new router called Mobility Anchor Point (MAP) is introduced. MAP is used by MN as its local Home Agent. It is similar to Foreign Agent of
MIPv4 but it need not reside in each subnet. It can be located at any level in a hierarchy of routers including the Access Routers (AR). In HMIPv6, MN gets two temporary IP Address - Regional Care-of Address (RCoA) and On-link Care-of Address (LCoA).

RCoA is an address which MN obtains from visited network in the MAP’s domain. This is the current temporary address used by MAP to register with MN’s HA i.e. HA knows RCoA of MN only. LCoA is an address obtained by MN in AR’s subnet inside MAP’s domain. MAP can help in providing seamless mobility for the MN as it moves from Access Router 1 (AR1) to Access Router 2 (AR2), while communicating with the CN [6].

Whenever MN moves from one subnet to other inside same MAP’s domain i.e. Intra Mobility, only it’s LCoA changes, RCoA remains the same. MN sends a Local Binding Update message to MAP in order to establish a binding between RCoA and LCoA. After a successful registration with the MAP, a bi-directional tunnel between the mobile node and the MAP is established. All packets sent by the mobile node are tunneled to the MAP.

RCoA only changes when MAP domain changes. HA and CA only knows RCoA and only MAP knows LCoA. When MN sends a packet to MN, 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 i.e. LCoA.

8. SOLUTION OF MIPV6

The movement of MN remains completely transparent from CN and HA in HMIPv6. Since HA and CN only knows RCoA of MN and any change in LCoA needs only to send Local Binding Update message to MAP. Sending update messages to MAP is quite faster than sending to HA and CN. Rest all work - registering with HA, retrieval of data, transmission of data - is managed by MAP. It solves the Location Privacy issue of MIPV6. HMIPv6 separates the local mobility from the global mobility hence speeds up the transmission. In HMIPv6 even a movement from one subnet to other requires to send BU message to both HA and CN and this becomes issue if the distance between MN and HA or CN is large and MN is changing network frequently. Here the Update Latency problem and Signal overloading problem certainly gets solved in case of Intra or local mobility.

9. ISSUE WITH HMIPv6

When MN moves from one MAP’s domain to other MAP’s domain i.e. for Inter Mobility it is again inefficient. It faces higher handover latency and packet loss which decreases its overall performance.

10. SOLUTION OF HMIPv6 ISSUES WITH DYNAMIC MAP MANAGEMENT

Dynamic MAP Management Scheme is presented in this paper. In this scheme there will be two levels of MAP as shown in Figure 5. First level MAP will be super MAP and have two load levels Low Load (LL) level and High Load (HL) level as shown in Figure 5. These LL and HL will represent the load level of super MAP. Second level MAP will be sub MAP. This sub MAP will be activated and will take load from super MAP if the load of super MAP goes beyond HL level. This sub MAP will again be deactivated, as soon as super MAP load level goes down. So when load goes beyond HL level load will be shared and as soon as load goes down load will be taken back from sub MAP. This scheme will work as follows:

1. When MN comes into the vicinity of AR in foreign link, it sends Registration signal to sub MAP.
2. Sub MAP will forward registration signal to super MAP after keeping a copy of registration information, although it is not an active MAP.
3. Super MAP will register all MN’s entry, coming from sub MAPs. These registration information is stored in separate tables, for each sub MAP, to solve searching problem.
4. Process at serial number 10.1 to 10.3 continues, till super MAP’s load reaches HL level.
highest number of MN’s registration signals sent from sub MAP, till any one of the sub MAP sends ready signal (ready to manage all MN’s sent via this particular sub MAP).

6. As soon as it receives the ready signal from sub MAP, it sends activate signal to that particular sub MAP and wait till it acknowledged back.

7. Sub MAP receives activate signal and as sub MAP has the copy of registration signals, sent to super MAP, it will just activate itself.

8. Sub MAP will now send new registration signal to all MN’s, it has, HA & CN & send activated signal as acknowledgement to super MAP.

9. Super MAP, after receiving acknowledgement from sub MAP:
   1. Encapsulates and forward those packets destine to MN, which has now been managed by sub MAP.
   2. Reduces its load level and ask all, if any active, sub MAP’s about their load, except to that sub MAP it last transferred the load.

10. All sub active MAP’s response super MAP by sending their load levels after being asked or after fixed intervals.

11. Super MAP always try to vanish as many as possible sub MAP, for this it calculates new load level by adding, its load with individuals sub MAP’s load, starting with lowest load sub MAP. If calculated level comes lesser then its LL Level it takes back the charge from that particular sub MAP.

12. To take back the charge Super MAP sends transfer signal to that particular sub MAP.

13. After receiving transfer signal, Sub MAP updates the registration record of super MAP, sends new registration signal of super MAP to all HA and CNs. After receiving acknowledgement from all HA and CNs, it becomes inactive. Then, it sends deactivated signal to super MAP.

Above mentioned processes ensure, to keep MAP area as bigger as possible without compromising the performance of MAP.

11. SECURITY OF MESSAGE IN MIPV6 & DYNAMIC HMIPV6

In above all schemes, there are several types of messages involved. Binding Update (BU) message which is common in both for informing Home Agent and Correspondent Node about current location of Mobile Node and Local Binding Update (LBU) message send to MAP for binding LCoA to RCoA. One problem is Binding Update messages are not authenticated. When a MN reaches foreign network ICMPv6 messages comes into play. For searching routers as agents Router Discovery messages - Router Solicitation & Router Advertisement are used. For generating IP address Address Resolution messages - Neighbour Solicitation and Neighbour Advertisement are use. Securing all these messages is quite important because they help in finding legitimate Agent and legitimate IP address for Mobile Node. BU And LBU plays a very important role in delivery of packets to right destination. But what if there is an intruder which generates an illegitimate BU or LBU and sends it to HA or CN. CN considering that message as legitimate sends packets to intruder’s address.

11.1. Types of Possible Attacks

11.1.1. Masquerading

Intruder pretends to be Mobile Node. Generates a fake BU or LBU and sends it to MN’s HA and CN or MAP and hence all the data will get directed to it.

11.1.2. Replay Attack

Intruder captures the messages coming from MN hence gets the current location of MN and then replays the message to the destination.

11.1.3. Modification of message

Intruder after capturing the BU or LBU changes the IP address of those messages so that HA, CN or MAP gets wrong CoA of MN and packets can never reach the correct MN or packets get directed to intruder instead of MN. Even the packets going from MN can also be modified in a way that they start suffering Ingress Filtering and firewall of destination rejects them even though the message was from legitimate MN. ICMPv6 messages can also be modified by intruder so that MN gets wrong router as agent or generates wrong IP address in stateless address auto-configuration.

11.1.4. Denial of Service Attack

A Denial of Service attack is an attempt by attackers to prevent legitimate users of a service from using that service. It includes bandwidth consumption, consumption of scarce resources, and alteration of network components or configuration so that MN can’t use service.

The solution for getting prevention from these security attacks is authentication of Binding Update message.
12. TOKEN BASED AUTHENTICATION SOLUTION FOR BINDING UPDATE MESSAGE

For securing and authenticating Binding Update messages key based encryption can be used. Encryption is simply the obfuscation of information in such a way as to hide it from unauthorized nodes while allowing authorized nodes to see it. Public Key Infrastructure (PKI) enables users of unsecure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

- A certificate authority (CA) is an authority in a network that issues and manages security certificate and public keys for message encryption.
- A registration authority (RA) is an authority in a network that verifies node’s request for a digital certificate and tells the certificate authority (CA) to issue it.
- A digital signature $DS[x,y,z]$ is an electronic signature is used to authenticate the identity of the sender of a message, and possibly to ensure that the original content of the message that has been sent is unchanged. In this $x$ has generated DS for $y$ node using $y$ key.
- Digital Certificate $DC[x,y]$ is issued by a certification authority (CA). It contains node’s name, a serial number, expiration dates, a copy of the certificate holder’s public key and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. In this $x$ has generated $DC$ for $y$ node.
- Authentication server (AS) is an application that facilitates authentication of a node that attempts to access a network. There is one AS for every subnet.
- The private key $Pr(x,y)/Pu(x,y)$ Public/Private key pair. $x$ denotes entity that generated it any $y$ denotes entity for which it is generated.
- Tentative Address (TA) is an IP Address generated by node before getting converted to permanent address.

12.1. Public-Private Key Pair Requested from CA

The Manufacturing Company (MC) of NIC card in node, requests CA to issue Private-Public key pair and Digital Certificates. RA verifies node’s request for DC and tells CA to issue it. CA issues DC that contains a Public Key $Pu(CA,MC)$, expiration date, digital signature of issuer. Then that public key is made publicly available. The matching private key $Pr(CA,MC)$ is also given to MC.

12.2. MC installs NIC card and writes information

Manufacturing company will firstly create $MD_1$ (using hash function) from $Pu(CA,MC)$, NIC number, $DC(CA,MC)$. Alongwith this $MD_1$, and $Pu(CA,MC)$, NIC number, $DC(CA,MC)$ Node 1 will encrypt all the above components using $Pr(CA,MC)$ which will give $DS[MC,N1,Pr(CA,MC)]$ as shown in Figure 6.

![Figure 6: Digital Signature by Manufacturing Company](image1)

This Digital Certificate, Digital Signature and NIC number is written on the interface card. This information is used to verify the NIC by AS, using public key $Pu(CA,CA)$ provided by CA.

12.3. Generating Digital Signature for Mobile Node

MN first generates a TA till the time it not gets a Care-of Address and $Pu-Pr$ pair $Pu(N1,N1) and Pr(N1,N1)$. DC from CA, $DS$ of $MC, Pr(CA,MC)$, TA, $Pu(MN,MN)$ and NIC number are collectively converted into fixed length message digest $MD_2$. Then Node N1 will encrypt $MD_2$ and $DS[MC,N1,Pr(CA,MC)]$, $Pu(CA,MC)$, $TA$, $Pu(N1,N1)$ using $Pr(N1,N1)$ to generate $DS[N1,AS1, Pr(N1,N1)]$ as shown in figure 7. Now this DS along with $Pu(N1,N1)$, $DC(CA,MC)$ and $Pu$, $CA$, $MC$ will be sent to AS 1.

![Figure 7: Digital Signature by Node (N1) Authentication Server](image2)

12.4. Verification of Digital Certificate of Mobile Node and generation of Token by Authentication server

After receiving the above components, the following steps would be followed by AS 1:-

1. Verify the Public Key, $Pu(CA,MC)$ and $DC(CA,MC)$ from Certification Authority(CA) or from its local Database.
2. After verification, AS 1 will decrypt $DS[N1,AS1, Pr(N1,N1)]$ using $Pu(N1,N1)$. This decryption will give $MD_2$, $DS[MC, N1, Pr(CA,MC)]$, $Pu(N1,N1)$, $TA$, $Pu(CA,MC)$.
3. Now AS1 will verify the token request. For this, AS1 generates a random number and encrypts it with Pr(AS1,AS1). This again is encrypted with public key of Mobile Node Pu(N1,N1) that has made request and send to requester node address along with Pu(AS1,AS1). If the Mobile Node has made a token request it must be verified. After receiving the message from AS, MN decrypts the this message with its private key Pr(N1,N1) and decrypts it again with Public key of public key of AS Pu(AS,AS) to get actual random number sent by AS. This random number is now encrypted firstly with public key Pu(AS,AS) of AS and then with private key of requester Pr(MN,MN) and sent to AS. AS decrypts encrypted number firstly with Public key Pu(MN,MN) and then with Private key Pr(AS,AS),to get the number sent by requester. The matching of number sent by AS and number received from requester validates that request is authentic.

6. After matching AS1 will decrypt DS[MC, N1, Pr(CA, MC)] using Pu(CA, MC). This will give NIC number of Node 1, DC( CA, MC),Pu(CA, MC) and MD 1.

7. Now AS 1 will generate MD 4 from NIC number of Node 1, DC( CA, MC),Pu(CA, MC) and matches this MD 4 with MD 1. Matching MD 4 and MD 1 prove the authenticity of NIC number.

8. Now AS 1 will store TA and corresponding Pu( N 1, N 1) in its data base.

9. Now, AS 1 will create MD 5 using DS[MC, AS 1, Pr (CA, MC)], Pu(CA, MC), TA,NIC of N 1, Pu( N 1, N 1).

10. This M D 5 alongwith its components would be encrypted using Pr(AS 1, AS 1) to generate DS[AS 1, N 1,Pr(AS 1, AS 1)]

11. This DS and Pu (AS 1, AS 1) will be known as token T 1 for Node 1 for this net work.

4. Now, AS 1 will generate MD 3 from DS[MC, N 1, Pr(CA, MC)], Pu, (N 1, N 1), TA, Pu,(CA, MC).

5. Now AS1 will match MD 2 and MD 3, if it matches, it proves the integration and the ownership of message received by AS 1.

12.5. Binding Update Message

Node 1 moves from Network NW 1 having AS 1 to network NW 2 having AS 2 as shown in above Fig. 10.
5. AS 2 will decrypt Token T 1 using Pu(AS 1, AS1), this decryption will give DS,[MC,AS 1, Pr( CA, MC)], Pu(CA, MC), MD 5, TA, NIC of N 1, Pu(N 1, N 1). After checking the integration of T 1, AS 2 will verify AS 1 with CA. After verification of AS 1, N 1 will also be verified.

6. This T 2 will be sent to N 1 to authenticate this node in this net work.

7. Now N 1 will encrypt T 2 using Pr( N 1, N 1) and now this encrypted T 2 would be sent to AS 1 as binding update message.

8. AS 1 is already having the public key of N 1 i.e. Pu( N 1, N 1). Now AS 1 will decrypt binding update message received from node N1, using the Public key of node N1 stored in AS1’s Database. After decryption, integration of Binding update message is performed. The integration of Binding Update message proves the authenticity of message.

9. Now AS1 will store this Care-of-address of node N1.

Figure 11: Exchange of Messages

Now authentication Server AS1 will send this Care-of-address to the correspondent node after encrypting it with the public of correspondent node.

The above mentioned scheme, for securely and efficiently services, is followed for exchanging the messages between Super MAP and Sub MAP in Dynamic HMIPv6.

13. CONCLUSION

The future of networking is Mobile Networking. If it is combined with authentication of nodes and encryption of messages, it can become the ultimate solution for all security issues and mobile networking issues.

Hierarchical MIPv6 though solves problems relating to MIPv6, still is not a perfect solution for mobile networking. Although, HMIPv6 reduces the Binding Update message cost to network but if the size of MAP increased bottle neck can be created at MAP. To provide smooth and secure communication in MIPv6 Dynamic MAP in HMIPv6 with token based authentication scheme is presented. This scheme will help to keep MAP as bigger as possible and avoid bottle neck even if the load increases. Further, it will also provide securely exchange of Binding Update and other messages.

REFERENCES

[4] packetlife.net/blog/2008/au/g/8/ipv6-neighbor-discovery/
[16] T. Aura; Request for Comments: 3972; March 2005; Cryptographically Generated Addresses (CGA)


