SUCV를 개선한 MIPv6 바인딩 갱신 프로토콜

원 유 석[†] · 조 경 산[††]

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 기존의 여러 바인딩 갱신 프로토콜들의 특성을 비교 분석하고, 그 중에서 보안성 및 성능에서 우수한 평가를 받는 SUCV 프로토콜에 대한 공격 취약점과 관리의 문제점을 제시하고, 이를 해결할 수 있는 개선된 바인딩 갱신 프로토콜을 제안한다. 또한, 상세한 분석을 통해 제안 프로토콜이 SUCV 프로토콜이 갖는 redirect 공격, DoS 공격 및 brute force 공격에 대한 취약성과 관리적 문제점을 개선하고 MN의 연산 부하를 감소시킴을 제시한다.

키워드 : MIPv6, 안전한 바인딩 갱신, 보안, SUCV

Improving SUCV Protocol for the Secure Binding Update in MIPv6

YouSeuk Won[†] · Kyungsan Cho[††]

ABSTRACT

The process of binding update for the routing optimization in MIPv6 can make the involved MN (Mobile Node) and CN(Correspondent Node) vulnerable to various attacks. Therefore, securing binding update process becomes an important research issue in the MIPv6, and several secure binding update protocols have been proposed. In this paper, we compare several existing binding update protocols, and analyze the vulnerability of MNs and CNs to the possible attacks and the management overhead of the SUCV(Statistic Uniqueness and Cryptographic Verifiability) which is considered to be superior to other protocols. Then, we propose an advanced protocol to resolve above drawbacks. Through the detailed analysis, we show that our protocol can reduce the computational overhead of MN, enable better management, and achieve a higher level of security against the redirect attacks, DoS(Denial of Service) attacks and brute force attacks, compared to SUCV.

Key Words : MIPv6, Secure Binding Update, Security, SUCV

1. 서 론

MIPv6(Mobile IPv6) 환경에서 이동성을 가진 모바일 호스트는 MN(Mobile Node)이라하고 MN과 통신하는 상대 호스트는 CN(Correspondent Node)이라하며, MN이 처음 위치한 홈 서브넷에 있는 라우터는 HA(Home Agent)라 한다. MIPv6에서는 호스트가 다른 서브넷으로 이동하여도 인터넷을 통한 통신을 계속하기 위해 2개의 주소 HoA(Home Address)와 CoA(Care-of Address)를 사용한다. HoA는 홈 서브넷에서 MN에게 부여된 IP주소로 연결 인식을 위해 사용되며, CoA는 MN이 이동한 후에 부여되는 임시 주소로 라우팅을 위해 사용되는데, HoA와 CoA와의 연계를 바인딩이라 한다. MIPv6에서는 MN이 새로운 서브넷으로 이동한 후에 CN이 MN의 새로운 주소로 직접 통신할 수 있는 경로 최적화(route optimization) 기능을 기본으로 제공하는데, 이를 위해서 MN은 CN에게 새로운 CoA를 제공하는 바인딩 갱신을 수행해야 한다[1, 2].

하지만 안전하지 않은 바인딩 갱신은 오히려 공격자로 하여금 MN과 CN에게 다양한 보안 공격을 가능하게 한다. 따라서, 안전한 바인딩 갱신이 MIPv6의 중요한 과제가 되고 있으며, 이를 위한 여러 프로토콜들이 제안되었다. 즉, IETF(Internet Engineering Task Force)에서 바인딩 갱신 보안을 위한 기본 프로토콜로 채택한 RR(Return Routability)[10], 주소기반 공개키(Public Key)를 사용하는 ABK(Address-based key)기법[12], PKI(Public Key Infrastructure)기반의 DH(Diffie-Hellman)키 교환을 이용하는 보안 프록시 기반 기법[11]등이 제시되었다. 또한, 전역 인터넷에서 유효한 CA의 필요 없이 주소로 MN의 공개키를 인증하는 CGA(Cryptographically Generated Addresses) 기법[4]이 제안됨에 따라, CGA 기법을 활용하는 CAM-DH(Child-proof Authentication for MIPv6 with Diffie-Hellman)[8], SUCV(Statistic Uniqueness

† 준 회 원 : 단국대학교 대학원 박사과정
†† 종신회원 : 단국대학교 정보컴퓨터학부 교수
논문접수 : 2005년 4월 1일, 심사완료 : 2006년 6월 23일

and Cryptographic Verifiability)[6, 7] 프로토콜이 제시되었다. 제안된 여러 프로토콜 중에서 CAM-DH와 SUCV가 보안성에서 우수한 것으로 평가되었으며[1], 특히 SUCV는 IPsec과의 유기적인 연동을 지원하는 장점을 갖는 것으로 분석되었다[6].

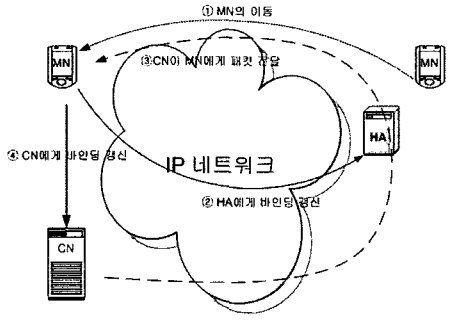
본 논문에서는 기존 프로토콜 중에서 보안성 및 성능에서 우수한 평가를 받는 SUCV 프로토콜(과 이의 최적화 프로토콜)이 갖는 다양한 공격에 대한 취약점과 관리적 제약점을 분석하여 제시하고, 이를 해결할 수 있는 개선된 프로토콜을 제안한다. 또한, 상세한 분석을 통해 제안 프로토콜이 SUCV 최적화 프로토콜에 비해 보안성과 성능 및 관리성에서 우수함을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 MIPv6의 바인딩 갱신과 가능한 공격의 유형을 설명하고, 안전한 바인딩 갱신을 위한 기존의 프로토콜들을 비교 분석한다. 3장에서는 기존의 프로토콜 중에서 우수한 평가를 받고 있는 SUCV와 SUCV 최적화 프로토콜을 설명하고 이들의 공격에 대한 취약점과 관리적 문제점을 분석한다. 4장에서는 분석된 취약점을 개선한 프로토콜을 제안하고, 5장에서는 제안 프로토콜이 SUCV에 비해 보안성, 성능, 관리성 면에서 우수함을 제시하고, 6장의 결론으로 끝맺음 한다.

2. MIPv6의 바인딩 갱신

2.1 MIPv6의 바인딩 갱신

MIPv6의 환경에서 MN의 이동을 지원하고 경로 최적화를 위해 HA와 CN은 MN의 HoA와 CoA의 새로운 바인딩을 유지해야 한다. 이를 위해 MN은 새로운 서브넷으로 이동한 후에 CoA와 HoA의 새로운 바인딩을 생성하고, HA와 CN에게 바인딩 갱신을 통해 새로운 CoA를 등록한다. MIPv6에서 MN의 이동에 따른 바인딩 갱신 과정은 (그림 1)과 같다.

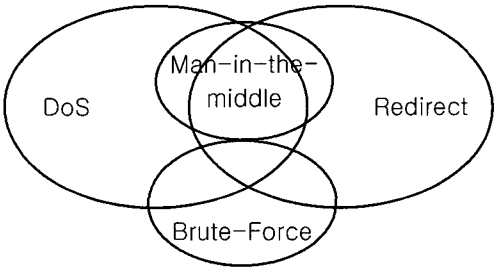


(그림 1) MIPv6의 바인딩 갱신 과정

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

2.2 가능한 공격 유형

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



(그림 2) 공격 유형의 연관성

Redirect(방향 전환) 공격은 패킷을 실제 목적지가 아닌 다른 노드(또는 네트워크)로 전송하는 공격이다. 모든 redirect 공격은 MN 또는 제3의 공격자에 의해 여러 방법으로 가능하며, redirect 공격의 대상이 되는 노드(또는 네트워크)에게는 DoS 공격과 범람(Flooding, Bombing) 공격이 동시에 가해질 수 있다.

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

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

man-in-the-middle(중개인) 공격은 제어 패킷이 평문으로 전송되는 경우에 이를 가로채어 패킷의 내용을 수정하여 전달하는 공격이다.

2.3 기존의 바인딩 갱신 프로토콜 분석

안전한 바인딩 갱신을 위해 다음에 같은 여러 프로토콜들이 제안되었다.

MN이 주장하는 2개의 주소 HoA와 CoA에서 MN의 수신을 확인하는 RR 프로토콜은 평문으로 전송되는 두 개의 쿠키를 해쉬을 통해 생성한 세션키로 바인딩 갱신 패킷을 암호화한다[5]. RR 프로토콜은 공격자가 CN과 HA(및 MN) 사이에 전송되는 평문의 HoT 및 CoT에서 정보를 가로채어 세션키를 생성하여 위조된 바인딩 갱신 패킷을 통한 재전송 공격이 가능하다. 또한, 사악한 MN이 CN에게 희생 노드로 이동하였다고 거짓으로 바인딩 갱신을 하여 대용량 통신을 희생 네트워크로 이동시켜 범람에 의한 DoS 공격이 가능하다. 암호화되지 않은 제어 패킷에 대한 man-in-the-middle 공격도 가능하다[3, 11].

HA가 MN의 보안 프록시로 동작하는 보안 프록시 기반 프로토콜은 비용이 많이 드는 공개키 연산을 MN대신 수행하고, DH(Diffie-Hellman) 키 교환 기법을 통하여 세션키를 생성하여 MN에게 전달한다[11]. 보안 프록시 프로토콜은 MN의 악의적인 redirect 공격과 이로 인한 DoS 공격이 가능하며, 전체 인터넷을 통한 전역적인 CA를 필요로 하는 비현실 적인 요소가 있다. 또한 CA에 의한 인증 및 CRL 검증에 과도한 연산으로 인한 DoS 공격이 가능하다[3, 9].

HA가 신뢰할 수 있는 IPKG(Identity-based Private Key Generator) 역할을 하는 ABK 기법은 HA가 자신의 홈 네트워크에 있는 모든 MN들의 개인키와 암호화 인수를 생성하

〈표 1〉 바인딩 갱신 프로토콜들의 비교

		RR	보안 프록시	ABK	CAM-DH	SUCV
바인딩 갱신시 MN과 CN의 암호화 연산		공유 세션키	공유 세션키	공유 세션키	공유 세션키	공유 세션키
		SHA-1 × 3 HMAC × 2	SHA-1 ×2	SHA-1 × 3 HMAC × 2	SHA-1 × 3 HMAC × 2	HMAC x2 암/복호 x2
세션키 분배 방법 및 MN과 CN의 암호화 연산		프로토콜 기반	PKI 기반	ABK 공개키 기반	주소 기반 공캐키	주소 기반 공개키
		SHA-1 × 3	SHA-1 × 2 HMAC × 4 DH agree × 1 DH gen × 1	HMAC × 4 SHA-1 × 2 암/복호 × 2	SHA-1 × 4 HMAC × 6 DH agree × 1 서명/서명검증 × 2	공개/개인키 쌍 생성 × 1 SHA-1 × 7 HMAC × 9 DH agree× 1 서명/서명검증 x 2
공격 취약성[1]	Redirect	X	△	△	△	△
	DoS	X	△	△	△	△
	Brute-Force	◉	◉	◉	△	△
	Man-in-the-middle	X	△	X	◉	◉
TTP의 기능		없음	보안 프록시	HA	없음	없음
MN의 인증		주소로 인증	프록시로 인증	공개키로 인증	공개키로 인증	공개키로 인증
IPSec과의 연동		없음	없음	없음	없음	있음

1) ◉ : 공격에 강함, △ : 공격이 가능함, X : 공격에 약함

여 MN에게 제공하고, CN에게는 암호화 인수를 평문으로 제공한다[12]. 그러나 ABK의 HoA의 인터페이스 식별자는 CoA의 인터페이스 식별자와 동일한 값을 갖는 전역적으로 유일한 주소를 가져야한다는 제약이 있으며, 암호 또는 서명되지 않은 제어 패킷에 대하여 man-in-the-middle 공격이 가능하다. 또한, HA가 자신의 홈 서브넷에 있는 MN의 개인키/공개키를 생성하여 자신이 이를 사용하거나, 사악한 MN이 바인딩 갱신에 위조된 CoA를 사용하여 재전송 공격과 DoS 공격이 가능하며, HA에 대한 공격으로 암호 인수가 유실되면 피해가 발생한다. 공개키 기반의 과도한 연산은 범람에 의한 DoS 공격이 가능하다[3].

CAM-DH는 RR 프로토콜 방식에 디지털 서명된 DH 키 교환 기법을 통합하여 안전한 바인딩 갱신을 추구하는 프로토콜이다[10]. MN은 디지털 서명된 DH 인수를 사용하여 세션키를 생성하고 바인딩 갱신에 활용한다. CAM-DH는 높은 수준의 보안성에도 불구하고 다음과 같은 취약점을 가진다. CAM-DH 최적화 프로토콜에서 HA는 인증 되지 않은 CN의 DH 키 인수를 사용하여 세션키 K_h를 생성한다. 이 취약점을 이용하여 공격자들은 대량의 DH 키 인수를 포함한 camdp2 메시지를 전송하여 서비스 공격과 범람 공격을 할 수 있으며, 제한된 자원을 가지고 있는 MN의 비대칭 암호화 연산을 감소시키지 못하였다. 또한 CAM-DH는 단일 해쉬 기반의 CGA를 사용하여 주소의 소유권을 인증한다. 단일 해쉬 기반의 CGA는 주소의 소유권을 인증하기 위해 인터페이스 식별자의 62비트만을 공개키 해쉬(hash)값으로 사용하는데, 62비트의 인터페이스 식별자는 전사 공격에 취약한 문제가 있다[9].

SUCV는 MN이 개인키와 공개키의 쌍을 생성하고 이로부터 인터페이스 식별자를 생성하도록 하여 MN을 인증하는 CGA개념을 적용하여 주소의 소유권 문제를 해결하였다. 또한, DH 키 교환 방법을 이용하여 MN과 CN 사이의 세션키를 생성한다[7]. 생성된 세션키는 IPsec ESP(Encapsulating Security Payload)에 사용하므로, SUCV는 IPsec와 유기적인 연동을 할 수 있는 장점이 있다[1, 6].

앞에서 설명된 바인딩 갱신 프로토콜들의 특성을 분석하여 비교하면 <표 1>과 같다.

3. SUCV 프로토콜

본 장에서는 SUCV 프로토콜과 이를 개선한 SUCV 최적화 프로토콜을 분석하고, SUCV 최적화 프로토콜의 문제점을 제시한다.

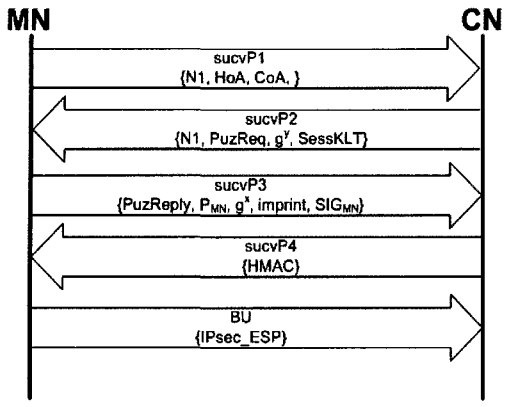
본장에서 사용되는 표기법은 다음과 같다.

- prf(): 의사 난수 함수로 160 비트를 생성.
- hash: 암호 해쉬 함수로 SHA-1을 사용.
- sucvHID: 64 비트 SUCV 식별자.
- Px/Sx: X의 공개키 개인키 쌍.

3.1 SUCV 프로토콜

SUCV는 MIPv6의 바인딩 갱신 과정에서 발생하는 주소의 소유권 문제를 해결하기위해 CGA개념을 사용한다. CGA 개념은 MN의 개인키와 공개키의 쌍을 생성하고, 생성된 공개키를 해쉬하여 인터페이스 식별자를 생성하도록 한다. 생성된 인터페이스 식별자는 MN의 주소 소유권을 인증하는데 사용한다. 즉, MN은 개인키로 서명된 바인딩 갱신 메시지를 CN에게 전송하고, CN은 MN의 인터페이스 식별자로 바인딩 갱신 메시지를 검증하고 MN 주소의 소유권을 확인한다.

(그림 3)은 SUCV 프로토콜의 동작 과정이며, 각 단계별 수행 내용은 다음과 같다.



(그림 3) SUCV 프로토콜

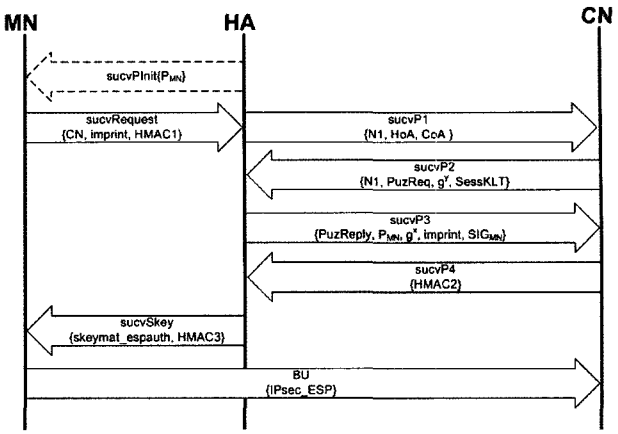
1) MN은 임의의 변수 N1과 HoA, CoA를 포함한 sucvP1 메시지를 CN에게 전송하여 바인딩 갱신을 시작한다.
2) 이를 수신한 CN은 DoS 공격을 막기 위한 클라이언트 퍼즐(PuzReq)과 DH값 g^y, 세션키 유효 기간(SessKLT) 등이 포함된 sucvP2 메시지로 MN에게 응답한다.
3) MN은 수신한 g^y와 자신이 생성한 g^x를 이용하여 IPsec에 사용될 세션키를 생성하고, 이후에 IPsec ESP을 사용하여 전송될 BU를 위하여 보안 연관(SA: security association)을 생성한다. 퍼즐의 응답(PuzReply), 공개키 P_{MN}, 임의의 변수 imprint, MN의 DH값 g^x값과 이 값들을 MN의 개인키 S_{MN}로 서명한 SIG_{MN}등이 포함된 sucvP3 메시지를 CN에게 전송한다.
4) sucvP3를 수신한 CN은 퍼즐의 올바른 응답인 경우에만 공개키를 이용하여 서명을 검증하고, MN의 주소 소유권을 확인하여 MN을 인증하게 된다. 또한 IPsec에 사용될 세션키를 생성하고, 이후에 IPsec ESP를 사용하여 전송될 BU를 위하여 보안 연관을 생성한다. sucvP4는 바인딩 갱신할 때, 보안 조합에 사용될 SPI(Security Parameter Index)와 HMAC를 구하여 MN에게 전송된다.
5) IPsec ESP에 사용될 세션키 및 보안 연관을 생성한 MN과 CN은 안전한 터널을 생성한 후에 바인딩 갱신 메시지를 전송한다.

3.2 SUCV 최적화 프로토콜

SUCV의 강력한 암호화 연산을 이용한 바인딩 갱신 방법은 PDA, 셀룰러폰, 센서 네트워크와 같은 제한된 계산능력과 한정된 전원 공급을 가진 MN에게는 과도한 연산 부담이 된다. 이러한 문제의 해결을 위해, SUCV 프로토콜에서 공개키와 개인키 쌍의 생성과 비대칭 암호화 연산을 MN대신 HA가 수행하는 SUCV 최적화 프로토콜이 제시되었다.

SUCV 최적화 프로토콜은 (그림 4)와 같이 수행된다.

1) SUCV 최적화 프로토콜에서 MN의 부하를 줄이기 위하여 각 MN의 공개키와 개인키의 쌍을 HA가 생성하여 MN에게 sucvPInit 패킷으로 전송한다.
2) MN은 임의의 변수 imprint 값과 공개키를 이용하여 sucvHID를 생성하고, CN과 안전한 바인딩 갱신을 하기 위하여 HA에게 imprint 값과 이것의 인증 헤더 HMAC1을 계산하여 전송한다.



(그림 4) SUCV 최적화 프로토콜

3) imprint값을 수신한 HA는 MN을 대신하여 앞 절에서 설명된 SUCV 프로토콜(sucvP1, sucvP2, sucvP3, sucvP4)을 수행하여 세션키를 생성한다.
4) 생성된 세션키는 sucvSkey 메시지안에 포함되어 HA와 MN 사이의 안전한 터널을 통하여 전송된다.
5) 세션키를 수신한 MN은 CN과 IPsec ESP으로 안전한 터널을 생성한 후에, 바인딩 갱신 메시지를 전송한다.

<표 2>는 SUCV의 최적화에 따른 MN과 HA에서의 연산량을 비교한 표이다.

SUCV 최적화 프로토콜은 비용이 많이 드는 공개키/개인키의 생성과 서명 및 DH 연산을 HA가 대신 수행하여 MN의 연산 부담을 경감시키므로 MIPv6 환경에서 제한된 계산능력을 가진 모바일 통신에 적합하다.

〈표 2〉 SUCV 와 SUCV 최적화 암호화 연산 비교

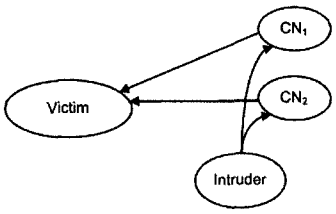
		SUCV	SUCV 최적화 프로토콜
MN	초기화	공개/개인키 쌍 생성: 1 hash: 2 HMAC: 1	hash: 2 HMAC: 2 암/복호: 1
	키 분배	hash: 2 HMAC: 4 서명: 1 DH agree: 1 암호: 1	HMAC: 3 암/복호: 3
HA	초기화	X	MN의 공개/개인키 생성: 1 HMAC: 1 암호: 1
	키 분배	X	1hash: 2 HMAC: 6 서명: 1 DH agree: 1 암/복호: 2

3.3 SUCV 최적화 프로토콜 취약점

제시된 효율성에도 불구하고, SUCV 및 SUCV 최적화 프로토콜은 다음과 같이 여러 측면에서 취약점이 있는 것으로 분석된다.

3.3.1 MN의 악의적인 redirect 공격

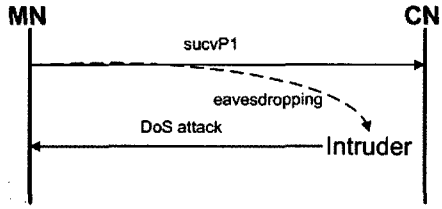
SUCV는 (그림 5)와 같이 MN의 악의적 바인딩 갱신 redirect 공격에 취약한 것으로 분석된다[11].



(그림 5) MN의 악의적인 redirect 공격

예를 들어, MN이 비디오 서버(CN_1, CN_2)들에게 서비스를 요청한 후에 다른 주소(희생자 노드)로 이동하였다고 허위 바인딩 갱신 메시지를 CN_1 및 CN_2에게 전송할 수 있다. 이 경우에 비디오 서버들로부터 대량의 비디오 자료가 허위 주소로 갱신된 희생자 노드에게 전송되어 서비스가 정지될 수 있다.

3.3.2 sucvP2를 이용한 DoS 공격



(그림 6) sucvP2를 이용한 MN의 DoS 공격

(그림 6)과 같이 공격자들은 sucvP1을 도청하고, 도청한 N1과 어려운 해쉬 연산을 요구하는 퍼즐을 포함한 sucvP2를 MN(최적화 프로토콜에서는 HA)에게 대량 전송하여 DoS 공격을 할 수 있다. 이러한 DoS 공격을 막기 위해 SUCV 프로토콜은 2가지 대안을 제시하고 있다[6]. 첫째 대안은 MN과 마찬가지로 CN 또한 SUCV 주소를 사용하고 개인키로 sucvP2를 서명하도록 한다. 이 제안은 추가적인 비대칭키 암호화 연산의 수행에 의해 성능이 저하되며, CN 역시 SUCV 주소를 사용하므로 관리성 및 확장성이 떨어지게 된다. MN에게 과도한 연산을 요구하는 해쉬 연산을 제거 하는 둘째 대안은 보안상의 취약점을 가지며 MN에게 한번 이상의 해쉬 연산을 요구하게 된다.

3.3.3 단일 해쉬 기반 CGA 사용으로 인한 전사 공격

SUCV는 단일 해쉬 기반의 CGA를 사용한다. CGA는 주소의 소유권을 인증하기 위해 인터페이스 식별자의 62비트만을 공개키 해쉬(hash)값으로 사용하는데, 62비트의 인터페이스 식별자는 전사 공격에 취약한 문제가 있다.

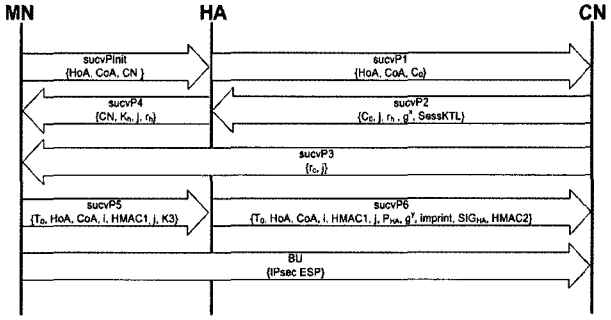
3.3.4 HA에 의한 공개키/개인키 관리의 과부하

MN 대신에 HA가 고비용 연산인 공개키 연산, 서명, 서명 검증 등을 대신 수행하는 SUCV 최적화 프로토콜에서 HA가 모든 MN의 공개키와 개인키 쌍들을 유지하고 관리한다. 따라서, MN의 개인키와 공개키 쌍의 관리가 복잡해지고 네트워크의 확장성이 떨어지게 된다. 또한 모든 MN의 개인키 및 공개키 연산을 수행하여 HA의 성능 저하가 예상된다.

4. 제안 프로토콜

4.1 제안 프로토콜의 동작

(그림 7)에 제시된 제안 프로토콜은 다음과 같이 동작한다.



C_0 = prf(K_{CN}, HoA|CN|N), K_{HA} is a secret key of HA
r_h = prf(K_{CN}, HoA|N_j|0), K_{CN} is a secret key of CN
r_c = prf(K_{CN}, CoA|N_j|0)
K_3 = hash(r_h|r_c)
K_h = hash(g^{xy}|r_h|imprint)
skymat_espauth = prf(K_h, r_c)
HMAC1 = prf(skymat_espauth, T_0|HoA|CoA|i)
SIG_{HA} = S_{HA}(HoA|CoA|g^y|imprint|P_{HA})
HMAC2 = prf(K_3, T_0, HoA, CoA, j, P_{HA}, imprint, g^y, SIG_{HA})

(그림 7) 안전한 바인딩 갱신을 위한 제안 프로토콜

1) MN은 HoA, CoA, CN을 포함한 sucvPInit을 HA에게 전송하여, CN으로의 바인딩 갱신 과정을 시작한다.
2) sucvPInit를 수신한 HA는 쿠키(C_0)를 추가한 sucvP1메시지를 CN에게 전송한다.
3) sucvP1를 수신한 CN은 MN의 HoA에게 sucvP2를 전송하고 CoA에게 sucvP3를 전송한다. RR 기법으로 MN의 새로운 CoA를 검증하고, DoS 공격을 방지한다.
4) sucvP2를 수신한 HA는 쿠키를 확인하여 그 값이 유효하면, 새로운 DH값 g^y를 생성하고 K_h = hash(g^{xy}|r_h|imprint)를 포함한 sucvP4를 MN에게 전송한다.
5) sucvP3와 sucvP4를 수신한 MN은 세션키(skymat_espauth)을 생성하고, 세션키를 사용하여 HMAC1을 계산한다. HMAC1과 K_3등을 포함한 sucvP5 메시지를 HA에게 전송한다.
6) sucvP5을 수신한 HA는 자신의 개인키 S_{HA}로 (HoA|CoA|g^y|imprint|P_{HA})를 서명하고, HMAC2를 계산하여 이들을 포함한 sucvP6를 CN에게 전송한다. 이를 수신한 CN은 K_3를 사용하여 HMAC2를 먼저 확인하여 MN의 새로운 주소 CoA를 인증하고, HMAC2가 유효하면 세션키를 이용하여 HMAC1을 검증한다.

4.2 제안 프로토콜의 특성

제안 프로토콜은 SUCV 및 SUCV 최적화 프로토콜을 다음과 같이 개선하였다.

4.2.1 RR 기법 적용

SUCV 최적화 프로토콜에서 MN은 HA로부터 수신한 세션키를 이용하여 CN에게 직접 바인딩 갱신 메시지를 전송하므로 MN의 악의적인 바인딩 갱신 redirect 공격에 취약하였다. 제안 프로토콜은 이러한 취약점을 개선하기 위하여 HoA와 CoA의 두 주소 모두에게 전송하여 MN을 인증하는 RR 테스트 기법을 도입하였다.

4.2.2 쿠키 사용

SUCV 및 SUCV 최적화 프로토콜에서 CN에 대한 DoS 공격을 막기 위하여 사용되는 퍼즐로 인한 보안적 취약점을 개선하기 위하여, 제안 프로토콜은 퍼즐 대신에 쿠키를 사용한다. 쿠키가 유효할 동안 HA는 비대칭 암호화 연산을 하므로 대량의 sucvP2를 이용한 DoS 공격에 대응할 수 있다.

4.2.3 CGA 강화

제안 프로토콜에서는 키 크기를 증가시키는 효과를 위해 Aura가 제안한 이중 해쉬 기반 CGA[4]을 도입하여 설계하였다.

4.2.4 보안 프록시 적용

제안 프로토콜은 HA가 MN의 보안 프락시로 동작하도록 설계되어 HA의 공개키/개인키 쌍을 유지하며 MN의 비대칭 암호화 연산을 대신하게 한다. 따라서, 관리성과 확장성 및 성능을 개선하였다.

5. 제안 프로토콜의 개선점 분석

본장에서는 제안 프로토콜이 SUCV 최적화 프로토콜을 보안성과 암호화 연산, 관리성 및 확장성 측면에서 어떻게 개선하였는가를 제시한다.

5.1 보안성 분석

5.1.1 redirect 공격

redirect 공격은 CN들에서 공격자가 선택한 네트워크로 트래픽의 방향 전환 공격하는 방법으로 세션 강탈 공격(Session Hijacking)과 적합한 MN의 악의적인 바인딩 갱신 redirect 공격(Malicious Mobile Node Flooding)으로 분류된다[11]. 제안 프로토콜은 RR기법과 이중 해쉬 기반의 CGA, 서명된 SIG_{HA}를 사용하여 강력한 주소 인증을 사용하므로 세션 강탈 공격에 대응할 수 있다. 또한, 제안 프로토콜은 HA를 통해 MN의 새로운 CoA을 인증하는 RR기법을 사용하여 적합한 사용자에 의한 악의적인 redirect 공격에 대응할 수 있다.

5.1.2 DoS 공격

1) sucvP1을 이용한 DoS 공격

공격자들은 sucvP1 메시지를 CN에게 대량으로 전송하여 DoS 공격을 할 수 있다. 제안 프로토콜에서는 추가적인 암호화 연산을 수행하거나 새로운 값을 생성하는 대신에 주기적으로 변화되는 CN의 DH 공개키 값 g^x를 사용하므로 이 공격에 취약하지 않다.

2) sucvP2를 이용한 DoS 공격

공격자들은 sucvP2를 대량으로 전송하여 DoS 공격을 할 수 있으므로, 제안 프로토콜에서는 쿠키를 사용하여 HA에 대한 공격에 대응한다. 즉, HA가 sucvP1 전송시에 생성한 쿠키 값과 sucvP2로 수신된 쿠키 값을 비교하여 유효한 경우에만 sucvP4에 사용될 비대칭 암호화 연산을 한다.

3) sucvP6을 이용한 DoS 공격

공격자들은 CN에게 대량의 sucvP6를 전송하여 DoS 공격을 할 수 있다. 제안 프로토콜은 RR 기법을 도입하여 새로운 CoA를 검증하므로 sucvP6를 이용한 DoS 공격을 막는다. 이 공격을 막기 위하여 CN은 MN의 HoA에게 sucvP2를 보내고, MN의 CoA에게 sucvP3를 전송한다. 즉, CN은 RR 기법을 통하여 MN의 새로운 CoA를 검증한다.

5.1.3 전사 공격

SUCV 프로토콜에서 채택한 단일 해쉬 기반 CGA는 62비트의 키를 사용하여 전사 공격에 취약점이 발생한다. 이러한 취약점을 해결하기 위하여, 제안된 프로토콜은 Aura의 이중 해쉬 기반의 CGA를 활용한다. 이중 해쉬 기반 CGA는 전사공격에 2^{12*SEC} (SEC은 CGA의 보안 인수) 인수를 사용하여 암호화 연산 증가 효과를 얻어 SUCV의 기밀 보호를 확장한다. 이중 해쉬 기반에서 첫 번째 해쉬1 값은 주소의 인터페이스 식별자를 생성하고, 두 번째 해쉬2 값은 새로운 주소 생성에 인위적으로 계산 복잡도를 증가시켜 전사공격을 방어하기 위해 사용한다. 따라서, 전사공격에 필요한 비용은 단일 해쉬 기반의 CGA를 사용한 SUCV의 2^{59}에서 이중 해쉬를 사용하는 제안 프로토콜의 $2^{59+12*SEC}$로 증가하여 전사 공격을 어렵게 만든다.

5.2 관리성 분석

SUCV 최적화 프로토콜은 HA가 모든 MN의 공개키/개인키 쌍을 관리하므로 관리성 및 확장성이 떨어지며, 또한 HA가 모든 MN의 개인키 및 공개키 연산을 수행하므로 성능 저하가 예상된다. 제안 프로토콜에서는 HA가 자신의 MIPv6 주소를 이용하여 CGA에 사용될 공개키/개인키 쌍인 P_{HA}/S_{HA}를 생성한다. 또한, HA의 주소를 이용하여 주소의 소유권을 인증하여 HA의 비대칭 연산을 감소시키므로 기존의 공개키 기반의 프로토콜에 비해 관리성 및 확장성을 높일 수 있다.

〈표 3〉 암호화 연산 비교

		제안 프로토콜	SUCV 최적화 프로토콜
MN	초기화	X	hash: 2 HMAC: 2 복호: 1
	키 분배	hash: 1 HMAC: 5 암/복호: 3	HMAC: 3 암/복호: 3
HA	초기화	HA의 공개/개인키 생성: 1 hash: 2 HMAC: 1	MN의 공개/개인키 생성:1 HMAC: 1 암호: 1
	키 분배	hash: 1 HMAC: 4 서명: 1 DH agree: 1 암/복호: 3	hash: 2 HMAC: 6 서명: 1 DH agree: 1 암/복호: 2

5.3 암호화 연산 분석

CN을 제외한 MN과 HA에서의 암호화 연산 요구를 제안 프로토콜과 SUCV 최적화 프로토콜에서 비교 분석하면 <표 3>과 같다.

SUCV 최적화 프로토콜에 비교하여 제안 프로토콜은 MN에게 키 분배 과정에서 2×HMAC와 1×hash 연산을 더 요구하지만 초기화 과정에서는 2×hash 및 1×HMAC의 연산을 감소시키므로, MN의 연산량은 감소한다. HA 역시 추가적인 1×암/복호가 필요하지만 2×HMAC을 감소시켜 SUCV 최적화 프로토콜과 비슷한 성능을 보인다.

제안 프로토콜은 새로운 MN이 생성 될 때마다 HA가 공개키/개인키를 생성하고 유지해야 하는 비용을 감소시킨다.

5.4 개선점 분석의 요약

제안 프로토콜을 SUCV 최적화 프로토콜과 보안성 및 성능, 관리 측면에서 비교 분석하면 <표 4>와 같다.

〈표 4〉 SUCV와 제안 프로토콜 비교

	제안 프로토콜	SUCV 최적화
공개키 소유권 메커니즘	이중 해쉬 기반 CGA	단일 해쉬 기반 CGA
공개키/개인키 생성 및 관리	HA	MN
Brute-force 공격에 대한 연산량	$O(2^{59+12*Sec})$	$O(2^{62})$
MN이 수행하는 비대칭 암호화 연산량	0	0
관리성 및 확장성	높음	낮음
DoS 취약성	◉	△
redirect, replay 공격에 대한 취약성	◉	△
MN의 암호화 연산	hash: 2 HMAC: 5 암/복호: 3	hash: 1 HMAC: 5 암/복호: 3

◉ : 공격에 강함, △ : 공격이 가능

제안 프로토콜을 RR, 보안 프록시, ABK, CAM-DH, SUCV 프로토콜과 공격에 대한 취약성을 포함한 보안 특성, 관리 특성, 패킷 교환 횟수와 암호화 연산 특성 측면에서 비교 분석하면 <표 5>와 같다.

6. 결 론

MIPv6에서 MN이 새로운 서브넷으로 이동한 후에 수행하는 CN으로의 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 위한 다양한 바인딩 갱신 기법들이 제시 되었다. 기

〈표 5〉 바인딩 갱신 프로토콜들의 비교

		RR	보안 프록시	ABK	CAM-DH	SUCV	제안 프로토콜
바인딩 갱신시 MN과 CN의 암호화 연산		공유 세션키	공유 세션키	공유 세션키	공유 세션키	공유 세션키	공유 세션키
		SHA-1 × 3 HMAC × 2	SHA-1 ×2	SHA-1 × 3 HMAC × 2	SHA-1 × 3 HMAC × 2	HMAC x2 암/복호 x2	HMAC x2 암/복호 x2
세션키 분배 방법 및 MN과 CN의 암호화 연산		프로토콜 기반	PKI 기반	ABK 공개키 기반	주소 기반 공캐키	주소 기반 공개키	주소 기반 공개키
		SHA-1 × 3	SHA-1 × 2 HMAC × 4 DH agree × 1 DH gen × 1	HMAC × 4 SHA-1 × 2 암/복호 × 2	SHA-1 × 4 HMAC × 6 DH agree × 1 서명/서명검증 × 2	MN의 공개/개인키 쌍 생성 × 1 SHA-1 × 7 HMAC × 9 DH agree× 1 서명/서명검증 x 2	MN의 공개/개인키 쌍 생성 × 1 SHA-1 x8 HMAC x11 DH agree x1 서명/서명검증 x2
공격 취약성[1]	Redirect	X	△	△	△	△	◉
	DoS	X	△	△	△	△	◉
	Brute-Forec	◉	◉	◉	△	△	◉
	Man-in-the-middle	X	△	X	◉	◉	◉
TTP의 기능		없음	보안 프록시	HA	없음	없음	없음
MN의 인증		주소로 인증	프록시로 인증	공개키로 인증	공개키로 인증	공개키로 인증	공개키로 인증
IPSec과의 연동		없음	없음	없음	없음	있음	있음

1) ◉ : 공격에 강함, △ : 공격이 가능함, X : 공격에 약함

존의 바인딩 갱신 기법들 중에서 우수한 평가를 받고 있는 SUCV와 SUCV 최적화 프로토콜도 외부 공격 및 관리의 취약점을 갖는 것으로 분석 되었다.

본 논문에서는 SUCV 프로토콜의 취약점을 개선한 바인딩 갱신 프로토콜을 제안하였다. 제안 프로토콜은 HA가 MN의 보안 프락시로 동작하도록 설계되었으며, HA가 MN의 CoA를 보증하여 CN은 MN을 간단히 인증할 수 있다.

제안 프로토콜은 다음과 같은 여러 공격적 취약점을 개선하였다. RR기법을 활용하여 MN의 악의적인 바인딩 공격 취약점을 해결하고, 쿠키를 사용하여 HA에 대한 DoS 공격에 대응하였다. 또한, 단일 기반 CGA를 사용하는 기존 프로토콜과 달리 Aura의 이중 해쉬 기반의 CGA를 활용하여 전사 공격에 대비하였다.

제안 프로토콜은 HA의 공개키/개인키 쌍을 사용하도록 하여 MN의 공개키/개인키 쌍을 사용하는 SUCV 최적화 프로토콜에 비해 관리성 및 확장성을 개선하였다. 이와 같이 제안 프로토콜은 SUCV 최적화 프로토콜과 비교하여 강한 보안성과 우수한 관리성 및 확장성을 제공할 뿐 아니라, 암호화 연산을 최소화하였다. 그러나 제안 프로토콜은 강한 주소 인증을 통한 바인딩 갱신을 수행함으로, RR과 같은 기본 프로토콜에 비해 암호화 연산이 많아 성능이 떨어지는 단점을 가진다.

제안 프로토콜에서는 기존 프로토콜들과 같이 MN의 모든 이동에 대해 동일한 키 분배 방법을 적용하고 있다. 향후, MN의 이동 패턴을 고려한 키 분배 방법에 대한 연구가 추가로 필요하다.

참 고 문 헌

[1] 이광수, "MIPv6에서의 바인딩 갱신 인증", TTA 저널, 제 81호, pp.56~65, 2001.

[2] 엄희용, 조경산, "Mobile IPv6의 빠른 핸드오버 기법의 성능 개선", 한국시뮬레이션학회논문지, 제11권 제1호, pp.1~9, 2002.

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

[4] Aura, T, Nikander, P. Leiwo. "DoS-resistant authentication with client puzzles," Proc. of the Security Protocols Workshop 2000, (Lecture Notes in Computer Science, Vol. 2133) pp.170~181, 2000.

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

[6] 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.

[7] G. Montenegro, C. Castelluccia, "SUCV IDentifiers and Addresses," <draft-montenefro-sucv-02.txt>, 2001. Work in progress.

[8] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6(CAM)," ACM Computer Communication Review, 2001.

[9] Il-Sun You, YouSeuk Won, Kyungsan Cho, "A Security Based Protocol for Authentication the Mobile IPv6 Binding Updates," The KIPS Transactions: Part C, Vol.11, No.5, pp.605~612, 2004.

[10] M. Roe, T. Aura, G. O'Shea, and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments," <draft-roe-mobileip-updateauthe-02.txt>, 2002. Work in progress.

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

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

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

[14] T. Koskiahde, "Security in Mobile IPv6," Tampere University of Technology, 2002.

원 유 석

e-mail : server11@dankook.ac.kr

2000년 단국대학교 전산통계학과(학사)

2002년 단국대학교 대학원 전산통계학과 (이학석사)

2002년~현재 단국대학교 대학원 박사과정

관심분야 : 네트워크 및 이동 통신 보안, 시뮬레이션, 에이전트

조 경 산

e-mail : kscho@dankook.ac.kr

1979년 서울대학교 전자공학과 학사

1981년 한국과학원 전기전자공학과(공학석사)

1988년 Univ. of Texas at Austin 전기전산공학과 Ph.D.

1988년~1990년 삼성전자 컴퓨터부문 책임 연구원, 실장

1990년~현재 단국대학교 정보컴퓨터학부 교수

관심분야 : 네트워크 시스템 및 이동 통신 보안, 웹 응용, 컴퓨터 시스템