ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A Novel Signaling Scheme for Route Optimization and Session Continuity In MIPV6 Networks

V. Valarmathi[1], C. Dhivya[2]

PG Student, Department Of ECE, DMI College of Engineering, Chennai-600123, India.[1]

Lecturer, Department Of ECE, DMI College of Engineering, Chennai-600123, India.[2]

Abstract: This paper presents a secure MIPv6 with secure and efficient Route optimization (RO). It uses DNSSEC to validate cryptographically generated address from trusted domain and provide strong authentication rather than weak sender. Route optimization which prevents the traffic occurring in the network while transferring the packets or data.Also session continuity is maintained during handover from one network to other network in the proposed work.MIPv6 networks is used to replace the triangle routing by MN to communicate bidirectional with the CN without passing through its home agent. This is done using network simulation (ns2) platform. This platform supports the real time applications.

Keywords - Route optimization, CGA, DNSSEC, MIPv6, Visiting Home agent.

I.INTRODUCTION

The main focus in this paper is on MIPv6, it is important to note that the proposed RO mechanism fits in the MN-initiated actions philosophy. Two modes are available for data to be transferred between MN and CN. First, the bidirectional tunneling (Fig.1) sends data in an IP-in-IP tunnel using the MN's home agent(HA) as the intermediary entity that encapsulates the received data.Although inefficient, especially when both the MN and CN are relatively close to each other,
establishing a bidirectional tunnel between the HA and nodes is currently the preferred way for the operator to provide services.

Route optimization enables data to be directly exchanged between the MN and CN,where MN fills the MIP destination option with its HA and then CN uses the routing to send packets back to the MN. Prior to exchanging data directly between the MN and CN. This paper presents secure MIPv6 which is a secure and efficient RO mechanism for MIPv6.

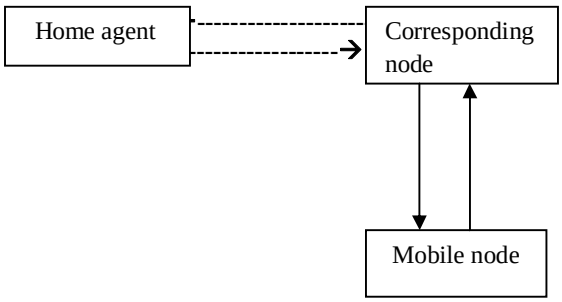

Fig. 1. Block diagram of tunneling and RO method

II.SECURE ROUTE OPTIMIZATION IN SMIPv6 USING ECGA AND DNSSEC

The main idea behind using DNSSEC and ECGA is to authenticate a message according to the domain from which it originated. This section first presents the objectives and assumptions of the proposals. Second, the integration of ECGA in the SMIPv6 is detailed execution in various MIPv6 scenarios leading to the RO.

A. objectives

The objectives of the secure RO proposal are as follows

1) Be as secure as HCBU while relying on the realistic assumptions.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

2) Lean toward providing strong authentication globally rather than the sender invariance by validating the CGA through the use of DNSSEC and trusted domains.
3) provide more flexibility and control to mobile operators when allowing RO.

B. Assumption

For the proposed solution to strongly authenticate the MN's HoA andCoA to vHA,respectively,the following Assumption are met.
1)64 b are sufficint for the care-of-subnet.
2)Whitelist of trusted domains is kept up to date by the operator administrators(in HA and vHA).
3)DNSSEC is deployed globally.
4)Operators protect their network by analyzing and filtering all incoming and outgoing messages.
5)A trusted authority that publishes a list of trusted mobile operator domains must be in place.

C.MN's Attachment to visiting network

When the MN enters a visting network(Fig.),the execution is similar to its home network's boostrap with the exception that the signature request is authenticated through the signed home token and the MN's public key used for its CGHoA.

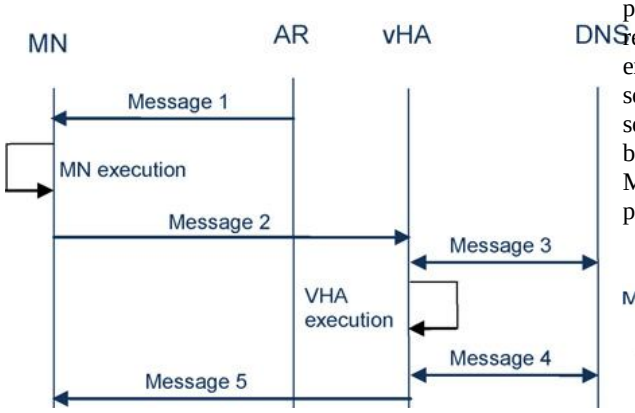

Fig.2 MN enters a new visiting network

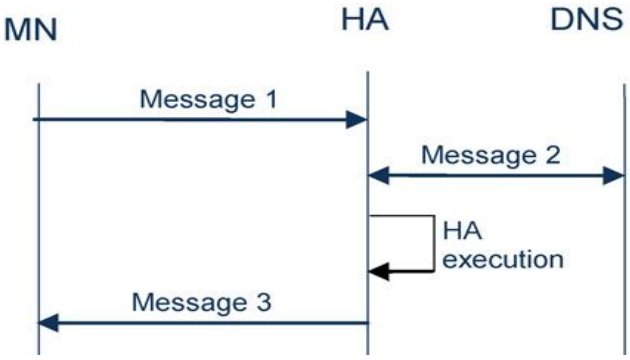

Fig.3 Binding update to HA

Once the MN successfully attaches to the visited network, it must send a BU to its HA and alert it of its new CGCoA.
1)weak authentication to ensure sender invariance of the router advertisement messages;
2)strong authentication for all other messages sent from the MN,HA,vHA and the DNS server;
3)secrecy to ensure confidentiality of symmetric keys held by the MN and shared with its HA and the CNs.
DNSSEC enables a node to securely verify if a CGA is part of a trusted domain.CGA cannot be spoofed, receiving a message from a CGA signed by a trusted entity (HA/vHA) of a trusted domain increases the security property to strong authentication instead of sender invariance. However, because no assumption has been given about the knowledge of trusted domains to the MN, it must rely initially on the sender invariance property for the router advertisements.

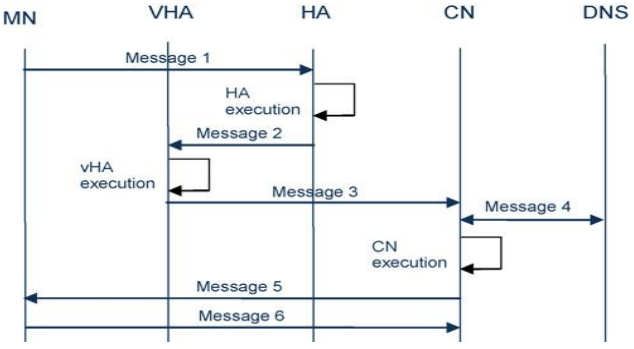

Fig.4 Secure and efficient route optimization message sequence.

For CN to validate the CGCoA,it requires a signature involving MN,VHA,HA.MN sends a message 1 to Home agent, it checks with DNS.After making sure that the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

domain name is same, message 2 is sent to visiting home agent.vHA checks with mobile node, then the message 3 is transferred to corresponding node.MN's new CGCoA must authenticate with corresponding, when the handover is executed inside the same network.Otherwise new vHA has to be signed,thus connection becomes invalid and route optimization execution must start from beginning.

The symmetric key $K_{MN-CN,}$along with the signed visited token,is used to authenticate MN's new CGCoA to the CN when the handover has been executed inside the same visited domain.Otherwise,the Auth token must be signed by the new vHA,and thus becomes invalid and the RO execution must starts from the beginning.

D.Flush Request for SMIPv6

When the MN detaches from its visited network while leaving ongoing flows active,vHA informs the CNs to stop sending their flow with a Flush request(FR)message
FR(CN\CGCoA\CGCoA Param)\CGvHA Param)\CGvHA Sign

III.SECURITY VALIDATION OF SMIPv6

The executions in the home and visited networks,the BT and the RO of SMIPv6 have been implemented in NS-2,runned by the VMware(virtual machine).The TCL coding is simulated in the virtual machine.The following coding is to setup ns and topology object.

```
set ns [new Simulator]
set tracefd [open out.tr w]
set namtrace [open out.nam w]
$ns trace-all $tracefd
$ns namtrace-all-wireless $namtrace $val(x) $val(y)
# set up topography object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
```

IV.SECURITY ANALYSIS OF SMIPv6

White List of Domains: For an entity to authenticate a message, it is crucial to have a list of domains that it can trust. The mobile operators must maintain a list of domains
that allow its MNs to:
1) connect to the domain, update the binding cache, and allow BT;
2) allow RO.
This adds control, flexibility, and scalability to operators who can configure its whitelist of domains according to the agreements it holds with its competitors. Wildcards cannot be used as it would make any registered domains be trusted.

DNSSEC Global Availability: As opposed to a global scale certificate authorities or subnet certification using chain
certificates.

Mobile Operators Secure Their Network: To keep their trusted status, mobile operators have every incentive to secure
their network by analyzing every incoming and outgoing messages. If attacks can be led from an operator, it may lose
its trust relationships with other operators and, consequently,
see its customers being denied RO or event BT in visited networks.

V. OUTPUTS AND GRAPH

Mobile node(MN) generates cryptographically generated home address(CGHA) and submit in home agent(HA).HA sends acknowledgement regarding storage success to MN.MN sends communication request to HA.HA sends fully qualified domain name(FQDN) to MN.HA adds the MN IP in the white list. After this the transferring of data packets takes place. weak authentication to ensure sender invariance of the router advertisement messages strong authentication for all other messages sent from the MN, HA, VHA and the DNS server.

secrecy to ensure confidentiality of symmetric keys held by the MN and shared with its HA and the CNs.DNSSEC enables a node to securely verify if a CGA is part of a trusted domain. Given that a CGA cannot be spoofed, receiving a message from a CGA signed by a trusted entity(HA/VHA) of a trusted domain increases the security property to strong authentication instead of sender invariance.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

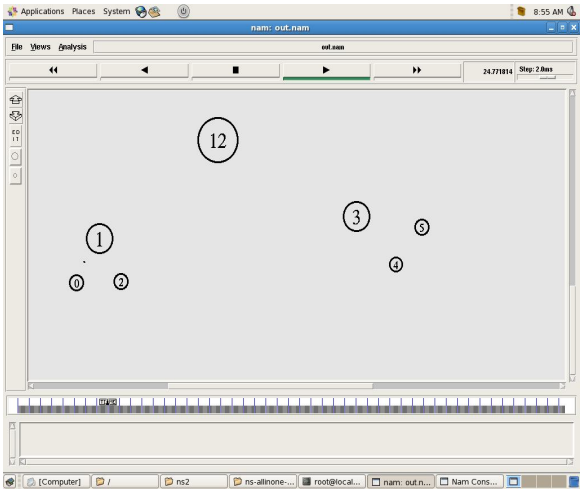

Fig.5 Control packets transfer through home agent

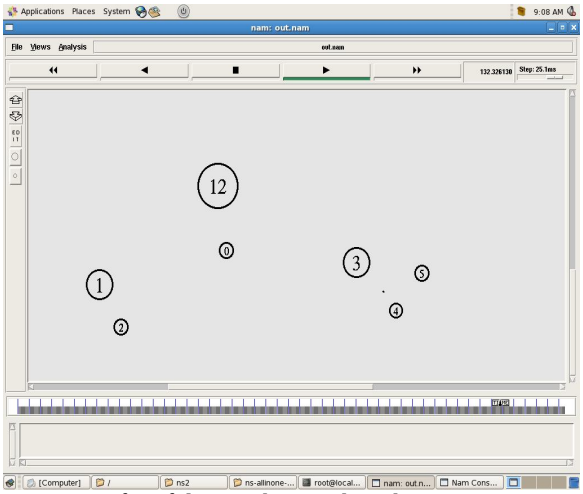

Fig.6 Transfer of data packets without home agent

The mobile node(0) sends CGHOA to HA(1)
1 registers MN FQDN
0 sends CGHOA to 12
0 received Acknowledgement
0 started communication to CN through 12
Data packets transfers
0 sends CGHOA to 12
0 received Acknowledgement
0 started communication to CN through 12

However, because no assumption has been given about the knowledge of trusted domains to the MN, it must rely initially on the sender invariance property for the router advertisements. Note that the sender invariance is implemented in NS2 using the weak authentication on goal along with a witness and request security predicates using the message's source identity as the authenticator and the authenticated.

The previous paper uses the AVANTSSAR tool for performing this route optimization and bidirectional tunneling method.The proposed system uses the network simulation software for performing the optimization algorithm.So this algorithm works better in network simulation software.

GRAPH

The curve denotes the packets transfer rate for the corresponding simulation time.At starting the initialization process is going on,so the packet transfer does not takes place.upto 100th point there is no transfer of packects,only communication request takes place between home agent and mobile node and between server and mobile node.After these process only tranfer of packets takes place.The curve increases corresponding to the simulation time.

The following commands are to be followed for getting the graph

```
[root@localhost ns-2.32_rpt]# cd rpt
[root@localhost rpt]# cd script
[root@localhost script]# ls
graph out.nam out.tr project.tcl project.tcl~ scen15 scen15~
[root@localhost script]# cd graph
[root@localhost graph]# sh graph.sh
set udp_(0) [new Agent/UDP]
$ns attach-agent $n(3) $udp_(0)
set null_(0) [new Agent/Null]
$ns attach-agent $n(4) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 1000
$cbr_(0) set interval_ 0.02
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 2000
$cbr_(0) attach-agent $udp_(0)
$ns connect $udp_(0) $null_(0)
$ns at 130.745845245079067 "$cbr_(0) start"
$ns at 156.745845245079067 "$cbr_(0) stop"
```

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

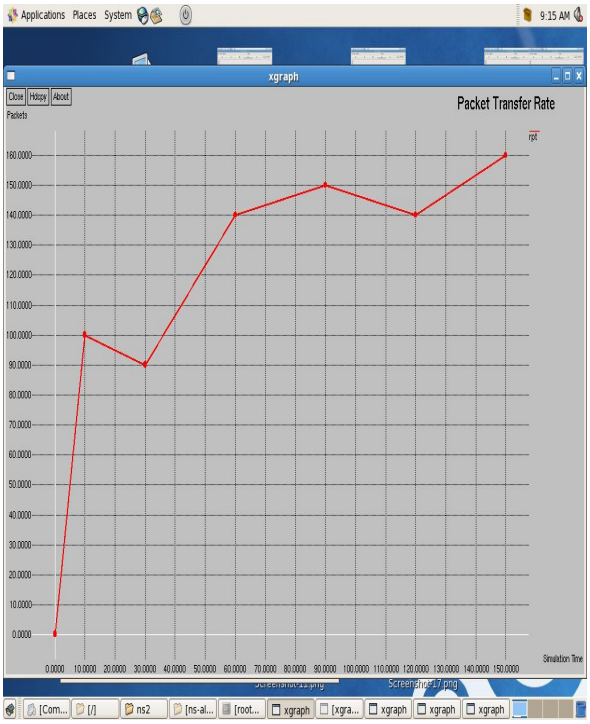

Fig Simulation Vs Packet transfer rate

VI. CONCLUSION AND FUTURE WORK

This paper proposed a secure MIPv6 (SMIPv6) that includes a new secure and efficient RO using an ECGA to tackle the RR weaknesses and the unrealistic assumptions of existing works. Moreover, the use of trusted domains allowed the HA, VHA, and CN to strongly authenticate all incoming messages, thus tackling all major attacks while relying on realistic assumptions and keeping the radio signaling overhead to a minimum. And also the future work includes session continuity during rapid handover. The way of implementation is done by mobility monitoring,vHA analysis and finally handover to VHA.There MN's services continue without any interruption. Results are simulated using network simulation.

REFERENCES

[1] *A.* Z. M. Shahriar and M. Atiquzzaman, "Evaluation of prefix delegation-based route optimization schemes for NEMO," in IEEE International Conference on Communication, Dresden, Germany, Jun. 14-18, 2009.

[2] Deguang Le, Jinyi Chang School of Computer Science & Engineering,Chang shu Institute of Technology Changshu 215500, China ''Tunnelling-Based Route Optimization for Mobile IPv6" {ledeguang,changjy}@cslg.edu.cn.

[3] D.Kavitha *, Dr.K.E.Sreenivasa Murthy, S.Zahoor ul Huq 2010 International Conference on Recent Trends in Information, Telecommunication and Computing '' Security Analysis of Binding Update Protocols in Route Optimization of MIPv6" .

[4] Abu Zafar M. Shahriar and Mohammed Atiquzzaman "Performance of Prefix Delegation-Based Route Optimization Schemes: Intra Mobile Network case" IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings,shahriar,atiq}@ou.edu.

[5] NamYeong Kwon School of Information and Communication Engineering
Sungkyunkwan University Suwon, Korea," The Reliable Packet Transmission Based on PMIPv6 Route Optimization" 978-1-4673-0990-5/12/$31.00 ©2012 IEEE.

[6] Li Xia, Lizheng Fang , Hong Liu "A Low-latency and Smooth Handover Scheme for Mobile IPv6", 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application,College of Information Science and Engineering, Northeastern University, Shenyang 110004, China,".

[7] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, "Routing optimization security in mobile IPv6," Comput. Netw., vol. 50, no. 13,pp. 2401–2419, 2006.

[8] B. S. V. R. S. u. H. D. Kavitha and K. E. Sreenivasa Murthy, "An efficient hierarchical certificate based binding update protocol for route optimization in mobile IPv6," Global J. Comput. Sci. Tech., vol. 10, no. 2, pp. 47–51, 2010.