Research Journal of Applied Sciences, Engineering and Technology 4(12): 1633-1636, 2012
ISSN: 2040-7467

Submitted: November 17, 2010 Accepted: February 09, 2012 Published: June 15, 2012

Securing Binding Updates in Routing Optimizaton of Mobile IPv6

S. Rajkumar, M. Ramkumar Prabhu and A. Sivabalan
Department of Electrical, SRM University, Chennai, Tamilnadu, India

Abstract: Mobile IPv6 (mipv6) is an internet protocol that allows mobile nodes to have continuous network connectivity to the internet without changing their ip addresses while moving to other networks. The packets sent from Correspondent Node (CN) to a Mobile Node (MN) go first through the mobile node's Home Agent (HA). Then the HA tunnels them to the MN's foreign network. This process of delivering the packets to CN is called triangle routing. Triangle routing problem appears when the indirect path between CN and MN through the HA is longer than the direct path. To overcome triangle routing, Route Optimization (RO) method is added in mobile Pv6. In route optimization, when MN changes its location, it sends a Binding Update (BU) to CN informing its CoA. To secure these Binding Updates, we present a new protocol called "Certificate Based Inquisition Approach" for securing Binding Updates in RO. Performance analysis of this shows that it is computationally efficient than RR protocol and is not susceptible to any security attacks. To show the effectiveness of the proposed technique, it is compared with the state of art of other RO protocols. Simulation results presented in this study are based on the ns2 mobility software on linux platform. The simulations results show that our proposed technique achieves better performance than the Return Routability (RR), Certificate Based Binding Update protocol (CBU), Hierarchical Certificate Based Binding Update protocol (HCBU).

Key words: Authentication, binding updates, mobile IPv6, route optimization, security

INTRODUCTION

Mobile IPv6 is an extension to support mobility to the nodes. When the mobile node moves to a different network link that uses a different subnet prefix, the MN needs to acquire a new IP address. Otherwise, the MN will not be reachable. To support this movement, MN use two addresses: a HoA (HOme Address) and a CoA (Care-Of-Address). A HoA is a static and permanent address that can be used to contact MN regardless of the node's current location. A CoA is a dynamic address that changes with respect to the node's current location. To allow MN to be reachable regardless of its location, Mobile IPv6 introduce a HA (Home Agent) that plays a role of a stationary proxy. The HA intercepts packets sent to an MN's HoA and forwards it to the node's current CoA when they are not located at their home link. In order to achieve this, MN must inform its new CoA to its HA. This process is known as the binding update. In this mode, all traffic from MN to its CN and vice-versa must be tunneled by the HA. Due to this, inefficient use of network bandwidth is inevitable and this problem is known as the triangular routing problem.

To overcome this problem, route optimization has been introduced in Mobile IPv6 Jong-Hyouk and Tai-Myoung (2008). In this method, a MN can update its new address with both the HA and the CN (Sangjin *et al*., 2006). After the update, future traffic can be directly exchanged between MN and its CN. If malicious attackers can corrupt the binding update process, it can hijack a session, attempt various DoS (Denial-of-Service) attacks and bomb neighbors (Nikander *et al*., 2005). To secure Binding Updates Mobile IPv6 recommends use of IPsec (Arkko *et al*., 2004). The use of IPsec can solve authentication and integrity requirement of binding update but cannot solve the location verification problem. The relationship between a MN and its HA is a long-term relationship and it is assumed that there exists a secure tunnel between them. Therefore, it is reasonable to assume that IPsec is used to secure binding update messages between a MN and its HA. Further, a certification path to verify each other's certificate may not exist and the cost involved with establishing a security association may be too heavy for mobile nodes. As a result, using IPSec to secure binding updates between an MN and its CN may not be feasible and not effective.

The location verification problem can be partially solved using the RR (Return Routability) technique (Johnson *et al*., 2004). The basic idea of RR is to test whether a node is reachable using both HoA and CoA before sending the binding update (Johnson *et al*., 2004). A MN initiates RR by sending HoTI (HOme Test Init) and CoTI (Care-Of-address Test Init) messages to its CN. HoTI is sent to CN indirectly through HA whereas CoTI is sent directly. In response to these messages, the CN returns two tokens separately in HoT (HOme address

Corresponding Author: S. Rajkumar, Department of Electrical, SRM University, Chennai, Tamilnadu, India

Test) and CoT (Care-Ofaddress Test) messages. The MN combines the two tokens to compute a symmetric key this technique is proposed as a standard way of doing binding updates between MN and its CN. However, RR technique does not satisfy other security requirements. But these tokens are not protected and hence available to any attackers who can obtain both tokens. Another issue about RR is that RR does not actually guarantee that the node is located at the claimed CoA. For example, a node can always claim the address of a neighbor.

To solve authentication problem, CGA (Cryptographically Generated Address) technique (Aura, 2005) has been introduced. But the drawback of CGA is that it is computationally very expensive to perform cryptographic operations. CGA approach can solve the problem of a node claiming its CoA using another address already used by some other node. In Mobile IPv6, an IP address of a node is normally generated using the stateless address auto configuration method. In this method, a node constructs its address by combining the subnet prefix information and its unique interface ID. In CGA, the public key of a node is used instead of the node's interface ID. As a result, a node can prove its ownership of an address by signing a message using the private key corresponding to the public key included in its address. Since the node itself generates its address dynamically, a node can generate many addresses. However, a node cannot claim the ownership of an address already used by some neighboring node, unless it can obtain the private key of that node. Moreover, once a node has been authenticated using its HoA, all of its CoAs must contain the same public key included in its HoA. This fact can be used to verify the correctness of CoAs claimed by a node. Only problem with this approach is the cost of signing and verifying signatures. Previous approaches using CGA O'shea and Roe (2001) and Montenegro and Castelluccia (2004) requires a new signature each time a binding update occurs. This cost may not be tolerable to mobile nodes. However, if a signature is used only once in a while, the cost of generating the signature can be regarded as acceptable. In Sangjin *et al*. (2006) proposed a Ticket Based Binding update Protocol that use a ticket to minimize the generation of signatures during binding updates. In this study, we propose a new binding update technique which is more efficient than using the basic RR and CGA together.

THE PROPOSED SCHEME

The goal in designing IPv6 is to make MIPv6 at least as secure as static IPv6. But MIPv6 introduced some security vulnerabilities. Among which weak authentication and authorization of BUs is considered as the biggest vulnerability. These malicious Binding Updates open the door for many types of attacks like False Binding Update attack, Man-in-the-Middle Attack, Denial-of-Service Attack. To authenticate Binding Updates many authentication methods based on plain text, hash function, shared secret key are analysed in (Jong-Hyouk and Tai-Myoung, 2008). Based on the results of performance analysis, it is shown that the shared secret key authentication consumes much more signaling cost than others, whereas it also provides a strong security protection. Also many RO protocols are proposed in Sangjin *et al*. (2006). But many of these are prone to some of the security attacks or have assumptions like MN's CoA is already known to HA or a secure tunnel exists between MN and HA. In this study we present a new protocol that does not depend on the security relationship between the home network and the mobile node. Also it is not suscep the security threats. The security of the protocol is analyzed and its performance evaluation is also given in terms of computation and communication efficiency.

Certificate management in the proposed protocol is similar to certificate management (Ren *et al*., 2006) in HCBU. Three layer hierarchical trust management framework is developed. This is a divide and conquer approach which improves flexibility and scalability. Certificates issued to the tier 1 ISP's has the following contents:

i) TLAs owned by the given ISP
ii) Public key of the ISP
iii) Valid interval
iv) A CA's signature on (i), (ii) and (iii)

These Tier-1 ISPs cooperate with each other and have well-established long term trust relationships. This reduces the difficult authentication problem of MIPv6 nodes to a much easier one. In the 2nd layer, each Tier-1 ISP issues certificate from its own domain to Next Level Aggregators (NLAs) of its downstream intermediate ISPs. The certificate structure issued at this layer is same as that with the top layer except one with difference in contents:

i) NLAs owned by the intermediate ISP
ii) Public key of that intermediate ISP
iii) Valid interval
iv) Tier-1 ISP's signature on (i), (ii) and (iii) using its own private key

The certificate's valid interval at each lower layer should be less than that of the upper layer certificate. Finally, each home link gets a certificate of its own on its Site Level Aggregator (SLA). At this layer, all the routing information in the subnet prefixes of a home link has been approved by the certificates from both the 1st and 2nd layer. Then in the 3rd layer, each home agent dynamically signs on the binding of (Mobile Node, Home Address) or (Home Address, Care-of-Address) upon request by MN. This proves the correctness of binding to Correspondent node.

The assumption of a secure tunnel has two drawbacks:

- In practice such a secure tunnel can be established by exchanging secret keys between HA and all other nodes in the home network. If the intruder performs eavesdropping on the packets that are used to exchange the secret keys, then the intruder also gets the secret key.
- If at all such a secure tunnel is established between MN and HA, it should also exist between HA and CN. It is because even a CN can be a MN.

As the proposed protocol does not assume the presence of a secure tunnel between MN and HA, it determines the presence of a MN in its CoA by sending a probe. Hence we named the protocol as "Certificate based Inquisition approach" and is described as follows:

Step 1: When the MN realizes an imminent hand over, it sends a BUReq to HA
BUReq = {BU, Nm, HoA, CN}
Nm = fresh random nonce
HoA = Home Address of MN
CN = Correspondent Node

Step 2: HA exchanges information with CN 2

- HA calculates DH public value g^x and sends EXCH0 to CN.EXCH0 = {Nm, HoA, CN, g^x}
- CN calculates a DH public value gy, a fresh random nonce Nc, a Cookie K_{CN} and creates a packet EXCH1 EXCH1 = {Nm, Nc, HoA, CN, g^x, g^y, $Cookie_{CN}$} where $Cookie_{CN}$ = prf(K_{CN}, Nm | Nc | HoA | CN | g^x | g^y} K_{CN} = Private key of CN.

Step 3: To prove the ownership of CoA, MN sends CoA Reg message to HA CoA Reg. = {CoA, HoA, Valid_interval, CN, $SIG_{HA'}$, $Cert\_Chain_{HA'}$}

Step 4: Then HA checks the validity of certificate chain and verifies the signature in step3.

Step 5: If ($Cert\_Chain_{HA'}$ = 0 OR $SIG_{HA'}$ = 0) Reject CoA Reg. message sent in step 3 and return

Step 6: HA sends a PROBE to MN's home address to determine if the MN is still in the HoA or not. PROBE: {HoA, CN, Np}

Step 7: If the HA receives a PROBE CONFIRM PROBE CONFIRM = {HoA, MN, $PREV\_SIG_1$, $PREV\_SIG_2$, $PREV\_SIG_3$}
From the MN then
HA understands that MN is still in its HoA and it is the intruder who sent the BU request. Return.
Else HA confirrms that MN has moved to the CoA

Step 8: HA then sends a Binding Update Request with Certified (HoA, CoA): Where SIG_{HA} = S_{HA}(HoA|CoA|Valid_Interval|CN|g^{xy}|Nm|Nc)

Step 9: HA sends a Binding Update Reply to MN. BURep: {HoA, CoA, CN, K_{BU}}.

Step 10: MN sends the Binding Update message certified by K_{BU} to CN.

ANALYSIS OF THE PROPOSED SCHEME

Certificate Based Inquisition Approach, a Routing Optimization protocol for securing Binding Updates, is proved efficient compared to Return Routabilty protocol. This protocol is also considered more secure than Certifcate Based Binding Update protocols.

Security analysis: The design goals of Mobile IPv6 is that it should atleast be as secure as IPv6. But the introduction of Route Optimization protocol reduces the burden on the Mobile node's HA but greatly increases the security risk of MPv6. This is because of the weak authentication and authorization of Binding Updates.

Unauthenticated or malicious Binding Updates open the door for many types of security attacks such as False BU attack, Man-in-the-middle attack, Denial of service attack.

False BU attack: The proposed protocol is not prone to False BU attack. Here, HA sends a probe to MN's HoA to determine whether MN is in its HoA or CoA. If BUReq received by HA is a false one, then HA receives a probe confirm packet. This proves HA that it is a false BU attack.

Man-in-the-middle-attack: If the nodes A and B are communicating with one another and the intruder C in the middle sends a spoofed packet to B claiming that MN A has moved to a new CoA i.e., C. Then, in our protocol HA immediately sends a PROBE to MN HoA, which confirms that it is the intruder playing the role of man in the middle attack.

The proposed scheme introduces an inquisition approach to determine the actual location of MN. Thus PROBE and PROBE CONFIRM packets sent by the HA and MN respectively avoids all the security threats.

Computational analysis: To compare with the other RO protocols like RR, CBU, HCBU, the proposed protocol is computationally efficient than RR and CBU protocols and shown in Fig. 1.

In RR protocol, MN performs one symmetric encryption, CN performs 2 hashing functions and one symmetric decryption while no computational task is involved at HA.

In CBU protocol, MN performs one symmetric encryption, CN performs 3 hashing functions, one signature verification, one exponentiation and one symmetric decryption while HA performs 4 hashing functions, 2 exponentiations and one signature generation.

In HCBU protocol, MN performs one symmetric encryption, 3 hashing functions (two in a secure tunnel), one exponentiation and one signature generation, CN performs 2 hashing functions, one exponentiation and one symmetric decryption while HA performs 4 hashing functions, 2 exponentiations and one signature generation.

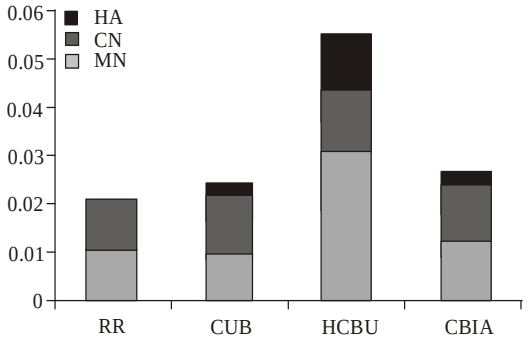

Fig. 1: Computational analysis

In our proposed "certificate Based Inquisition approach "protocol, MN performs one symmetric encryption, 5 hashing functions, one exponentiation and one signature generation, CN performs 2 hashing functions,, one exponentiation and one symmetric decryption while HA performs 5 hashing functions, 2 exponentiations and one signature generation.

To calculate the delays at MN, CN, HA, the time required to perform different operations are taken as follows. When 0.0001 ms for exponentiation, 0.0004 for performing hashing, 0.001 for symmetric encrytion and decryption and also for hashing function over a secure tunnel, 0.005 for generating the signature and 0.0002 for verifying the signature are taken, the following delays are obtained when simulated on NS2 simulator on linux platform. Figure represents computational delay in all the protocols at Mobile Node (MN), Correspondent Node (CN), Home Agent (HA) where the time taken on Y-axis is represented in milliseconds.

In RR protocol no computation is done at Home Agent, while in HCBU which assumes a secure tunnel between MN and HA has maximum computational delay at HA. The proposed protocol has computational delays similar to CBU protocol but the proposed is more secure than CBU.

Communication efficiency analysis: In the proposed protocol MN is required to send 3 messages, HA is required to send 4 messages while CN sends only message. In total, 8 messages are sent among 3 protocol participants. Of these the first 3 messages are sent right before an imminent handover. This greatly reduces the protocol latency. The protocol latency is reduced more than half when compared to Return Routability protocol. So lower latency and higher efficiency may be critical for a mobile node to successfully finish the protocol in the error-prone wireless communication environment without the assumption of a secure tunnel between MN and HA.

CONCLUSION

The proposed protocol is efficient in the following sense:

- Certificate management in our protocol is relatively simple and efficient
- Computation costs on the protocol participants are greatly reduced, compared to the previous Return Rouability and certificate-based protocols
- The latency of our protocol is low and thus ensures fast handovers

The security efficiency is achieved by introducing an inquisition approach to determine the presence of Mobile Node. The communication efficiency is achieved in our protocol by taking advantage of early binding update technique.

REFERENCES

Arkko, J., V. Devarapalli and F. Dupont, 2004. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. IETF RFC 3776.

Aura, T., 2005. Cryptographically Generated Addresses (CGA). IETF RFC 3972.

Johnson, D., C. Perkins and J. Arkko, 2004. Mobility Support in IPv6. IETF RFC 3775.

Jong-Hyouk, L. and C. Tai-Myoung, 2008. A Traffic Analysis of Authentication Methods for Proxy Mobile IPv6. International Conference on Information Security and Assurance IEEE.

Montenegro, G. and C. Castelluccia, 2004. Crypto-based dentifiers(CBID): Concepts and application. ACM Trans. Inf. Syst. Security, 7(1): 97-127.

Nikander, P., J. Arkko, T. Aura, G. Montenegro and E. Nordmark, 2005. Mobile IP Version 6 Route Optimization Security Design Background. IETF RFC 4225.

O'shea, G. and M. Roe, 2001. Child-proof Authentication for MIPv6 (CAM). ACM Comput. Commun. Rev., 31(2): 4-8.

Ren, K., W. Lou, K. Zeng, F. Bao, J. Zhou and R.H. Deng, 2006. Routing optimization security in mobile IPv6. Comput. Netw., 50(13): 2401-2419.

Sangjin, K., K. Jungdoo and O.H. Heekuck, 2006. Ticket-Based Binding Update Protocol for Mobile IPv6. Springer-Verlag, Berlin Heidelberg, pp: 63-72.