Issues of Security in Routing Optimization at Mobile IPv6

Vijaya Raju MULLAGIRI [1] Igli HAKRAMA[1], Jonilda BAHJA[1] , Erion SEVAJ[1]
vrmullagiri@epoka.edu.al , ihakrama@epoka.edu.al, bahjajonida@yahoo.com,
Erion Sevaj esevaj@gmail.com

[1.] *Department of Computer Engineering, EPOKA University, Tirana, ALBANIA*

Abstract

Mobile Internet Protocol version 6 (MIPv6) adds the mobility function to IPv6. An IPv6 host that supports the Mobile IPv6 function can move around the IPv6 Internet. A connection between two nodes is maintained by the pairing of the source address and the destination address. The IPv6 node address is assigned based on the prefix of home network. The assigned address on a given network becomes invalid when the host leaves that network and attaches itself to another network. The reason for this problem came from the nature of IP addresses when a node visits a foreign network: it is still reachable through the indirect packet forwarding from its home network. This triangular routing feature supports node mobility but increases the communication latency between nodes.

So it can be supposed to be overcome by using a Binding Update (BU) scheme, which let nodes to update IP addresses and communicate with each other through direct IP routing. To protect the security of Binding Update, a Return Routability (RR) procedure is developed which results vulnerable to many attacks. In Route Optimization, the mobile node sends the binding message to its peer node, the message contains the new address of the mobile node, called as Care of Address, which confirms that the mobile node is infect moved to the new location from its Home Network. After receiving the binding message, the peer node sends all packets which are destined to the Mobile's Home Address to the Care of Address.

There are many security risks involved, when a malicious node might be able to create a connection with the mobile node by sending the false binding messages. By doing so malicious node can divert the traffic, can launch the DOS Attacks and can also resend the authenticated messages, etc. So considering these security issues, we will discuss for a secure protocol which prevents the attacker to establish false connections and assures the secrecy and integrity of the mobile node and its peers.

Keywords*:* Mobile Internet Protocol version 6 (IPv6), Home Agent, Care of Address, DOS attacks, Security

1. Introduction

The Internet Protocol (IP) makes possible the connection in a wireless and non-wireless network. Mobile IP support different mobile data and wireless networking applications like Wireless local area networks WLAN , Wireless wide area networks, Wireless personal area networks (WPAN), Broadband wireless access network (BWA)etc,[13].IPv6 is an IP-layer protocol that is designed to provide mobility support. It allows an IPv6 node to arbitrarily change its location in the IPv6 network while maintaining the same IP address. Route optimization in Mobile IPv6 is used to eliminate inefficient triangle routing, [1].Different methods were proposed to secure route optimization like: Return routability (RR) which is an infrastructure less, lightweight procedure that enables a Mobile IPv6 node to request another IPv6 node to check and test the ownership of its permanent address in both home network and current visited network. RR protocol is used only to protect messages but can not detect or prevent an attacker tampering against data, [13].To ensure the accuracy and integrity of the collected data, the Network Time Protocol (NTP) was used between the packet generator (Mobile Node) and packet receiver (Correspondent Node) to synchronize the time. The aim is to make communication between Mobile Node and Correspondent Node as secure as IPV4 today, [13].

2. Mobile IPv6 Mobility

Mobility is becoming an increasingly critical need because of the inclusion of IP stacks in PDAs, mobile phones, and various forms of notebooks and PCs. The goal of mobility is to perform intended service anytime, anywhere, anyhow, [13]. In IPV6 any node can be a mobile or stationary node, as we cannot differentiate between mobile and stationary node just looking on the IPV6 address [3]. Like stationary nodes, a mobile node is attached to a particular network, known as its home network. In Figure1 is shown the Mobile IPv6 architecture. A mobile host, called mobile node (MN), may have multiple IP addresses at the same time. When it is currently attached to its home network, it is only addressed by its home address (HoA) (Fig.2). The Home Address remains unchanged regardless of where the mobile node is attached to the Internet, unless its home subnet prefix is changed.

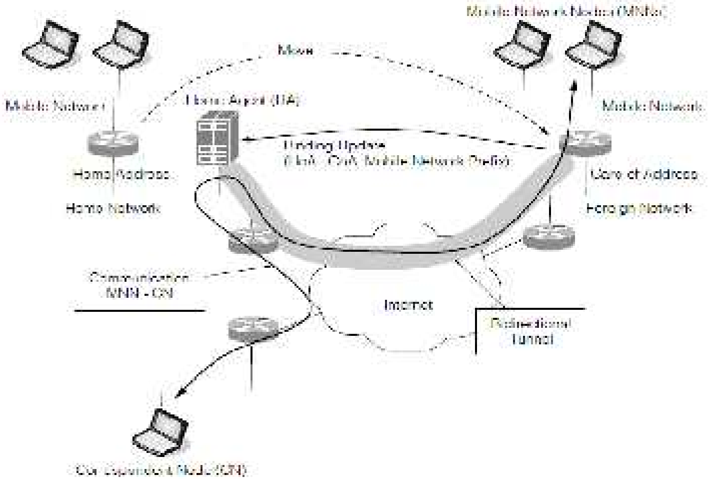


Figure 1

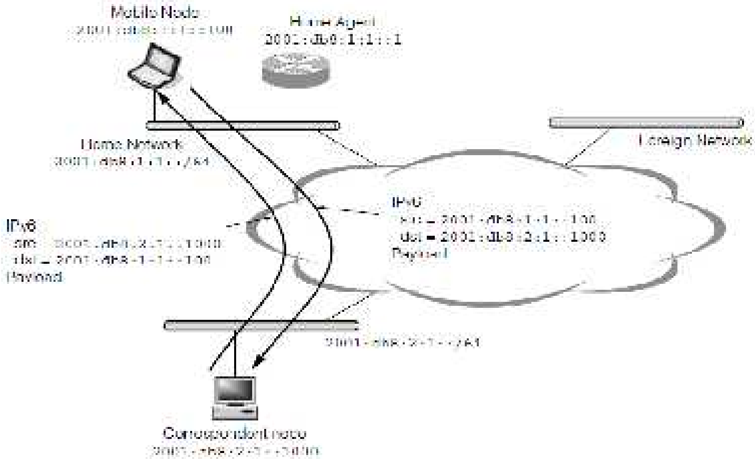


Figure2.

The home agent (HA) is a router on the mobile node's home link. Any node communicating with a mobile node is called a correspondent node (CN). It may be either a stationary node or a mobile node. An IPv6 address can be divided into two parts: the first part is the subnet prefix, and the second part is the interface identifier. An IPv6 node periodically broadcasts Router Solicitation messages and waits for Router Advertisement messages. The IPv6 node can thus discover the subnet prefix from the Router Advertisement message, and then combine this subnet prefix with its own embedded Media Access Control (MAC) address to form a new IPv6 address. This feature in IPv6 is called auto-configuration. A Mobile Node is able to acquire a temporary local address, called the Care-of Address (CoA) without the use of a foreign agent (FA). The Home Agent remembers the association between the

Home Address and the Care-of Address of a mobile node, referred to as "binding". When a (MN) is away from its home network, all messages sent to its Home Address will be routed to the Mobile Node by its Home Agent. The (HA) keeps a binding list (called **Binding Cache**) so that it is able to know the current binding between a HoA and a CoA. A Mobile Node registers and updates its primary CoA associated with its HoA by sending **a Binding Update (BU)** message to the Home Address. (Figure3).

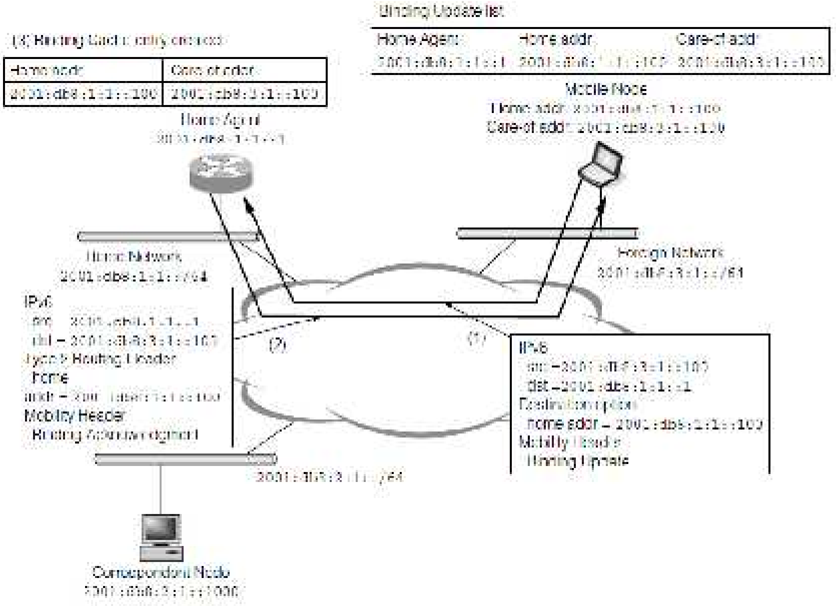


Figure .3

Wherever it is, any packet sent to the MN in its HoA will be forwarded to its CoA from Its HA. Even if an MN moves to a new network, all packets of its existing transport-layer sessions will be routed to its new CoA. This is called bidirectional tunneling in Mobile IP. Mobile IPv6 provides security between the HA and the MN by a secure tunnel with IPSec. Packets from the CN are routed to the HA; then they will be encapsulated in the IPSec headers and destined to the MN and vice-versa (Figure 3). The HA decapsulates these packets, and then forwards them to the destination. The CN working this scenario does not need to implement the Mobile IP protocol. In addition, it is notable that the communication link between the CN and the HA is not secure. In order to improve the efficiency of routing data packets, Mobile IPv6 defines a route optimization (RO) procedure which improves reliability by reducing dependence on the home network, the HA and the path to and from it.

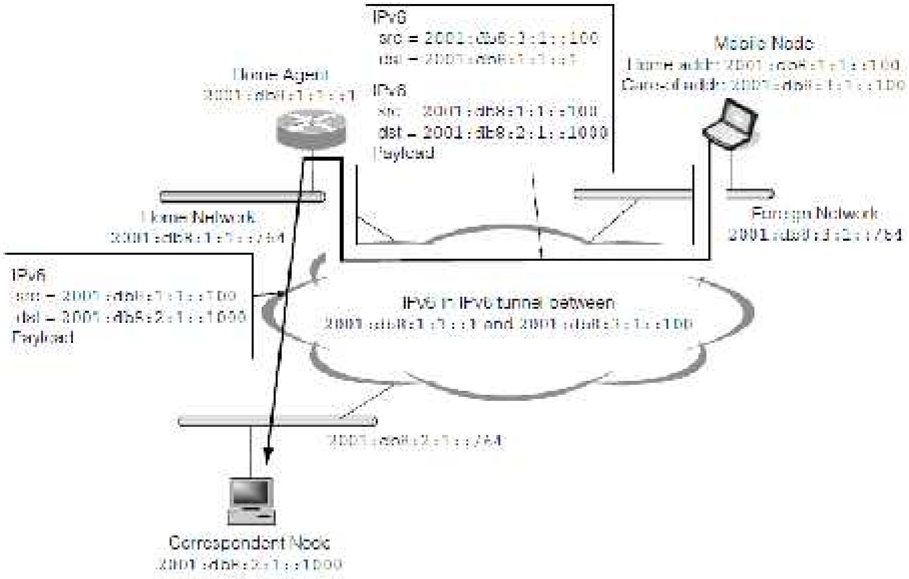


Figure 4

3. Route Optimization Protocol

To enhance the performance, Route Optimization protocol is used. Route optimization is a technique which enables a mobile node and a correspondent node to communicate directly, bypassing the home agent completely, [4]. The concept of route optimization is that, when the mobile node receives the first tunneled message, it informs correspondent node about its new location, i.e. care-of-address, by sending a binding update message. The correspondent node stores the binding between the home address and care-of address into its Binding Cache, [5].

Route Optimization provides four main operations and these are:

a. *Updating binding caches,*

b. Managing smooth handoffs between foreign agents,

c. Acquiring registration keys for smooth handoffs,

d. Using special tunnels.

a. Updating binding caches: Binding caches are maintained by correspondent nodes for associating the home address of a mobile node with its care-of address. A binding cache entry also has an associated lifetime after which the entry has to be deleted from the cache. If the correspondent node has no binding cache entry for a mobile node, it sends the message addressed to the mobile node's home address. When the home agent intercepts this message, it encapsulates it and sends it to the mobile node's care-of address. It then sends a Binding Update message to the correspondent node informing it of the current mobility binding.

b. Managing smooth handoffs between foreign agents: When a mobile node registers with a new foreign agent, the basic Mobile IP does not specify a method to inform the previous foreign agent. Thus the datagram in flight which had already tunneled to the old care-of address of the mobile node are lost. This problem is solved in Route Optimization by introducing smooth handoffs. Smooth handoff provides a way to notify the previous foreign agent of the mobile node's new mobility binding. If a foreign agent supports smooth handoffs, it indicates this in its Agent Advertisement message. When the mobile node moves to a new location, it requests the new foreign agent to inform its previous foreign agent about the new location as part of the registration procedure. The new foreign agent then constructs a Binding Update message and sends it to the previous foreign agent of the mobile node. Thus if the previous foreign agent receives packets from a correspondent node having an out-of-date binding, it forwards the packet to the mobile node's care-of address. It then sends a Binding Warning message to the mobile node's home agent. The home agent in turn sends a Binding Update message to the correspondent node. This notification also allows datagram sent by correspondent nodes having out-of-date binding cache entries to be forwarded to the current care-of address.

c. Acquiring registration keys for smooth handoffs: For managing smooth handoffs, mobile nodes need to communicate with the previous foreign agent. This communication needs to be done securely as any careful foreign agent should require assurance that it is getting authentic handoff information and not arranging to forward in-flight datagram to a bogus destination. For this purpose a registration key is established between a foreign agent and a mobile node during the registration process. The following methods for establishing registration keys have been proposed in the order of declining preference:

- *If the home agent and the foreign agent share a security association, the home agent can choose the registration key.*
- *If the foreign agent has a public key, it can again use the home agent to supply the registration key.*
- *If the mobile node includes its public key in its Registration Request, the foreign agent can choose the new registration key.*

d. Using special tunnels: When a foreign agent receives a tunneled datagram for which it has no visitor list entry, it concludes that the node sending the tunneled datagram has an out-of-date binding cache entry for the mobile node. If the foreign agent has a binding cache entry for the mobile node, it should re-tunnel the datagram to the care-of address indicated in its binding cache entry. On the other hand, when a foreign agent receives a datagram for a mobile node for which it has no visitor list or binding cache entry, it constructs a special tunnel datagram. The special tunnel datagram is constructed by encapsulating the datagram and making the outer destination address equal to the inner destination address. This allows the home agent to see the address of the node that tunneled the datagram and prevent sending it to the same node. This avoids a possible routing loop that might have occurred if the foreign agent crashed and lost its state information.

4. Security and Threats

Route optimization protocol makes mobile IPV6 more vulnerable. The attacker can either corrupt binding message, or it can change the destination address so that packets to be delivered to the false address of the attacker. Secrecy and integrity of communication is no more valid and can lead to denial-of-service (DoS) attacks. Different attacks which are possible in MIPV6 are described as follow:

4.1. Attacks against Address 'Owners' ("Address Stealing"): In address stealing an attacker illegitimately claims to be a given node at a given address, [2] and tries to "steal" traffic destined to that address. It is the most dangerous attack, where traffic reaches to the malicious node instead of reaching to the actual destination. There are different variant of this attack;

4.1.1. *Basic Address Stealing*: If Binding Updates were not authenticated at all [2], an attacker can send spoofed binding updates from anywhere in the Internet. Any IPv6 address any node including stationary node as well, is vulnerable.

4.1.2. *Attacks against Secrecy and Integrity*: By spoofing Binding Updates, an attacker could redirect all packets between two communicating nodes to itself, [2]. Sending a false BU to correspondent node, the attacker could get control over the data intended between MN and CN. It means that attacker can hijack the connections opened between them. The attacker could also launch man-in the-middle attack by sending spoofed BU to both MN and CN. By doing so all traffic between two nodes will pass through the attacker. Hence, the attacker would be able to see and modify the packets sent between MN and CN.

4.1.3. *Basic Denial-of-Service Attacks*: By this attack, the attacker prevents the legitimate node to access the resources of the node (victim of attack). This attack might stop or disrupt communication between the nodes, [2]. This attack can be launched on any Internet node.

4.1.4*. Replaying Binding Updates*: An attacker may replay the binding message which is previously authenticated by the correspondent node. Hence attacker can direct packets to the mobile node's previous location.

4.2. **Basic Flooding**: In this attack, the attacker redirects heavy data stream, which is intended for Mobile Node from Correspondent Node, to the target address. This attack is serious in nature because by doing so target receiving cache is over flood, which also lead to DoS attacks.

4.3**. Reflection and Amplification**: In this attack, attacker forces node to send more number of packets to the target than the attacker sent to the node. Reflection is particularly dangerous as packets are being reflected multiple times. If packets are sent into a looping path, this can halt the target node as well as the sender.

5. Securing Route Optimization

We can secure the route optimization by using PKI with IPSec, [6]. But the protocol must work between any mobile node and any other Internet node that have no previous relationship, and so we cannot assume the existence of a global PKI or other global security infrastructure, [6]. Many approaches were suggested by different authors to make route optimization secure, which prevents all of the major threats, which were described above. But those approaches cost in terms of packets, delay and processing is excessive. Here the goal has been to propose a complete protocol whose security is close to that of a static IPv4 based Internet, and whose cost in terms of packets, delay and processing is not excessive. In our approach we use the idea of public and private key, but without PK Infrastructure. The idea is simple, Correspondent Node generates the pair of public and private key, any other Internet node doesn’t need to verify the public key of the Correspondent Node. Same for Home Agent, which generates the public and private key pair for all of its connected nodes (including Mobile Node), and handover each different pair to the particular node, and Home Agent makes the entry into its database that which pair of key is assigned to which node. Home Agent acts like a Certification authority (CA), for the connected nodes. So assume that the MN moves to the new location and registers its new care-of address with the Home Agent. Any message from Correspondent Node, which was communicating with Mobile Node, is tunneled to the mobile’s care-of-address by Home Agent, (As Shown in Fig.1a).On receiving the tunneled message, the route optimization protocol is activated; in which MN directly communicates to the Correspondent Node. On receiving first tunneled packet by HA, RO is initiated in which MN sends BU message to the Correspondent Node; As Binding Update is not authenticated yet so Correspondent Node rejects the packet. As shown in Fig. 1 (b), Correspondent Node sends public key in plain text to the mobile’s home address. The HA intercepts the message and forwards it to the MN via a secure tunnel. The MN then encrypts its BU with the public key of CN.

Request = [EncCN_pub (BU)]

This mechanism is called return-routability test for the home address because the mobile node must return to the correspondent (a function of) a value sent by the correspondent to the home address .This way, the correspondent verifies that the mobile is associated with its home agent and it can receive messages at its home address. This protocol avoids from the Basic Address Stealing, because the attacker cannot illegitimately claims to be a given node at a given address due to the return routability test for the home address, where Correspondent Node verifies that the Mobile Node’s original attachment with the Home Network. Attacks against Secrecy and Integrity are also not possible in a sense that BU is encrypted with the public key of CN, thus only Correspondent Node is able to decrypt that message. Reflection and Amplification is also not possible due to the fact that Correspondent Node only sends one packet, i.e. public key to the HA on receiving one packet, i.e. BU. This variant of protocol is sufficient to authenticate the sender of the binding update, but the sender can send false BU, and can launch the attacks such as Basic Denial-of-Service Attacks, Replaying Binding Updates and Basic Flooding etc. So some variations are required in the above protocol.

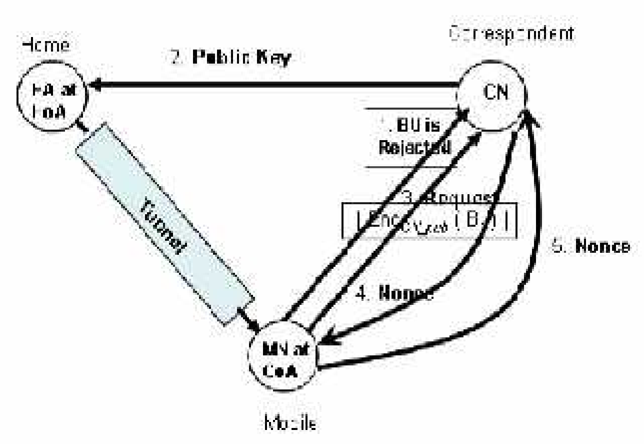


Figure5a.

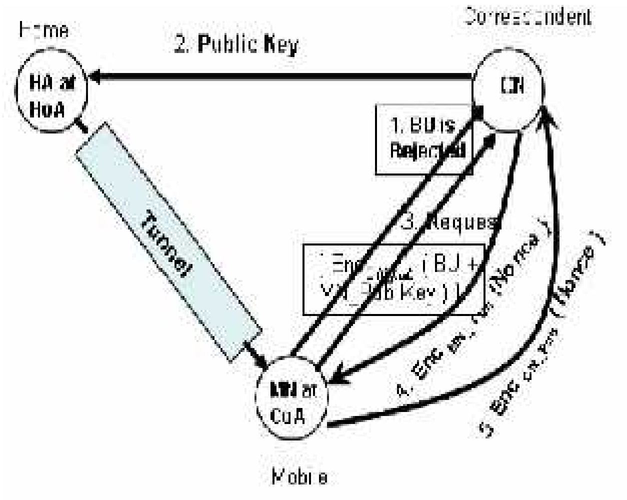


Figure5b.

Now we modify the idea and we say that Correspondent Node sends a Nonce to the MN, as shown in Fig. 5a, When the Correspondent node receives the packet; it decrypts the packet by its private key and gets the BU out of the packet. CN then generates a Nonce and sends this Nonce directly to Mobile Node, to verify that whether the MN's address is same as mentioned in BU. MN will reply to CN by sending the same Nonce. This proves to the CN that the mobile is able to receive messages sent to the new care-of address. This mechanism is called return-routability (RR) test for the care-of address [7]. Now attacker cannot launch Replaying Binding Updates Attack, because the attacker cannot re-authenticate the BU message, as correspondent will not receive any acknowledgement (Nonce) from MN's old address, so CN will not authenticate the address. Basic Denial-of Service Attacks are still possible because the attacker can initiate the communication and sends the false BU. When CN will send Nonce to verify the target position, and then attacker steals the packet and sends the same Nonce to the correspondent. The CN will verify and start sending traffic to the unwanted node. This attack becomes more severe when the attacker initiates CN to send the video stream to the target. We may say that Correspondent Node will soon stop transmitting the video stream because it does not receive acknowledgments from the target node. Unfortunately, this does not work much because the attacker can spoof the acknowledgments. In this case, the attacker initiates the communication and received the first packets of the data stream; so it knows the initial TCP sequence numbers and can spoof TCP acknowledgments. The attacker only needs to send one acknowledgment per TCP window, which will cause CN to send a large data stream to the target. As recipient of unwanted TCP packets usually sends a TCP Reset signal to the source of the packets, which puts in immediate stop to the data stream. So readers may say that target can stop the communication by sending TCP Reset signal. Unfortunately, this does not work as well in our case. The packets sent by CN to the target have a routing header that says the packets are intended for HA [reference 6]. When the IP layer in the target stack processes the routing header, it encounters a strange address i.e. home address of the target, and drops the packet without ever processing the following TCP header. Thus, no TCP Reset will ever be sent. This problem can be tackled by securing the communication between MN and CN while BU is being authenticated.

Request = [EncCN_pub (BU + MN_Pub Key)] EncMN_Pub (Nonce) EncCN_Pub (Nonce)

MN sends its BU message and its public key, both encrypted by the public key of the CN. CN generates the Nonce and sends it by encrypting with the public key of MN, where MN decrypts the message and gets the Nonce and verifies that desired CN had replied. It then sends the same Nonce, encrypted by the public key of CN, to CN. Where CN decrypts the message and gets back the same Nonce, which it sent to MN. Now CN can now that MN is actually moved to the new location and its new location is also verified. Now attacker cannot launch Basic Denial-of-Service Attacks and Basic Flooding Attacks because the communication between MN and CN is secured while BU is being authenticated, so attacker cannot send spoofed BU, because the destination address in BU is authenticated securely. In this way the protocol works against major threats in the MIPV6.

6. Comparison of Two Techniques

Techniques work against the attacks so if we compare the approaches in terms of cost of packets and the delays. Referred to Fig. 3, Mobile Node sends two Init messages to CN, so that to avoid from the Amplification and Reflection Attacks; and CN sends two keys K0 and K1 so that to do return-routability test for the home and the correspondent address. The Figure 4 compares two techniques in terms of packets sent by each. Fig. 4(a) shows the number of packets sent in [6], according to Fig. 3, where 4(b) shows the number of packets sent in our protocol, according to Fig. 2(b). Its is shown clearly that total 7 packets are required for authenticating BU in 4(a), where total of 6 packets are required in 4(b). Hence, our protocol is better over [6], in terms of packets communicated for BU authentication.

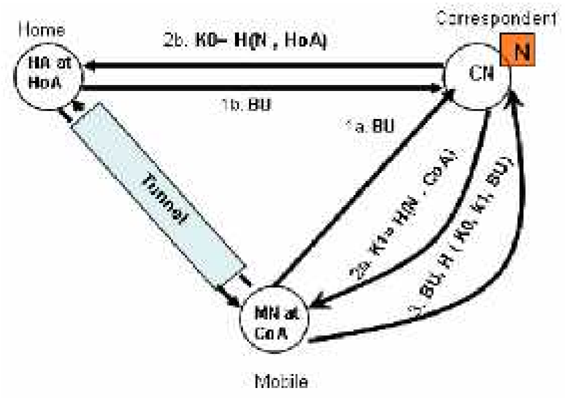
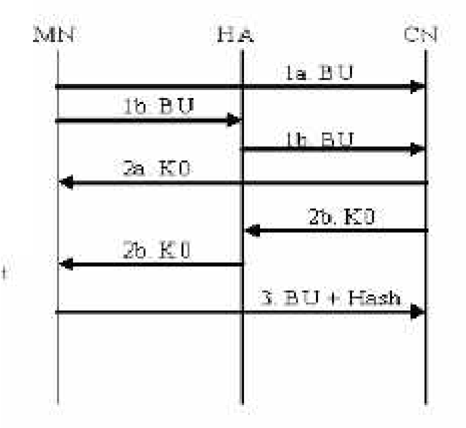


Figure3.



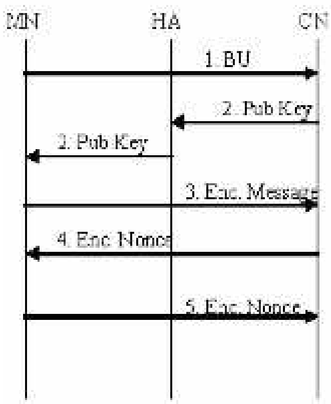


Figure4a. Figure4b.

When a mobile node is being authenticated from a large number of correspondents, then we can see the major difference between two protocols. When the MN authenticates itself with the large number of correspondents, it sends as more packets in [6], as the total number of CNs with which authentication occurs, than in our protocol. When the authentication occurs between the MN and 10 CNs, then the MN sends 70 packets in protocol [reference 6], whereas it send 60 packets in our protocol So our protocol's performance become significant against the protocol described in [reference 6], when MN authenticates itself with greater number of CNs. Authentication time in our protocol is less than to the one proposed in [reference 6]. According to the authentication process shown in the Figure 4, for authentication, messages travel twice through home agent in the protocol describe in [reference 6], whereas in our approach the packets pass only once through home agent. As we know that home agent tunnels the messages to the new care-of address of the MN. So it takes some time to add tunneling header and encrypting the message. This overhead is appeared twice in [reference 6], but once in our protocol. Hence our protocol also reduces the delays.

7. Conclusions

In conclusion we have described how to make Mobile IPv6 route optimization protocol more secure. While proposing this protocol, we kept in mind that the Mobile IPv6 route optimization security design was never intended to be fully secure. Instead, as we stated earlier, the goal was to be roughly as secure as Non Mobile IPv4. We started from describing major threats faced by Mobile IPV6, and then formulated our approach against these threats. The ideas presented in this paper, is based on asymmetric cryptography without public key infrastructure. At the end we compared our technique with the famous technique proposed in [reference 6]. Our results show clearly that our protocol is better in performance, with less delays and the less number of packets sent for authentication, which proves the efficacy of our protocol. We hope that this work will help secure other Internet mobility protocols as well.

Reference

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", Internet Draft draft-ietfmobileip-ipv6-22.txt, work in progress, May 26, 2003

[2]S. Zeadally and N. Deepakmavatoor, "Mobile IPv6 Support for Highly Mobile Hosts", in Proceedings of IASTED International Conference on Communications Systems and Networks (CSN'03), Benalmadena, Spain, September 2003.

[3] W. Al-Salihy, Azman Samsudin, and R.Sureswaran, "New Approach to Secure Mobile IPv6 Signals", in IASTED, 22 April2005.

[4]W. Al-Salihy, Azman Samsudin, and R. Sureswaran, "New Approach to Secure Mobile IPv6 Signals", in IASTED, 22 April 2005.

[5] Tuomas Aura. "Mobile IPv6 Security", in 10th International Workshop, vol. 2845 of LNCS, pg. 215-228, Cambridge, UK, April 2002. Springer2003.

[6] http://www.ietf.org/id/

[7] Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete "Deploying IPv6 Networks"

[8 Migrating to IPv6, A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks

[9] Mobile Inter-Networking with IPv6, Concepts, Principles, and Practices

[10] Security in an IPv6 Environment