Approach towards realizing the Security Threats for Mobile IPv6 and Solution Thereof

Amrit Ghosh
Assistant Professor, Electronics & Communication Engg. Department
Sir Padampat Singhania University, Bhatewar
Udaipur-313601, India

Prasun Chakrabarti
Associate Professor, Computer Science Engg. Department
Sir Padampat Singhania University, Bhatewar
Udaipur-313601, India

Pierluigi Siano
Aggregate Professor, Industrial Engg. Department
University of Salerno
Fisciano (SA) 84084, Italy

ABSTRACT
Mobile IPv6 has been developed to sustain a seamless mobility in IP network which consists of many favorable characteristics in comparison to the previous Mobile IP protocol, i.e. Mobile IPv4. Unfortunately, Mobile IPv6 is badly affected by security threats like eavesdropping, secure route optimization, connection hijacking and denial of services and security issues are one of the major concerns which should be rectified. This paper entails an algorithm that contains all security components viz. authentication of services, confidentiality and integrity of data packets during communication, secrecy of key management and thus it would be able to nullify all types of security threats in Mobile IPv6 in anycast environment.

General Terms
Security issues related to Mobile IPv6 should be detrimental as per mobile communication and hence should be rectified, integrated and later on implemented to make every single device as a Mobile IPv6 device, thus enabling the Mobile Internet as more efficient, robust, and secure, which would be ensured by the proposed algorithm.

Keywords
Mobile IPv6, Secure route optimization, Anycast, Register Agent.

1. INTRODUCTION
Mobile IP [1] developed by Internet Engineering Task Force (IETF), is a protocol for mobile communication as well as mobile computing. The Mobile IP is classified into Internet Protocol version 4 [2] and Internet Protocol version 6 [3].Security of mobile IPv6 is a primary and major concern. There are several security issues and as per present scenario, Mobile IPv6 has recently been degraded in standardization. Hence, these issues should be detrimental as per mobile communication and should be rectified, integrated and later on implemented into the protocol itself, making every single device in near future as a Mobile IPv6 device, thus enabling the Mobile Internet as more efficient, robust, and secure[4,5,6,7].

2. THE PRPOSED ALGORITHM IN ANYCAST ENVIROMENT
In Mobile IPv6, it was seen that it would suffer from handoff delay (after the introduction of anycast, still the problem used to persist) when a mobile node could change its point of attachment in the network. The proposed algorithm is based on the experimental analyses.

1. In the handover initiation, tunnel establishment and packet forwarding has got a profound effect for mobile node as well as specialized mobility agents in a particular network. For a particular MN (i.e. mobile node) handover, the information would be sent to an authorized and secured agent, known as register agent (i.e. RA) (by following rules of Anycast),

2. The information (in the form of data packets) would be obtained from lower network layers (by following rules of Anycast),

3. The mobile node would send a solicitation (i.e. RASOL) for the purpose of accessing the message from the register agent and in response the register agent would send an advertising message (i.e. RAADV) (by following rules of Anycast),

4. Then the MN would communicate a secured register binding update message (i.e. RBU) through an authenticated and secured care-of-address (i.e. CoA) for the purpose of authentication of RBU with the register agent to bind the previous CoA of the lower network layer to the new CoA by tunneling procedure and on accepting this RBU, the new CoA would be verified by the RA by exchanging the handover initiation and handover acknowledgement messages (by following rules of Anycast),

5. Then RA would send back the binding acknowledgment message to the MN which would be meant for data packet under tunneling procedure would be in progress and meanwhile, the MN hands over the information message to the new CoA (by following rules of Anycast),

6. Then the MN would declare its attachment handoff procedure to a nearby secured authenticated neighbour by using one more new CoA. In this initiated handover procedure, the unsolicited messages would be deposited number wise in a secured container, known as register message stack (i.e. RMS) and which would be refreshed after every ten minutes (by following rules of Anycast). This register message stack would be sub-divided into vast numbers of sub stacks (i.e. RM sub-stack) with huge capacity and they would also be refreshed after every ten minutes as per condition,

7. The MN would configure anew, secured and authenticated care of address on the new subnet by sending an RBU to the old CoA before getting transferred to a new link. The mobile node would also encapsulate the RBU in this handover process (by following rules of Anycast).

2.1 Experimental Set-up

Although, Mobile IPv6 would continue in maintaining the existing connections of MN after changing its locations and addresses, it has been severely affected with the problems associated to any fast moving hosts. This research paper has been deployed with an algorithm of register message stack for the analysis and study assigned to the effect of transferring data during MN's movement on the performance of handover, and comparing it with the existing performance of fast Mobile IPv6 and normal Mobile IPv6 respectively. The study was carried out using an open source ns-2 simulator [9] to analyze the behaviour of handover protocol in Mobile IPv6, based on some parameters such as throughput, and latency during handoff. The figure 1 shown below would be emphasizing on the certain topology as per the proposed algorithm.

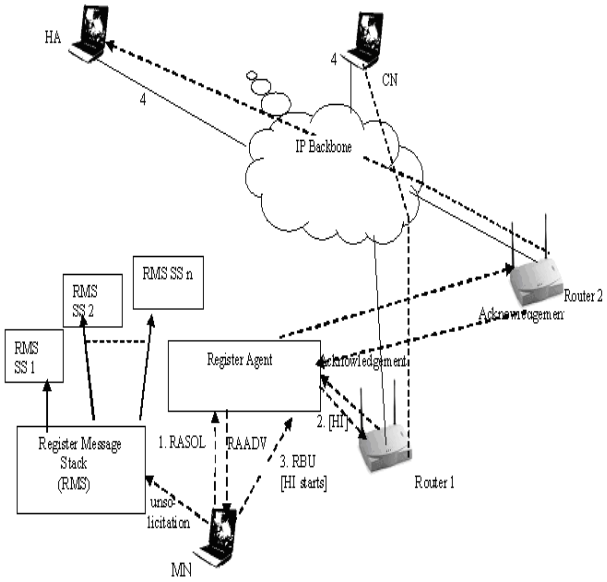

Figure 1 Mobile IP performance Topology

As per the above figure, RMS SS1, RMS SS2 up to RMS SSn have been termed as Register Message Sub – sets 1, followed by 2, which would be completed by n. As per the proposed algorithm, RASOL could be termed as Register Solicitation, RAADV could be termed as Register Advertising Message, HI would be termed as first Handover Initialization related to Router 1, HI + 1 would be termed as second Handover Initialization related to Router 2 and RBU would be termed as Register binding update message.

2.2 Simulation and analysis

The detailed and through study of performance analysis of Mobile IPv6 has been done to tackle the problem associated with handover latency. The simulation was done using network simulator NS2.31 as per the proposed algorithm followed by FHMIP (i.e. Fast Handover Mobile IP) extension [10] for fast handover procedure and Mobi Wan patch [11] for Mobile IPv6. The scenario consists of one mobile node, two base stations, register message stack, sub stacks, routers, one home agent, and a corresponding node. The types of data traffics have been used are under TCP category. The associated bandwidth in megabits per second and the latency in milliseconds have been shown beside the wired link. In this proposed topology, nodes CN, N_A, N_B, and N_C have been used as wired nodes, while nodes RMS, RM sub stack, and HA would come under the category of the combination of wireless and wired nodes. MN would be treated as a special node in wireless mode.

2.3 Latency Associated with the particular handover

In this section, the handover latency has been measured as the time interval between the ultimate packet received through the register message stack via the router associated with it and the penultimate packet received through the register message stack via the router associated with it. It has been observed that the latency would be the least as per the proposed algorithm compared to the Fast Mobile IPv6 and the conventional Mobile IPv6.

2.4 Implementation of Mobile IPv6 as per proposed algorithm in anycast

At first, Mobile IPv6 would be enabled on the register agent, register message stack, register message sub-stacks and router which would be followed by configuration of binding information for Mobile IPv6. After that, the enabling and configuration of NEMO (i.e. Network Mobility) would be performed on the IPv6 mobile router and register agent along with register message stack and sub-stacks followed by enabling of NEMO on the IPv6 mobile router home agent as per the proposed algorithm. It was followed by the enable procedure for roaming on the IPv6 mobile router interface and filtering the Mobile IPv6 Protocol headers and options as per the proposed algorithm. Controlling of ICMP unreachable messages would be executed in the later stage (related with register message stack and sub-stacks) which would be immediately followed by the verification of the native IPv6 tunneling for Mobile IPv6. At last, the configuration, authentication and verification of host groups for Mobile IPv6 for completely secured data packets transmission would be executed along with the customization of Mobile IPv6 on the Interface.

2.5 Output from the Mobile IPv6 binding command

Router # show IPv6 mobile binding

Mobile IPv6 Binding Cache Entries:
2006:DB8:2005::1111/64 via care-of address
2006:DB8::A8BB:CCFF:FE01:F612

home-agent 2006:DB8:2005::2004

Prefix 2006:DB8:8002::/64

Prefix 2006:DB8:2005::1111/128

Prefix 2006:DB8:1010::1111/128 installed

State ACTIVE, sequence 25, flags AHRlK

Lifetime: remaining 52 (secs), granted 60 (secs), requested 60 (secs)

Interface Ethernet0/2

Tunnel interface Tunnel0

0 tunneled, 0 reversed tunneled.

2.6 Output from the IPv6 mobile globals command

Router# show IPv6 mobile globals

Register Agent# show IPv6 mobile globals

Register Message Stack# show IPv6 mobile globals

Register message Sub-stack# show IPv6 mobile globals

Mobile IPv6 Global Settings: 1 Home Agent service on following inter

Faces:Ethernet1/2

Bindings: Maximum number is unlimited.1 binding is in use at a time

1 binding is peak

Binding lifetime permitted is 263284 seconds; recommended refresh time is 660 seconds.

2.7 Output from the IPv6 mobile traffic command

In the following information is about Mobile IPv6 traffic is displayed:

Router# show ipv6 mobile traffic

MIPv6 statistics:

Rcvd: 6477 total

0 truncated, 0 format errors

0 checksum errors

Binding Updates received: 6476

0 no HA option, 0 BU's length

0 options' length, 0 invalid CoA

Sent: 6476 generated

Binding Acknowledgements sent: 6476

6477 accepted (0 prefix discovery required)

0 reason unspecified, 0 admin prohibited

0 insufficient resources, 0 home reg. not supported

0 not home subnet, 0 not home agent for node

0 DAD failed, 0 sequence number

Binding Errors sent: 0

0 no binding, 0 unknown MH

Home Agent Traffic: 6476 registrations, 0 deregistration

00:00:23 since last accepted HA registration

unknown time since last failed HA registration

unknown last failed registration code

Traffic forwarded: 0 tunneled, 0 reversed tunneled

Dynamic Home Agent Address Discovery: 1 request

received, 1 reply sent

Mobile Prefix Discovery: 0 solicitations received, 0

advertisements sent.

2.8 Output from the IPv6 mobile tunnels Command

The following displays information about the Mobile IPv6 tunnels on the home agent:

Router# show ipv6 mobile tunnels

Tunnel1:

Source: 2004:0DB1:1:1

Destination: 2004:0DB1:2:1

Encapsulation Mode: IPv6/IPv6

Egress Interface: Ethernet 1/0

Switching Mode: Process

Keep-Alive: Not Supported

Path MTU Discovery: Enabled

Input: 20 packets, 1200 bytes, 0 drops

Output: 20 packets, 1200 bytes, 0 drops

NEMO Options: Not Supported.

2.9 Enabling Mobile IPv6 on the router

The following example shows how to enable and configure NEMO on the IPv6 mobile router. The /128 subnet must be used; otherwise, the IPv6 mobile router will fail to register because it will believe the home network is locally connected:

ipv6 *unicast-routing*

!

interface ethernet0/0

no ip address

ipv6 address 2005:DB8:2004::1111/128

ipv6 nd ra mtu suppress

!

interface ethernet0/1

no ip address

ipv6 address 2005:DB8:1100::1111/128

ipv6 nd ra mtu suppress

!

interface Ethernet0/0

description Roaming Interface to AR2

no ip address

ipv6 address autoconfig

ipv6 enable

ipv6 nd ns-interval 5000

ipv6 mobile router-service roam

ipv6 rip home enable

!

interface Ethernet0/1

description Mobile Network Interface

no ip address

ipv6 address 2005:DB8:8004::8005/64

ipv6 enable

ipv6 nd advertisement-interval

ipv6 nd ra interval msec 1110

ipv6 rip home enable

!

interface Ethernet1/1

description Roaming Interface to AR1

no ip address

ipv6 address autoconfig

ipv6 enable

ipv6 nd ns-interval 5004

ipv6 mobile router-service roam priority 99

ipv6 rip home enable

!

ipv6 router rip home

!

ipv6 mobile router

host group mr-host-group

nai mr1@cisco.com

address 2005:DB8:2004::1112/128

authentication spi hex 110 key ascii hi

exit

home-network 2005:DB8:2004::/64 discover priority 127

home-network 2005:DB8:1110::/64 discover

home-address home-network eui-64

explicit-prefix

register lifetime 60

register retransmit initial 1110 maximum 1110 retry 1

register extend expire 20 retry 1 interval

2.10 Throughput

This characteristic would be defined as total number data packets communicated in the network divided by the total number of communicated data packets excluding the control packets. Throughput under the proposed algorithm, Mobile IPv6 and Fast Mobile IPv6 are shown in figures shown below. From these figures, it would be observed that throughput reached a maximum and optimized possible value in comparison with Fast Mobile IPv6 and conventional Mobile IPv6 under anycast topology.

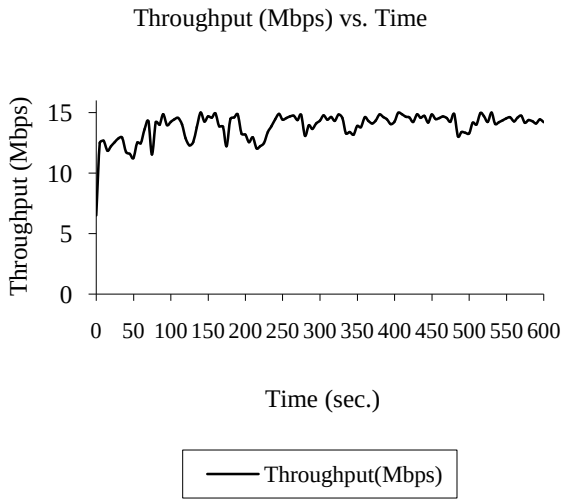

Figure 2 Throughput for Conventional Mobile IPv6

At the time t = 140 seconds, the value of throughput in Mbps observed as 15 Mbps which would be the most optimum one.

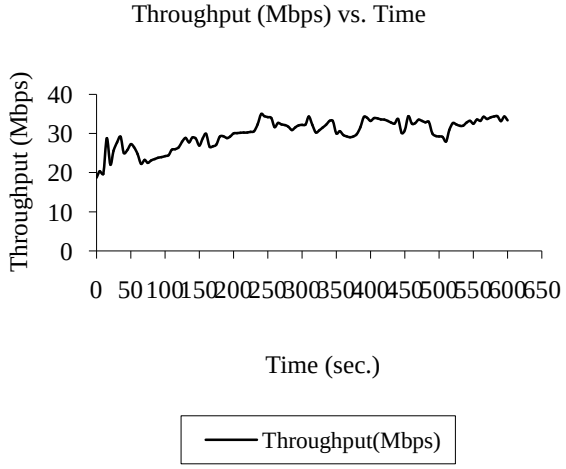

Figure 3 Throughput for Fast Mobile IPv6

At time t = 240 seconds, the value of throughput obtained as 35 Mbps (which would seem as the most optimum value) followed by two undershoots at t = 370 seconds, when the value of throughput obtained as 29.09 Mbps and at t = 510 seconds, when the value of throughput obtained as 28.02 Mbps.

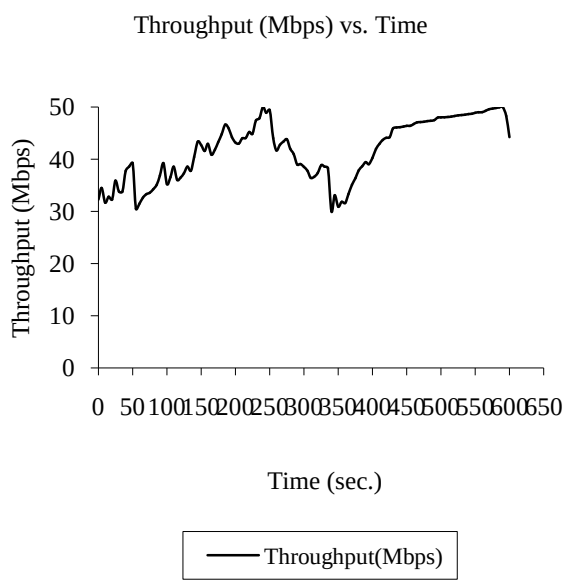

Figure 4 Throughput for as per proposed algorithm for Mobile IPv6

At time t = 0 second, the initial value of the throughput observed as 32.27 Mbps, which would be much higher compared to those of conventional Mobile IPv6 and fast mobile IPv6. The highest value of throughput observed as 50 Mbps at time t = 240 seconds, followed by a sharp decrease at time t = 340 seconds , when throughput observed as 30 Mbps. There would be a gradual increase in the throughput (in Mbps) from t = 395 second to t = 595 seconds followed by a sharp decrease which would be recorded as 44.19 Mbps at time t = 600 seconds.

4. CONCLUSION

In this research paper, by the application and the topology based on the proposed algorithm in anycast environment various threats in Mobile IPv6 have been discussed along with its optimal solution. These threats prevent secure communication in Mobile IPv6 based nodes in anycast. From the graphical representations, it was seem that for conventional Mobile IPv6 at the time t = 140 seconds, the value of throughput in Mbps observed as 15 Mbps which would be the most optimum one. In case of fast Mobile IPv6, it was seen that at time t = 240 seconds, the value of throughput obtained as 35 Mbps (which would seem as the most optimum value) followed by two undershoots at t = 370 seconds, when the value of throughput obtained as 29.09 Mbps and at t = 510 seconds, when the value of throughput obtained as 28.02 Mbps. As per the proposed algorithm, it was seen that the result would be showing the highest value of throughput in Mbps in authenticated and secured data packet transmission where at t = 0 second, the initial value of throughput observed as 32.27 Mbps, which would be much higher compared to those of conventional Mobile IPv6 and fast mobile IPv6. The highest value of throughput observed as 50 Mbps at time t = 240 seconds, followed by a sharp decrease at time t = 340 seconds, when throughput observed as 30 Mbps. There would be a gradual increase in the throughput (in Mbps) from t = 395 second to t = 595 seconds followed by a sharp decrease which would be recorded as 44.19 Mbps at time t = 600 seconds. After a detailed and through analysis, it can be concluded that the proposed algorithm in Mobile IPv6 security mechanism, would be able to successfully integrate all the security enhancing techniques and provide better security to Mobile IPv6 in anycast environment.

5. REFERENCES

[1] Perkins, C., E., "Mobile IP: Updated", IEEE Communications Magazine, Volume-40, Number-5, Pages: 66-82, 2002.

[2] Perkins, C., E., "IP Mobility Support for IPv4: Revised ",

[3] Request for Comments - 5944, Internet Engineering Task

[4] Force (IETF), November 2010.

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

[6] Sudanthi, S., "Mobile IPv6 GSEC", Version 1.4b, SANS Institute InfoSec Reading Room.

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

[8] Zao, J., K. and Condell, M., "Use of IPSec in Mobile IP", November 1997.

[9] Perkins, C., E., Charles, E. and Johnson, D., B., "Route Optimization in Mobile IP", 6th Sept.

[10] Soliman, H., Castelluccia, C., Malki, K., and Bellier, L., "Hierarchical MIPv6 mobility management", Internet Draft, IETF, 2002.

[11] Network Simulator ns-2 http://www.isi.edu/nsnam/ns/.

[12] Hsieh, R., Fhmip ns extension, 2003.

[13] Ernest, T., "Mobi Wan: A NS-2.26 simulation platform for Mobile IPv6 in Wide Area Networks", 2001.