성능과 보안성을 함께 개선한 MIPv6 바인딩 갱신☆

MIPv6 Binding Update scheme to improve performance and security

원 유 석* 조 경 산**
You-Seuk Won Kyung-san Cho

요 약

MIPv6에서 경로 최적화를 제공하기 위한 바인딩 갱신은 다양한 공격에 취약할 수 있다. 따라서 안전한 바인딩 갱신이 MIPv6의 중요한 연구 과제가 되었으며, 이를 위한 여러 프로토콜들이 제안되었다. 본 연구에서는 MIPv6가 기본적으로 제공하는 RR과 기존의 대표적인 프로토콜인 SUCV와 OMIPv6를 상세히 분석하여 MN의 암호화 연산 및 각 프로토콜의 공격 취약성, 주소 생성 및 관리와 확장성의 문제점을 제시하고, 안전한 바인딩 갱신을 위한 설계 목표를 제시한다. 이를 근거로 새로운 바인딩 갱신 프로토콜을 제안한다. 제안 프로토콜은 기존 프로토콜들보다 다양한 공격에 대한 방어를 강화하며, 주소 관리와 확장성을 개선하고, 위치 보안성을 제공하며, 제한된 계산 능력을 갖는 MN의 연산 부하를 감소시킨다.

Abstract

Binding update for the routing optimization in MIPv6 can make the involved nodes vulnerable to various attacks. Therefore, secure binding update becomes an important research issue in MIPv6, and several protocols have been proposed for this purpose. In this paper, we compare several existing binding update protocols such as RR, SUCV and OMIPv6 and analyze the vulnerability of nodes to the possible attacks and drawbacks of address management and scalability and overhead of encryption operations. Then, we suggest the design requirements for the secure binding update and propose an advanced protocol based on the design principle. Through the analysis, we show that our protocol can achieve a higher level of security against the various attacks and enable better management of address, provide the location privacy and reduce the computational overhead of mobile nodes with constraint computational power.

☞ Keyword : MIPv6, secure binding update, RR, SUCV, OMIPv6

1. 서 론

인터넷 기술의 빠른 발전과 무선통신 기술 및 단말기의 급속한 확산에 따라 무선 이동 인터넷 환경이 급진적으로 발전하고 있다. 인터넷에서는 고정된 IP 주소를 사용하므로, 모바일 노드가 새로운 서브넷으로 이동하면 고정된 IP주소로는 인터넷을 통한 접속과 통신이 불가능하다. 이러한 문제를 해결하고 IP에서 호스트의 이동성을 제공하기 위해서 IETF(Internet Engineering Task Force)는 모바일 IP를 제안하였고, IP의 새로운 버전인 IPv6에 따라 새로운 모바일 IP 버전인 MIPv6가 제안되었다[1-5].

MIPv6에서 이동성을 가진 모바일 호스트는 MN(Mobile Node)이라 하고, MN과 통신하려는 호스트는 CN(Correspondent Node)이라 하며, MN이 처음 위치한 홈 서브넷에 있는 라우터는 HA(Home Agent)라 한다. MIPv6에서는 호스트가 다른 서브넷으로 이동하여도 인터넷을 통한 통신을 계속 허용하기 위해 2개의 주소 HoA(Home Address)와 CoA(Care-of Address)를 각각 연결 인식과 라우팅을 위해 사용한다. 또한 MN이 새로운 서브넷으로 이동하여도 CN이 MN에게 직접 통신할 수 있는 경로 최적화(Route Optimization)

* 준 회 원 : 단국대학교 대학원 박사과정
server11@dankook.ac.kr
** 정 회 원 : 단국대학교 정보컴퓨터학부 교수
kscho@dankook.ac.kr
[2007/04/12 투고 - 2007/04/19 심사 - 2007/05/22 심사완료]
☆ 이 연구는 2006학년도 단국대학교 대학연구비의 지원으로 연구되었음

기능을 기본으로 제공하는데, 이를 위해서 MN은 자신의 이동을 CN에게 바인딩 갱신 과정을 통해 등록해야 한다[1-5].

그러나 안전하지 않은 바인딩 갱신은 오히려 공격자로 하여금 MN과 CN에게 다양한 보안 공격이 가능하므로, 안전한 바인딩 갱신을 위한 여러 프로토콜들이 제안되었다. 즉, MIPv6에서 기본으로 지원하는 RR[5], 주소기반 공개키(Public Key)를 사용하는 ABK기법[6], PKI기반으로 DH키 교환을 이용하는 보안 프록시 기반 기법[7]등이 제시되었다. 또한, 인터넷에서 전역적으로 사용할 수 있는 CA 없이 주소로 MN의 공개키를 인증하는 CGA 기법[8]이 제안됨에 따라, CGA 기법을 활용하는 CAM-DH[9], SUCV[10] 프로토콜이 제시되었으며, 강한 암호화를 사용하여 보안성 강화 및 네트워크의 통신량을 감소시키는 OMIPv6[11]가 제안되었고, 위치 보안성을 제공하는 Ext-RR[12]프로토콜도 제안되었다.

본 논문에서는 기존의 프로토콜중에서 RR과 SUCV 및 OMIPv6를 상세히 분석하여 취약점을 제시하고, 성능과 보안성을 개선한 새로운 바인딩 갱신 기법을 제안한다. 또한 제안 프로토콜의 우수성을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 MIPv6의 바인딩 갱신과 가능한 공격의 유형을 설명하고, 3장에서는 IETF의 표준 프로토콜인 RR과 기존 프로토콜중에서 우수하다고 평가된 SUCV 및 OMIPv6을 설명하고, 이들의 성능적 특성과 보안적 특성을 분석하고 취약점을 제시한다. 4장에서는 분석된 취약점을 개선한 프로토콜을 제안하고, 5장에서는 제안 프로토콜이 기존의 프로토콜에 비해 성능 및 보안 특성과 확장성 및 관리성에서 우수함을 제시하고, 6장의 결론으로 끝맺음한다.

2. MIPv6의 바인딩 갱신

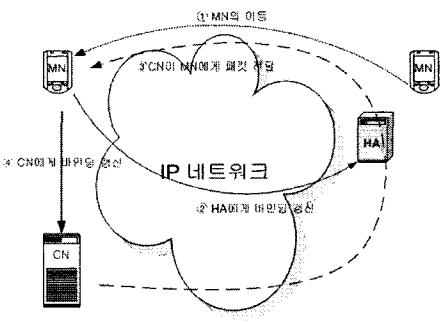
본 장에서는 MIPv6 바인딩 갱신에 관한 기본 개념 및 경로 최적화와 가능한 공격 등을 설명한다.

2.1 MIPv6의 바인딩 갱신

모바일 IP에서 모바일 호스트는 HoA와 CoA의 두 개의 주소를 갖는다. HoA는 홈 서브넷에서 MN에게 부여된 IP주소로 연결 인식을 위해 사용되며, MN은 항상 HoA에 의해 주소 지정될 수 있다. CoA는 MN이 이동된 서브넷에 연결되어 있는 동안 유효한 임시 주소로 라우팅을 위해 사용된다. MN이 가진 두 주소인 HoA와 CoA와의 연계를 바인딩이라 한다.

새로운 버전의 IPv6에 따라 등장한 새로운 모바일 IP 버전인 MIPv6는 MIPv4와 달리 경로 최적화를 기본으로 제공한다. MN의 이동을 지원하고 경로 최적화를 위해 HA와 CN은 MN의 HoA와 CoA의 바인딩을 저장하는 바인딩 캐쉬를 유지해야 한다. 즉, 이를 위하여 MN은 CN에게 자신의 새로운 CoA를 알리는 바인딩 갱신을 수행한다. 바인딩 갱신을 통해 CN은 MN의 새로운 CoA를 CN의 바인딩 캐쉬에 저장하고, MN에게 패킷을 전송할 때마다 해당 CoA에게 직접 그 패킷을 전송하는 경로 최적화를 사용한다[5, 13].

MIPv6에서 MN의 이동에 따른 바인딩 갱신 과정은 (그림 1)과 같다.

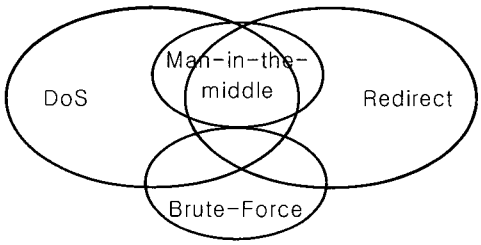


(그림 1) MIPv6의 바인딩 갱신 과정

MN은 HA에게 안전한 IPsec를 사용한 터널을 통해 전송하지만, MN과 CN사이에는 안전한 보안 설정이 없어 CN으로의 바인딩 갱신은 다양한 보안적 공격이 가능하다[13, 14].

2.2 바인딩 갱신시 가능한 공격 유형

CN으로의 바인딩 갱신 과정에서 가능한 공격 유형은 (그림 2)와 같으며, 각 공격의 특성은 다음과 같다.



(그림 2) 공격 유형의 연관성

방향전환(Redirect) 공격은 패킷을 실제 목적지가 아닌 다른 노드(또는 네트워크)로 전송하는 공격이다. 모든 방향전환 공격은 MN 또는 제3의 공격자에 의해 여러 방법으로 가능하며, 방향전환 공격의 대상이 되는 노드(또는 네트워크)에게는 서비스 거부 공격과 범람(Flooding, Bombing) 공격이 동시에 가해질 수 있다. 가장 대표적인 방향전환 공격인 세션 강탈(Session Hijacking) 공격으로 CN과 MN의 통신을 도청하여 세션을 획득하고, MN인척 거짓의 바인딩 갱신을 CN에게 전송하여 거짓의 주소를 등록하는 공격이다.

서비스 거부(DoS) 공격은 공격을 받은 노드 또는 네트워크가 더 이상 서비스를 제공하지 못하도록 하는 공격이다.

전사(Brute force) 공격은 바인딩 갱신 프로토콜에서 각 제어 패킷의 암호화에 사용하는 키의 크기가 작은 경우에 가능한 모든 경우를 대입하여 암호화키를 생성하는 공격이다.

중개인(Man-in-the-middle) 공격은 제어 패킷이 평문으로 전송되는 경우 또는 약한 인증을 사용할 경우 패킷이 쉽게 강탈되고, 패킷의 내용을 수정하여 목적지로 전달하는 공격이 가능하다.

반사(reflection) 공격 및 증폭(amplification) 공격은 다른 노드를 통해 공격 패킷을 목적지로 전송하고, 패킷의 근원지를 감추어 공격자의 신분이 들어나지 않도록 하는 공격이다. 또한 노드가 수신한 메시지 수보다 더 많은 수의 메시지를 전송하도록 하는 것이 증폭 공격이다.

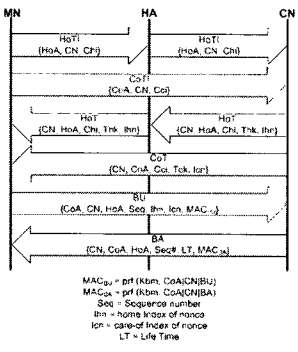
3. 기존 바인딩 갱신 프로토콜

앞 장에서 설명된 다양한 공격으로부터 안전한 바인딩 갱신을 수행하기 위해 HoA로 식별되는 MN이 실제로 CoA로 이동하였는가를 검증하고, 또한 이후의 안전한 통신을 위해 사용될 MN과 CN 사이의 비밀키(또는 세션키)를 생성하는 인증 과정이 바인딩 갱신 과정보다 선행되어야 한다. MIPv6에서 기본적으로 지원하는 RR(Return Routability) 프로토콜은 안전한 바인딩 갱신을 위한 대표적인 인증 프로토콜이다[5, 7].

본 장에서는 RR 프로토콜과 RR의 취약점을 개선하여 우수한 평가를 받고 있는 SUCV 프로토콜과 OMIPv6 프로토콜을 분석하여 이들의 특성과 취약점을 비교 제시한다. 본 장의 분석 결과는 4장의 제안 프로토콜의 근거로 활용한다.

3.1 RR 프로토콜

RR프로토콜은 MN이 제시한 HoA와 패킷을 수신할 수 있는가를 확인하여 MN을 인증하고 바인딩 갱신을 위한 비밀키를 생성하는 프로토콜이다.



(그림 3) RR 프로토콜

RR은 (그림 3)에 표시된 6개의 메시지 교환으로 MN의 두 주소(HoA, CoA)에서 수신이 가능한가를 검증하고, MN과 CN이 공유하는 비밀키를 생성하여 바인딩 갱신과 응답에 사용한다.

먼저 MN의 HoTI는 HA를 경유하고, CoTI는 직접 CN에게 전송한다. CN은 HoTI와 CoTI의 2개의 메시지를 수신한 후에 그에 대한 응답으로 HoT와 CoT 메시지를 각각 HoTI와 CoTI의 역 경로를 따라 MN에게 전송한다. MN은 HoT와 CoT에 전달되는 Thk과 Tck의 두 값을 해쉬하여 비밀키(Kbm)를 생성한다. MN이 비밀키를 정상적으로 생성할 수 있다는 것은 MN이 HoA, CoA에서 각각 HoT와 CoT를 CN으로부터 수신하였음을 입증한다. 이후 MN과 CN은 비밀키를 이용하여 바인딩 갱신 및 바인딩 응답(BA: Binding Acknowledgement)을 안전하게 전송한다.

RR은 다음과 같은 장점들을 가진다.

1) MN이 주장하는 2개의 주소 HoA, CoA에서 수신 가능함을 구조적으로 간단히 입증하고, 간단한 토큰 해쉬 연산을 통해 비밀키를 생성한다.
2) 제한된 계산 능력을 갖는 MN을 위해 과부하가 심한 연산과정을 제거하였다.
3) MN의 주소가 인증되기 전까지 CN은 어떤 정보도 저장하지 않아, 자원 고갈 서비스 거부 공격을 방지 하였다.

그러나 RR 프로토콜은 다음과 같은 단점들을 가진다.

RR 프로토콜은 HoTI, CoTI, HoT, CoT, BU, BA의 6개 메시지로 구성되어 있는데, 강력한 주소 인증을 사용한다면, CoTI 메시지는 기능적으로 불필요하다.

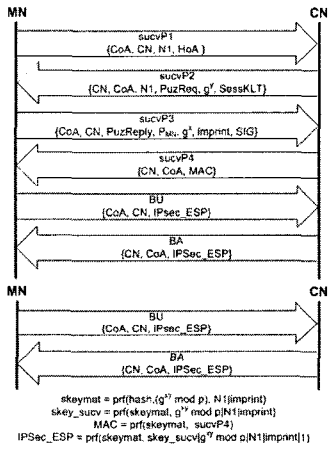
MN이 새로운 서브넷으로 이동할 때마다 또는 420초마다 6개의 메시지 교환 과정을 주기적으로 수행해야 하므로 경로 최적화를 위한 메시지의 수가 MN과 CN 및 HA에게 부담을 초래한다.

또한 RR 프로토콜은 메시지를 암호화하지 않은 평문으로 전송하여 공격자들에게 세션 강탈 공격, 중개인 공격 및 서비스 거부 공격을 허용한다.

3.2 SUCV 프로토콜

RR 프로토콜의 보안 취약점을 해결하기 위해 강력한 인증 기법을 사용하는 SUCV(Statistic Uniqueness and Cryptographic Verifiability) 프로토콜이 제안되었다[10]. SUCV는 MN이 주장하는 주소의 소유권 문제를 해결하기 위해 주소기반 공개키 방식을 사용한다. 주소기반 공개키 방식에서 MN은 공개키를 해쉬하여 HoA (및 CoA)의 IID(Network Interface Identifier)을 생성하고, CN은 MN의 공개키로부터 HoA 주소의 소유권을 인증한다. 또한, 개인키 서명과 DH 키 교환 방법을 이용하여 MN과 CN 사이의 세션키를 생성한다.

SUCV 프로토콜은 MN의 주소 소유권을 통해 MN을 인증하고, 안전한 세션키를 분배하는 초기 인증 과정(첫 번째 바인딩 갱신 및 응답 포함)과 MN이 이동한 후에 새로운 주소를 등록하는 바인딩 갱신 과정으로 구성된다. 각 단계별 수행 내용은 (그림 4)와 같다.



(그림 4) SUCV 프로토콜의 초기 인증 과정과 바인딩 갱신 과정

초기 인증 과정은 다음과 같이 수행된다.

1) MN은 임의의 변수 N1과 HoA, CoA를 포함한 sucvP1를 CN에게 전송하여 바인딩 갱신 처리

를 요청한다.

2) 이를 수신한 CN은 자원 고갈 서비스 거부 공격을 방지하기 위한 클라이언트 퍼즐(PuzReq)과 공유 비밀키 생성을 위한 DH값 g^y등이 포함된 sucvP2로 MN에게 응답한다.
3) MN은 변수 N1을 통해 sucvP2의 유효성을 검증하고, 클라이언트 퍼즐(PuzReply)을 계산하며, 세션키를 생성한 후에 개인키로 서명하여 sucvP3 메시지를 CN에게 전송한다.
4) sucvP3를 수신한 CN은 클라이언트 퍼즐(PuzReply)를 확인하고, 이것이 유효하다면 MN의 공개키를 이용하여 서명을 검증하고, MN의 공개키로 주소의 소유권을 검증하며, 세션키를 생성한다. 그 후 MAC를 포함한 sucvP4를 MN에게 전송한다.
5) 세션키 및 보안 연관을 생성한 MN과 CN은 안전한 터널을 통해 바인딩 갱신과 응답 메시지를 전송한다.

SUCV에서는 주소기반 공개키를 사용하여 MN의 HoA IID를 생성하고, 주소 소유권을 검증하므로 보안이 강화되었다. 또한 초기 인증 과정을 통해 생성된 세션키는 24시간 유효하여 잦은 재인증의 필요성을 제거하고, 불필요한 네트워크 트래픽을 감소 시켰으며, HA에게 발생되었던 네트워크 병목 현상도 해결하였다.

제시된 보안성 및 효율성에도 불구하고, SUCV 프로토콜은 다음의 추가적인 취약점이 있는 것으로 분석된다.

1) 주소 소유권 인증의 문제
SUCV는 주소의 IID만을 검증하므로, 다른 네트워크에서 동일한 IID를 갖는 모든 호스트들은 동일한 주소의 소유권을 가진 것으로 처리된다.

2) sucvP2를 이용한 서비스 거부 공격
SUCV 프로토콜은 sucvP3를 이용한 서비스 거부 공격을 방지하기 위해 MN에게 퍼즐(PuzReq)을 계산하여 CN에게 전송하도록 한다. 퍼즐(PuzReplay)을 수신한 CN은 퍼즐의 유효성을 검증하고, 유효하다면 고비용의 비대칭 암호화 연산을 한다. 따라서 고비용의 암호화 연산을 하기 전에 간단한 해쉬 연산으로 유효성 검증하므로, 자원 고갈 서비스 거부 공격을 방지한다. 하지만 공격자는 sucvP1을 도청하여 N1과 어려운 해쉬 연산을 요구하는 퍼즐을 포함한 sucvP2를 MN(최적화 프로토콜에서는 HA)에게 대량 전송하여 자원 고갈 서비스 거부 공격이 가능하다[3, 10].

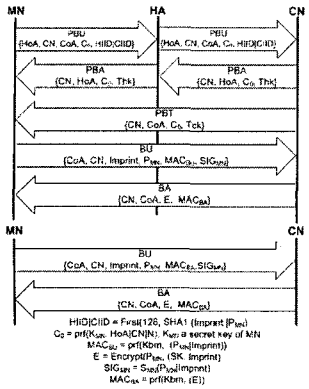
3) 단일 해쉬 기반 연산 사용으로 인한 전사 공격
SUCV는 주소의 소유권을 인증하기 위해 사용하는 인터페이스 식별자의 62비트는 전사 공격에 취약한 문제가 있다.

4) MN의 암호화 연산 과부하 및 HA의 공개키/개인키 관리의 과부하
SUCV 방식은 제한된 계산 능력을 갖는 MN에게 과부하가 심한 암호화 연산을 다수 요구한다. 이 문제의 해결을 위해 SUCV 최적화 프로토콜이 제시되었지만, HA에서 키 관리의 복잡성과 성능저하가 발생하고, 네트워크의 확장성도 떨어진다.

3.3 OMIPv6 프로토콜

RR의 잦은 재 수행으로 인한 성능적 문제점 및 공격 취약성을 보완하기 위해 OMIPv6 (Optimizing Mobile IPv6) 프로토콜이 제안되었다[11]. OMIPv6 프로토콜은 주소의 소유권을 인증하기 위해 주소 도달성 검증과 주소의 소유권을 검증하는 주소기반 공개키 방식을 함께 사용한다. 또한 공개키 암호화를 사용하여 MN과 CN사이의 세션키를 분배한다.

OMIPv6 프로토콜은 SUCV 프로토콜과 같이 초기 인증 과정(첫 번째 바인딩 갱신 및 응답 포함)과 그 이후의 바인딩 갱신 과정으로 나눠서 (그림 5)와 같이 수행한다.



(그림 5) OMIPv6 프로토콜의 초기 인증 과정과 바인딩 갱신 과정

OMIPv6의 초기인증 과정은 다음과 같이 수행된다.

1) MN의 공개키를 해쉬하여 HoA와 CoA의 IID를 생성하고, PBU를 HA를 통해 CN에게 전송한다.
2) CN은 MN의 주소 HoA와 CoA로부터 Thk와 Tck를 생성하여 HA를 통해 MN에게 PBA를 전송하고, PBT는 MN에게 직접 전달한다.
3) 두 메시지를 수신한 MN은 Thk와 Tck를 해쉬하여 공유 비밀키(Kbm)를 생성하고, 이 키를 사용하여 MAC_{BU}을 계산하며, 자신의 공개키로 서명하여 CN에게 세션키(SK)가 포함된 BA를 전송한다.

생성된 세션키는 24시간 동안 유효하여 MN과 CN 사이에서 양방향 장시간 보안 연관 구축이 가능하다. 초기 인증과정 이후의 이동 시에는 세션키를 이용한 단순 바인딩 갱신을 수행하여 지연을 감소 시켰으며, 공유된 세션키로 MAC_{BU} 및 MN의 개인키 서명을 포함하여 메시지의 안전함을 보장 하였다.

그러나 OMIPv6도 다음의 추가적인 취약점이 있는 것으로 분석된다.

1) 새로운 CoA 주소 생성의 문제점
MIPv6에서는 MN이 이동하면 새로운 CoA IID는 세션키(SK) 및 이전 주소(pCoA)와 새로운 네트워크 전치부를 사용하여 다음과 같이 생성한다.
- 새로운 CoA IID = First(64, SHA1 (SK | 새로운 네트워크 전치부 | pCoA))

그러나 MN의 CoA IID는 세션키를 사용하여 생성하므로 다수의 CN과 통신시에는 주소의 유일성을 위반하여 사용할 수 없다.

2) 주소 소유권 인증의 문제
OMIPv6는 SUCV과 같이 주소의 IID만을 검증하므로, 다른 네트워크에서 동일한 IID를 갖는 모든 호스트들은 동일한 주소를 가진 것으로 처리된다.

3) MN의 과부하 연산
OMIPv6는 비대칭 암호화 연산 및 서명을 이용한 바인딩 갱신 방식을 사용하므로, 제한된 계산능력을 가진 MN에게 과부하 연산을 요구한다.

4. 개선된 바인딩 갱신 프로토콜 제안

3장에서 분석된 바와 같이 기존의 바인딩 갱신 프로토콜은 다음과 같은 문제점을 가진다.

1) PDA, 셀룰러 폰과 같이 제한된 계산 능력을 가지고 있는 MN에게 고비용의 비대칭키 및 대칭키 암호화 연산을 요구한다.
2) 방향전환 공격, 서비스 거부 공격, 중개인 및 반사 공격 등 다양한 공격에 취약하다.
3) MN이 이동 중 다수의 CN과 통신을 못하는 문제점이 있으며, 주소의 IID을 검증하는 경우 다른 네트워크의 동일한 IID를 갖는 호스트 경우에는 CoA의 충돌 가능성이 발생하는 등의 주소 선택권 제약이 발생하여 주소의 관리성 및 확장성에 문제가 있다.
4) 바인딩 갱신 프로토콜에서 공격자는 도청만으로 손쉽게 MN의 HoA와 CoA를 획득할 수 있다. HoA와 CoA의 인터페이스 식별자에는 모바일 노드를 판별할 수 있는 식별 값, 모델번

호 등이 포함되어 있어, HoA와 CoA를 통해 네트워크에 존재하는 각 노드들의 이동성을 추적하여 공격에 사용할 수 있다. 이렇게 획득된 주소를 사용하여 방향전환 공격, 서비스 거부 공격, 중개인 공격이 가능하다. 따라서 프로토콜이 MN의 이동성을 은닉할 수 있는 기능이 필요하다.

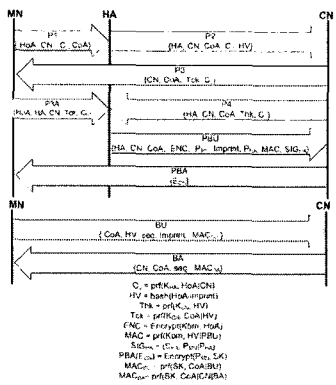
본장에서는 제시된 문제점을 해결한 개선된 새로운 바인딩 갱신 프로토콜을 제안한다.

4.1 제안 프로토콜

본 논문에서 제안하는 개선된 바인딩 갱신 프로토콜은 다음과 같은 설계 요구사항을 갖는다.

1) 주소의 도달성을 확인하여 MN을 인증한다.
2) 공개키 기반으로 MN이 주장하는 주소의 소유권을 인증한다.
3) 위치 보안성을 제공한다.
4) 보안 프록시 방식을 적용하여 MN의 암호화 연산을 최소화한다.
5) 공개키 암호화를 사용하여 안전한 세션키 분배한다.

위와 같은 요구 사항을 만족시키도록 제안 프로토콜의 동작은 MN의 초기인증 과정(첫 번째 바인딩 갱신 및 응답 포함)과 바인딩 갱신 과정으로 (그림 6)과 같이 수행한다.



(그림 6) 제안 프로토콜의 초기인증 과정 및 바인딩 갱신 과정

(1) MN의 새로운 CoA를 등록 요청하는 P1은 HA를 경유하여 CN에게 전송한다.

(2) P1을 수신한 HA는 MN의 HoA를 위치 보안성을 위한 HV와 쿠키값을 생성하여 P2를 CN에게 전송한다.

(3) P2를 수신한 CN은 자신만이 알고 있는 비밀키(K_{CN})을 사용하여 Thk, Tck를 생성하고, 이를 각각 포함한 P3와 P4를 MN의 CoA, HA(MN의 HoA 대신)에게 전송한다.

(4) CN으로부터 P3를 수신한 MN은 쿠키값을 확인하여 HA에게 P3A을 전달한다.

(5) P3A 와 P4를 수신한 HA는 Thk, Tck로 비밀키(Kbm)를 생성하여 HoA를 암호화하고, MAC를 생성하며, 개인키로 서명한 PBU를 CN에게 전송한다.

(6) PBU를 수신한 CN은 비밀키로 MAC를 검증하고, HoA를 복호화하고, HA의 공개키로 서명을 검증하며, MN의 주소를 인증한다. CN은 추후 사용할 세션키를 MN의 공개키로 암호화하여 전송한다.

초기인증 과정 이후에는 MN이 새로운 서브넷으로 이동하면, 세션키로 생성한 MAC이 포함된 바인딩 갱신과 응답을 전송하는 과정만 수행하는 바인딩 갱신 과정(BU/BA)만 진행한다.

제안 프로토콜에서 MN이 이동 후 새로운 CoA는 MN의 공개키(P_{MN}) 및 이전 주소(pCoA)와 새로운 네트워크 전치부를 사용하여 다음과 같이 생성한다.

- 새로운 CoA IID = First(64, SHA1 (P_{MN} | 새로운 네트워크 전치부 | pCoA))

4.2 제안 프로토콜 특징

본 연구에서 제안하는 프로토콜의 특징은 다음과 같다.

1) MN의 인증

제안 프로토콜은 공개키의 해쉬값을 MN의 CoA IID로 사용하여 MN의 소유권을 검증하며,

MN의 인식 주소 HoA는 이미 HA에 의해 검증되었으므로 별도의 확인 과정을 추가하지 않는다. 또한 제안 프로토콜에서는 MN의 주장하는 CoA에서 패킷을 수신할 수 있는가를 확인하여 MN을 인증한다.

2) 보안 프록시

제안 프로토콜은 HA가 MN의 보안 프록시로 동작하도록 설계되어, MN의 암호화 연산을 최소화하여 최적의 성능을 제공한다.

3) 안전한 세션키 분배

제안 프로토콜은 CN 자신만이 알고 있는 비밀키(K_{CN})을 사용하여 세션키를 생성하고, 이를 MN의 공개키로 암호화하여 MN에게 전송하여 세션키를 안전하게 분배한다.

4) 위치 보안성

기존 바인딩 갱신 프로토콜에서는 공격자는 메시지의 도청만으로 손쉽게 MN의 HoA, CoA를 획득하여 위치 보안성이 침해된다[10, 12]. 제안 프로토콜은 HoA를 메시지에 노출시키지 않으므로 각 노드의 위치에 대한 보호가 가능하다.

5. 제안 프로토콜의 개선점

본 장에서는 제안 프로토콜을 앞 장에서 분석한 RR, SUCV, OMIPv6 프로토콜과 비교하여 개선된 사항들을 제시한다.

5.1 성능적 측면

제안 프로토콜은 초기인증 과정 이후, 바인딩 갱신 과정에서 CN이 간단한 해쉬만을 사용하여 MN의 새로운 CoA를 인증하여 RR에 비해 빠른 핸드오프 지연시간을 제공한다. 또한, 공개키 암호화를 통해 안전하게 전송된 세션키를 이후 바인딩 갱신에서 사용하여 보안 연관의 수명을 24시간으로 확장하고, 불필요한 전송 메시지의 양을 대폭 감소 시켰다. SUCV, OMIPv6에서 제한된 계산 능력의 MN에게 부여된 암호화 연산 과부하의 취약점을 개선하기 위해 보안 프록시 방식을 적용하였으므로, 대부분의 암호화 연산을 MN대신 HA가 수행하여 MN의 성능 최적화를 제공하였다.

5.2 보안적 측면

1) 방향전환 공격과 세션 강탈 공격의 방어

제안 프로토콜은 주소 도달성 검증과 공개키 기반 주소 체계를 사용하여 주소의 소유권을 인증하고, HA의 서명을 사용하여 메시지를 최종 검증하는 강력한 주소 인증 기법을 사용하므로 세션 강탈 공격에 대응한다.

2) 서비스 거부 공격의 방어

다음과 같이 각 메시지에 대한 서비스 공격에 방어한다.

(1) P2에 대해 CN은 간단한 해쉬 연산만을 수행하여 서비스 거부 공격에 대응한다.

(2) P3 및 P4에 대해 쿠키값을 사용하여 HA에 대한 공격에 대응한다.

(3) 키 생성 토큰(Thk, Tck)을 HoA, CoA에 각각 전송하고, 이를 해쉬한 비밀키로 MAC의 유효성을 확인하여 PBU를 이용한 서비스 거부 공격에 대응한다.

(4) MN의 CoA IID로 소유권 확인 및 공유 세션키로 MAC_{BU}를 검증하여 BU를 이용한 서비스 거부 공격에 대응한다.

3) 중개인 공격의 방어

주소 기반 공개키를 통한 MN의 공개키 인증을 통해 주소 소유권 인증하고, 공개키로 암호화하여 세션키를 분배하므로 중개인 공격을 할 수 없다.

4) 위치 보안성

제안 프로토콜은 MN의 HoA 정보를 공격자에게 감추어 각 노드의 위치 보호 기능을 제공한다.

5.3 주소의 관리 및 확장성

제안 프로토콜에서는 HA가 자신의 MIPv6 주소를 이용하여 공개키 기반 주소에 사용될 공개키/개인키를 생성한다. 또한, HA의 주소를 이용하여 주소의 소유권을 인증하여 MN의 비대칭 연산을 감소시키므로 기존의 공개키 기반의 프로토콜에 비해 관리성 및 확장성을 높일 수 있다. 또한 MN이 이동 후 새로운 CoA 주소 체계를 제공하여 보안성이 그대로 유지한 상태에서 MN은 여러 CN과 동시에 통신을 할 수 있는 기능을 제공 하였다.

5.4 암호화 연산 비교

제안 프로토콜은 OMIPv6에 비교하여 초기인증 과정에서 1×비대칭 암호화(1×서명) 연산과 1×해쉬, 1×MAC 연산을 감소시켰으며, 바인딩 갱신 과정에서는 비대칭 암호화 연산을 제거하여 2×MAC만을 사용한다. 또한 초기인증 과정에서 3×비대칭 암호화(1×서명, 2×DH) 연산을 사용하는 SUCV에 비교하여 제안 프로토콜은 1×MAC 및 2×비대칭 암호화 연산을 감소 시켰으며, 바인딩 갱신 과정에서도 대칭키 암호화 연산을 최소화하여 2×MAC만을 사용하였다.

5.4 개선점 요약 분석

제안 프로토콜을 RR, SUCV, OMIPv6 프로토콜과 공격에 대한 취약성을 포함한 보안 특성, 관리 특성, 패킷 교환 횟수와 암호화 연산 특성 측면에서 비교 분석하면 (표 1)와 같다

6.0 결론

MIPv6에서 MN이 새로운 서브넷으로 이동한

(표 1) 바인딩 갱신 프로토콜들의 비교

			RR	SUCV	OMIPv6	제안 프로토콜
성능적 특성	전송 교환 횟수[1]	초기인증 과정	6T	6T	6T	6T
		바인딩갱신 과정	6T	6T	2T	2T
		N번 이동	6TN	6T + 2TN	6T + 2TN	6T + 2TN
		Y분 동안 N번 이동	6TN×(Y/7)	6T + 2TN	6T + 2TN	6T + 2TN
	MN의 암호화 연산	초기 인증 과정	해쉬: 1 MAC: 2	해쉬: 1 MAC: 1 서명: 1 DH: 2	해쉬: 2 MAC: 1 서명: 1 비대칭 복호화: 1	해쉬: 1 비대칭 복호화: 1
		바인딩 갱신 과정	해쉬: 1 MAC: 2	해쉬: 2 암호화: 1 복호화: 1	해쉬: 1 MAC: 1 서명: 1 비대칭 복호화: 1	MAC: 2
	SA의 수명		7분	24시간	24시간	24시간
보안적 특성	소유권 검증		X	HoA(, CoA)	HoA, CoA	CoA
	도달성 검증		HoA, CoA	CoA	HoA, CoA	HoA, CoA
	세션키 생성 및 분배		KeyGenToken	DH	CN 생성, 공개키 암호화	CN 생성, 공개키 암호화
	BU/BA의 전송		MAC	IPSec	MAC, 서명	MAC
	위치 보안성		없음	제공	없음	제공
	공격 취약성2)	세션 강탈 공격	X	◉	◉	◉
		방향전환 공격	X	△	△	◉
		서비스거부 공격	△	△	△	◉
		중개인공격	X	◉	◉	◉

1) 한 노드에서 다른 노드까지의 전송시간을 T라 정의함
2) ◉: 공격에 강함, △: 공격이 가능함, X: 공격에 취약함

후에 수행하는 바인딩 갱신은 경로 최적화를 통한 패킷 전송의 효율성을 높이는 중요한 기능이다. 하지만, MN과 CN 사이에는 보안 연관의 규정이 없으므로 보안에 취약할 수 있다. 따라서 취약한 보안에 대한 외부의 다양한 공격에 대응하기 위해 MN을 인증하고 향후 MN과 CN 사이의 통신에 사용될 비밀키를 생성하는 인증 과정을 포함하는 다양한 바인딩 갱신 기법들이 제시되었다.

본 논문에서는 MIPv6 바인딩 갱신에서 할 수 있는 방향전환(세션 강탈), 서비스 거부, 중개인, 반사 및 증폭 공격 등을 분류 하였으며, IETF에서 기본으로 제공하는 RR과 SUCV, OMIPv6 프로토콜의 특성을 분석하고, 각 프로토콜이 갖는 취약점을 제시하였다.

이를 기반으로 본 논문에서는 MIPv6의 안전한 바인딩 갱신을 위한 프로토콜의 설계 요구사항을 제시하였고, 개선된 프로토콜을 제안하였다.

제안 프로토콜은 SUCV과 OMIPv6에서 제한된 계산 능력을 갖는 MN의 암호화 연산 취약점을 개선하기 위해 보안 프록시 방식을 적용하여 대부분의 암호화 연산을 MN대신 HA가 수행하여 MN의 성능 최적화를 제공하였으며, 보안성 강화를 위해 제안 프로토콜은 주소의 도달성 확인 및 공개키 기반의 주소를 사용하여 MN을 인증하므로, 세션 강탈, 중개인, 서비스 거부 공격에 취약한 RR 프로토콜의 보안 취약점을 개선하였고, 쿠키값을 사용하여 각 메시지를 이용한 서비스 거부 공격을 방지 하여 SUCV의 공격 취약점을 개선하였으며, MN의 공개키 암호화를 통해 24시간 동안 안전하게 바인딩 갱신을 할 수 있는 세션키를 분배하였다. 또한 공격자에게 HoA를 감추는 위치 보안성을 제공하여 각 노드에 대한 위치 보호 기능을 제공 하였다.

MN이 다른 서브넷으로 이동후에도 공개키 기반 주소를 제안하여 MN의 새로운 CoA 주소 소유권을 간단히 검증하며, MN이 이동 중 한 개의 CN과만 통신을 할 수 있는 OMIPv6 주소 생성의 취약점을 개선하여 다수의 CN과 통신 할 수 있게 하는 주소 방식을 제안하여 주소의 관리성 및 확장성을 제공하였다.

이와 같이 제안 프로토콜은 기존 프로토콜과 비교하여 강한 보안성과 우수한 관리성 및 편리한 확장성을 제공할 뿐 아니라, MN의 암호화 연산을 최소화하였다.

향후 연구로는 사용자의 이동 패턴을 고려하여 바인딩 갱신 방법 및 보안 연관 시간을 결정하는 적응적 바인딩 갱신 프로토콜의 개발이 가능하다.

참 고 문 헌

[1] 조 경산, 엄 희용, "Mobile IPv6의 빠른 핸드오버 기법의 성능 개선," 한국시뮬레이션학회 논문지, 제11권 제1호, pp. 1-9, 2002

[2] 조 경산, 원 유석, "MIPv6의 안전한 바인딩 갱신을 위한 프로토콜 비교 분석," 정보처리학회 논문지 C, 제10-C권, 제6호, pp. 755-762, 2003

[3] 조 경산, 유 일선, 원 유석, "안전한 모바일 IPv6 바인딩 갱신을 위한 개선된 프로토콜", 정보처리학회 논문지 C, 제11-C권 제5호, pp. 605-612, 2004.

[4] 조 경산, 원 유석, "SUCV를 개선한 MIPv6 바인딩 갱신 프로토콜," 정보처리학회 논문지 C, 제13-C권, 제3호, pp. 267-274, 2006

[5] D. Johnson and C. Perkins, "Mobility Support in IPv6," IETF RFC 3775, 2004.

[6] S. Okazaki, et al., "Securing MIPv6 Binding Updates Using Address Based Keys (ABKs)," draft-okazaki-mobileip-abk- 01.txt, 2002. Work in progress

[7] R. Deng, et al., "Defending Against Attacks in Mobile IP," Proc. of ACM CCS '02, pp 59-67, 2002.

[8] T. Aura, et al., "Cryptographically Generated Addresses (CGA)," draft-aura-cga-00.txt, 2003.

Work in progress

[9] G. O'Shea, M. Roe, "Child-proof authentication for MIPv6(CAM)," ACM SIGCOMM Computer Communication Review, ACM Press, Vol. 31, No. 2, pp. 4-8, April 2001.

[10] G. Montenegro, C. Castelluccia, "Crypto-Based Identifiers(CBIDs): Concepts and Applications", ACM Transations on Information and System Security, Vol.7, No. 1, pp 97-127, 2004.

[11] F. Dupont, CELAR, W. Hadded, "Optimizing Mobile IPv6(OMIPv6)," draft-dupont-mipshop-omipv6-00.txt, 2006. Work in progress

[12] F. Zhao, S F, Wu, UC Davis, S. Jung, "Extensions on Return Routability Test in MIP6," <draft-zhao-mip6-rr-ext-01.txt>, 2005. Work in progress

[13] T. Koskiahde, "Security in Mobile IPv6," Tampere University of Technology, 2002. and Acknowledgments," <draft-roe-mobileip-updateauthe-02.txt>, 2002. Work in progress

[14] W. Al-Salihy and R. Sures, "Security Threats Analysis of Route Optimization Mechanism in Mobile IPv6," 2003.

◐ 저 자 소 개 ◑

원 유 석(You-Seuk Won)
2000년 단국대학교 전산통계학과 졸업(학사)
2002년 단국대학교 대학원 전산통계학과 졸업(이학석사)
20002년 ~현재 단국대학교 대학원 박사과정
관심분야 : 네트워크 시스템 및 이동 통신 보안, Mobile IPv6, 프로토콜 보안
E-mail : server11@dankook.ac.kr

조 경 산(Kyung-san Cho)
1979년 서울대학교 전자공학과 졸업(학사)
1981년 한국과학원 전기전자공학과 졸업(공학석사)
1988년 Univ. of Texas at Austin 전기전산 공학과 Ph.D.
1988년 ~ 1990년 삼성전자 컴퓨터부분 책임연구원, 실장
1990년 ~ 현재 단국대학교 정보컴퓨터학부 교수
관심분야 : 네트워크 시스템 및 이동 통신 보안, 웹 응용, 컴퓨터 시스템
E-mail : kscho@dankook.ac.kr