Security Issues in Mobile IPv6

Arun Kumar Tripathi
Department of Computer Application
Krishna Institute of Engineering and Technology,
Ghaziabad, India

Anchal Srivastava,Harish Pal,
Somendra Tiwari, Sukrati Pandey
Krishna Institute of Engineering and Technology,
Ghaziabad, India

ABSTRACT
Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. When a node moves and visits a foreign network, it is still reachable through the indirect packet forwarding from its home network. This triangular routing feature provides node mobility but increases the communication latency between nodes. The route optimization reduces packet loss tremendously but suffers from security threats. In this paper we have discussed various existing MIPv6 security issues and threats with their solutions.

Keywords
MIPv6, Security, Return Routability Protocol, BindingUpdate,authentication,cryptographically generated address.

1. INTRODUCTION
The tremendous advancements in the field of communication and information technology over the last decades have influenced our lives greatly. IP-based next-generation wireless networks are widely adopted for transporting media such as voice, data, etc. Mobile IP is the mobility protocol widely used for Internet and standardized by IETF in 1995.

Mobile IP is intended to enable nodes to move from one IP subnet to another. It is just as suitable for mobility across homogeneous media as it is for mobility across heterogeneous media. That is, Mobile IP facilitates node movement from one Ethernet segment to another as well as it accommodates node movement from an Ethernet segment to a wireless LAN, as long as the mobile node's IP address remains the same after such a movement. The Mobile IP is categorized into IPv4 [1] and IPv6 [2]. When an IPv6 node changes its location, it might also change its link. When an IPv6 node changes its link, its IPv6 address might also change in order to maintain connectivity. There are mechanisms to allow for the change in addresses when moving to a different link, such as stateful and stateless address autoconfiguration for IPv6. However, when the address changes, the existing connections of the mobile node, which are using the address assigned from the previously connected link, cannot be maintained and are ungracefully terminated.

The key benefit of Mobile IPv6 is that even though the mobile node changes locations and addresses, the existing connections through which the mobile node is communicating are maintained. To accomplish this, connections to mobile nodes are made with a specific address that is always assigned to the mobile node, and through which the mobile node is always reachable. Mobile IPv6 provides Transport layer connection survivability when a node moves from one link to another by performing address maintenance for mobile nodes at the Internet layer.

Mobile IPv6 (MIPv6) provides transparent mobility [3] to MN. It contains four key elements: mobile node (MN), Correspondent node (CN), Home Agent (HA) and Access Router (AR). The architecture of MIPv6 is shown in Fig 1.

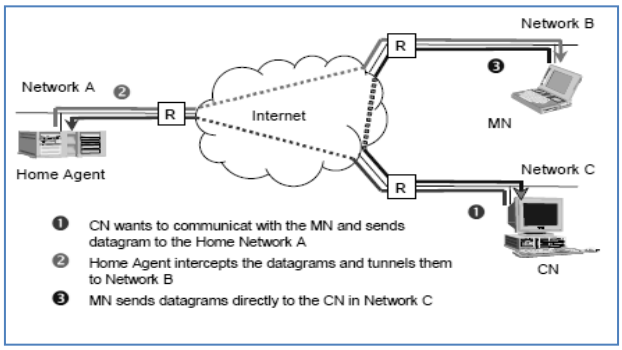

Fig. 1: MIPv6 Architecture

Mobile IPv6 provides seamless handover [4]. As soon as MN moves to new network known as foreign network a prefix is received via router advertisement (RA) message through access router to which it is connected. MN randomly generates a 64-bit suffix and combines with the prefix obtained from the router to get the 128-bit IPv6 address known as care-of-Address (CoA)[1].

Once the CoA is configured the MN should registers its CoA with HA via sending binding update message to HA. HA stores (HoA, CoA) pairs in binding cache. To keep this mapping up-to-date, MN has to periodically inform its Home Agent (HA) about its new CoA via Binding Update (BU) message. After successful registration MN and CN can communicate in two ways. The first mode is known as "Bidirectional" mode. In this mode, CN continues sending its packets to MN's Home Address and then, the Home Agent intercepts the packets and forwards them to the MN Care-of-Address. However, when MN wishes to send CN a data packet, then it is routed directly to CN. Triangle routing [2] suffers from a long trip time that affects real time traffic. The technique used in forwarding data packets is represented in Figure 2.

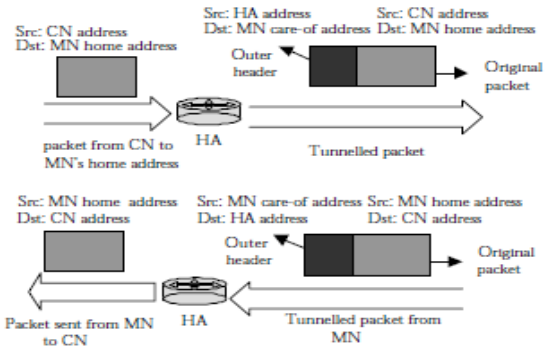

Fig. 2: Packet forwarding Mechanism

While forwarding data packets from source to destination triangular path a triangular path [5] has to establish. This causes loss of data packets. To overcome from this problem route optimization technique is used. Route optimization is about routing packets between a mobile node and a correspondent node, using the shortest possible path (as it is normally done between two communicating hosts relying on normal routing). The mobile node is aware when packets are routed through the home agent when it receives tunneled packets addressed to its home address.

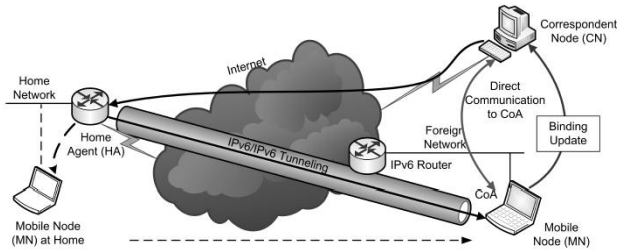

Fig. 3: Route Optimization Mechanism

Fig 3 illustrates route optimization for tunneling path.
Route optimization reduces the packet loss in MIPv6 network, but it suffers from security problems such as how a MN can verify the CN and vice versa.
The rest of the paper organized as follows: Section II deals with classification security issues in MIPv6. Section III describes solutions to problems in section II. Conclusion is made in Section IV.

2. SEUCRITY ISSUES IN MIPv6

Although MIPv6 is have a lot of features in comparison to MIPv4. But it suffers from various security threats. Some of them are as follows:

A. Secure Route Optimization

To enhance the performance, Route Optimization protocol is used. Route optimization [5] is a technique which enables a mobile node and a correspondent node to communicate directly, bypassing the home agent completely. The concept of route optimization is that, when the mobile node receives the first tunneled message, the mobile node 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. Then after communication directly take place between MN and CN. The route optimization discussed is not secure because there is no authentication mechanism between MN and CN.

B. Connection hijacking:

The connection-hijacking [6] attack is shown in Figure 4. A, B and C are IPv6 addresses. The Internet nodes A and B are honest and communicating with each other. An attacker at the address C sends a false binding update to B, claiming to be a mobile with the home address A. If B, acting in the role of a correspondent, believes the binding update and creates a binding, it will redirect to C all packets that are intended for A. Thus, the attacker can intercept packets sent by B to A. The attacker can also spoof data packets from A by inserting a false home-address option into them. This way, it can hijack existing connections between A and B, and open new ones pretending to be A. The attacker can also redirect the packets to a random or non-existent care-of address in order to disrupt the communication between the honest nodes. It has to send a new binding update every few minutes to refresh the binding cache entry at the correspondent.

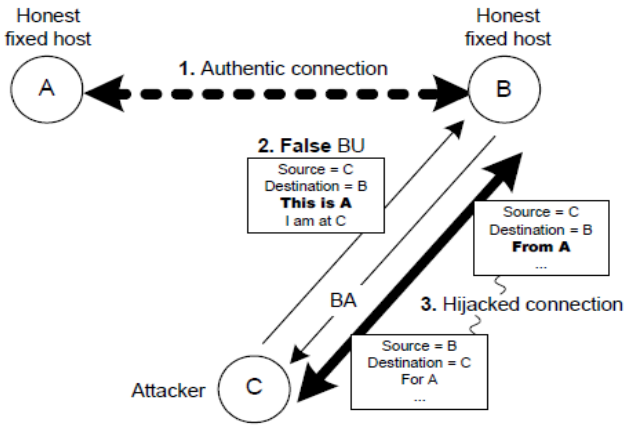

Fig. 4: Representation of connection Hijack technique

C. Firewall traversal Problem in MIPv6

Firewall technologies do not support Mobile IPv6 or are not even aware of IPv6 mobility extension headers. Since most networks in the current business environment deploy firewalls, this may prevent future large-scale deployment of Mobile IPv6. Secondly, another mode of communication in Mobile IPv6, namely Bi-directional Tunneling, does not work under some scenarios, for example, when a firewall is placed in the access network or the home network. In addition, it is difficult or, in some scenarios, even impossible for the Mobile IPv6 Binding Update messages to traverse Firewalls [7] as they are encapsulated using IPsec ESP. In summary, these deployment issues with firewalls occur due to the nature that the commonly used firewalls possess.

D. Eavesdropping

Eavesdropping [9] is type of a theft of information attack. It may be passive or active. A passive eavesdropping attack happens when an attacker start to listen to the traffic and get useful information by gathering the session data that is transferred between mobile device and its home agent. In case of wireless network an intruder is able to receive packets transmitted by radio signals. In case of active eavesdropping 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. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances

E. Denial of Service

In denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) [9] is an attempt to make a MIPv6 based network resource unavailable to its intended users. This is a very harmful attack for commercial providers whose services are dropping. Some of the methods for DoS are SYN Flood, SYN-ACK Flood, UDP Flood, ICMP Flood etc.

3. SOLUTIONS TO VARIOUS SECURITY ISSUES

To overcome from above existing problems some solution are proposed. The solutions try minimizing the problems in large scale.

F. Return Routability for Secure Route Optimization

Return Routability (RR) [10],[11] provides adequate authentication between a MN and a CN. First, it ensures that the

MN is able to receive messages with its HoA and CoA, after that it protects the binding messages between the MN and the CN. The MN can receive messages with the HoA only if the MN has created a valid binding to the HA in advance.

In Return Routability HoTI and CoTI messages are sent simultaneously by the Mobile Node to the Correspondent Node. Upon the receipt of the HoTI and CoTI messages, the Correspondent Node computes two cookies based on the information contained in the messages, combined with its own secret key and nonce value. These cookies are inserted into the respective HoT and CoT messages, which are then sent back simultaneously to the Mobile Node. The sequence diagram is depicted in Figure5.

Once the Mobile Node has received both the HoT and CoT messages, it has the cookies necessary to send the BU to the Correspondent Node.

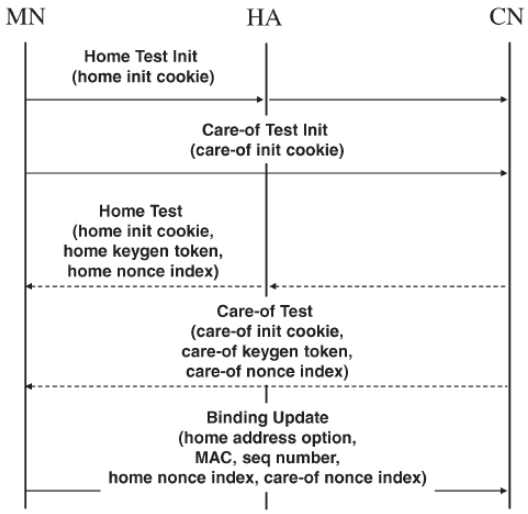

Fig. 5: Return Routability Test

It hashes together the cookies to form a session key which is then used to authenticate the BU that is sent to the Correspondent Node. When the Correspondent Node receives the BU, it can verify the information using its cookies and create a binding cache entry for the Mobile Node. The Correspondent Node may optionally acknowledge the Binding Update with a Binding Acknowledgemenety. By Return Routability technique, the route is securely optimized.

G. IP Seurity(IPSec)

IPSec consists of a set of cryptographic protocols that provide for securing data communication and key exchange. IPSec is used to authenticate and encrypt packets at IP level. That is why it was naturally the first proposed method for authentication of the binding messages.

The biggest problem with the IPSec [9] method is the key distribution. Key distribution of the IPSec, which is called Internet Key Exchange (IKE), uses either preshared secrets or public keys in the key exchange. When authentication is needed between a MN and a HA, which must have some relationship in advance, because the MN uses services of the HA, the needed secrets might be exchanged beforehand or some private public key distribution can be utilized. After several discussions, IPSec ESP was chosen for binding message authentication between MN and HA instead of IPSec AH. When considering authentication of the binding messages between a MN and some unknown CN, no preshared secret can be used. There doesn't either exist global public key infrastructure that could be utilized, so at least some other key distribution system than IKE is needed. IPSec keep track of this information to guarantee that communication continues to be secure up to the end. It helps to prevent from following attacks

- Spoofing
- Session hijacking
- Electronic eavesdropping
- Man- in -middle

H. Cryptographically Generated Addresses

Cryptographically Generated Addresses [12] is a technique for the authentication of IPv6 addresses that provides an intermediate level of security below strong public-key authentication but above no authentication. The idea, first introduced in a BU authentication protocol, is to select the least significant 64 bits of the IP address (the interface identifier) by computing a 64-bit one-way hash of the node's public signature key. The node signs its location information with the corresponding private key and sends the public key along with the signed data. The recipient hashes the public key and compares the hash to the address before verifying the signature on the location data. This prevents anyone except the node itself from sending location updates for its address. The attraction of this technique is that it provides public-key authentication of the IP address without any trusted third parties or PKI.

Several BU authentication protocols were proposed based on this idea. While the authentication of the sender's IPv6 address would be of little value in most applications, it is exactly what is needed to authorize the binding update. The mobile signs the binding update and attaches its public key to the message. The correspondent can verify without any additional infrastructure that the binding update was signed by the owner of the home address. Nevertheless, this mechanism was rejected by the Mobile IPv6 designers in favor of an even simpler routing-based protocol. The addresses with an embedded public-key hash have since been standardized under the name cryptographically generated addresses (CGA) for use in other security protocols.

These are the solutions of security threats exists in MIPv6 based network. Although these methods are not provides guaranty of optimized communication but provides secure communication.

4. CONCLUSION

In this paper, we have discussed Mobile IPv6 and various threats associated with it. These threats prevent secure communication in MIPv6 based nodes. To make the communication secure some methodologies such as IPSec, cryptographically generated addresses etc. are discussed. The secure communication is possible among MIPv6 node with the help of these methods. In future, these methods can be optimized to reduce the packet loss.

5. REFERENCES

[1] C. Perkins, "IP Mobility Support for IPv4: Revised ", Request for Comments – 5944, Internet Engineering Task Force (IETF), November 2010.

[2] C. Perkins, Ed., D. Johnson, J. Arkko, "Mobility Support in IPv6" , "A Survey of Mobility Support in the Internet" Request for Comment 6275, Internet Engineering Task Force, July 2011

[3] C. Perkins, "Mobile IP: Updated", IEEE Communications Magazine, Volume-40, Number-5, Pages: 66-82.

[4] Z. Zhu, R. Wakikawa, L. Zhang, "A Survey of Mobility Support in the Internet" Request for Comment-6301, Internet Engineering Task Force, July 2011.

[5] MIPv6,www.media.techtarget.com/searchNetworking/Downloads/mobileIPv6.pdf

[6] Tuomas Aura, Michael Roe, " Designing the Mobile IPv6 Security Protocol" , Technical Report MSR TR-2006-42, Page:27.

[7] Jordi Palet Martinez, "Enabling efficient and operational mobility in large heterogeneous IP networks" , ISBN:978-84-691-0647-1, 2008

[8] Qing Li, Tatuya Jinmei, Keiichi Shima, "Mobile IPv6: Protocols and Implementation" Morgan Kaufmann Publishers,2009.

[9] Qiu Ying; Bao Feng , "Authenticated binding update in Mobile IPv6 networks", IEEE- Conference on Computer Science and Information Technology (ICCSIT), Chengdu, Singapore, ISBN: 978-1-4244-5537-9, July 2010, Pages: 307 – 311.

[10] R Radhakrishnan, Majid Jamil, Shabana Mehfuz, Moinuddin, "A robust return routability procedure for mobile IPv6", International Journal of Computer Science and Network Security (IJCSNS), volume-8, No-5, May 2008, pages 243-240.

[11] Youngsong Mun, Kyunghye Lee, Seonggeun Ryu and Teail Shin, "Using Return Routability for Authentication of Fast Handovers in Mobile IPv6", Computational Science and Its Applications (ICCSA 2007), published in Lecture Notes in Computer Science-4706, Volume 2, Published by Springer, ISBN:3-540-74475-4 978-3-540-74475-7, 2007, Page: 1052-1061.

[12] Aura, Tuomas, "ryptographically Generated Addresses (CGA)", White Paper, http://www.6journal.org/archive/00000184/, 2003.