A Novel Scheme for Supporting Location Authentication of Mobile Nodes

Osama Elshakankiry[1,2], Andy Carpenter[1], and Ning Zhang[1]

[1] School of Computer Science, the University of Manchester,
Oxford Road, Manchester, M13 9PL, UK
[2] Lecturer Assistant at the Faculty of Electronic Engineering, Minufiya University, Egypt
{elshakao,andy,nzhang}@cs.man.ac.uk

Abstract. A home registration scheme is typically used for a mobile node to inform its home agent about the mobile node's current location when it is away from its home link. The Mobile IPv6 protocol protects a home registration scheme against outsider attacks, but it fails to protect from attacks by legitimate mobile nodes behaving maliciously. A malicious mobile node could pretend to own a third-party's address and luring its home agent to flood that victim with useless packets. This paper attempts to address this weakness by proposing a novel secure home registration scheme to support location authentication of mobile nodes to their home agents in Mobile IPv6 networks. The proposed scheme makes use of a combination of two ideas. Firstly, the care-of addresses are formed using a symmetric key cryptographic address generation technique that prevents the stealing of other nodes' addresses. Secondly, concurrent care-of addresses reachability tests are used to verify mobile nodes' reachability at the claimed care-of-addresses. In addition, this paper proposes the idea of segmenting the IPv6 address space into three parts: home addresses, care-of addresses, and stationary addresses to differentiate between nodes based on their IPv6 address. Segmenting IPv6 address space could reduce the number of targets that are vulnerable to flooding attacks launched by malicious MNs. To investigate the efficiency and efficacy of the proposed scheme, the performance, in terms of home registration delay, is investigated using simulation (built with the OPNET™ Modeler version 14.5).

1 Introduction

The Mobile IPv6 (MIPv6) [3] protocol allows mobile Internet host devices (called mobile nodes (MNs)) to remain connected to other correspondent nodes (CNs) while roaming the IPv6 Internet. This is achieved by: (1) allowing an MN to have two IPv6 addresses, a permanent home address (HoA) that identifies the node and a transient care-of address (CoA) that gives its location while away from its home link, (2) introducing a router designated home agent (HA) on an MN's home link, (3) requiring an MN to register its current CoA with the HA when it is away from the home link, and (4) requiring the HA to intercept any packets on the home link destined for the MN's HoA and forward them to the MN's registered CoA, i.e. to the MN's current location.

A.U. Schmidt et al. (Eds.): MobiSec 2010, LNICST 47, pp. 91–102, 2010.

The registration of an MN's current CoA with a HA is done through the use of a home registration scheme. In this, the MN sends a binding update (BU) message to the HA. The HA replies to the MN by returning a binding acknowledgement (BA) message. These mobility messages exchanged between MNs and HAs, i.e. BUs and BAs, are protected using IPsec Encapsulating Security Payload (ESP) and sequence numbers [1, 3]. Upon receipt of the BU message, a HA authenticates the origin of the BU message (**Verification 1**) to ensure that it is indeed sent by the legitimate owner of the claimed HoA. The HA also verifies the integrity of the BU message (**Verification 2**) to detect any unauthorised modification of the message. Furthermore, the HA verifies that the BU message is fresh (**Verification 3**), i.e. it is not a replay. These three verifications prevent an attacker from impersonating the MN by sending a false BU message to the HA. In other words, they protect against outsider attacks.

While MIPv6 provides all these protections against outsider attacks on the home registration scheme, it fails to protect against attacks by legitimate MNs behaving maliciously. In other words, MIPv6 does not provide any assurance that a CoA given by an MN in a BU message is correct. As a result, it is possible for an authorised MN to launch denial-of-service (DoS) attacks against third parties. These attacks are not addressed by MIPv6 because it is assumed that an MN can only register one CoA and if the MN cheats the HA with a fake CoA then the MN will lose the communication with the HA, thus losing its mobility. However, recent research [5, 12] has suggested that MNs could be multi-homed. In such a scheme, a multi-homed MN can: (1) have multiple HoAs connected to different home links, and (2) bind a HoA to more than one CoAs. As a result, the MN may cheat one or more of its HAs with victim addresses while maintain mobility through other HAs. If this cheating is successful, it is possible for the cheated HAs to flood the victims located at the fake CoAs with unwanted packets. This paper proposes a solution to this threat. The solution allows a HA to verify an MN's ownership of claimed CoAs, i.e. to ensure that the CoAs claimed by the MN match with its real locations. By supporting location authentication of MNs to their respective HAs, the solution is able to prevent malicious MNs from luring their HAs to flood victims with useless packets using MIPv6.

The rest of the paper is organised as follows. Section 2 discusses three existing state-of-the-art approaches to the authentication of nodes' addresses, and identifies their security and performance limitations. Section 3 is devoted to our novel home registration scheme and its analysis. In section 4, we further examine the performance of the proposed scheme, in terms of home registration delay measured using OPNET™ Modeler 14.5 simulation [9]. Finally, Section 5 concludes the paper.

2 Related Work

Existing protocols that support the authentication of a node's address to other nodes generally use one of the three approaches; using a third trusted entity to sign the address, using an address reachability test, or using a cryptographically generated address.

Ren, et al.'s protocol [11] uses the first of these approaches, i.e. MNs' CoAs are signed by the foreign links and both HAs and CNs authenticate the addresses by verifying the signatures. Although this allows HAs to authenticate MNs' CoAs, it requires

an infrastructure that supports this authentication service, i.e. it requires the use of trusted third parties to verify the CoAs used by MNs. In addition, it requires both the HAs and foreign access routers to perform computationally expensive signature generation and verification operations. This can significantly degrade routing performance and reduce throughput at both the home network as well as the foreign network. The protocol also increases home registration handover delay because the access router in the foreign link needs to sign the CoA, and the HA needs to perform certificate and signature verifications before accepting the CoA as the current location of the MN.

The second approach is used by a number of protocols such as return routability [3] and early binding update [13] to assure CNs that MNs are reachable at the claimed addresses. With this approach, a CN sends two pieces of information, i.e. two different tokens, to the MN's claimed HoA and CoA. If the CN is able to receive a reply from the MN, this means that the MN is reachable via its HoA and CoA. A major limitation with this approach is that it only provides a proof that the MN can receive messages sent to the claimed addresses; it gives no assurance that the MN is connected to the claimed addresses. In addition, it requires at least two additional messages and one additional round-trip delay between the claimed address and the CN address, thus it increases signalling overheads and handover delay.

The third approach to support the authentication of a node's address is through the use of a cryptographically generated address (CGA). The CGA based technique was first proposed to prevent stealing and spoofing of existing IPv6 addresses [7]. A CGA-based address is an IPv6 address for which the interface identifier part is generated using a cryptographic one-way hash function that takes the address owner's public key and some auxiliary parameters as its input. The address owner can protect a message sent from the address by attaching its public key and auxiliary parameters to the message and signing it with the corresponding private key [2]. Thus, the address owner asserts its ownership of the address by using the corresponding private key. Upon receipt of the signed message, the intended recipient verifies the binding between the public key and the address by re-computing and comparing the hash value with the interface identifier part of the address. In addition, it authenticates the address by verifying the signature. In the context of MIPv6, the CGA-based technique is used to assure CNs that an MN is the legitimate owner of a HoA in a number of protocols [4, 8]. However, there are no proposals that use a cryptographically generated CoA to prove a node's ownership of a CoA. The main limitations of the CGA-based technique [14] are, firstly, it is computationally expensive to generate and verify CGA addresses and digital signatures. Secondly, the short length (64-bits) of the interface identifier means that it is vulnerable to a preimage attack. That is, the number of attempts needed by an attacker to generate the same cryptographic address using an alternative public key is about (2^{62}) attempts, which is not sufficient to provide enough protection. Thirdly, it does not guarantee the owner's reachability at the address, i.e. an attacker can use its own public key and a spoofed subnet prefix to cryptographically generate a non-used address with a subnet prefix from a victim network. Fourthly, although it can effectively stop attackers from impersonating valid IPv6 addresses to launch attacks, it can not thwart attacks on an entire network by redirecting data to a non-used address. Finally, as a message needs to carry address

owner's public key and signature, and auxiliary parameter values that are used to generate the address cryptographically. There is a certain amount of overhead incurred to the bandwidth consumption.

3 New Home Registration Scheme

In this paper, we present a novel home registration scheme that provides assurance that a CoA claimed by an MN is indeed its real location. The proposed scheme extends the home registration scheme defined in the MIPv6 base document [3] by making use of a combination of two ideas. Firstly, it uses an improved version of the CGA-based technique, i.e. a symmetric key CGA-based technique, to cryptographically generate MNs' CoAs. Secondly, it applies concurrent CoAs reachability tests to ensure HAs that MNs are reachable at the claimed CoAs. In addition, this paper proposes the idea of dividing the IPv6 address space into home addresses, care-of addresses, and stationary addresses to determine nodes' types based on their IPv6 addresses.

3.1 Symmetric Key Cryptographically Generated CoAs

The first idea of our proposed scheme aims to prevent stealing of other nodes' addresses. It uses an improved version of the CGA-based technique, i.e. a symmetric key CGA-based technique, to cryptographically generate MNs' CoAs. The symmetric key CGA-based technique makes use of a secret key shared between an MN and its HA in the CGA generation and verification processes. This key replacement brings the following advantages. Firstly, the MN (CoA owner) and its HA (CoA verifier) are not required to generate and verify a digital signature, respectively, in order to verify the authenticity of the CGA-based CoA, and this can reduce computational overhead imposed on the MN and the HA as the result of using the CGA based technique. Secondly, it removes the need to include MN's public key and signature in the BU message sent by the MN to the HA to be able to verify the CGA-based CoA, and this can reduce amount of signalling overheads.

In order for an MN to be able to register a CGA-based CoA with a number of HAs, the key used in the address generation and verification processes must be shared with all of the HAs. To achieve this, when the MN is in an initial state (not registered with any HA), it generates a random number that represents a new key. The MN uses this key to cryptographically generate subsequent CoAs when roams away from home and securely sends this key to each HA when first registers with that HA. The HA stores this key in its binding cache entry for the MN's HoA and uses it to verify subsequent MN's claimed CoAs. Using this method, the MN can register its CoA with all the home links. In addition, the original secret key shared with each of the HAs is protected from brute force attacks, as it is not used in the CGA generation process.

The details of the symmetric key CGA-based CoA generation and verification processes are largely similar to those described by Aura [2] and are depicted in Figure 1. When generating a CGA-based CoA, two input values are used: (1) a 64-bit subnet prefix and (2) the current secret key shared between an MN and its HA. The outputs of the address generation algorithm are (1) a new CGA-based CoA and (2) a 128 bit number representing the final value of the modifier. The modifier is carried in a BU

message that is sent by MNs to their HAs in order to convey modifier value. When a HA receives a BU message from an MN, it verifies the claimed CGA-based CoA. The verification process requires the inputs of an IPv6 CGA-based CoA, a 128-bit modifier, and a shared secret key. If the verification fails, the HA will reject the received BU message and reply with a BA message in which binding status field is set to 'Rejected due to failure in CoA verification'. However, if the verification result is positive, the HA will get a strong confidence that the CGA-based CoA was generated by the MN within that specific foreign link and it either belongs to the MN itself or it is a non-used address. To summarise, with our symmetric key CGA-based technique, if an MN behaving maliciously wishes to steal a victim's IPv6 address, the MN will need to attempt about (2^{62}) tries to find a modifier that when used with the subnet prefix and the shared secret key produces the same address.

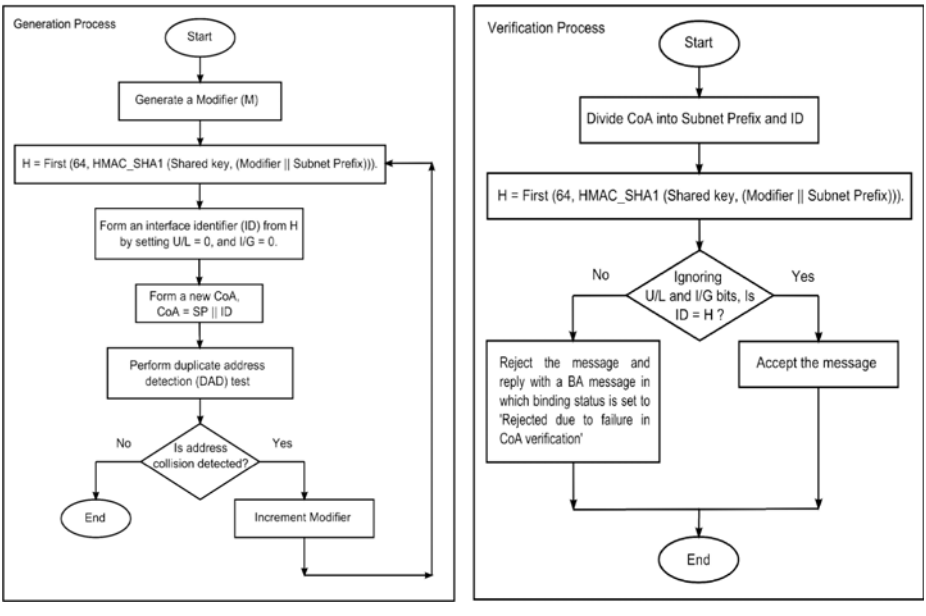

Fig. 1. Symmetric Key Cryptographic Address Generation and Verification Algorithms

3.2 Concurrent CoA Reachability Test

The idea of generating CoAs cryptographically is complemented with the idea of concurrent CoAs reachability tests. A concurrent CoA reachability test allows a HA to register and use a MN's new CoA while concurrently verifying MN's reachability at that CoA. The reachability test uses two additional messages, a binding acknowledgement with care-of token (BACoT) message and a binding update with care-of token (BUCoT) message. Thus, it increases signalling overheads. However, it does not affect handover delay as it runs in parallel with data transfer to and from the new CoA.

The test is initialised as soon as a HA receives a valid BU message from either one of the MNs it has registered with or from a new MN that is requesting the HA to function as a home agent for the MN. The HA replies by sending a BACoT message to the MN. The BACoT message acknowledges the binding of the new CoA and delivers to the MN a care-of token (CoT). The MN uses the received CoT to show its presence at the new CoA, i.e. the MN sends a BUCoT message to the HA that contains the received CoT. When the test concludes, the HA sends a BA message to the MN to acknowledge the receipt of CoT; hence the successful completion of the reachability test. In order to prevent malicious MNs from bypassing reachability tests by keeping sending valid BU messages, the HA limits number of valid BU messages that can be received from unreachable CoAs.

A CoT is a 64-bit number that is produced using the idea of "node key" [3]. The node key is only known to a HA, and it allows the HA to verify that the CoTs contained in BUCoT messages are indeed its own. The HA generates a fresh node key (K_{HA}) at regular intervals and identifies it by an index (I). The HA produces a fresh CoT based on its active node key as well as values of the MN's HoA, the MN's claimed CoA, and sequence number (Seq) received in a valid BU message. The HA may use the same node key with all the MNs with which it is in communication to avoid the need to store a CoT per MN.

The operational procedure of this reachability test is summarised as follows:

1. When a HA receives a valid BU message from an MN, the HA performs Procedure 1, which is shown in Figure 2:
2. Upon receipt of a valid BACoT message from a HA, the MN sends a BUCoT message that includes the received CoT and index (I) back to the HA requesting a longer lifetime through the binding lifetime request field.
3. Upon receipt of a valid BUCoT message from an MN, the HA performs Procedure 2, which is shown in Figure 3:
4. Upon receipt of a valid BA message with 'Binding accepted' status from a HA, the MN accepts the message and the current run of the protocol ends.

3.3 Segmenting IPv6 Address Space

As just discussed, by generating CoAs cryptographically and testing MNs' reachability at claimed CoAs, HAs get a strong confidence that CoAs claimed by MNs match with the MNs' real locations. However, there is still a chance that a malicious MN can falsely claim a third-party's address as its CoA; thus, enabling it to launch redirect attacks against a third-party. To do this, the third-party's address must have a long lifetime, and the malicious MN must be located on the path between a HA and the third-party (so that reachability tests succeed). In this case, the malicious MN can attempt about (2^{62}) tries to find a modifier that when used with the third party's subnet prefix and the shared secret key produces the third party's IPv6 address. Therefore, the ideas of generating CoAs cryptographically and testing MNs' reachability at CoAs are complemented with the idea of segmenting IPv6 address space into three parts: home addresses, care-of addresses, and stationary addresses.

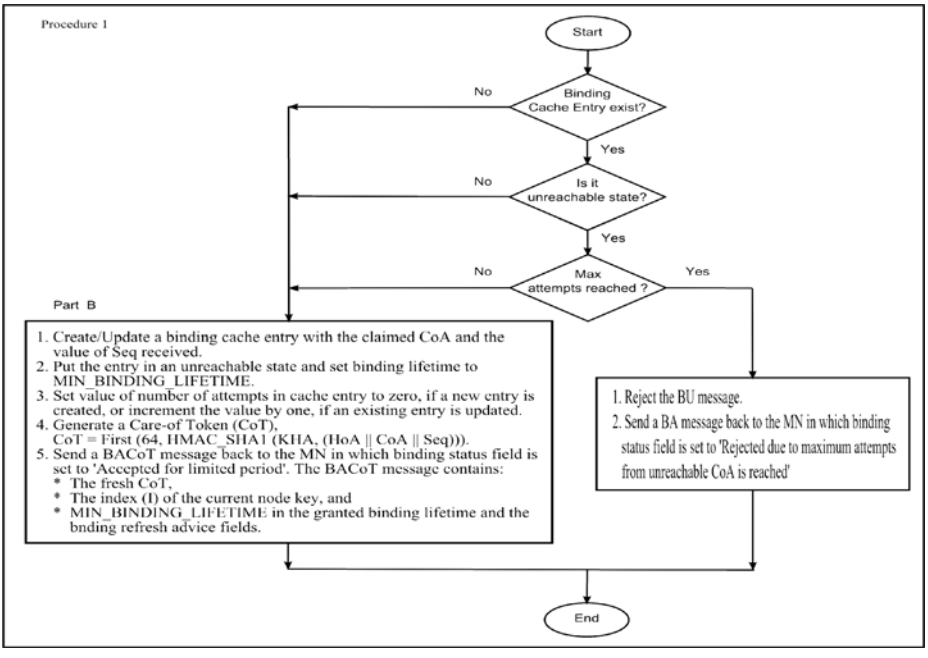

Fig. 2. Procedure 1 (Executed by a HA upon receipt of a valid BU message)

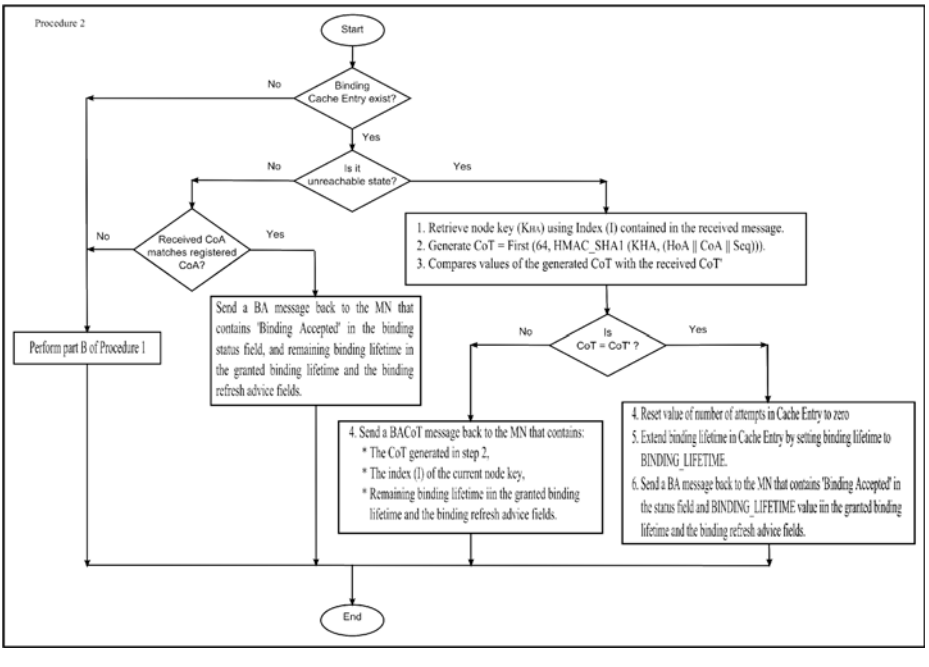

Fig. 3. Procedure 2 (Executed by a HA upon receipt of a valid BUCoT message)

The segmenting IPv6 address space method divides the IPv6 addresses into those that identify stationary nodes ((SNs) - group 1) and those that identify MNs (group 2). Furthermore, the group 2 can be further divided into those that identify MNs located at their home links (group 2.1) and those that identify MNs located at foreign links (group 2.2). In this way, the IPv6 addresses that are vulnerable to flooding attacks launched by malicious MNs are scoped to group 2.2 addresses. In other words, this method (i.e. segmenting IPv6 address space) on its own can protect the IPv6 addresses in group 1 and group 2.1 against flooding attacks.

The segmenting IPv6 address space method uses two bits of the IPv6 64-bits interface identifier field to distinguish between SNs' addresses and MNs' addresses, and between MNs' HoAs and MNs' CoAs. As shown in Table 1, the first bit, i.e. the Mobile/Stationary (M/S) bit, is used to indicate whether an address is for a mobile or a stationary node, and the second bit, i.e. the Home/Care-of (H/C) bit, is used to indicate whether the address is for a mobile node at home link or at a foreign link. The M/S and H/C bits are part of the addresses; hence if a malicious MN changes them that will change the address and the address owner will not be flooded by any directed packets. Consequently, the proposed method prevents malicious MNs from impersonating either stationary nodes or other MNs located at their home links.

The use of the proposed method must be deployed on a global scale on the IPv6 Internet. It requires changing the way every IPv6 node in the world chooses an IPv6 address that seems to be unrealistic. However, the authors can argue this requirement as follows: (1) "IPv6 is still in its infancy in terms of general worldwide deployment" [6] that makes it possible to be changed to support the proposed method; (2) the current IPv6 lack any way to know about a node from its address that makes it necessary to find a way to differentiate between nodes especially with the rapid growth of number of mobile devices connected to the Internet; (3) the authors believed that the benefits of the proposed method far outweigh the costs as it will not only be used to support location authentication of mobile nodes but also in other applications to differentiate between redirectable and non-redirectable IPv6 addresses such as in MIPv6 Route Optimization [3, 4], in protecting against future address stealing [10], and in future protocols that allow redirecting of IP packets from one IPv6 address to another one.

In summary, in the context of supporting location authentication of MNs to HAs, the segmenting IPv6 address space method could protect nodes that use stationary IPv6 addresses as well as MNs' HoAs from being attacked as the result of using MIPv6 protocol. This is because, with this method in place, it is not possible for an MN to falsely claim that a SN's address or another MN's HoA is its CoA.

Table 1. The M/S and the H/C bits

M/S	H/C	
0	X	Stationary nodes (stationary IPv6 addresses)
1	0	Mobile nodes at foreign links (CoAs)
1	1	Mobile nodes at home links (HoAs)
X means either 0 or 1.		

3.4 Whole Picture of the Proposal

The proposal came up with three ideas that (1) cryptographically generate MNs' CoAs based on a shared secret key, (2) verify MNs' reachability at claimed CoAs, and (3) differentiate between different address types. It combines the three ideas mentioned above together to help HAs to authenticate MNs' CoAs. The whole picture of our proposal is illustrated in Figures 4 and 5.

4 Simulation Setup and Performance Evaluation

In this section, we report the performance evaluation of the proposed scheme. The performance is measured in terms of home registration delay (HR-Delay) experienced by an MN when executing the scheme. The HR-Delay is defined as the total amount of time taken for the MN to receive a BACoT message from the HA, after sending a BU message. In order to measure the performance, OPNET™ Modeler 14.5 has been used to simulate the performance of the proposed scheme under varying network conditions. In particular, the performance of the proposed scheme is investigated when varying levels of background traffic on the network are applied and when various numbers of simultaneously roaming MNs are served by the same HA. The simulation results obtained are then compared to those when the standard home registration scheme is run.

The chosen scenario, depicted in Figure 6, is composed of six CNs that are connected via routers (R1 to R6) to the Internet. A HA and three access routers (AR) – each one representing a different IPv6 subnet – are also connected to the Internet. The HA and ARs have been positioned in such a way that provide a continuous wireless coverage area for the MNs. Each MN is communicating with all CNs at the same time and running three Internet applications, i.e. web browsing, e-mail and file transfer. The MNs perform 100 passes (movement between HA and AR3) with 6 handoffs in each pass (5 registration and 1 deregistration). The MNs move from one subnet to another with constant speed and wait an interruption time of 1 hour at each subnet before moving to the next destination.

The average HR-Delay at different network load is measured and illustrated in Figure 7. From this figure, it can be seen that the proposed scheme does not significantly increase the HR-Delay. The increase over the standard scheme is 3.76%, which is caused by the additional two (computationally light) HMAC-SHA1 operations.

Figure 8 compares performance of the standard and proposed schemes as the number of simultaneously roaming mobile nodes increase. It can be seen from the figure that the proposed scheme has a larger rate of increase than the standard scheme. This is because the HA in the proposed scheme is required to perform more operations during registration than in the standard scheme. Consequently, the queuing time at HA side in the proposed scheme increases at a greater rate than it does in the standard scheme. However, the performance of the two schemes is still comparable where the difference in HR-Delay between them increases only by about 668 microseconds when number of simultaneously roaming mobile nodes increases from 1 to 80. This increase is largely insignificant.

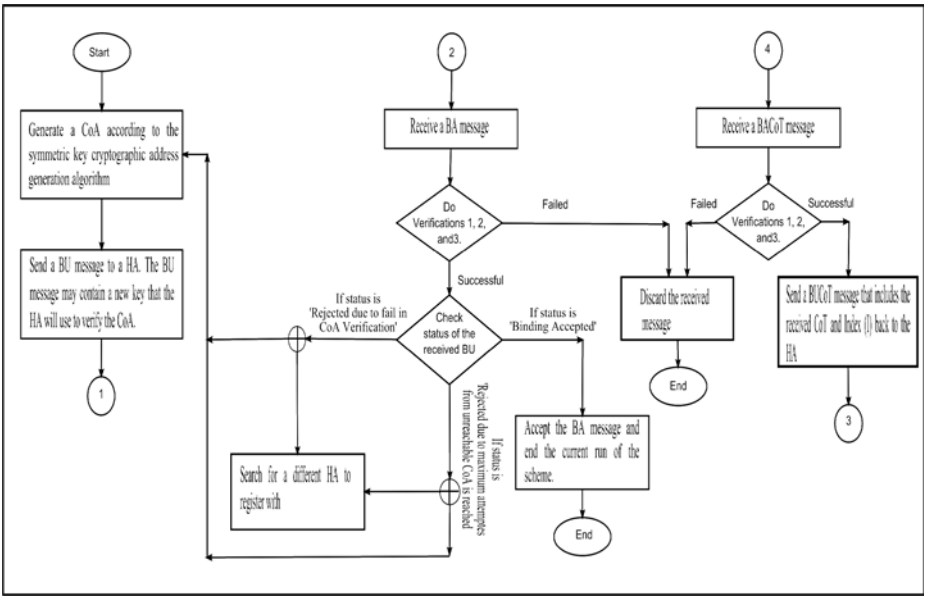

Fig. 4. The proposal at mobile node side

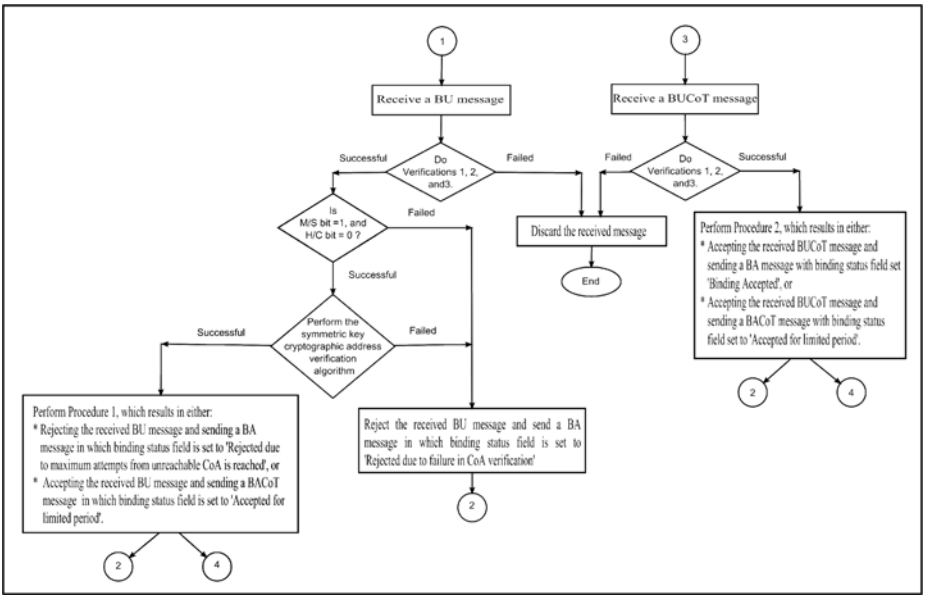

Fig. 5. The proposal at home agent side

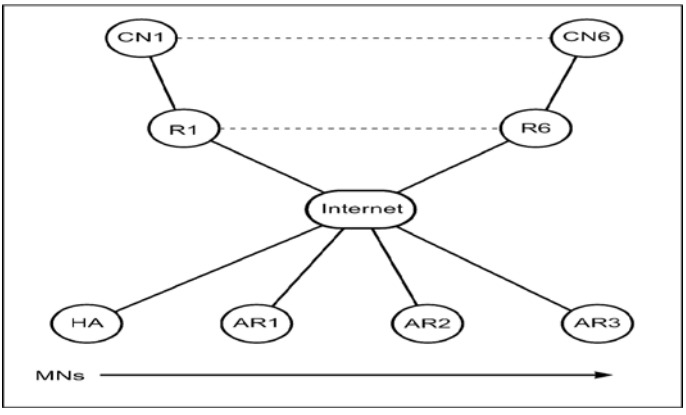

Fig. 6. Simulation scenario

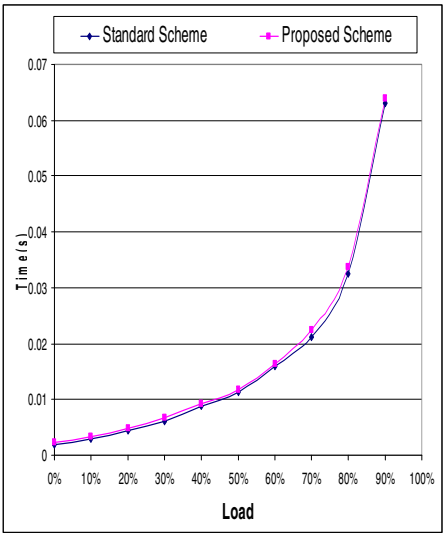

Fig. 7. HR-Delay for standard and proposed schemes vs. load

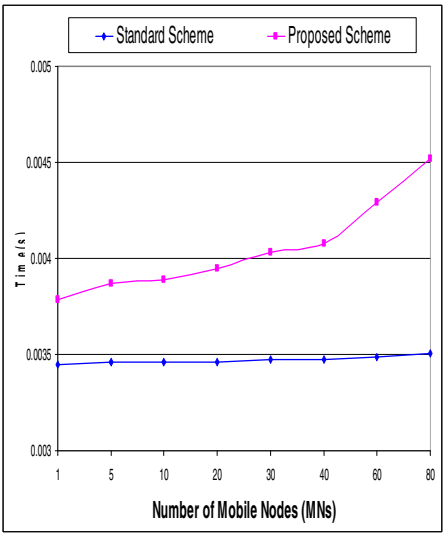

Fig. 8. HR-Delay for standard and proposed schemes vs. number of MNs

5 Conclusions

Home registration scheme implemented in current Mobile IPv6 protocol may introduce flooding attacks against third parties. By claiming to own a third-party's address, a maliciously behaving legitimate mobile node could lure its home agent to flood that victim with useless packets. This paper proposes a novel secure home registration scheme in Mobile IPv6 networks that allows home agents to verify mobile nodes' ownership of claimed CoAs, i.e. provide assurance that a CoA claimed by an MN is

indeed its real location. The proposed scheme uses a combination of two ideas, i.e. generating CoAs cryptographically using a symmetric key cryptographic address generation technique, and using concurrent CoAs reachability tests. In addition, it proposes the idea of segmenting IPv6 address space, to determine nodes' types based on their IPv6 addresses. The performance evaluation of the proposed scheme, measured in terms of home registration delay, has shown that the proposed scheme takes only a 3.76% longer delay than the standard scheme for an MN to register a CoA with its HA. In addition, the results also show that the proposed scheme is scalable, i.e. the effect of increasing number of simultaneously roaming mobile nodes is insignificant.

Further research is required to determine optimal values of: (1) MIN_BINDING_LIFETIME, (2) BINDING_LIFETIME, and (3) interval to generate a fresh K_{HA}.

Acknowledgments. Osama Elshakankiry gratefully acknowledges the faculty of Electronic Engineering, Minufiya University, Egypt for financial support.

References

1. Arkko, J., Devarapalli, V., Dupont, F.: Using IPsec to Protect Mobile IPv6 Signalling Between Mobile Nodes and Home Agents. RFC 3776 (2004)
2. Aura, T.: Cryptographically Generated Addresses (CGA). RFC 3972 (2005)
3. Johnson, D., Perkins, C., Arkko, J.: Mobility support in IPv6. RFC 3775 (2004)
4. Arkko, J., Vogt, C., Haddad, W.: Enhanced Route Optimization for Mobile IPv6. RFC 4866 (2007)
5. Lim, B., et al.: Verification of Care-of Addresses in Multiple Bindings Registration. IETF working draft (2008) (work in progress)
6. Global IPv6 Statistics - Measuring the current state of IPv6 for ordinary users, `http://www.ripe.net/ripe/meetings/ripe-57/presentations/Colitti-Global_IPv6_statistics_-_Measuring_the_current_state_of_IPv6_for_ordinary_users_.7gzD.pdf`
7. O'Shea, G., Roe, M.: Child-Proof Authentication for MIPv6 (CAM). ACM Computer Communications Review 31(2), 4–8 (2001)
8. Elshakankiry, O., Carpenter, A., Zhang, N.: A New Secure Binding Management Protocol for Mobile IPv6 Networks. In: 4th International Conference on Information Assurance and Security (IAS 2008), Naples, Italy, pp. 281–286 (2008)
9. OPNET University Program, `http://www.opnet.com/university_program/`
10. Nikander, P.: An Address Ownership Problem in IPv6. Expired IETF draft (2001)
11. Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J., Deng, R.H.: Routing Optimization Security in Mobile IPv6. The International Journal of Computer and Telecommunications Networking 50(13), 2401–2419 (2006)
12. Wakikawa, R., et al.: Multiple Care-of Addresses Registration. RFC 5648 (2009)
13. Vogt, C., Bless, R., Doll, M., Kuefner, T.: Early Binding Updates for Mobile IPv6. In: Wireless Communications and Networking Conference, vol. 3, pp. 1440–1445 (2005)
14. Cao, Z., Deng, H., Ma, Y., Hu, P.: Integrating Identity Based Cryptography with Cryptographically Generated Addresses in Mobile IPv6. In: Gervasi, O., Gavrilova, M.L. (eds.) ICCSA 2007, Part II. LNCS, vol. 4706, pp. 514–525. Springer, Heidelberg (2007)