International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 10
ISSN: 2454-4248
248 – 254

Enhanced Home Registration Security Protocol in MobileIPv6

Dr. Sridevi
Assistant Professor, Department of Computer Science,
Karnatak University, Dharwad

Abstract:- The Enhanced Home Registration (EHR) protocol extends the basic home registration protocol defined in MIPv6 to support the location authentication of MNs to their HAs. The EHR is based on novel ideas of segmenting the IPv6 address space, using a symmetric CGA-based technique for generating CoAs, and applying concurrent CoAs reachability tests. As a result, EHR is able to reduce the likelihood of a malicious MN being successful in luring an HA to flood a third party with useless packets using MIPv6. In addition, EHR enables HAs to help in correspondent registrations by confirming MNs' CoAs to CNs.

Keywords: MobileIPv6, Enhanced Home Registration,Cryptographically generated addresses,Mobile Node. Etc.

*****

1. Introduction

A mobile node can commence a procedure called Home registration, with the purpose of reporting the HA on the present physical coordinates of the mobile node. It is achieved by the implementation of BU and BA mobility messages. In the instance that mobile node travels farther away from the reach of home link, the node transmits a query towards the home router to fulfil the function of a home agent through registering its CoA under the router. This procedure also facilitates the mobile node to provide updated information towards the HA regarding the CoA following transition onto a separate, foreign link. In order to lengthen the cycle of registration reaching expiry, or eradicate a registry once home link has been returned. MIPv6 considers safety and protection of home routers as critical to mitigate the possibilities of invasions. The mobile node utilizes HA services belonging to identical management platform. Therefore, it can be thought that a relation between the HA and mobile node previously exists, and therefore the two elements are capable of sharing previously-defined security codes (or different recognition platforms, i.e. certifications) to facilitate development of a bidirectional IPSec Security Association (SA), which could afterwards be deployed for the protection of home registrations. As conclusion, MIPv6 platform utilizes IPSec Encapsulating Security Payload (ESP) and sequence numbering as measures to secure exchange of traffic amidst HA and MN. The administrative traffic incorporates BU and BA mobility messages, carried though Mobility Header under IPv6.

A mobile node begins registration through transmitting with the HA an BU message, the constituents of the message incorporates the mobile node's HoA, sequence number, present CoA and binding contract. It is necessary for the mobile node to offer its CoA under the header even under the condition that the CoA imitates the BU's source address. This occurs given the fact that IPSec ESP under transmission setting provides no security towards the IPv6 header. In order to mitigate potential invasions, the mobility node allocates the sequence number as a value above the one sent in the prior BU towards the HA (only if applicable). Moreover, if the primary objective is eradicating the node's binding entry at HA, the mobile note will establish the CoA as identical with its HoA and present the binding contract as nil. Conclusively, if a span of a single second passes without the MN receiving appropriate response to the BA message, the message will be resubmitted by the mobile node. The transformation procedure is multiplied through each retransmission, until either appropriate response is acquired, or the entire process spans over the highest permissible thirty-two seconds. Subsequently, the mobile node will continuously request transmission through BU messaging, however, this is only expected if the locality hosts only a single HA. After sufficient delay has passed, the mobile node will attempt connection to another HA, if available.

A BA message is constituted by the mobile node's HoA, the provided binding lifetime, a sequence number, which is identical the number held under the BU message, and possibly, binding refresh advice. The granted binding should ideally be lesser compared to binding refresh advice, could be facilitated through the BA message recommending that the mobile node refresh home registrations over shorter spans. Conversely, in the condition the the mentioned assessments yield negative results, or the DAD evaluation shows failure, the binding will be entirely rejected by the HA, alongside appropriate response citing the reason and motive for termination through a provided value.

In the condition that a BA is being acquired through the HA, the mobile node assesses IPSec SA that has to be utilized. Subsequently, the mobile node reaffirms the credibility and viability of the received BA messages. The sequence number provided through the BA is too reaffirmed for credibility and viability, compared against the number provided by the mobile node, as kept under corresponding Binding Update List. In the condition that even a single authentication fails, the messages will be immediately discarded by the mobile network with no possible alternatives

 ISSN: 2454-4248
248 – 254

The utilization of sequence numbers and IPSec provides limited security to home registrations against invasions. Particularly, invaders can be prevented from transferring decayed or infected messages. Moreover, it can also mitigate the capability of an actual mobile node to send a BU as representative of some other mobile node accessing through identical HA.

2. Enhanced Home Registration (EHR) Protocol

The basic home registration process included in the MIPv6 protocol to enable an MN to register its current CoA with an HA. The investigation showed that the HA could not authenticate the given CoA. Therefore, the MN could lie about its current location and lure the HA to redirect traffic to a third party causing a DoS attack against that third party. An enhanced home registration process to support location authentication of MNs to their respective HAs. This is called the Enhanced Home Registration (EHR) protocol. The EHR protocol allows an HA to verify that a claimed CoA is indeed an MN's real location. As a result, the EHR protocol can reduce the likelihood of a malicious MN being successful in luring an HA to flood a third party with useless traffic using the MIPv6 protocol.

The EHR protocol extends the basic home registration protocol defined in the MIPv6 base document by making use of a combination of three ideas. Firstly, it uses a novel lightweight version of the traditional CGA-based technique to cryptographically generate and verify MNs' CoAs. This is called the symmetric CGA-based technique. This technique makes use of a secret key shared between an MN and its HA in the CoA generation and verification processes.

3. The Concurrent CoA Reachability Test

The entire aspect of creation CoA through cryptography is preceded by the consideration of present CoA viability evaluations to assess the mobile node's viability over the claimed CoAs. Such an assessment would facilitate HA to register and utilize the mobile node's new CoA whilst evaluating the mobile note's viability towards the CoA. Two messages are utilized by the assessment: Binding Acknowledgement with Care-of Token (BACoT) message and a Binding Update with Care-of Token (BUCoT) message.

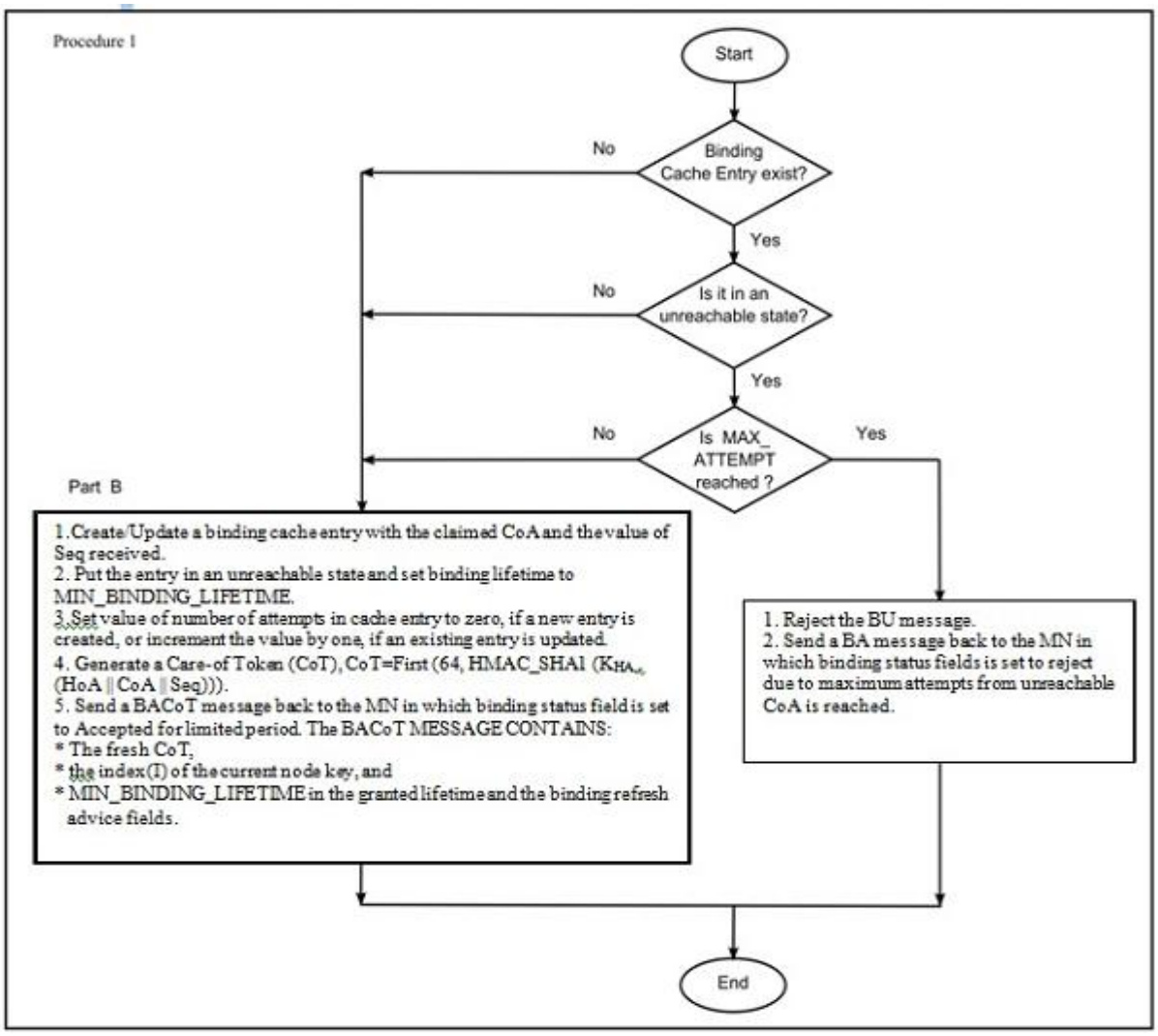

Figure 1: Procedure 1 - executed by an HA upon receipt of a valid BU message

ISSN: 2454-4248
248 – 254

The reachability test is initiated as soon as an HA receives a valid BU message from an MN. HA replies by sending a BACoT message to the MN. The BACoT message acknowledges the binding of the new CoA and delivers a fresh care-of token to the MN. The MN uses the received token to show its presence at the new CoA, i.e. the MN sends a BUCoT message containing the received token to the HA. When the test concludes, the HA sends a BA message to the MN acknowledging the receipt of the token; hence, the successful completion of the reachability test. A care-of token is a 64-bit number that is produced using the idea of a `node key. The node key is only known to an HA, and it allows the HA to verify that a token enclosed in a BUCoT message is indeed its own. The HA generates a fresh node key at regular intervals and identifies it by an index. The HA produces a fresh care-of token based on its active node key as well as values of the MN's HoA, the MN's claimed CoA, and the sequence number received in a valid BU message. The HA may use the same node key with all of the MNs it is in communication with to avoid the need to store a token per MN.

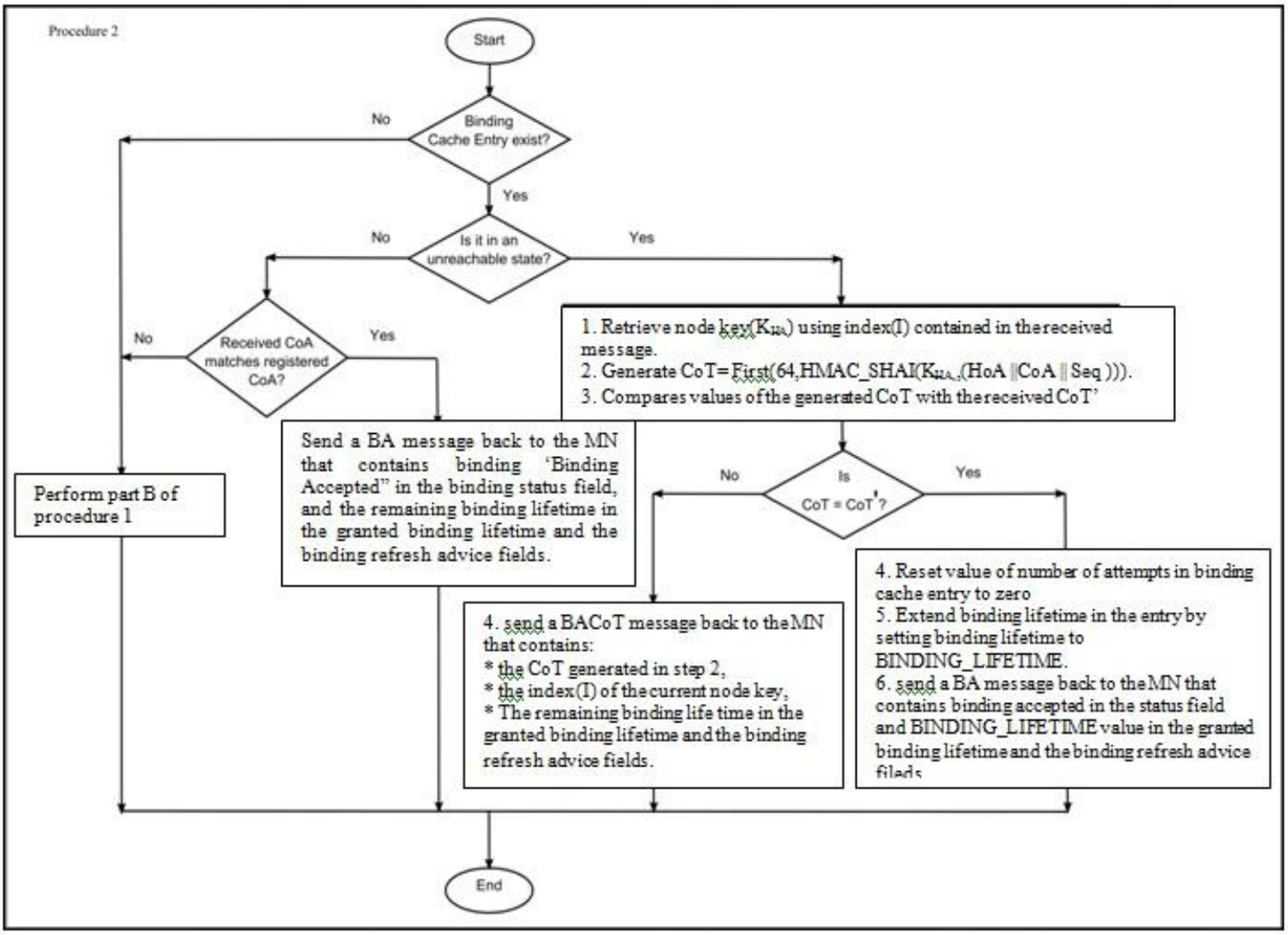

Figure 2: Procedure 2 – implemented through HA based on affirmation of a received, reliable BUCoT message

4. EHR Protocol Description

The EHR protocol is based on three fundamental ideas; (1) cryptographically create CoA of mobile nodes through a shared secret key; (2) affirm the MNs' credibility regarding the claimed CoAs; and (3) discern amongst various types of addresses. The EHR protocol adds the three ideas mentioned above to the basic home registration protocol to help HAs authenticate MNs' CoAs. The whole picture of the EHR protocol is illustrated in Figures 3 and 4.

ISSN: 2454-4248
248 – 254

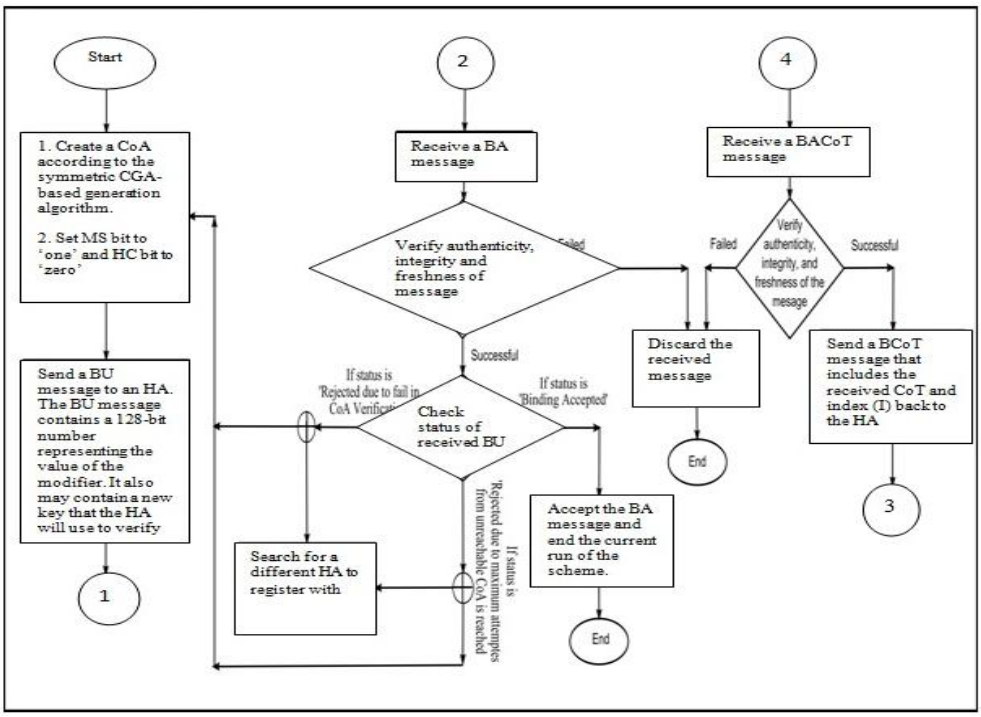

Figure 3: EHR protocol at mobile node side

The EHR protocol is based on the BHR protocol; it also uses IPSec ESP and sequence numbers to protect home registrations. Therefore, the EHR protocol has the same security protection as the BHR protocol. Specifically, it can protect home registrations against outsider attacks; an attacker cannot send a spoofed or a replayed BU message instead of the MN. It also can prevent malicious MNs from falsely sending BU messages on behalf of other MNs. Furthermore, the EHR protocol extends the BHR protocol to support the location authentication of MNs to their HAs. It adds the novel ideas of segmenting the IPv6 address space, using a symmetric CGA-based technique for generating CoAs, and applying concurrent CoAs reachability tests to the basic home registration protocol.

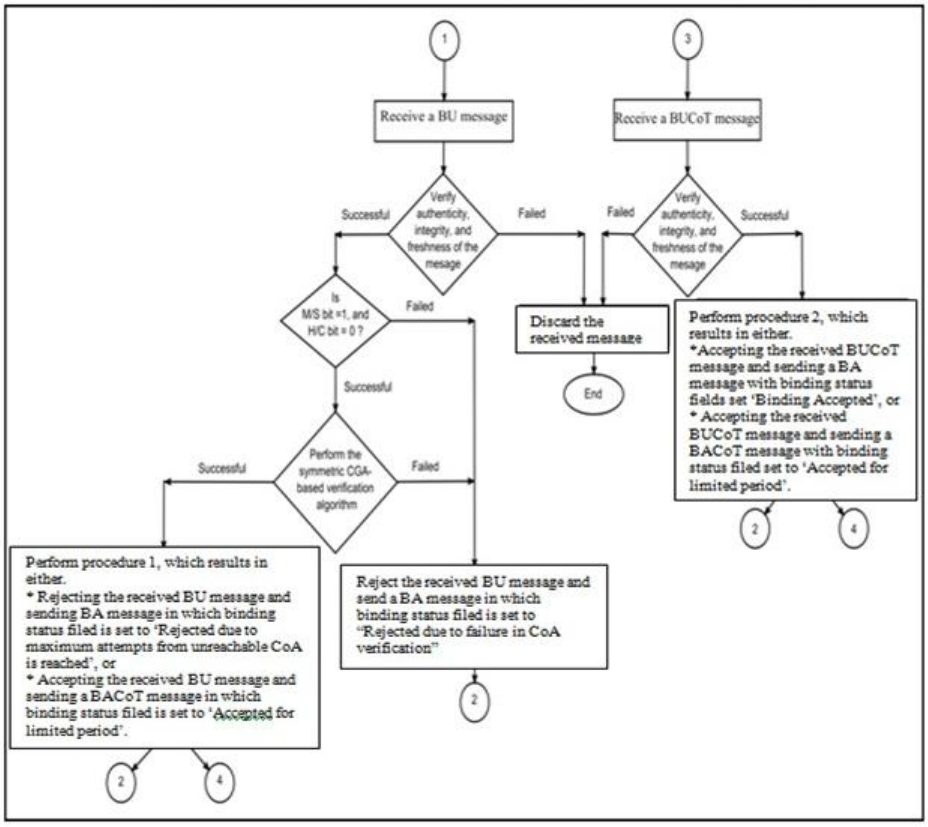

Figure 4: EHR protocol at home agent side

 ISSN: 2454-4248
248 – 254

5. Performance Evaluation

Assessment of ERH performance through contrasting it with basic (BHR) protocol. This can be facilitated through utilizing OPNET Modeler simulation software and CryptoSys Cryptography Toolkit. A concise introduction on these elements is provided under Appendix C. The productivity is assessed in regards to delay in home registration, assessed in seconds while overhead signalling evaluated through bits per second. The HR-Delay is elaborated as the aggregate time consumed by the mobile node to achieve a message of acknowledgement (i.e. a BACoT in the EHR protocol or a BA in the BHR protocol) from HA, following release of a BU message. Overhead signalling is the aggregated volume of Mobile IPv6 signaling traffic exchanged over the HA and mobile node

5.1 Simulation Model Validation

For achieving such, an authentication procedure comprising two phases is utilized. The first phase includes utilization of OPNET debugger to signify that the EHR protocol to be operating as normal. The OPNET debugger is implemented to assess the performance of both processes; CoT and CoA. Moreover, applicable packet details (i.e., value of CoT, packet size, source address, destination address and value of modifier) has been evaluated during operational procedures.

5.2 Theoretical Model

In order to facilitate validation and simulation, the equation for calculating theoretical value of the HR-Delay is provided below:

HR _Delay = Delay for BU message + Delay for BACoT message
+ Delay for HoA DAD test (4.1)

Four types of delays are responsible for causing the delay in the transmission of both BU and BACoT: transmission delay, propagation delay, queuing delay, and processing delay.

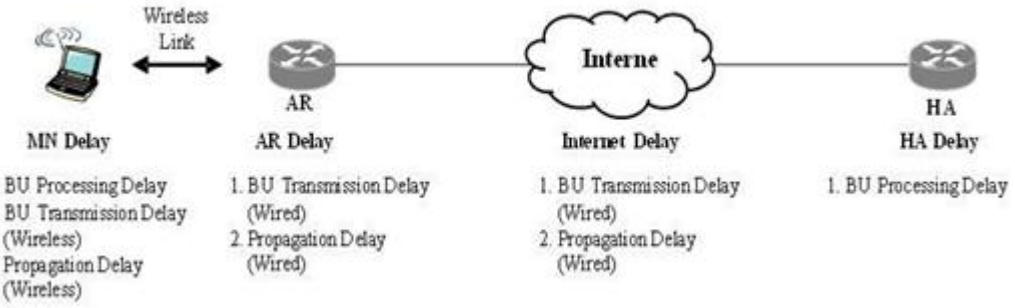

Figure 4.8: Theoretical delay for BU message

Total Delay for BU Message = MN Delay + AR Delay + Internet Delay + HR Delay

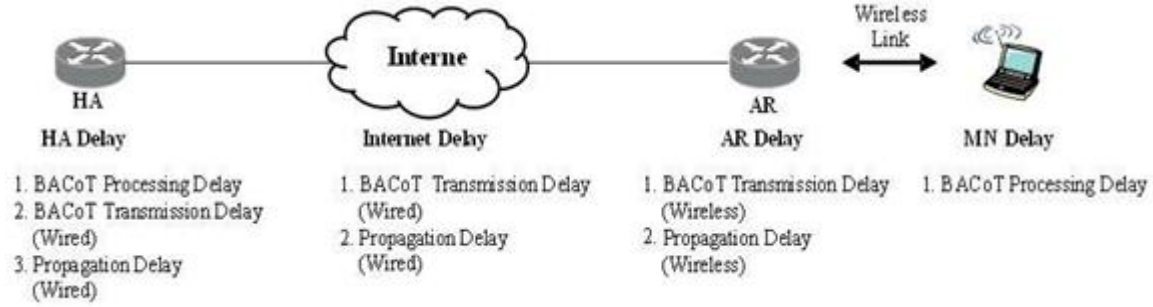

Figure 4.9: Theoretical delay for BACoT message

Total Delay for BACoT Message = HA Delay + Internet Delay + AR Delay + MN Delay

Transmission Delay: Transmission delay is the necessary volume of time for transmission of packets towards their intended designation, the formula for assessment of transmission delay is provided below:

Transmission-Delay = Packet Size / Bandwidth

Packet Size is the determination of aggregate bits present under a packet, whilst Bandwidth elaborates the particulate rate of data transmission for a link.

Propagation Delay: Propagation delay is aggregate time consumed by packet's bits to proliferate onto other networks. The formula for assessment of propagation delay is provided below:

Propagation -Delay = Distance / Propagation Speed

Queuing Delay: Queuing delay constitutes of delays in regards to both the transmission and receiving messages. The latter is the volume of time that a message has to wait before processing can occur, whilst the former is the measurement of time spent on waiting for the transmission of the message.

Processing Delay: Processing delay points towards the

 ISSN: 2454-4248
248 – 254

necessary time spent for the processing of inbound and outbound packets at both nods, respectively. The procedure delay towards EHR protocols dependant on HMAC_ SHA1 delay. The HMAC_SHA1 element is utilization through home agent two times to affirm the CoA's integrity and create a new CoT. The HMAC_SHA1 latency is assessed.

6.Simulation Results

Results from the simulation provides and processes simulation results acquired from the research regarding both HR-Delay and control signaling overhead. It contrasts the conclusion regarding both EHR and BHR protocols.

Home Registration Delay: This provides an assessment on the HR-Delay simulation conclusions. An entire assortment of simulation results is depicted, beginning from Figure 5shows that the HoA DAD delay is programme to nil, even during the initial registration of CoA at a HA, i.e. set to zero even during the first registration of a CoA at an HA, i.e. when an mobile node transition from subnet towards a foreign subnet. The delay is assessed through utilizing an arbitrary values generated through a random generator, which greatly influences the viability of acquired results.

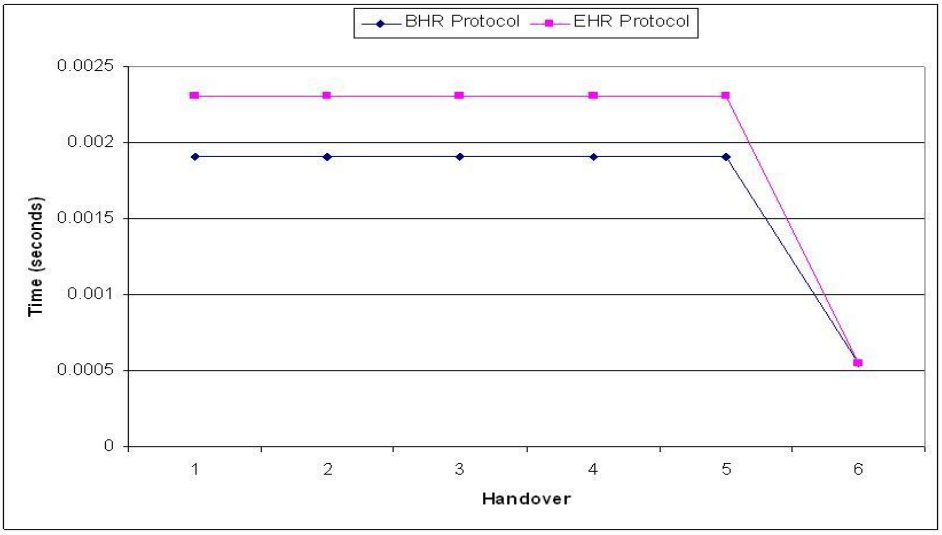

Figure 5: HR-Delay for BHR and EHR protocols vs. handover (one MN, three CNs, 0% load)

6.1 Control Signaling Overhead

Figure 6 depict control signalling overheads towards the mobile node side and HA's side, respectively. Commonly, the motive for any deviation in control signalling at the mobile nodes is primarily due to the fluctuation in length and volume of the signalling messages exchanged.

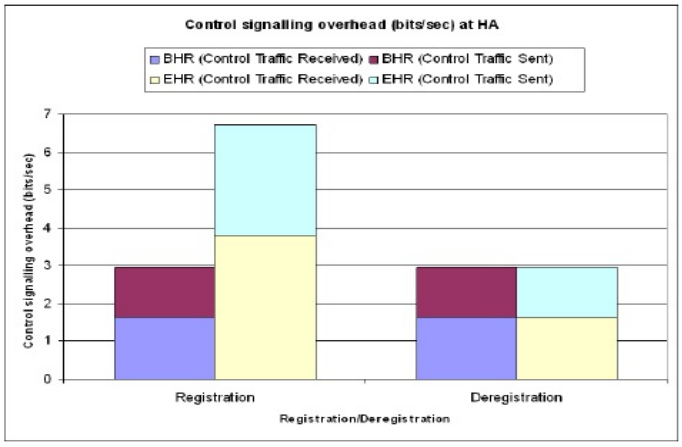

Figure 6: Control signalling overhead (bits/sec) for BHR and EHR protocols at HA

The following observations have been drafted from results of thorough simulation, provided below:

- Firstly, the productivity of both protocols can be considered virtually the same when it comes to delisting.
- Secondly, the productivity of both protocols can be considered virtually the same it comes to HR-Delay.
- Thirdly, the influence of incrementing number of transitioning mobile nodes facilitated by the same HA, on which the productivity of the EHR protocol is greater in comparison to BHR protocol.
- Fourthly, the EHR facilitates multiplies control signalling at both the mobile node and HA as significant payment for adding the location authentication of MNs towards their HAs.

The primary conclusion would be that if a contrast between both protocols was to be executed, and the valuation in performed on basis of efficiency and safety, the ERH would begin consolidating soon enough.

7. Conclusion

This paper brought forward comprehensive detail regarding designing for novel enhanced home registration (EHR) platform which allows HAs to assess mobile node's

 ISSN: 2454-4248
248 – 254

ownership over claimed CoAs. The EHR platform utilizes a combination of three fundamental ideas. Firstly, CoAs is established through cryptography means through utilizing cryptographically using a symmetric CGA-based technique. Secondly, it implements a simultaneous CoA viability and reachability to affirm MN's reachability at a CoAs. Finally, a novel procedure is used for assessing the host type based on their IPv6 addresses. A simulation model of EHR has been constructed using the OPNET Modeller and relevant calculations. The assessment of simulation conclusion expressed that EHR provides trivial delay in the entire registering process, however, but also substantially increments signaling overhead.

References

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6." RFC 3775 (Proposed Standard), June 2004.
[2] C. Vogt, R. Bless, M. Doll, and T. Kuefner, "Early Binding Updates for Mobile IPv6," in Wireless Communications and Networking Conference, 2005 IEEE, vol. 3, pp. 1440{1445, March 2005.
[3] C. Vogt, "Credit-Based Authorization for Concurrent IP-Address Tests," Tech. Rep. TM-2005-3, Institute of Telematics, University of Karlsruhe, Germany,June 2005.
[4] S. Bradner, A. Mankin, and J. Schiller, "A Framework for Purpose Built Keys (PBK)," Expired Internet-Draft: draft-bradner-pbk-frame-06.txt, June 2003.
[5] C. Perkins, "Securing Mobile IPv6 Route Optimization Using a Static Shared Key." RFC 4449 (Proposed Standard), June 2006.
[6] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)." RFC 4861 (Draft Standard), Sept. 2007.
[7] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconconfiguration" RFC 4862 (Draft Standard), Sept. 2007.
[8] M.-S. Hwang, C.-C. Lee, and S.-K. Chong, "An improved address ownership in mobile IPv6," Computer Communications, vol. 31, no. 14, pp. 3250-3252,2008.
[9] S. Gunderson, \Global IPv6 Statistics - Measuring the current state of IPv6 for ordinary users." A study by Google, reported in November 2008.