Binding Update Authentication Scheme for Mobile IPv6

Irfan Ahmed, Usman Tariq, Shoaib Mukhtar, Kyung-suk Lhee , S.W. Yoo, Piao Yanji, ManPyo Hong
Graduate School of Information and Communication, Ajou University, Korea
{irfan, usman, shoaib, klhee, swyoo, piaoyj, mphong} @ajou.ac.kr

Abstract

Mobile IPv6 provides route optimization mechanism for fast communication by lessening the overhead of indirection. Although it ameliorates the communication latency but it also needs good authentication mechanism to make route optimization more effective and reliable. In this paper, we improve one of the route optimization security mechanisms called Bombing Resistant Protocol, and propose a new binding update authentication scheme. Both mechanisms perform the care of address validation of the mobile node and maintain the integrity of the binding update message during binding update process, while the latter performs better in terms of latency and computation. They also resolve reflection and amplification, intensive computation problem.

Keywords: Mobile IPv6, Care-of-Address Validation, Key Management, Binding Update Authentication, Route Optimization

1. Introduction

The mobile IPv6 provides an efficient and scalable mechanism in terms of mobility [1,2,3]. Although mobile node (MN) changes its locations by traversing different networks but it maintains its home address through home agent (HA). MN (acronyms are defined in table 1) sends its current location to HA by sending binding update (BU) packets to HA that are first authenticated by HA [4] before updating MN's current location in its cache. This makes correspondent nodes (CN) communicate with MN without knowing its current location or care-of address (CoA). The CN sends data to MN's home address which is intercepted by HA and forwarded to MN. By this mechanism, the transport and higher layer association remains unaffected. But this is not an efficient way by routing the data through any third entity like HA. The good thing about MIPv6 is that data packets can also be sent directly between the MN and its CN. This mode is called Route optimization [1,5,6] which is not properly supported by MIPv4 [7]. To start communication through route optimization, the MN sends a BU packet to CN to inform it about its CoA. After knowing about the MN's CoA, the CN starts sending the packets directly to the MN by evading the HA's mediation. However, it could be possible that MN sends incorrect BU packet to the CN and redirects the stream to its desired location that can cause denial of service. Therefore a BU authentication mechanism is needed to avoid the route optimization from denial of service attack or false redirection attack. This paper proposes two efficient and robust BU authentication mechanisms. One is an improvement in the Bombing-Resistant Protocol [9], which is a BU authentication mechanism. Our improvement mitigates the limitations that are found in the Bombing-Resistant Protocol, such as the intensive computation and the lack of validating MN's CoA during BU process. The second BU authentication mechanism proposed in this paper does not only contain all the features of our improved Bombing-Resistant Protocol but is also more efficient in terms of the performance and reliability.

MN	Mobile Node	HA	Home Agent
CN	Correspondent Node	BU	Binding Update
CoA	Care-of Address	LCP	Location Confirmation Packet
MAC	Message Authentication Code	Init	Initiation Packet for route optimization

Table 1 Mobile IPv6 acronyms

This paper is organized as follows. Section 2 presents related work for route optimization and BU authentication in MIPv6. The problem statement is illustrated in section 3 and subsequently in section 4, the proposed validation and authentication schemes for care-of-address is explained. Section 5 describes the analytical evaluation, followed by conclusion in section 6.

*This research is supported by the Ubiquitous Computing and Network (UCN) Project, the Ministry of Information and Communication (MIC) 21st Century Frontier R&D Program in Korea.

0-7695-2876-7/07 $25.00 © 2007 IEEE
DOI 10.1109/IAS.2007.21

2. Related Work

Unlike the HA, the CN is not likely to have any established security relationship with a MN [8]. However, route optimization is the direct communication between MN and the CN. This communication can only be possible if a trust between these entities can be developed. This can be achieved by devising an authentication mechanism between them. In this section, we discussed the previously proposed BU authentication mechanisms.

The Early Binding Update (EBU) [10] for Mobile IPv6 avoids the latency of both address tests. A home-address test occurs when the MN can still use its old CoA. A concurrent CoA test runs parallel with data transfer to and from the new CoA. An optimized correspondent registration eliminates at least 50% of additional delay that a standard correspondent registration adds to the network. In EBU, the MN initiates the home address test just before the old link breaks as the local link layer triggers the indication. After moving to the different network, it configures a new CoA, initiates a home registration, and sends an EBU with Home keygen Token to CN for tentative CoA. The CN knows the new CoA and validates the MN's home address through the Home keygen Token that is received by MN during the proactive home address test. The CN hence starts using new CoA but during the communication, it also validates the new CoA through Credit-Based Authorization Technique [10]. In this technique, the CN and MNs exchange packets to confirm the new CoA of the MN.

The internet draft "Using IPsec between Mobile and Corresponding IPv6 Nodes" from MIP6 Working Group introduces a new approach by using the IPsec between MN and CN for protecting mobility signals for route optimization and for home address validation. [11].

The RFC4449 [12] describes a mechanism in which a MN and a CN may pre-configure the shared secret keys that is before the BU authentication process for authorizing BU and Binding Acknowledgment messages. The applicability of this mechanism is limited due to the need for pre-configuration. The distributed authentication mechanism [13] can be used to mitigate this limitation.

A new security mechanism [16] for improving the return routability protocol makes use of a digital signature scheme where the private key is kept by the HA in the home link. The home link obtains public key certificates from a certification authority. When MN wants to start route optimization with CN, it sends route optimization request directly to CN and through HA. The CN takes source IP of the request packets and generates home cookie and care-of cookie and sends them to MN. MN then requests HA to sign the message and sends it back to the MN which forwards it to CN. The CN receives and validates the cookies. If all validation and checks are positive, CN starts sending the packets directly to the MN.

3. Problem Statement

The security features for route optimization in Mobile IPv6 raised new threats like unauthenticated traffic redirection, replay attacks, inducing unnecessary binding updates, forcing of non-optimized routing and reflection attacks [17]. Some of these threats are solved by the Bombing-Resistant Protocol [9,14,15]. But still this protocol has some limitations like overhead of additional *Init* packet for key exchange and the lack of validating new CoA during BU process. These limitations make this protocol vulnerable to unauthenticated traffic redirection, and the overhead of sending two *Init* packets degrades the performance of the BU authentication process.

Consider a scenario where MN becomes an adversary node and sends a wrong CoA to CN through BU. If CN can not verify the CoA, it considers this information as valid and starts sending packets to the wrong CoA. This scenario represents an unauthenticated traffic redirection.

3.1. Fail to validate the CoA

Figure 3(a) shows the Bombing Resistant Protocol. In this figure, MN (C) after receiving the keys K0 and K1 on step 2a and 2b respectively, generates a MAC and sends it with the BU packet to CN (B) as shown in step 3. After receiving the BU packet, CN (B) can check the integrity or validity of the BU packet through the MAC by regenerating and comparing a new MAC with the received MAC. BU packet contains the CoA which tells about the current location of the MN. This CoA needs to be validated to avoid reflection attack or unauthenticated redirection attack. In Bombing-Resistant Protocol, there is no mechanism to validate and prove the correctness of the CoA sent by node C through BU packet.

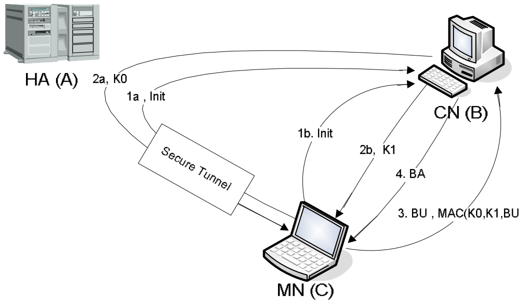

Figure 3(a): Bombing Resistant Protocol

3.2. Keying Problem

In figure 3(a), the key K1 which is sent to the MN (C) at step 2b is unnecessary. The main purpose of the key is to validate the CoA, which however is not achieved as mentioned in section 3.1. The HA knows about the CoA and it forwards the key K0 to the CoA of the MN through secure tunnel. It is sufficient for the CN (B) to verify the BU packet integrity through MAC generated only with key K0. At this point, assuring the correctness of CoA information in the BU packet is needed, which the Bombing-Resistant Protocol fails to do so.

4. Proposed CoA Validation Mechanisms

In this section, we propose two binding update authentication mechanisms: an improvement over the Bombing Resistant Protocol, and our own mechanism. These mechanisms have all the features that Bombing-Resistant Protocol has. In addition, they also efficiently and reliably verify the correctness of CoA in BU authentication process.

4.1. Improved Bombing-Resistant Protocol

Figure 4(a) shows how the Improved Bombing-Resistant Protocol works. The CN (B) sends the key K0 after receiving the *Init* packet. After receiving the key K0, MN(C) sends the BU to CN (B) with MAC. CN (B) sends the second key K1 to the MN(C) on the CoA mentioned in the BU packet. The MN (C) receives the key K1 and sends a location confirmation packet (LCP) to the CN (B). The MN (C) computes a hash value by using both the keys K0 and K1 and sends the computed hash value with the LCP. With this hash value, CN can find out about the validity of LCP and the CoA of the MN.

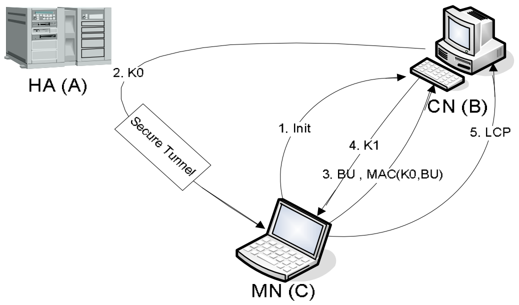

Figure 4 (a): Improved Bombing Resistant Protocol

4.2. Proposed scheme for CoA validation

Though the change in the Bombing-Resistant protocol, described above, verifies the CoA effectively but it also added the overhead of LCP. Figure 4(b) shows our new mechanism, which avoids the LCP overhead in validating the CoA.

In figure 4 (b), the MN (C) initiates the BU protocol. The CN (B) sends a secret key K to the MN's home address which HA (A) forwards it to the MN (C). The idea is that when HA (A) forwards the key K to the MN (C), at the same time it sends the CoA to the CN (B). Because we assume that the HA is legitimate and knows where to forward the packet and also the CN knows about the HA therefore the CoA provided by the HA to the CN must be valid. Later when CN (B) compares this CoA with the CoA provided by MN (C) via BU packet, it finds out the validity of CoA.

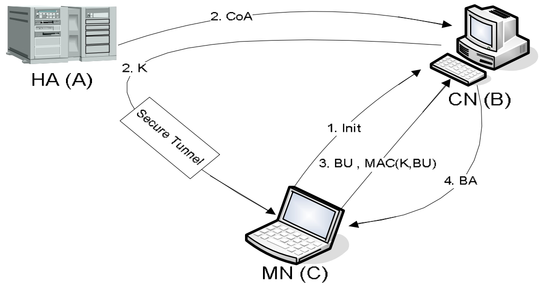

Figure 4 (b): Proposed Scheme

4.2.1. Prevention of Reflection and Amplification

In Aura's paper [9], the Bombing-Resistant Protocol is described in incremental fashion in such a way that firstly it is initially defined to send one *Init* packet to CN, and later it is refined to send two *Init* packets to rectify the reflection problem. Consider the following scenario, when the initial version of the Bombing Resistant Protocol is used: an attacker sends one *Init* packet to the CN but two arrive at the MN because CN sends two keys to the MN. Thus, the attacker can use the binding-update authentication protocol to amplify a packet flooding attack against a MN by a factor of two. This problem is called reflection and amplification problem [9].

Although the reflection and amplification problem was resolved by duplicating the initial message in the Bombing-Resistant Protocol, but it also incurs an overhead of additional message by sending two *Init* messages instead of one. In contrast, our both mechanisms send only one *Init* message, without incurring such overhead.

4.2.2. Performance advantages

4.2.2.1. Computation time

With this scheme, the hash function uses only one secret key to generate hash value to authenticate BU message, which requires less computation.

4.2.2.2. Communication latency

Although the number of messages are the same as our improvement over the Bombing Resistant Protocol, in our new mechanism HA forwards the key value to MN and sends the CoA to CN concurrently, reducing the overall latency of BU process.

5. Analytical Evaluation

If we evaluate the Bombing Resistant protocol, our improvement over the Bombing Resistant Protocol, and our new mechanism (described in figure 3(a), 4(a) and 4(b)), we come to the following conclusions.

- Our two mechanisms have less packet count than the Bombing Resistant protocol, hence consume lower bandwidth.
- The Bombing Resistant protocol and our new mechanism have better latency. However, our mechanism is secure in that it validates the correctness of CoA while the Bombing Resistant protocol does not.
- Our new mechanism is more efficient than the other two in terms of the computation requirement.

In this section, we demonstrate a probabilistic approach to evaluate our proposed schemes for securing binding updates in Mobile IPv6.

5.1. Delay Time Analysis (T)

In this section, we analyze the latency time of the BU process when using three mechanisms. The total binding update delay time (T) comprises of the following components:

- Initial Data Transfer Time for Authentication (T_i)
- CoA Registration Time (T_r)
- MN Location Confirmation Time (T_{LC})

$T = T_i + T_r$ For figure 5(a)
$T = T_i + T_r + T_{LC}$ For figure 5(b)
$T = T_i + T_r$ For figure 5(c)

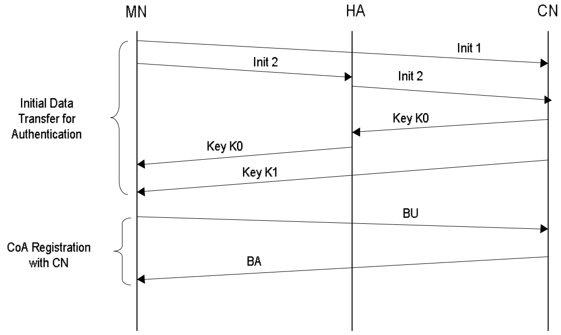

Figure 5 (a): Bombing-Resistant Protocol

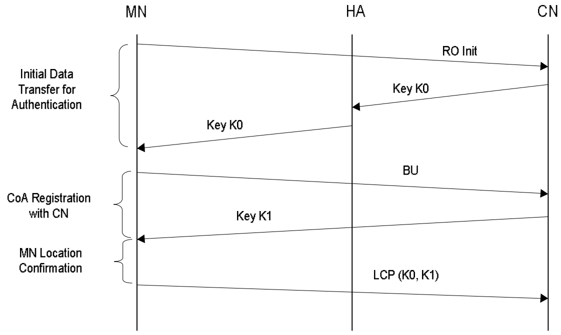

Figure 5 (b): Improved Bombing-Resistant Protocol

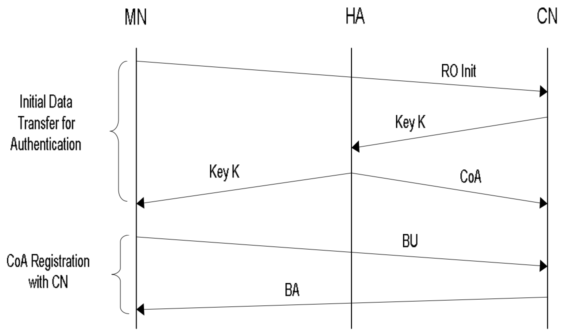

Figure 5 (c): New proposed scheme to validate CoA

5.1.1. Initial Data Transfer Time for Authentication (T_i)

Initial Data Transfer Authentication time (T_i) is the time in which initial request for route optimization is received (T_{ro}) and CN sends key to MN through HA (T_k).

$T_i = T_{Init1} + T_{Init2} + T_k + T_{K1}$ For Figure 5(a)
$T_i = T_{ro} + T_k$ For Figure 5(b)
$T_i = T_{ro} + T_{k\ CN\text{-}HA} + T_{k\ HA\text{-}MN}$ if $T_{k\ HA\text{-}MN} > T_{CoA}$
$T_i = T_{ro} + T_{k\ CN\text{-}HA} + T_{CoA}$ if $T_{CoA} > T_{k\ HA\text{-}MN}$
For Figure 5(c)

Where,

T_{ro} → Time taken by the packet for initial request for route optimization
T_k → Time taken by the packet containing key K / K0 to reach from CN to MN
T_{CoA} → Time taken by CoA to reach from HA to CN mentioned in Figure 5(b)
T_{K1} → Time taken by packet containing Key K1 to reach from CN to MN directly
T_{Init1} → Time taken by packet Init1 to reach from MN to CN directly
T_{Init2} → Time taken by packet Init1 to reach from MN to CN through HA

5.1.2. CoA Registration Time (T_r)

The CoA registration time (T_r) is defined as the transmission delay incurred during registration of MN's location.

$T_r = T_{BU} + T_{BA}$ For Figure 5(a)
$T_r = T_{BU} + T_{K1}$ For Figure 5(b)
$T_r = T_{BU} + T_{BA}$ For Figure 5(c)

Where,

T_{BU} → Time taken by BU packet to reach from MN to CN
T_{BA} → Time taken by BA packet to reach from CN to MN

5.1.3. MN Location Confirmation Time (T_{LC})

Location confirmation time (T_{LC}) is the time when MN sends computed hash value generated by using both the keys. This time is only occurred in our improved Bombing-Resistant Protocol (in Figure 5(b)).

5.2. BU latency time comparison

Consider a multi-hop wireless ad hoc network environment as shown in figure 5(c). The medium of communication is based on 802.11 families.

Let's consider that a MN is moving dynamically hop-by-hop fashion in ad hoc environment. Whenever the node crosses a certain range, it needs to be updated its position through binding update. In this section, we compare the latency time (time to complete the BU process) of the three mechanisms.

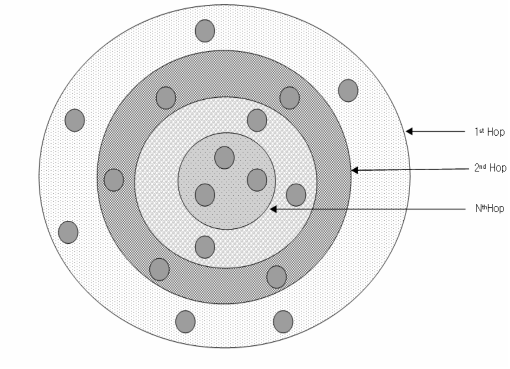

Figure 5(c): Multi-hop wireless adhoc network environment

Consider the following variables with respect to hop counts (HC) to analyze the BU process completion time.

$T_{HC=0}$ → Time to complete binding authentication process having no hop count among CN, HA and MN

$T_{HC>0}$ → Time to complete binding authentication process having hop count greater than zero among CN, HA and MN

N → No. of hops between source and destination

N_{PC} → Total No. of packet counts to complete one binding update authentication process

N_{CPT} → No. of times concurrent packet transfer occurred in different steps during binding update process

$T_{HOP(j,i)}$ → Time to reach from (i-1)th hop to ith for jth packet during binding update process but in concurrent packet transfer case, the packet which takes longer time to reach, only includes in time calculation.

$$T_{HC>0} = \sum_{j=1}^{N_{PC}-N_{CPT}} \sum_{i=0}^{N} T_{HOP(j,i)} \forall HC > 0 \text{ -------- (1)}$$

From equation (2), for HC=0, we can drive the following formula.

$$T_{HC=0} = \sum_{j=1}^{N_{PC}-N_{CPT}} \sum_{i=0}^{0} T_{HOP(j,i)}$$

$$T_{HC=0} = \sum_{j=1}^{N_{PC}-N_{CPT}} T_{HOP(j)} \forall HC = 0 \text{ ------------- (2)}$$

To draw the graphs for comparisons, we have to assume that the time to reach the packet from one node to the nearest another node is 100µs approximately [18]. We can conclude the following Table 2 from figures 3(a), 4(a) and 4(b).

	Bombing Resistant Protocol	Improved Bombing-Resistant Protocol	New Proposed Scheme
N_{PC}	6	5	5
N_{CPT}	2	0	1
$T_{HOP(j,i)}$	100µs (Assumed)	100µs (Assumed)	100µs (Assumed)

By using equation (1 & 2), we have drawn the following graph.

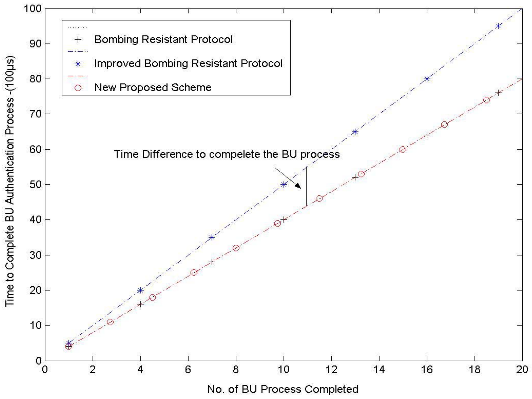

Figure 5(d)

Bombing resistant protocol was failed to validate the location of the MN. Although this limitation is improved by the Improved Bombing-Resistant Protocol but it also creates an overhead of LCP which is quite evident from the graph in figure 5(d). This overhead does not occur in the newly proposed scheme. In addition, it is as efficient as bombing resistant protocol in terms of latency, and has also overcome many limitations left in bombing resistant protocol including the CoA validation in BU authentication process.

6. Conclusion

Mobile IP presents efficient mobility support over current internet infrastructure. Mobile IPv6 route optimization technique deals with indirect routing by making the direct communication between CN and MN possible. This technique requires authentication mechanism to make it invulnerable.

This paper enhances the bombing-resistant protocol by adding a CoA validation feature in BU authentication process. This paper also proposed a new scheme that solves the CoA validation problem. This mechanism is robust, efficient, involves minimum overhead specially in terms of number of packets for the BU process, and requires no additional infrastructure support. The new proposed scheme also gives an effective solution against unauthenticated traffic redirection, reflection and amplification problems.

If we compare the Bombing-Resistant Protocol, Improved Bombing-Resistant Protocol and new proposed scheme, we find that new proposed scheme has all the features and security of Improved Bombing-Resistant Protocol and the efficiency and the performance of the Bombing Resistant Protocol.

References

[1] Johnson, D., Perkins, C., and J. Arkko; Mobility Support in IPv6; RFC 3775, June 2004

[2] Byungjoo Park, Latchman H.; Fast handover scheme based on Enhanced Access Point for Mobile IPv6; In proceedings of ICACT 2006; February 2006

[3] J Xie, IF Akyildiz; A novel distributed dynamic location management scheme for minimizing signaling costs in Mobile IP; In Proceedings of Mobile Computing, IEEE Transactions on, 2002

[4] A.Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury; Authentication Protocol for Mobile IPv6; RFC 4285, January 2006

[5] S.H. Hwang, B.K. Lee, Y.H. Han, C.S. Hwang; An adaptive hierarchical mobile IPv6 with route optimization; In Proceedings of Vehicular Technology Conference, April 2003

[6] CE Perkins, DB Johnson; Route Optimization for Mobile IP; In Proceedings of Cluster Computing, 1998 - Springer

[7] C Perkins; IP Mobility Support for IPv4; RFC 3344, 2002

[8] H Soliman; Mobile IPv6: Mobility in Wireless Internet; Book, 2004

[9] T Aura; Mobile IPv6 Security. In Proceedings of Security Protocols, 10th International Workshop, volume 2845 of LNCS, pages 215-228, Cambridge, UK, April 2002

[10] C Vogt, R Bless, M Doll, T Kuefner; Early BUs for Mobile IPv6; In Proceeding of Wireless Communications and Networking Conference, 2005

[11] F Dupont, JM Combes, Using IPsec between Mobile and Correspondent IPv6 Nodes; draft-dupont-mipv6-cn-ipsec-03; August 2006

[12] C. Perkins; Securing Mobile IPv6 route optimization using static share key; RFC 4449, June 2006

[13] Neeraj Jaggi, Koushik Kar; Distributed Authentication Mechanism for Mobile IP Route Optimization; In proceedings of Wireless Networks and Mobile Computing; June 2005

[14] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark; Mobile IP Version 6 Route Optimization Security Design Background; RFC 4225; December 2005

[15] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark; Mobile IP Version 6 (MIPv6) Route Optimization Security Design; In Proceedings of IEEE Vehicular Technology Conference, October 2003

[16] H Zhu, F Bao, RH Deng; Securing return routability protocol against active attack; In Proceedings of Vehicular Technology Conference, September 2004

[17] James Kempf, Jari Arkko, Pekka Nikander; Mobile IPv6 Security; Wireless Personal Communications Journal; June 2004

[18] D. Fober; Wireless Networks 802.11b performances; GRAME; 2004