Firewall for Dynamic IP Address in Mobile IPv6

Ying Qiu, Feng Bao, and Jianying Zhou

Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
{qiuying,baofeng,jyzhou}@i2r.a-star.edu.sg

Abstract. Mobile communication is becoming the mainstream with the rapid growth of mobile devices penetrating our daily life. More and more mobile devices such as mobile phones, personal digital assistants, notebooks etc, are capable of Internet access. Mobile devices frequently change their communication IP addresses in mobile IPv6 network following its current attached domain. This raises a big challenge for building firewall for mobile devices. The conventional firewalls are primarily based on IPv4 networks where the security criteria are specified only to the fixed IP addresses or subnets, which apparently do not apply to mobile IPv6. In this paper we propose three solutions for mobile IPv6 firewall. Our approaches make the firewall adaptive to dynamic IP addresses in mobile IPv6 network. They have different expense and weight corresponding to different degree of universality. The paper focuses the study more from practical aspect.

Keywords: Firewall, Mobile IP6.

1 Introduction

Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, such as intranets. All messages entering or leaving the intranet need to pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. In the traditional firewall, the security criteria are specified only for fixed IP addresses or subnets.

Along with the increasing number of 3G networks and WiFi hotspots, people can now easily gain access to the Internet anywhere using their mobile devices, such as mobile phones, personal digital assistants (PDA) and laptop computers etc. Mobile IPv6 [1] enables IP mobility for IPv6 nodes. It allows a mobile IPv6 node to be reachable via its home IPv6 address irrespective of the link and the domain that the mobile attaches to. The Route Optimization is also supported in the mobile IPv6 specification. The Route Optimization technology enables optimized routing of packets between a mobile node and its correspondent nodes.

To build up firewall for mobile devices, we are facing the challenge: the firewalls need a series of fixed IP addresses or subnets to specify the security criteria, meanwhile the roaming mobile nodes need variable IP addresses to indicate their current location so that the mobile nodes can be reached seamlessly. In this paper we analyze the mobile IPv6 specification and firewall technology, and then present in detail of building a dynamic firewall in mobile IPv6 environment. For Ethernet devices, we suggested to

S. Qing, H. Imai, and G. Wang (Eds.): ICICS 2007, LNCS 4861, pp. 467–479, 2007.

employ the feature of MAC address filter. For the mobile nodes with traceable addresses, masking the low 64-bits of source address is a simple and efficient solution. For general mobile nodes, we introduced an extended firewall and the improved Return Routability protocol.

The rest of this paper is organized as follows. Section 2 reviews the basic operation of Mobile IPv6 and firewalls. Section 3 presents our solution for configuring the firewall rules in mobile IPv6 networks. Section 4 describes an analysis of security and performance of our approaches. Section 5 concludes the paper.

2 Mobile IPv6 and Firewall

2.1 Mobility Support in IPv6

In the current IETF Mobile IPv6 specifications [1], every mobile node (*MN*) has a home address (*HoA*), an IP address assigned to a mobile node within its home subnet. A *MN* is always addressable by its home address, whether it is currently attached to its home subnet or is away from home.

While a mobile node roams and attaches to some foreign subnet, it is also addressable by one or more care-of addresses (*CoA*s), in addition to its home address. A care-of address is an IP address associated with a mobile node while visiting a particular foreign subnet. The subnet prefix of the mobile node's care-of address is the subnet prefix of the foreign subnet being visited by the node. A mobile node typically acquires its *CoA* through stateless [3] or stateful (eg., DHCPv6 [4]) address autoconfiguration.

After getting a new *CoA* on the foreign subnet, a mobile node informs its current *CoA* to its home agent (*HA*) [1,5] by sending a Home Binding Update (BU_{HA}) message to the home agent:

$$BU_{HA} = \{Src=CoA,\ Dst=HA,\ Opt=HoA,\ \ldots\ \ldots\ \}$$

As the paper deals with the problem how a MIPv6 packet goes through firewalls, we just discuss and analyze the IP address in the header of a traffic packet and ignore its payload.

The home binding update message creates an association between *HoA* and *CoA* for the mobile node with the specified lifetime at the home agent. *HA* thereafter uses proxy Neighbor Discovery [6] to intercept any IPv6 packets addressed to *MN*'s *HoA* on the home subnet, and tunnels each intercepted packet to *MN*'s *CoA* [1]. To tunnel intercepted packets, *HA* encapsulates the packets using IPv6 encapsulation, with the outer IPv6 header addressed to *MN*'s *CoA*.

The mobile node may also initiates *route optimization* operation with its correspondent node (*CN*) to inform its current *CoA* by sending a Correspondent Binding Update (BU_{CN}) message to the correspondent nodes. Figure 1 shows the procedure:

When *MN* wants to perform route optimization, it sends

$$HoTI = \{Src=HoA,\ Dst=CN,\ \ldots\ \ldots\}$$

and

$$CoTI = \{Src=CoA,\ Dst=CN,\ \ldots\ \ldots\}$$

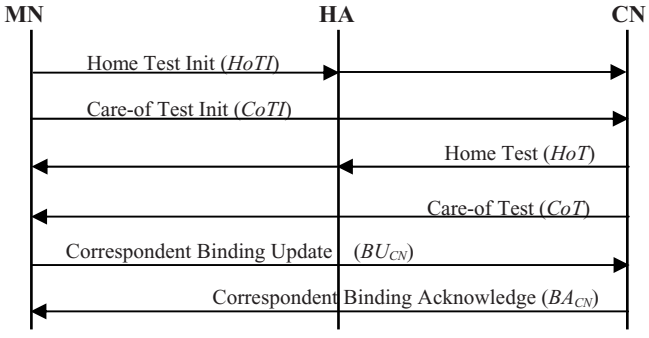

Fig. 1. The procedure of Correspondent Binding Update

to *CN*. *HoTI* tells *MN*'s home address *HoA* to *CN*. It is reverse tunneled through the home agent *HA*, while *CoTI* informs *MN*'s care-of address *CoA* and is sent directly to *CN*.

When *CN* receives *HoTI*, it takes the source IP address of *HoTI* as input and generates a *home cookie* and replies *MN* with *home cookie*

$$HoT = \{Src=CN, Dst=HoA, \ldots \ldots\}.$$

Similarly, when *CN* receives *CoTI*, it takes the source IP address of *CoTI* as input and generates a *care-of cookie* and sends it

$$CoT = \{Src=CN, Dst=CoA, \ldots \ldots\}$$

to *MN*. Note that *HoT* is sent via *MN*'s home agent *HA* while *CoT* is delivered directly to *MN*.

When *MN* receives both *HoT* and *CoT*, it hashes together the two cookies to form a session key which is then used to authenticate the correspondent binding update message to *CN*:

$$BU_{CN} = \{Src=CoA, Dst=CN, HoA, \ldots \ldots\}.$$

Note that *CN* is stateless until it receives BU_{CN} and verifies the authentication MAC_{BU}. If MAC_{BU} is verified positive, *CN* may reply with a binding acknowledgement (BA_{CN}) message

$$BA_{CN} = \{Src=CN, Dst=CoA, HoA, \ldots \ldots\}.$$

CN then creates a binding cache entry for the mobile node *MN*. The binding cache entry binds *HoA* with *CoA* which allows future packets to *MN* be sent to *CoA* directly.

When sending a packet to the *MN*, the *CN* checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses an IPv6 Routing Header [7] to route the packet to the *MN* by way of the *CoA* indicated in this binding. If, instead, the *CN* has no cached binding for this destination address, the node sends the packet normally (i.e., to the *MN*'s *HoA* with no routing header), and the packet is subsequently intercepted and tunneled to the *MN* by its *HA* as described above. Therefore, route optimization allows a *CN* to communicate directly with the *MN*, avoiding delivering traffic via the *MN*'s *HA*.

From the above brief review, we observed that the source/ destination addresses in the packets from/to *MN*s are not fixed. It would occur the transmit problem through firewalls.

2.2 Problem Statement of Mobile IPv6 and Firewall

Firewalls usually decide whether to allow or to drop packets based on source IP address and destination address as well as protocol type and port numbers. RFC4487 [2] analyzed various scenarios involving MIP6 and firewalls. It classified three scenarios of firewall networks:

1) When the correspondent node is within a network protected by firewall(s), the major issue is how the firewall accepts the packets from/to the address *CoA*, which has no associated rule with the diverse *CoA* in the firewall. Requiring the firewalls to update the connection state upon detecting Binding Update messages from a node outside the network protected by the firewall does not appear feasible or desirable, because changing the firewall states without verifying the validity of the Binding Update messages could lead to denial of service attacks.
2) When the *HA* is within a network protected by a firewall, the firewall(s) may drop connection setup requests from *CN*s and packets from *MN*s' *CoA*s if the firewall(s) protecting the *HA* block unsolicited incoming traffic (e.g., as stateful inspection packet filters do).
3) When a mobile node is within or moves from outside into a network protected by firewall(s), the firewall blocks the traffic to the *MN* due to the its new *CoA*.

2.3 IPv6 Address Generation

An interface which uses IPv6 usually gets link-local address and global address allocated at least. Link-local address is used for control functions, while global address is used for usual data communications.

In mobile IPv6, IP address is usually generated by the following three methods: Stateless Address Autoconfiguration, Stateful Address Autoconfiguration & Manual Configuration.

Stateless Address Autoconfiguration [3]
Address autoconfiguration in IPv6 usually means that a node can configure its own IP address, using information on the network.

In IPv6, the 128 bit IP address is separated to two parts: i) network prefix (64 bits), which identifies network; and ii) interface ID (64 bits), which identifies a node (interface). Interface ID is configured by the node on its own (usually derived from the MAC address), and the prefix is advertised by the network (usually router). These two parts are combined to form an IPv6 address.

Stateful Address Autoconfiguration
Stateful Address Autoconfiguration uses a server, such as DHCPv6 [4], to manage and allocate address to nodes.

With DHCPv6, DHCP servers are placed on the network to allocate addresses to a network interface.

Note that the DHCP server manages address information and maintains which address is allocated to whom. In address allocation with DHCP, a node can use only one DHCP server (although there may be multiple DHCP servers on the same network).

Manual Configuration
It means to set IP address to an interface manually. This includes setting a pre-configured address based on a configuration file at the boot.

3 Deploying Firewall in Mobile IPv6

3.1 Traceable IP Address and Untraceable IP Address

From the brief description in subsection 2.3, we know the IP address generated by the method of stateless address autoconfiguration is traceable, because its low 64 bits is fixed even though its prefix depends on the router. In contrast, the IP address obtained by the method of stateful address auto-configuration is untraceable because there is no association between the previous and subsequent addresses of an interface if it attaches different routers.

We can define the following two types of addresses.

Traceable Address: If the series of IP addresses for an interface are derived from certain data (e.g. MAC address), no matter it is generated by manual configuration or stateless autoconfiguration, we call the IP addresses are traceable.

Untraceable Address: If the series of IP addresses for an interface are not derived from certain data, no matter it is generated by manual configuration or stateful auto-configuration or other stateless autoconfiguration [8, 9], we call the IP addresses are untraceable.

In the following subsections, we will discuss how to configure and deploy the firewall in a variety of scenarios. We will focus on how to manage the variation of *MN*'s IP address. Other firewall filtering issues, such as protocol type, port number, etc., will be ignored because they are not changed along with the locations of mobile nodes and can be set in advance.

3.2 Scenario of the CN Protected by Firewall(s)

Figure 2 presents the scenario that the correspondent node of a mobile node is protected by firewall.

Firewall Configuration if *MN*'s *CoA* is Traceable Address
The disadvantage of IPv4 is that its address is only 32 bits meanwhile the MAC address is 48 bits. Therefore the IPv4 address is not able to include the MAC address information. If a mobile node roams to foreign networks, its new IPv4 address is totally

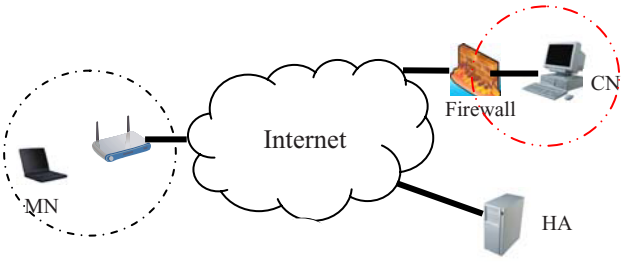

Fig. 2. CN is protected by a firewall

different from its previous IPv4 address and we are not able to trace back any information of its previous address from its new address.

In IPv6, the stateless address autoconfiguration is wildly deployed due to efficiency and lightweight. If a *MN*'s IPv6 address is generated by the stateless address autoconfiguration, the IPv6 address always contains the interface identity (derived from the unique MAC address). Hence, if two IPv6 addresses share the same 64-bit interface identity, we consider them to be the same device.

Therefore, the firewall rules for a mobile node could mask the low 64-bits of the IPv6 address. For example, if a mobile node's home address (*HoA*) is *y:y:y:y:xxxx:xxff :fexx:xxxx*. Its care-of address in the network A would be *a:a:a:a:xxxx:xxff:fexx:xxxx* and its IPv6 address in network B would *be b:b:b:b:xxxx:xxff:fexx:xxxx*, we could set the firewall rules with following pattern for the mobile node:

TARGET INPUT
--source y:y:y:y:xxxx:xxff:fexx:xxxx
--source mask 0::ffff:ffff:ffff:ffff
--destination address_of_CN
--protocol 135

and

TARGET OUTPUT
-- destination y:y:y:y:xxxx:xxff:fexx:xxxx
-- destination mask 0::ffff:ffff:ffff:ffff
--source address_of_CN
--protocol 135

where protocol 135 specifies the protocol of Mobility Header.

After filtering by mask *0::ffff:ffff:ffff:ffff*, all of the source addresses from/to *MN* are the same *xxxx:xxff:fexx:xxxx* and match the firewall rules. However, only messages *HoTI, HoT, CoTI, CoT,* BU_{CN} and BA_{CN} can go through the firewall because they are with the mobile protocol type 135.

From above analysis, we could summarize that the firewall, which protects the correspond node of mobile node, does not block the communication between the mobile node with traceable address and the correspondent nodes. However, the traceable addresses are not always available. The next subsection will discuss solution for mobile nodes with untraceable addresses.

Firewall Configuration if *MN*'s *CoA* is UntraceableAddress

If the mobile device is an Ethernet device, we could use the MAC feature in firewall to filter it. The rule pattern is:

TARGET INPUT
--mac-source xx:xx:xx:xx:xx:xx
--destination address_of_CN

where, *xx:xx:xx:xx:xx:xx* is the MAC address of the *MN*.

The filter feature for MAC source addresses only makes sense for packets coming from an Ethernet device. It is not suitable for the mobile devices that do not support Ethernet, such as mobile phone. Hence, we have to come back IP layer.

From the perspective of the correspondent node, the care-of address of mobile node is an untraceable address. It is not able to set up firewall rules based on the kind of addresses. Mobile IPv6 specification [1] introduces a new herder "Type 2 Routing Header" which carries the home address of the mobile node. The new routing header uses a different type to that defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. Therefore, we suggest that the current firewalls extend a feature to filter the field of Home Address Option in the mobility header as well as the field Type 2 Routing Header. With the new feature, we use 3 firewall rule patterns for the mobile node, which home address is *y:y:y:y:xxxx:xxff:fexx:xxxx* and its current care-of address is *a:a:a:a:xxxx:xxff:fexx:xxxx*:

TARGET INPUT
--source y:y:y:y:xxxx:xxff:fexx:xxxx
--destination address_of_CN

TARGET OUTPUT
--destination y:y:y:y:xxxx:xxff:fexx:xxxx
--source address_of_CN

and

TARGET INPUT &OUTPUT
--home-address y:y:y:y:xxxx:xxff:fexx:xxxx
--protocol 135

where --protocol 135 specifies the protocol of Mobility Header.

Accordingly, we proposed an improved Return Routability (RR) procedure [10] in which the message of *HoTI, HoT, CoTI* and *CoT* bundles *HoA* and *CoA* together instead of *HoA* or *CoA* alone in the original RR procedure. (The analysis in [10] indicated that binding *HoA* and *CoA* together makes the original RR protocol much stronger.)

Now let's look every message in the improved RR procedure:

The *HoTI* message: its source address is *y:y:y:y:x:xxxx: xxff:fexx:xxxx* and destination address is *address_of_CN*. The *HoTI* message meets the firewall rules and then passes the firewall.

The *HoT* message: its destination address is *y:y:y:y:xxxx: xxff:fexx:xxxx* and source address is *address_of_CN*. The *HoT* message meets the firewall rules and then passes the firewall.

The *CoTI* message: the message with source address *a:a:a:a:xxxx:xxff:fexx:xxxx,* destination address *address_of_CN*, home address *y:y:y:y:xxxx:xxff:fexx:xxxx* and mobility header protocol 135. The *CoTI* message meets the extended firewall rule and is also able to pass the firewall.

The *CoT* message: the message with destination address *a:a:a:a:xxxx:xxff:fexx:xxxx*, source address *address_of_CN*, home address *y:y:y:y:x:xxff:fexx:xxxx* and mobility header protocol 135. The *CoT* message meets the extended firewall rule and is also able to pass the firewall.

The BU_{CN} message: the message with source address *a:a:a:a:xxxx:xxff:fexx:xxxx* and destination address *address_of_CN,* home address *y:y:y:y:x:xxff:fexx:xxxx* and mobility header protocol 135. The BU_{CN} message meets the extended firewall rule and can pass the firewall.

The BA_{CN} message: the message with destination address *a:a:a:a:xxxx:xxff:fexx:xxxx*, source address *address_of_CN*, home address *y:y:y:y:x:xxff:fexx:xxxx* and mobility header protocol 135. The BA_{CN} message meets the extended firewall rule and can pass the firewall.

Upon receiving the BU_{CN} message, the correspondent node opens a dynamic pinhole for the address *a:a:a:a:xxxx:xxff:fexx:xxxx* so that following traffic packets from this address with any protocols can reach the correspondent node.

After this modification, the firewall, which protects the correspondent node of mobile node, will not block any more the communication between the mobile node with untraceable address and the correspondent nodes.

Of course, the application of the solution is more general. It is certainly suitable for the mobile nodes with traceable addresses.

Based on the same mechanism, the description of other scenarios is simple in the following subsections.

3.3 Scenario of the HA Protected by Firewall(s)

Figure 3 displays the scenario that the home agent of a mobile node is protected by firewall. In the specification of mobile IPv6 [1, 5], the following messages from the mobile node will send to/through its home agent: Home Binding Update BU_{HA}, Home Test Init *HoTI* and Home Test *HoT*.

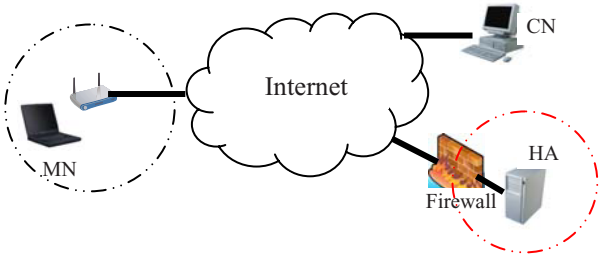

Fig. 3. HA is protected by a firewall

Firewall Configuration if *MN*'s *CoA* is Traceable Address
Similar to the usage described in above section, we set the below firewall rules in the firewalls that protect the *HA*.

TARGET INPUT
--source y:y:y:y:xxxx:xxff:fexx:xxxx
--source-mask 0::ffff:ffff:ffff:ffff
--destination address_of_HA
--protocol 135

and

TARGET OUTPUT
--destination y:y:y:y:xxxx:xxff:fexx:xxxx
--destination-mask 0::ffff:ffff:ffff:ffff
--source address_of_HA
--protocol 135

After masking by *0::ffff:ffff:ffff:ffff*, all of the addresses from/to *MN* become the same *xxxx:xxff:fexx:xxxx* and match the firewall rules. But, only the messages BU_{HA} and BA_{HA} can go through the firewall because they are with the mobile protocol type 135.

According to RFC 3776 [5], the *HoTI*/*HoT* message is encapsulated by ESP tunneling mode in the MN-HA path, so the headers do not contain the mobile protocol type 135. However, upon receiving the BU_{HA} message, the home agent opens a dynamic pinhole and sets up a security tunnel for *MN*'s *CoA* so that following traffic packets from this address with any protocols can reach the home agent. Thereafter, the encapsulated *HoTI* and *HoT* can pass through the firewall.

From above analysis, we summarize that the firewall, which protects the home agent of mobile node, does not block the communication between the mobile node with traceable address and the home agent.

Firewall Configuration if *MN*'s *CoA* is UntraceableAddress
If the mobile device is an Ethernet device, we could also use the MAC feature in firewall to filter it:

TARGET INPUT
--mac-source xx:xx:xx:xx:xx:xx
--destination address_of_HA

For general purpose, we propose a firewall configuration based on the improved RR protocol and add 3 firewall patterns for the mobile node:

TARGET INPUT
--source y:y:y:y:xxxx:xxff:fexx:xxxx
--destination address_of_HA

TARGET OUTPUT
-- destination y:y:y:y:xxxx:xxff:fexx:xxxx
--source address_of_HA

and

TARGET INPUT&OUTPUT
--home-address y:y:y:y:xxxx:xxff:fexx:xxxx
--protocol 135 -j ACCEPT

where --protocol 135 specifies the protocol of Mobility Header.

Now let's look at every message in the improved RR procedure in which the *HoA* and *CoA* are bundled together:

The BU_{HA} message: the message with source address *a:a:a:a:xxxx:xxff:fexx:xxxx* and destination address *address_of_HA*, home address *y:y:y:y:x:xxff:fexx:xxxx* and mobility header protocol 135. The BU_{HA} message meets the extended firewall rule and can pass the firewall.

The BA_{HA} message: the message with destination address *a:a:a:a:xxxx:xxff:fexx:xxxx*, source address *address_of_HA*, home address *y:y:y:y:x:xxff:fexx:xxxx* and mobility header protocol 135. The BA_{HA} message meets the extended firewall rule and can pass the firewall.

Upon receiving the BU_{HA} message, the home agent opens a dynamic pinhole and sets up a security tunnel for the address *a:a:a:a:xxxx:xxff:fexx:xxxx* so that following traffic packets from this address with any protocols can reach the home agent. Thereafter, the encapsulated *HoTI* and *HoT* can pass through the firewall.

3.4 Scenario of the MN Protected by Firewall(s)

Figure 4 indicates the scenario where the *MN* is within a network protected by firewall. In the specification of mobile IPv6 [1, 5], the *MN* will send/receive following messages: BU_{HA}, BA_{HA}, *HoTI, HoT, CoTI, CoT*, BU_{CN} and BA_{CN}.

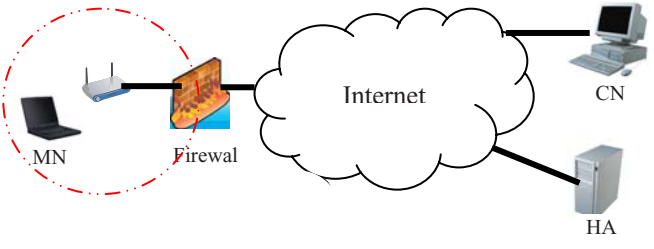

Fig. 4. MN within a network protected by a firewall

No matter if a *MN* is roaming into a visiting network or already stays in the visiting network and need to update its *CoA*, after allocated or authorized a new *CoA*, it informs its *HA* and *CN* of its current *CoA*. Since the *MN* is always the initiator, it is able to apply the pinholes from the firewall for the communications with other parties.

The procedure of the home binding update is:

1) the mobile node gets current care-of address;
2) the mobile node solicits a firewall pinhole for the communications between the care-of address and its home agent (a fixed address) with the protocol number 50 (ESP) and 135 (Mobility Header);

3) the mobile node sends the home binding update message BU_{HA} to its home agent through the pinhole;
4) the home agent sends back a acknowledgement BA_{HA} through the pinholes and set up security tunnel between the home agent and its home agent;
5) thereafter every packet between the mobile node and its home agent goes through the security tunnel.

The procedure of the correspondent binding update is:

1) the mobile node sends the *HoTI* message to its home agent through the security tunnel;
2) after receiving the *HoT* message from the correspondent node, the home agent forwards the *HoT* message to the mobile node through the security tunnel, too;
3) the mobile node solicits a firewall pinhole with protocol number 135 for the communications between the care-of address and the correspondent node;
4) the mobile node sends the *CoTI* message to its correspondent node through the pinhole;
5) the correspondent node sends back the *CoT* message through the pinhole;
6) the mobile send the binding update message BU_{CN} to its correspondent node through the pinhole;
7) the correspondent node sends back a acknowledgement BA_{CN} through the pinholes;
8) the mobile node requires to open more ports for the pinhole;
9) thereafter every packet between the mobile node and its correspondent node goes through the pinhole.

4 Analysis of Security and Performance

The purpose of the paper is to provide some schemes to make conventional firewalls suitable for mobile IPv6 network, and should not bring new threats. The paper proposed three methods: filtering MAC address, masking low 64 bits of source address and extending the firewall functions. Below we discuss and analyze the security and performance of these approaches.

1) Method of filtering MAC address: Since the method just employs the feature of the ordinary firewalls, it does not bring any further security issue. However, its application scope is limited due to the restriction of Ethernet devices.
2) Method of masking low 64 bits: As the method ignores the address prefix, it fails to detect the source location of the packets. This brings the threat of address spoofing because the firewall is opened to all nodes if they have the same interface identity, no matter where these nodes are. In order to reduce the risk, the protocol option is switch on to filter the mobility header (135). As the messages with mobility header are very small in term of size and need a little processing, it would not bring a serious threat.

   The method does not introduce any new fields and operations. Hence its performance is the same as the ordinary firewall.

   The application scope is also restricted due to the requirement of traceable addresses.

3) Method of extending the firewall function: In mobile IPv6 network, the *CoA* in the source address field of binding update message is no sense to the firewall rules, an identity field is required so that the firewall recognizes the packets' owner. The method extends the ordinary ip6tables' features to filter the home address in the home address option header or in typing 2 routing header.

   The improved RR protocol [10] is also needed as the *CoTI*/*CoT* messages in original RR protocol do not contain the home address information.

   The improved RR protocol provides much stronger security than the original RR protocol. It can prevent three redirect attacks: Session Hijacking Attacks, movement Halting Attacks and Traffic Permutation Attacks. This protocol just bundles *HoA* and *CoA* together in the messages of *HoTI*, *HoT*, *CoTI* and *CoT*, and does not change the original RR's architecture.

   If the firewalls deployed in IPv6 networks support the 3rd addresses (Routing Header, Home Address Option or Destination Options Header), the concern of performance by the modification is minor because the architecture and operation are the similar as the original one. After all, either Routing Header or Home Address Option is an inner address and not always next to the IPv6 Header, the firewall performance will suffer and hardware implementations become difficult in this solution comparing with traditional firewalls that just check the most outside IP addresses.

5 Conclusions

We first reviewed the mechanism of mobile IPv6 networking and analyzed the exchanging messages among the mobile nodes, home agents and correspondent nodes. Then we proposed three potential solutions to make the firewall friendly in mobile IPv6 network.

For Ethernet devices, we suggested to employ the feature of MAC address filter. For the mobile nodes with traceable addresses, masking the low 64-bits of source address is a simple and efficient solution. For general mobile nodes, we introduced an extended firewall and the improved Return Routability protocol. The extended firewall could always monitor the home addresses of mobile nodes as well as the care-of addresses. It also improved the security capability of the original RR protocol without changing its architecture

References

1. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6., IETF RFC 3775 (June 2004)
2. Le, F., Faccin, S., Patil, B., Tschofenig, H.: Mobile IPv6 and Firewalls: Problem Statement. IETF RFC 4487 (May 2006)
3. Thomson, S., Narten, T.: IPv6 Stateless Address Autoconfiguration. IETF RFC 2462 (December 1998)
4. Droms, R., et al.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). IETF RFC 3315 (July 2003)
5. Arkko, J., Devarapalli, V., Dupont, F.: Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. IETF RFC 3776 (June 2004)

6. Narten, T., Nordmark, E., Simpson, W.: Neighbor Discovery for IP Version 6. IETF RFC 2461 (December 1998)
7. Deering, S., Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification. IETF RFC 2460 (December 1998)
8. Narten, T., Draves, R.: Privacy Extensions for Stateless Address Autoconfiguration in IPv6. IETF RFC 3041 (January 2001)
9. Aura, T.: Cryptographically Generated Addresses (CGA). IETF RFC 3972 (March 2005)
10. Qiu, Y., Zhou, J.Y., Deng, R.: Security Analysis and Improvement of Return Routability Protocol. In: Burmester, M., Yasinsac, A. (eds.) MADNES 2005. LNCS, vol. 4074, pp. 174–181. Springer, Heidelberg (2006)
11. Linux HOWTO: ip6tables