Mobile Personal Firewall-Design

Prof. Sangita Chaudhari*, Darshan Desai,**
Sajit Menon, Manish Waghela****
*(Asst. Professor, Dept. Of Computer Engineering, VCET, Vasai Road-401202
Email: sangita123sp@rediffmail.com)
**(Dept. of Computer Engineering, VCET, Vasai Road-401202
Email: ddrockin@gmail.com)

Abstract: In this paper, we will discuss the issues on the design of a mobile personal firewall framework. Under this framework, the Home Agent (HA) will act as the centralized controller for the firewall, and the mobile nodes (MN) will be protected by the access routers (AR) that they are connected to. The ARs will serve as a security proxy for the MN, where the HA will forward the corresponding MN's security rules to access router (AR) whenever MN changes its point of attachment. Security rules for each of the MN can be modified and updated dynamically at their respective HA.

Keywords - **Firewall, MIPV6, Mobile devices, Mobile network.**

I. Introduction

More and more activities rely on mobile devices. It is an important issue on how to protect mobile users engaged in mobile services. Due to the tremendous growth in technology, an increasing number of 3G networks and WiFi hotspots are surfing up. This has made possible for people to asccess internet for various purposes like Mobile Banking, Online bill and tax payment using their mobile devices such as mobile phones, laptops, PDAs, etc. Often this task deals with the confidential details of the person involved, such as Account details, Bank passwords, address, etc. Thus it is very important to protect leakage of such sensitive information. Firewall is one of the security solutions.

With the presence of firewall, we can avoid any unauthorized person to access devices and also

avoid illegal outflow of data to unauthorised destinations.

There are basically two categories under which firewall falls, namely, Conventional Onboard Firewall and Mobile Personal Firewall.

The conventional onboard firewall is present of the device itself. So it's impossible for the Network Administrator to dynamically update the rules for mobile nodes in real time. Even if the administrator is aware of the attack or the loop-hole, he would not be able to implement the patch meant for it until and unless the device is free. As all the rules are stored in the mobile device, the computational speed of the mobile device becomes very slow.

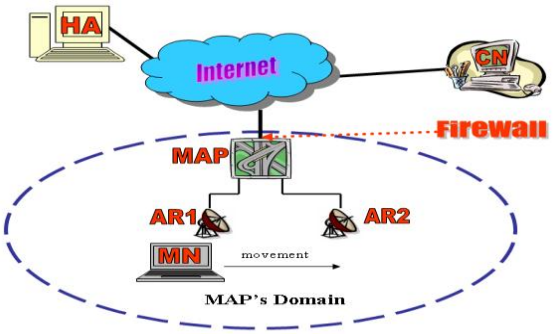
Using Mobile personal firewall, the administrator can change the security rules present at the home agent (HA) and the same will be updated to the access router (AR). This technique doesn't affect the computational speed of the device.

In this paper, we will focus on design of various modules and functionality of firewall as mobile node changes its position.

II. Location of Mobile Firewall

In the MIPv6 framework, the Mobility Anchor Point (MAP) is introduced. The MAP is an access router located in a domain visited by

mobile nodes. The MAP provides the localized mobility management for the visiting mobile nodes. Every MN bundles three addresses: home Address (HoA), Care-of-Address (CoA). If the MN sends the packets to its HA the source address of the packets would be set to CoA. On the contrary, when the MAP receives packets with the destination address CoA from the HA, the MAP tunnels the packets to the related CoA.



The CNs and HA always connect to the MN with its CoA.

According to MIPv6 framework, every packet from the CN to the MN will pass through the router MAP. Hence, in our scheme, the HA authorizes the MAP as the security proxy (firewall) on behalf of the HA when the MN visits the MAP subnet. Figure below shows the firewall location in MIPv6 framework.

III. Mobile Personal Firewall

In this technique, each mobile node is provided with a constant home address (HoA) which is a combination of network prefix + MAC address of the mobile node, used to uniquely identify the device in its home network and automatic configure the Care of Address (CoA) which is combination of the network prefix + home address, used to uniquely identify the mobile node when it is out of the home network.

Various characteristics of the mobile personal firewall are:

1. Makes use of Mobile IPV6 to make MN reachable via its HoA. Home agent acts as a central controller for storing rules and regulations specified for a mobile device.
2. While at home network, mobile node is monitored through its home agent.
3. While at foreign network, mobile node is monitored through the corresponding access router (AR).

In mobile personal firewall all rules during the MN in home network are directly updated without interrupting any other device in the firewall but when MN moves to foreign link then a series of steps are to be performed for dynamically updating the rules in future during any threat.

Various phase of the firewall

A] *MN moves to foreign network from home network*

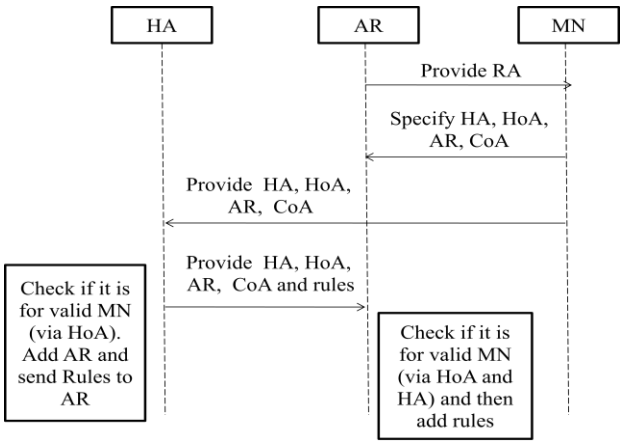
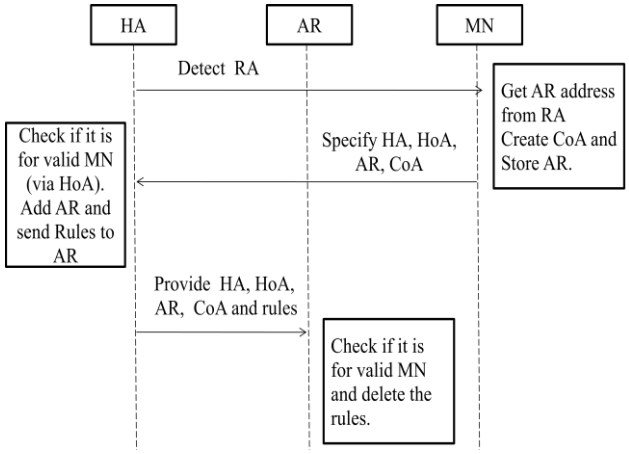


Fig above shows the data flow structure that will occur in this phase. The MN first has to register itself to the new foreign router (access router). For this purpose it first finds the RA (router address) of nearby router and gets itself registered with it by specifying all needed address to the router. After this process it gets all needed address from the new access router and sends all address(HA, HoA, CoA, AR) to its home agent as all rules are stored at home agent. Home agent validates all the address and performs a check to confirm the requested access router is not black listed and then

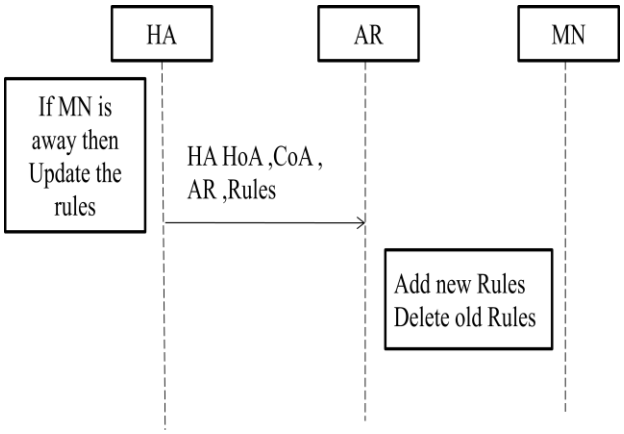
forward's all rules to the new Access router. Hereafter if any updates are to be made then it can be directly done at the access router, no need to contact home agent everytime. According to current status all the device will be aware about current connection point and status of the mobile node.

B] *MN moves back to the home network*



Initially the MN will inform the HA that it wants to return back to the home agent. Ha will send a disassociation message to the current AR to which the MN was connected. As soon as the AR receives this message it immediately removes all rules and regulations stored in it about the mobile node.
When it enters the home network all previous binding entry will be removed and a new connection will be available which includes all the rules and regulations about the mobile node.

C] *Dynamic update of security rules*

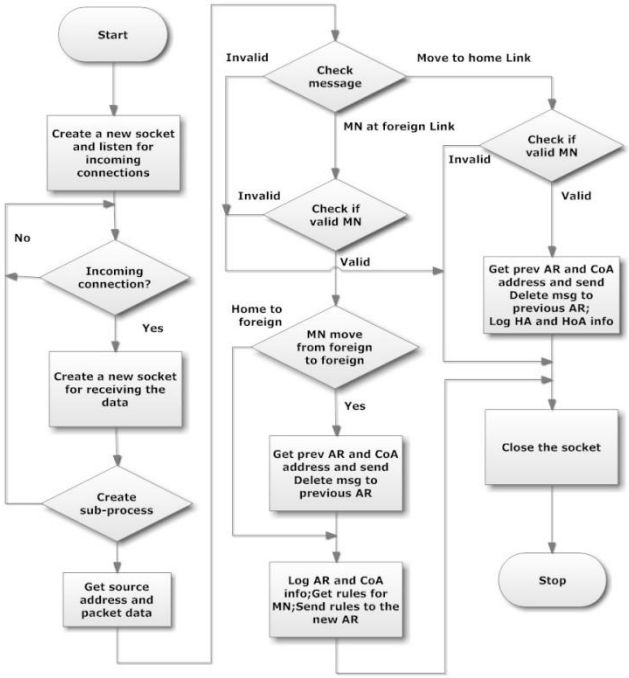


Whenever there is need to update any rules for the mobile node than initially the HA is contacted. If the MN is in home network then it can be done directly by a verification process that the person changing the rules is the authorized person. If the mobile node is at foreign link the updating is done through the access router.

IV. Design of basic modules of Firewall.

A] *HA Firewall module*

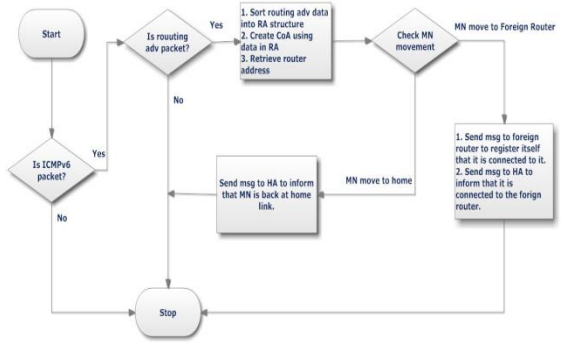
It consists of two important functions for which two threads are executed simultaneously.
1. Receiver function: which is used to receive and process incoming messages &
2. Polling function: which is used to detect the modification in the security rules and perform the necessary updates.
The polling function is used to detect the modification in the stored security rules for each MN. As the rules are stored in a text file, a temporary cache copy of the security rules will be used to compare against the original file during the poll. Updating of the security rules is done by a child sub-process.



B] *AR firewall Module*

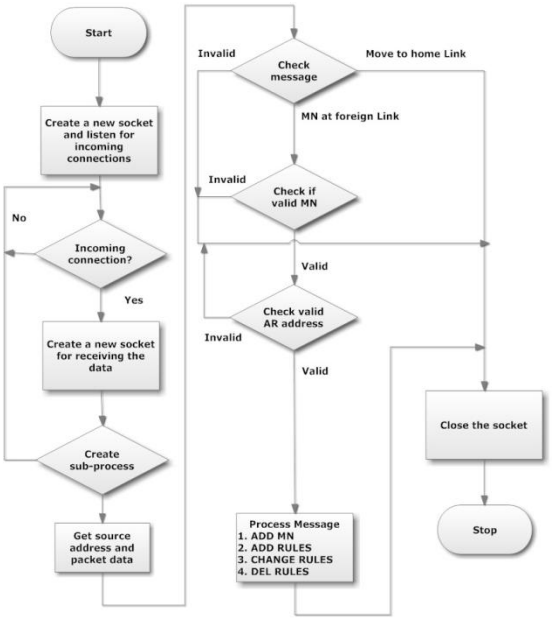
The firewall module running at the AR is designed to receive messages from both the HA and the MN. A receiver function is used to receive and process incoming messages received from a predefined open port. 3 types of messages received by the AR are:

1. The notification to the AR when a MN node is connected to it
2. To deploy the security rules when a MN joins the AR subnet.
3. To tear down the security rules when a MN leaves the AR subnet.



C] *MN Firewall module*

The firewall module at the MN is designed with the least amount of processing needed to reduce the computational load on the MN as it has limited computing capacity and resources. The security rules for the MN are created during the registration at the HA to obtain the HoA for the MN. Information such as the MN's HoA and the HA's address will be stated in a configuration file over at the MN. Unlike the HA, the module has one main process running that is used to grab the routing advertisement packets that are advertised by the routers. From the advertisement packets, the module will retrieve information such as the network prefix and the router's IPv6 address. A callback function will be used to activate the function to detect if the incoming packet is a advertisement packet. Similarly a child sub-process will be used to retrieve and process the information from the advertisement packets at the child sub-process. During this process, the module will create the MN's CoA by concatenating the network prefix with its preconfigured HoA.



Advantages:

Mobile personal firewall provides the portability of firewall policy at the Home Agent (HA) for the Mobile Nodes (MN). If Mobile Nodes (MN) changes its location, then firewall policy is transferred from Access Router to the corresponding Mobile Nodes at the Home Agent (HA). The firewall running on conventional routers provides protection on network layer, whereas in Mobile Firewall, it provides protection on top of the network layer as well.

Another advantage of Mobile Personal Firewall is that it provides the dynamic update of security rules. The administrator will be able to update the firewall policies for the mobile devices without the need of having physical access to the mobile devices. Hence it is protected from Zero-day attack. The Administrator will only able to change the firewall policy at the Home Agent (HA), and the rules will be updated according to the access routers that the MN connected to it.

Administrator will be able to restrict the access to the prohibited sites on office equipments. This reduces risk of Mobile device being infected by any malware or viruses.

Disadvantages:

The Access Router (AR), which is not enabled with the firewall module, then it doesn't protect the Mobile device. Hence its increase the risk of Mobile Device to be affected by malware or viruses or any attacks.

Another disadvantage is that the Mobile Personal Firewall can't be implemented on peer to peer (P2P) ad-hoc network. The peer to peer network doesn't contain the Access Point that is Access Router. Hence we cannot implement Mobile Personal Firewall.

Performance Analysis:

There are two major disadvantages that are to be analyzed. First is Memory Overhead and another is Communication Overhead.

1. Memory Overhead

In Mobile Personal Firewall, consists of various files used to store relevant information used by system. This file includes configuration files, list of mobile nodes connected to it, Firewall policies of each individual Mobile Node (MN) and Access Router (AR) information associated with mobile nodes. Hence maintaining this file is very difficult. It increases the bulk of overhead. Home Agent must have to keep the track of each an individual firewall policy of Mobile Node (MN). So this increases the Memory Overhead.

2. Communication Overhead

When Mobile Node (MN) changes its location, firewall policy is forwarded to the Access Router (AR) for the Mobile Node (MN) or when there is a modification in the MN's firewall rules. This overhead will be in terms of the bandwidth used to send the rules over to the access router. So for transferring information from one access router to other access router, communication overhead increased.

Future Improvements:-

The prototype can be further improved with security features such as the encryption of the messages being sent and implementation the Internet Key Exchange (IKE) scheme. IKE will help to distribute the security keys that will be needed for IPSec, authentication or encryption.

V. Conclusion

As a conventional firewall is unsuitable for mobile networks, we introduced the concept of mobile personal firewall, and described how to implement a stateful firewall in the mobile IP infrastructure. There are three main parts in our scheme:

-Authentication and authorization: this part focuses on how to authenticate between the HA and the MAP as well as between the MN and the MAP.

- Control and monitor: this part focuses on how the guardian of the

MN can control and monitor the MN's activities.

- Management: this part focuses on how to effectively manage the security stuff. All the operations are transparent to the mobile user, and he will be served in a way specified by his guardian no matter where he roams. The mobile firewall could have full features of a conventional stateful firewall.

REFERENCES

[1] Han Chiang Tan, Jianying Zhou, Ying Qiu, "A Mobile Firewall Framework - Design and Implementation", IEEE Communications Society, 2007

[2] Y. Qiu, J. Zhou, F. Bao, "Mobile Personal Firewall", 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC04), Spain, September 2004.

[3] Ying QIU, Jianying ZHOU, Feng BAO, "Design and Optimize Firewall for Mobile Networks", IEEE Communications Society

[4] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6".

[5] J. Arkko, V. Devarapalli, F. Dupont "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents".

[6] F. Le, S. Faccin, B. Patil, H. Tschofenig, "Mobile IPv6 and Firewall".