논문 2007-44TC-10-17

Kang-Park의 Mobile IPv6 바인딩 갱신 보안 프로토콜 개선

(Improving the Kang-Park's Protocol for Securing Binding Update in MIPv6)

유 일 선*

(Ilsun You)

요 약

MIPv6의 경로 최적화 모드는 이동노드와 대응노드사이의 직접적인 통신을 위해 제안되었다. 그러나 경로 최적화 모드는 뛰어난 효율성에도 불구하고 다양한 보안위협을 초래하였고, 그 결과 바인딩 갱신 과정을 보호하기 위한 보안 프로토콜들이 개발되었다. 특히, 2005년도에 강현선과 박창섭이 제안한 Kang-Park 프로토콜은 홈에이전트 중심의 독창적인 보안 프록시 구조를 바탕으로 이동노드의 연산 부담을 최소화하는 동시에 보안성을 강화하였다. 이러한 장점에도 불구하고 Kang-Park 프로토콜은 보안성과 효율성측면에서 문제점을 드러내었다. 본 논문에서는 강력한 CoA 유효성 검증과 이른 바인딩 갱신 기법을 통해 Kang-Park 프로토콜의 문제점을 개선한다. 또한, 기존 프로토콜들과의 비교를 통해서 개선 프로토콜이 우수함을 보인다.

Abstract

The routing optimization mode, which Mobile IPv6 provides for the direct communication between a mobile node and its correspond node, introduces various security threats, thus causing several protocols to be proposed for the secure binding update procedure. In particular, the Kang-Park protocol, which Kang and Park presented in 2005, achieves the optimized cryptographic operations and the strong security, while based on its unique security proxy structure. In spite of such advantages, it has some drawbacks in terms of security and efficiency. This paper improves the Kang-Park protocol through the strong CoA validation and early binding update methods. Also, we show that the improved protocol is better than others.

Keywords : Mobile IPv6, OMIPv6, Binding update protocol, Security Proxy, CGA

I. 서 론

Mobile IP Version 6 (MIPv6)는 IPv6 네트워크 환경의 구성 노드(Node)들이 움직임과 위치에 상관없이 지속적인 통신을 할 수 있도록 이동성을 제공하는 프로토콜이다[1]. 이를 위해 MIPv6는 각각의 이동노드(MN: Mobile Node)에게 두 개의 주소 HoA(Home Address: 홈네트워크에서 할당되는 주소로 이동노드의 지속적인 식별을 위한 주소)와 CoA(Care-of Address: 외부네트워크에서 할당되는 주소로 이동노드의 라우팅을 위한 주소)를 부여하고 이동노드의 홈에이전트(HA: Home Agent)로 하여금 이동노드를 위한 데이터 패킷을 중계하도록 한다. 그러나 이러한 삼각 라우팅 방식은 이동노드와 대응노드(CN: Corresponding Node) 사이의 모든 통신이 항상 홈에이전트를 통하여 이루어지기 때문에 비효율적이다. 따라서 MIPv6는 이동노드와 대응노드가 직접 통신을 할 수 있도록 경로 최적화(RO: Route Optimization) 모드를 지원한다. 이처럼 RO 모드에 의해 삼각 라우팅 문제가 해결되고 효율적인 통신이 가능해 졌으나 그에 상응하는 새로운 보안 위협이 대두되었다. 즉 RO 모드의 적용을 위해 이동노드는 위치변경마다 외부 네트워크에서 할당된 새로운 CoA를 홈에이전트와 대응노드에게 알리는 바인딩 갱신(Binding Update)을 수행해야 하는데 바인딩 갱신 과정이 안전하

* 정회원, 한국성서대학교 정보과학부
(School of Information Science, Korean Bible University)
접수일자: 2007년8월27일, 수정완료일: 2007년10월18일

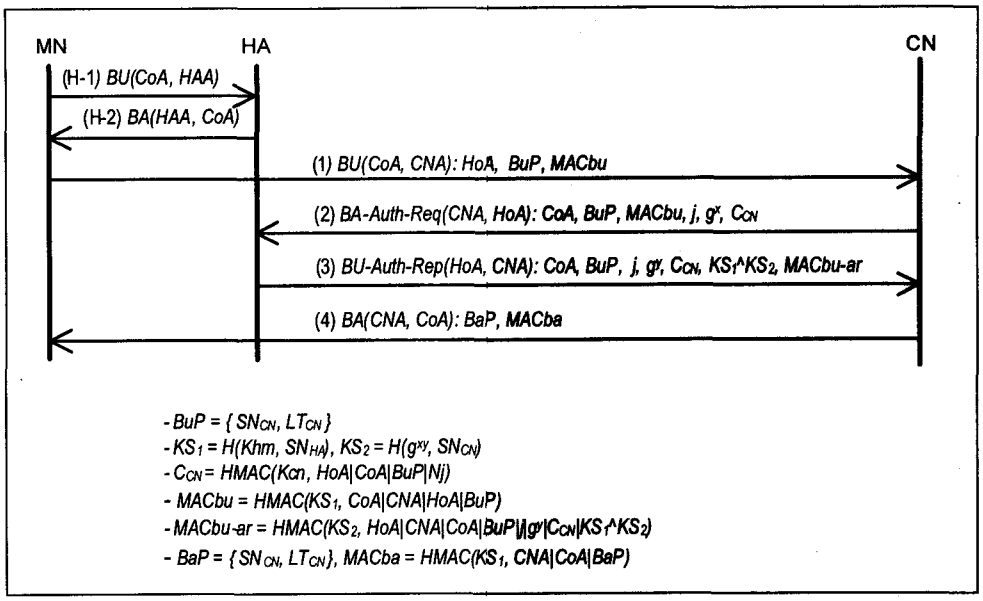

그림 1. Kang-Park의 MIPv6 바인딩 갱신 보안 프로토콜
Fig. 1. The Kang-Park's protocol for the secure binding update.

게 보호되지 않는다면 RO 모드는 구성 요소 모두를 다양한 보안 위협에 노출시키는 결과를 초래한다.

안전한 바인딩갱신을 위하여 MIPv6는 주소 테스트 기반의 경량화 된 암호화 연산을 제공하는 RR(Return Routability) 프로토콜을 표준안으로 채택하였다[1]. 그러나 RR 프로토콜이 효율성과 보안성에 있어서 한계를 드러냄에 따라 이를 개선하기 위하여 다양한 공개키 기반의 프로토콜들이 제안 되었으며[2~7], 그 결과 OMIPv6(Optimized MIPv6) 프로토콜이 RR 프로토콜의 최적화 옵션의 하나로서 표준화 되었다[7]. 이러한 공개키 기반 프로토콜 중에서 2005년도에 강현선과 박창섭이 제안한 프로토콜(이하 Kang-Park 프로토콜)은 홈에이전트 중심의 독창적인 보안 프록시 구조를 바탕으로 이동노드의 연산 부담을 최소화함과 동시에 보안성 강화를 통해 그 우수성을 입증하였다[4]. 하지만 Kang-Park 프로토콜은 여러 가지 장점에도 불구하고 보안성과 효율성 측면에서 개선의 여지를 남겼다. 본 논문에서는 강력한 CoA 검증기법과 이른 바인딩 갱신을 통해 Kang-Park 프로토콜을 개선하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 Kang-Park 프로토콜의 문제점을 분석하고, Ⅲ장에서는 이를 바탕으로 개선 프로토콜을 제안한다. Ⅳ장에서 개선 프로토콜을 다른 프로토콜들과 함께 보안성과 효율성 측면에서 비교분석한 후, Ⅴ장에서는 향후 연구 제시와 함께 결론을 맺는다.

Ⅱ. Kang-Park의 바인딩 갱신 프로토콜

1. 기호

- *Msg(SA, DA)*: 프로토콜 메시지를 나타내며 *Msg*는 메시지의 이름이고 *SA*는 메시지의 송신자 주소, *DA*는 수신자 주소를 나타냄
- *H(msg)*: *msg*의 해쉬값을 계산하는 일방향 해쉬함수를 의미함
- *HMAC(k, msg)*: 대칭키 *k*를 통해 *msg*의 *HMAC* 값을 계산하는 *HMAC* 함수를 의미함
- | : 메시지 결합 연산자, ^ : 배타적 논리합 연산자
- *MN*: 이동노드, *HA*: 홈에이전트, *CN*: 대응노드
- *CNA*: 대응노드의 주소, *HAA*: 홈에이전트의 주소
- SN_X: *X*에게로 보내는 메시지의 일련번호, LT_X: *X*의 바인딩 정보의 생명주기
- (H-1)과 (H-2)는 홈 등록 과정을 나타냄
- *Khm*: 홈에이전트와 이동노드 사이의 공유 대칭키
- g^x, *x* : 각각 대응노드의 Diffie-Hellman 공개키와 개인키를 의미함
- g^y, *y* : 각각 이동노드의 Diffie-Hellman 공개키와 개인키를 의미함
- *Kcn* : 대응노드의 비밀키, K_{HA} : 홈에이전트의 비밀키
- *Nj*: 대응노드의 *j* 번째 nonce값을 의미함

2. 프로토콜 특성

그림 1과 같이 Kang-Park 프로토콜은 대응노드가 홈에이전트를 전적으로 의존하여 이동노드의 HoA와 CoA 주소의 유효성 검증을 한다. 즉 홈에이전트는 이동노드의 홈 등록에 의해 갱신된 바인딩 정보를 참조하여 대응노드가 의뢰한 유효성 검증(*BU-Auth-Req* 메시지에 포함된 HoA와 CoA의 바인딩 존재여부 확인)을 실행하고 *BU-Auth-Rep* 메시지를 통해 그 결과를 대응노드에게 알려준다. 홈에이전트는 *BU-Auth-Rep* 메시지의 보호와 공유키 KS_1의 분배를 위해 대응노드와 함께 Diffie-Hellman(이하 D-H)의 키교환 기법을 적용하여 생성한 KS_2를 이용한다. D-H 키교환은 이동노드와 대응노드의 D-H 공개키쌍에 의해 이루어지며 공개키에 대한 중간자 공격(Man-in-the-middle attack)에 대응하기 위하여 이동노드의 HoA와 대응노드의 주소를 D-H 공개키로부터 파생된 CGA(Cryptographically Generated Address)로 지정한다[2, 5]. 또한, 이동노드의 계산부담을 최소화하기 위해 홈에이전트가 이동노드의 D-H 공개키쌍을 직접 보관하고 이동노드를 대신하여 키교환에 참여한다.

3. 프로토콜 문제점

가. 악의적인 이동노드에 의한 반사공격에 취약함

Kang-Park 프로토콜은 홈 등록 과정에서 이동노드가 항상 유효한 CoA를 등록한다고 가정하면서 CoA검증을 오직 홈에이전트의 바인딩 캐쉬에 있는 이동노드의 바인딩정보에 의존한다. 그러나 이러한 방법은 그림 2와 같은 악의적인 이동노드에 의한 반사공격(Redirection Attack)에 취약하다[2~3]. 즉 악의적인 이동노드가 실제로 자신이 위치하지 않은 의도된 CoA로 거짓 홈 등록을 한다면 이동노드는 대응노드나 홈에이전트에 의해 발견되지 않고 성공적으로 Kang-Park 프로토콜을 수행할 수 있다.

비록 [4]에서 주장하는 것처럼 공격발생 이후에 홈에이전트의 바인딩 캐쉬에 있는 홈 등록 정보를 통해 악의적인 노드를 추적을 할 수 있다고 하지만 이러한 방법은 두 가지 문제가 있다. 첫째로 공격과정에서 어떠한 대응도 할 수 없다는 것과 둘째로 공격이후에 악의적인 노드가 자신의 유효한 CoA를 이용하여 홈 등록 및 대응노드 등록을 한다면 홈에이전트와 이동노드의 바인딩 캐쉬는 새롭게 갱신되어 공격에 대한 증거가 남지 않는다.

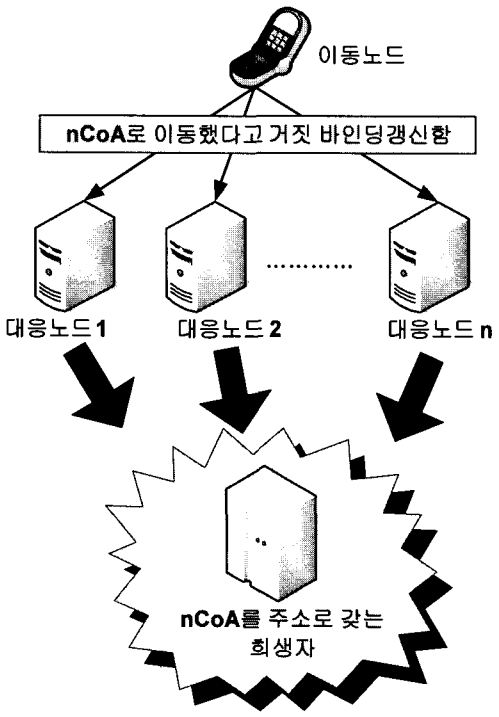

그림 2. 악의적인 이동노드에 의한 반사공격
Fig. 2. The redirection attack by the malicious mobile node.

나. 비효율성

공개키 기반의 바인딩 갱신 프로토콜들은 일반적으로 공개키 암호화 기법을 사용하여 이동노드를 인증하고 강력한 장기키(long-term key)를 생성하는 초기 단계와 장기키를 바탕으로 이후의 바인딩 갱신 과정을 최적화 하는 후속 단계로 구성된다[2~3, 6~7]. 그러나 Kang-Park 프로토콜은 최적화된 후속 단계 없이 이동노드의 바인딩갱신 마다 공개키 연산이 포함된 (1)-(4) 단계를 매번 반복해야 하는 비효율적인 구조를 갖는다. 이러한 비효율성은 공개키 연산 부담이외에도 (H-1)과 (H-2)에 해당하는 홈 등록(Home Registration)과 (1)-(4)에 해당하는 대응노드 등록(Correspondent Registration)이후에 데이터 패킷 전송이 시작되기 때문에 3 round-trip time (이하 RTT)의 과도한 네트워크 지연을 유발한다.

III. Kang-Park 프로토콜 개선

본 장에서는 앞서 언급된 문제점을 해결하기 위해 다음과 같이 Kang-Park 프로토콜을 개선한다. 첫째로 악의적인 이동노드에 의한 반사공격을 방어하기 위하여 이동노드가 임의로 CoA를 생성하지 못하게 함과 동시

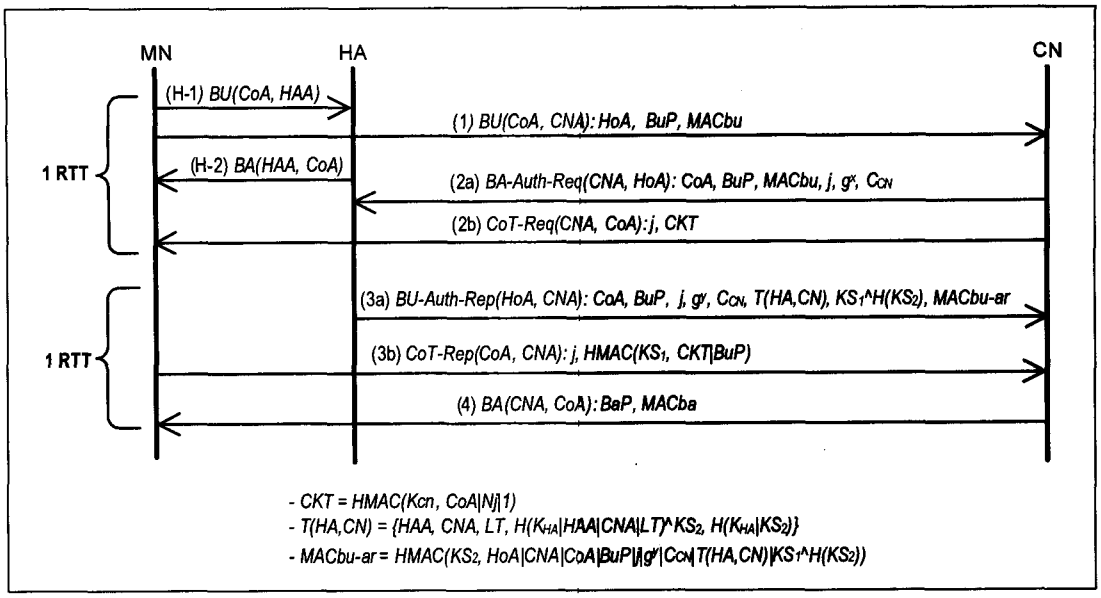

그림 3. 개선 프로토콜의 초기 단계
Fig. 3. The initial phase of the improved protocol.

에 CoA 주소 테스트를 수행하는 강력한 CoA 유효성 검증 기법을 추가하고, 둘째로 프로토콜을 초기 단계와 후속 단계로 나누어서 효율성을 극대화 한다.

1. CoA 유효성 검증 기법

본 논문에서 제안하는 CoA 유효성 검증 기법은 아래에서 언급될 CoA 생성 및 검증과 실제 CoA에 패킷을 전송하여 패킷 수신 여부를 확인하는 CoA 주소 테스트로 구성된다.

가. CoA 생성 및 검증

(1) CoA 생성

*CoA(n)*은 이동노드의 *n*번째 CoA이고 *FPrefix(n)*는 *n*번째 방문한 외부 네크워크의 prefix, *seq(n)*는 홈 등록을 위한 바인딩 갱신 메시지의 *n*번째 순서번호, *IID(n)*은 *n*번째 이동노드의 Interface Identifier, *First(64,IID(n))*는 *IID(n)*의 상위 64비트, *CoA(0)*=HoA라 할 때 이동노드의 CoA는 다음과 같이 생성된다.

$$IID(n)=HMAC(Khm, CoA(n-1)|FPrefix(n)|seq(n)) \quad (1)$$

$$CoA(n)=FPrefix(n)+First(64,IID(n)) \quad (2)$$

(2) CoA 검증

이동노드가 새로운 외부 네트워크로 이동했을 때 이동노드는 식 (1)과 (2)를 적용하여 새로운 CoA를 생성한 후, 홈 등록을 해야 한다. 홈 등록 요청이 발생하면 홈에이전트는 *Khm*을 통해 이동노드의 새로운 CoA를 검증하고 CoA가 유효할 경우 바인딩 정보를 갱신한다. 이처럼 이동노드가 식 (1)과 (2)에 의해 CoA를 선택해야 하기 때문에 특정 노드를 희생자로 선택하고 반사공격을 시도하기가 매우 어렵다.

나. CoA 주소 테스트

가에서 제안된 주소 제한 기법만으로는 특정 네트워크의 prefix를 갖는 거짓 CoA를 생성하여 반사공격을 시도하는 네트워크 단위의 공격을 방어할 수 없다. 이에 대응하기 위하여 이동노드는 대응노드 등록과정에서 이동노드가 주장하는 CoA에 패킷을 전송하고 수신여부를 확인하는 CoA 주소 테스트를 수행하도록 한다.

2. 개선 프로토콜의 초기 단계 및 후속 단계

개선 프로토콜은 기존 Kang-Park 프로토콜에 해당하는 초기 단계와 비밀키 KS_1을 바탕으로 효율적인 바인딩 갱신을 수행하는 후속 단계로 구성된다.

가. 초기 단계

그림 3과 같이 개선 프로토콜의 초기 단계는 악의적인 이동노드에 의한 반사공격을 방어하기 위해서 기존 Kang-Park 프로토콜에 *CoT-Req*와 *CoT-Rep* 메시지를 추가 하였고, 후속 단계에서 홈에이전트와 대응노드 사이의 메시지 공유 비밀키 KS_2를 사용할 수 있도록

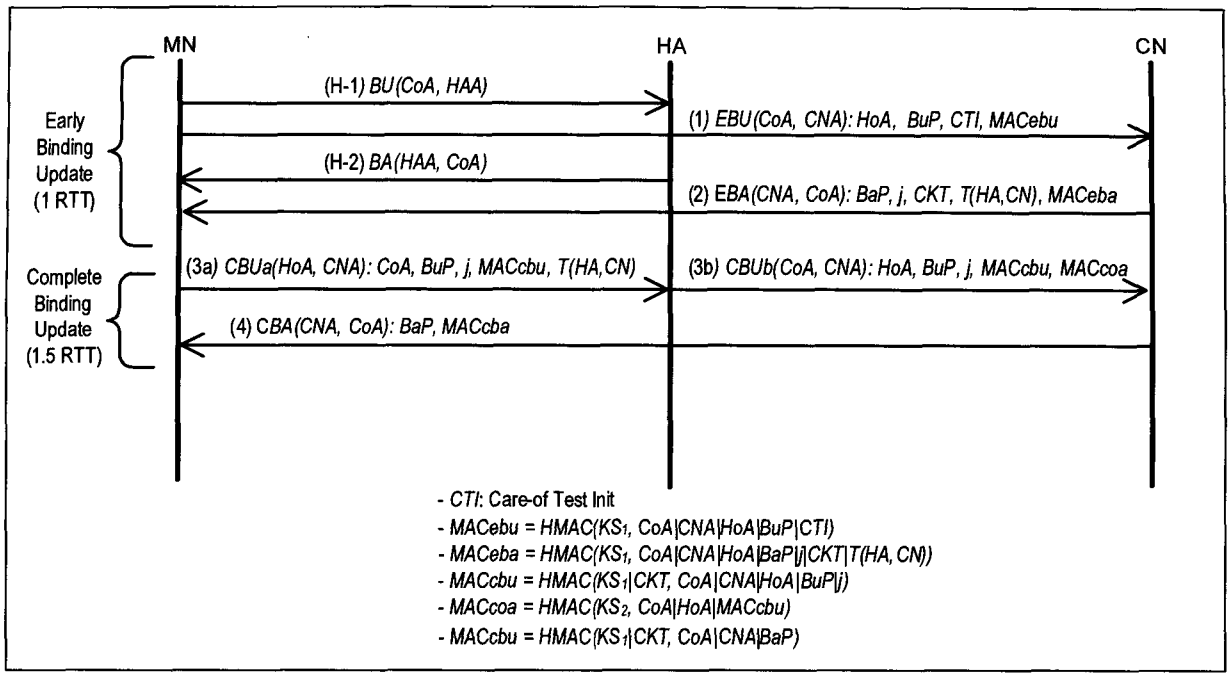

그림 4. 개선 프로토콜의 후속 단계

Fig. 4. The subsequent movement phase of the improved protocol.

BU-Auth-Rep 메시지를 수정하였다.

단계 (1)-(2): 이동노드가 새로운 외부 네트워크를 방문하여 CoA의 변경이 발생하게 되면 홈 등록과 대응노드 등록을 해야 한다. 이를 위해 이동노드는 식 (1)과 (2)에 따라 적절한 CoA를 생성한 후, 바인딩 정보의 갱신을 위해 홈 등록 *BU* 메시지를 홈에이전트에게 대응노드 등록 *BU* 메시지를 대응노드에게 동시에 전송한다. *BU* 메시지를 수신하면 홈에이전트는 식 (1)과 (2)에 따라 이동노드의 새로운 CoA를 검증하고 바인딩 정보를 갱신한다. 이동노드의 경우, 비밀키 KS_1을 사용하여 *BU* 메시지의 *MACbu* 값을 검사하고 *BU-Auth-Req* 메시지와 함께 CoA 테스트를 위해 *CoT-Req* 메시지를 전송한다.

단계 (3)-(4): 이동노드가 *CoT-Req* 메시지를 수신하면 이에 대한 응답으로 *CoT-Rep* 메시지를 대응노드에게 전송한다. 대응노드는 (3)단계에서 *BU-Auth-Rep* 메시지와 *CoT-Rep* 메시지를 통해 이동노드의 HoA와 CoA에 대한 강력한 신뢰를 갖게 되며 이와 더불어 홈에이전트와 비밀키 KS_2를, 이동노드와 비밀키 KS_1을 공유하게 된다. 특히, 대응노드는 *BU-Auth-Rep* 메시지에 의해 이동노드의 CoA가 식 (1)과 (2)에 따라 적절히 생성되었다는 것을 알 수 있고, *CoT-Rep* 메시지에 의해 이동노드가 CoA에서 *CoT-Req* 메시지를 수신했다는 것을 신뢰할 수 있다. 이는 대응노드가 악의적인 이동노드에 의한 반사공격을 강력하게 방어할 수 있도록 한다. 또한, 홈에이전트는 KS_2에 의한 자원고갈을 회피하기 위해 KS_2를 저장하는 대신 대응노드에게 티켓 *T(HA,CN)*을 발급한다.

나. 후속 단계

그림 4와 같이 제안 프로토콜의 후속 단계는 바인딩 갱신 지연시간을 최소화하기 위해 이른 바인딩 갱신 (Early Binding Update) 기법[7]을 기반으로 구성되고, 강력한 CoA의 유효성 검증을 위해 식 (1)과 (2)에 의한 올바른 CoA가 생성되었는지를 홈에이전트가 검사할 수 있도록 하였다.

단계 (1)-(2): 이동노드가 새로운 외부 네트워크를 방문할 경우, 식 (1)과 (2)에 따라 올바른 CoA를 생성하고 홈 등록과 대응노드 등록을 시도한다. 이동노드는 이른 바인딩 갱신[2~7]의 적용으로 *EBU* 메시지를 보내자마자 즉각 데이터 패킷을 전송할 수 있다. *EBU* 메시지를 수신하면 대응노드는 비밀키 KS_1으로 메시지를 검증한 후, *EBA* 메시지로 응답한다. 이때 *EBU* 메시지가 유효하다면 대응노드는 이동노드에게 즉각 데이터 패킷을 전송할 수 있다. 단, 대응노드는 이동노드에게 무조건 데이터 패킷을 전송하는 것이 아니라 이동노드로부터 *CBU* 메시지가 도착할 때까지 신용기반의 접근통제(Credit-Based Authorization)[7]에 따라 계산된 패

킷량 이내로 전송하며 만일 그 이상을 벗어나면 RO 모드를 적용하지 않는다. *EBA* 메시지는 이동노드에 의해 홈에이전트에게 전송될 티켓 *T(HA,CN)*을 포함하는데 이는 (3) 단계에서 홈에이전트가 *MACcoa*를 검증할 수 있도록 비밀키 KS_2를 제공한다.

단계 (3)-(4): *EBA* 메시지 수신후, 이동노드는 *CBUa* 메시지를 자신의 HoA를 통해서 대응노드에게 전송을 한다. 이때 홈에이전트는 *CBUa* 메시지를 대응노드에게 그대로 전달하지 않고, *CBUa* 메시지에 포함된 티켓 *T(HA,CN)*에서 비밀키 KS_2를 추출하고 현재 등록된 이동노드의 바인딩 갱신정보를 증명하는 *MACcoa*를 계산하여 *CBUb* 메시지를 생성하고 전송한다. 만일 *CBUb* 메시지가 유효하다면 대응노드는 이때부터 신용기반의 접근통제를 적용하지 않고 제한 없이 데이터 패킷을 전송할 수 있다. 또한, 대응노드는 이동노드가 CoA에서 *EBA* 메시지를 수신하였고 CoA는 식 (1)과 (2)에 의해 생성된 올바른 주소라는 것을 확신하게 된다.

Ⅳ. 개선 프로토콜 분석

1. 보안성 분석

제안 프로토콜은 Kang-Park 프로토콜을 개선하였기 때문에 Kang-Park 프로토콜의 보안성을 그대로 계승하며 프로토콜 개선에 의한 새로운 취약점을 노출하지 않는다. 특히, 제안 프로토콜은 Kang-Park 프로토콜의 치명적 약점이었던 악의적인 이동노드에 의한 반사공격을 방어하기 위하여 CoA에서의 패킷수신 여부를 검사하는 CoA 주소 테스트를 수행하고 이와 함께 CoA 주소 생성을 생성규칙에 따라 엄격히 제한하였다. 또한, 대응노드와 홈에이전트 사이의 공유 비밀키 KS_2는 기존 Kang-Park 프로토콜과 달리 후속 단계에서 사용되어야 하기 때문에 각 노드에 보관되어야 한다. 만일 홈에이전트가 이동노드의 대응노드별로 KS_2를 보관한다면 이를 악용하여 자원이 고갈되도록 하는 공격이 가능해 진다. 본 논문에서는 이 문제를 해결하기 위해 암호화된 KS_2를 포함하는 티켓을 이용하였다. 즉 홈에이전트는 KS_2를 보관하는 대신 대응노드에게 KS_2가 포함된 티켓을 발행한다.

2. 효율성 분석

본 절에서는 개선 프로토콜의 효율성 분석을 핸드오버 지연시간과 연산 오버헤드의 측면에서 분석한다.

*L[X-Y]*는 *(X)*과 *(Y)* 사이에서 발생하는 지연시간을 나타내고, RTT_{path}는 *path* 에서 패킷이 전송되는데 걸리는 *RTT*, *LSend(X)*는 *X* 단계에서 패킷을 전송하기 위해 발생하는 지연시간, *LRecv(X)*는 *X* 단계에서 패킷을 수신하기 위해 발생하는 지연시간이라 할 때, 초기 단계의 핸드오버 지연시간 *LSend(초기)*와 *LRecv(초기)*는 식 (3)-(7)과 같이 구할 수 있다.

$$L[1\text{-}2] = 0.5\times(RTT_{MN\text{-}CN}+Max(RTT_{HA\text{-}CN},RTT_{MN\text{-}CN})) \quad (3)$$

$$L[H1\text{-}H2] = RTT_{BU} = RTT_{HA\text{-}MN} \quad (4)$$

$$LSend(초기) = Max(L[1\text{-}2],L[H1\text{-}H2]) \quad (5)$$

$$L[3\text{-}4] = 0.5\times(Max(RTT_{HA\text{-}CN},RTT_{MN\text{-}CN})+RTT_{MN\text{-}CN}) \quad (6)$$

$$LRecv(초기) = LSend(초기)+L[3\text{-}4] = 1RTT+1RTT \quad (7)$$

후속 단계의 경우, 이른 바인딩 갱신 기법이 적용되기 때문에 이동노드가 *EBU* 메시지를 전송하자마자 데이터 패킷을 보낼 수 있어 *LSend(후속)*의 값은 0 *RTT* 이고 대응노드가 *EBA* 메시지를 전송하자마자 데이터 패킷을 보낼 수 있기 때문에 *LRecv(후속)*은 *RTT [1-2]=1RTT* 이다.

개선 프토토콜의 전체 연산 오버헤드는 표 1과 같으며 강력한 보안성을 위해 많은 암호화 연산량이 요구되는 초기 단계에 비해 후속 단계에서는 적은 연산량이 요구됨을 알 수 있다. 이동노드의 연산량을 보면 오히려 후속 단계에서 연산량이 증가하였는데 이는 이른 바인딩 갱신에 기인한 것으로 핸드오버 지연시간의 개선을 고려해 볼 때 충분히 회생할 수 있는 오버헤드라 할 수 있다.

3. 비교분석

본 절에서는 표 1과 같이 Kang-Park 프로토콜과 MIPv6를 위한 표준안인 RR 프로토콜 및 OMIPv6 프로토콜을 개선 프로토콜과 함께 비교분석하였다. 핸드오버 지연시간을 보면 개선 프로토콜은 Kang-Park 프로토콜에 비해 *1RTT* 이상 향상되었고, 특히 후속 단계에서는 OMIPv6와 동일한 수준을 갖는다. 암호화 연산 측면에서는 Kang-Park 프로토콜이 개선 프로토콜의 초기 단계에 비해 우수하다고 볼 수 있으나 이는 개선 프로토콜의 핸드오버 지연시간 개선 및 보안성 강화에 기인한 것이며 후속 단계의 경우에는 개선 프로토콜의 암호화 연산이 최소화되어 Kang-Park 프로토콜이나

표 1. 개선 프로토콜의 비교분석
Table 1. Analysis of the improved protocol.

1) ○: 강력대응, △: 허용가능, ×: 취약 2) H: 해쉬연산, M: HMAC 연산, P: 공개키 연산

프로토콜	RR	Kang-Park	OMIPv6		개선안	
지연시간 (*LSend/LRecv*)	3/4 (*RTT*)	3/3	초기	후속	초기	후속
			0/1	0/1	1/2	0/1
이동노드의 암호화 연산 (홈 등록 제외)	H: 1, M: 2	H: 1, M: 2	초기	후속	초기	후속
			H: 1, M: 4, P: 2	H: 1, M: 4	H: 1, M: 3	H: 1, M: 4
전체 암호화 연산 (홈 등록 제외)	H: 2, M: 8	H: 7, M: 6, P: 2	초기	후속	초기	후속
			H: 6, M: 12, P: 4	H:2, M: 12	H:14, M: 8, P: 2	H: 4, M: 10
저전력 혹은 제한된 계산 능력의 이동노드 지원	○	○	×		○	
SA의 수명	7분	24시간	24시간		24시간	
HoA 검증	주소테스트	CGA	CGA		CGA	
CoA 검증	주소테스트	×	주소테스트		주소테스트 + 주소생성제한	
세션 강탈 공격[2][8]	×	○	○		○	
악의적인 노드에 의한 반사 공격	△	×	△		○	
서비스 거부 공격[2][8]	○	○	○		○	

RR 프로토콜에 비해 효율적임을 알 수 있다. OMIPv6와 비교해 보면 전체 연산량에서는 거의 비슷한 수준의 연산량이 요구되지만 초기 단계에서 이동노드에게 공개키 암호화 연산을 요구하지 않기 때문에 OMIPv6와 달리 저전력 혹은 제한된 계산 능력을 갖는 이동노드를 지원할 수 있다. 보안성을 고려해 보면 개선 프로토콜은 타 프로토콜에 비해 세션강탈공격, 악의적인 이동노드에 의한 반사공격, 서비스거부공격(혹은 자원고갈공격)에 가장 강력히 대응할 수 있음을 알 수 있다.

전체적으로 개선 프로토콜은 가장 강력한 보안성과 함께 OMIPv6와 비슷한 수준의 효율성을 제공할 수 있다. 비록 개선 프로토콜은 초기 단계의 핸드오버 지연에서 OMIPv6보다 *1RTT*의 핸드오버 지연을 유발하지만 암호화 연산량에서는 개선 프로토콜이 효율적이고 무엇보다 이동노드에게 공개키 암호화 연산을 요구하지 않기 때문에 프로토콜 보급에 있어서 제한이 적다는 장점이 있다.

V. 결 론

본 논문에서는 2005년에 강현선과 박창섭이 제안한 바인딩 갱신 보안 프로토콜을 개선하였다. 개선 프로토콜은 강력한 CoA 유효성 검증기법을 통해 악의적인 이동노드에 의한 반사공격을 방어할 수 있게 되었고, 프로토콜 구조를 초기 단계와 후속 단계로 나누어 효율성을 극대화 하였다. 특히, 최근에 MIPv6의 표준안으로 채택된 OMIPv6를 포함한 기존 프로토콜들과의 비교를 통해서 개선 프로토콜이 효율적인 암호화 연산 및 핸드오버 지연시간과 함께 우수한 보안성을 지원함을 알 수 있었다. 또한, 이동노드상에서의 경량화된 연산은 OMIPv6에 비해 우수한 적용성을 제공한다.

향후연구로는 이동노드의 이동빈도와 망의 환경에 따른 성능 분석 및 동시에 움직이는 이동노드 사이의 효율적인 바인딩 갱신 지원, 위치 보안성 강화를 통한 이동노드의 프라이버시 보호가 요구된다.

참 고 문 헌

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," *IETF RFC 3775*, June 2004.
[2] C. Vogt and J. Arkko, "A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization," *IETF RFC 4651*, Feb. 2007.
[3] Kui Ren, Wenjing Lou, Kai Zeng, Feng Bao, Jianying Zhou, and Robert H. Deng, "Routing optimization security in mobile IPv6," *Computer Networks*, vol. 50, issue 13, pp. 2401-2419, Elsevier, Sep. 2006.
[4] 강현선, 박창섭, "Redirect 공격과 DoS 공격에 안전한 MIPv6 바인딩 갱신 프로토콜," *한국정보보호*

학회논문지, 제15권, 제5호, 115-124쪽, 2005.
[5] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," *ACM Computer Communications Review*, vol. 31, no. 2, April 2001.
[6] G. Montenegro, C. Castelluccia, "Crypto- Based Identifiers(CBIDs): Concepts and Applications," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 97-127, Feb. 2004.
[7] J. Arkko, C. Vogt and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," *IETF RFC 4866*, May 2007.
[8] Tuomas Aura. "Mobile IPv6 Security," In Proc. Security Protocols, 10th International Workshop, *LNCS*, volume 2845, pp. 215-228, Cambridge, UK, April 2002. Springer 2003.

저 자 소 개

유 일 선(정회원)
1995년 단국대학교 전산통계학과 학사 졸업
1997년 단국대학교 전산통계학과 석사 졸업
2002년 단국대학교 전산통계학과 박사 졸업
2005년~현재 한국성서대학교 정보과학부 전임강사
<주관심분야 : MIPv6, 인터넷 보안, 접근통제>