MIPv6 최적화 프로토콜 시리즈의 후속 단계 개선 연구

유일선* · 김흥준**

A Study on Improving the Subsequent Phase of OMIPv6 Protocol Series

Ilsun You* · Heung-Jun Kim**

요 약

최근에 RR(Return Routability) 프로토콜을 개선하기 위해 공개키 기반의 OMIPv6 시리즈가 제안되었다. OMIPv6 시리즈는 강력한 장기키(long-term key)를 생성하는 초기 단계와 장기키를 바탕으로 이후의 바인딩 갱신 과정을 최적화 하는 후속 단계로 구성된다. 본 논문에서는 OMIPv6 시리즈의 후속 단계를 성능과 보안성, 적용성 측면에서 비교 분석한 후, 비교 분석 결과에 근거하여 개선안을 제시한다. 또한, 제안한 개선안이 성능과 보안성, 적용성을 전체적으로 고려할 때 다른 프로토콜에 비해 우수함을 보인다.

ABSTRACT

Recently, OMIPv6 series, based on public-key cryptography, have been proposed to improve RR protocol. This series are typically composed of the initial and subsequent phases. In the initial phase, the mobile node and its corresponding node build a strong long-term key, by which successive binding updates are optimized in the subsequent phase. In this paper, we compare and analyze the subsequent phases of OMIPv6 series in terms of performance, security and applicability, then presenting an improvement on the subsequent phase. Also, we show that the proposed improvement is reasonable considering performance, security and applicability overall.

키워드
MIPv6, Binding Update, RR protocol, CGA, CBID

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(Mobile Node)에게 2개의 주소 즉 HoA(Home Address)와 CoA(Care of Address)를 부여한다. HoA는 이동노드가 소속된 홈네트워크에서 부여하는 주소로서 이동노드의 지속적인 연결을 위한 네트워크 연결 식별자로 사용되며 CoA는 이동노드가 새로운 외부네트워크로 이동할 때마다 부여받는 주소로서 라우팅을 위해 사용된다. HoA와 CoA의 관계를 '바인딩'(Binding)이라 하며 새로운 네트워크로 이동할 때마다 이동노드는 자신의 홈에이전트(Home Agent: 이동노드의 홈네트워크에 배치된 라우터)와 대응노드(Corresponding Node)에게 바인딩 정보를 알려 주어야 한다. (이를 바인딩 갱신이라 한다) 바인딩 갱신은 이동노드가 자신의 대응노드 혹은 홈에이

* 한국성서대학교 정보과학부 전임강사
** 교신저자, 진주산업대학교 컴퓨터공학과 부교수

접수일자 : 2007. 9. 12

전트와 바인딩 갱신(Binding Update) 메시지와 바인딩 응답(Binding Acknowledgment) 메시지를 교환함으로써 이루어진다.

MIPv6는 이동노드와 대응노드(Corresponding Node) 사이의 직접적인 데이터 전송을 위해 경로 최적화(RO: Route Optimization) 모드를 지원한다. RO 모드는 이동노드의 CoA를 통해 직접 통신이 이루어지기 때문에 이동노드를 식별하는 HoA와 CoA와의 관계 즉 바인딩 정보가 안전하게 대응노드에게 인증되어야 하며 이를 위한 표준 보안 프로토콜로서 RR(Return Routability) 프로토콜이 제안되었다[1]. RR 프로토콜은 네 개의 이동 시그날 메시지(mobility signal message) HoTI(Home Test Init)와 CoTI(Care-of Test Init), HoT(Home Test), CoT(Care-of Test)를 통하여 이동노드의 HoA와 CoA의 유효성을 검증하고 바인딩 갱신 및 응답 메시지의 인증을 위한 바인딩 갱신키를 분배한다. RR 프로토콜은 공개키 암호화 연산을 사용하지 않고 광역의 보안인프라를 요구하지 않기 때문에 IPv6 네트워크 환경의 이동장치들에 적합하다. 그러나 암호화 기법이 아닌 CoT와 HoT 메시지 수신 여부를 통해 키교환이 발생하기 때문에 다양한 보안 공격에 취약하며 이러한 보안문제로 인해 바인딩 갱신키를 최대 420초마다 재설정해야 하는 한계를 갖는다. 특히, 주기적인 바인딩 갱신키의 설정은 핸드오버(hand over) 지연 및 과도한 이동 시그날 메시지의 증가문제를 유발한다. 이러한 RR 프로토콜의 문제점을 개선하기 위해 MIPv6 최적화 프로토콜(OMIPv6: Optimizing MIPv6) 시리즈가 제안되었다[2-7]. OMIPv6 시리즈는 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. OMIPv6 시리즈에서는 초기 단계 이후에 주로 후속 단계가 실행되기 때문에 후속 단계의 보안과 성능은 매우 중요하다. 본 논문에서는 OMIPv6 시리즈의 후속 단계를 보안과 성능 측면에서 비교 분석한다. 또한, 비교 분석 결과에 근거하여 개선안을 제시 한다.

본 논문의 구성은 다음과 같다. 2장에서 OMIPv6 시리즈의 일반 구조와 프로토콜별 특성을 기술하고 3장에서는 각 프로토콜의 후속 단계를 분석한다. 4장에서는 3장의 분석을 바탕으로 성능과 보안측면에서 프로토콜들을 비교한 후, 후속 단계를 위한 개선안을 제안한다. 5장에서는 향후 연구 제시와 함께 결론을 맺는다.

II. MIPv6 최적화 프로토콜 시리즈

OMIPv6 시리즈는 그림 1과 같이 이동노드와 대응노드가 강력한 장기키를 교환하는 초기 단계와 장기키를 바탕으로 이후의 바인딩 갱신 과정을 최적화 하는 후속 단계로 구성된다[2-7]. OMIPv6 시리즈는 공개키 암호화 기법을 통해 이동노드와 대응노드가 초기 단계에서 장기키를 생성 및 교환하도록 하며 이동노드의 공개키 검증을 위한 방법으로 PBK(Purpose-Built Keys)[8], CGA(Cryptographically Generated Addresses)[9], CBID (Crypto-based Identifier)[6] 등을 적용한다. 특히, CGA와 CBID의 경우 이동노드의 HoA를 사용하여 공개키를 체크할 수 있기 때문에 대응노드는 이동노드의 전자서명을 검증함으로써 바인딩 갱신 메시지의 무결성과 함께 이동노드가 HoA를 소유한다는 사실을 강력하게 신뢰할 수 있다. OMIPv6 시리즈는 이러한 신뢰를 바탕으로 초기 단계 이후 바인딩 갱신 과정에서 HoA 검증을 생략하여 효율을 극대화 한다.

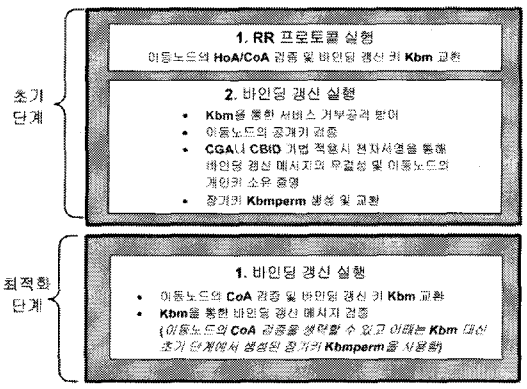

그림 1. OMIPv6 프로토콜 시리즈의 구조
Fig. 1. Structure of the OMIPv6 Protocol Series

OMIPv6 시리즈의 첫 번째 프로토콜인 OMIPv6-DH는 공격위협의 범위를 최소화함으로써 전체적인 보안을 강화하는 PBK 프레임워크의 실용적인 철학에 근거하여 설계되었다[3, 8]. OMIPv6-DH는 이동노드와 대응노드 사이에 장기키를 설정하기 위해 초기 단계에서 RR 프로토콜과 함께 Diffie-Hellman의 키 교환 프로토콜을 실행한다. RR 프로토콜을 실행하는 이유는 키 교환 과정에서 발생할 수 있는 중간자 공격 및 서비스 거부 공격에 대비하기 위함이며, 초기 단계 이후에는 교환된 키를

통해 바인딩 갱신 및 응답 메시지가 인증되기 때문에 RR 프로토콜은 더 이상 반복되지 않는다. 이처럼 OMIPv6-DH는 초기에 RR 프로토콜에서 단 한 번의 공격기회를 허용함으로써 전체적인 보안을 향상시켰을 뿐만 아니라 핸드오버 지연 시간과 이동 시그널 메시지의 양을 최적화 하였다. 그러나 OMIPv6-DH는 초기 단계에서 RR 프로토콜 붕괴시 중간자 공격 등에 취약하고 후속 단계에서 CoA 검증 없이 바인딩 갱신 및 응답 메시지가 전달되기 때문에 악의적인 이동노드에 의한 반사공격(redirection-attack)에 취약하다 [10].

이러한 문제점을 개선하기 위해 그림 2와 같이 OMIPv6-CGA, OMIPv6-CGA-Proxy, OMIPv6-CGA-CBA, OMIPv6-CBID 등의 프로토콜이 제안되었다 [2-7].

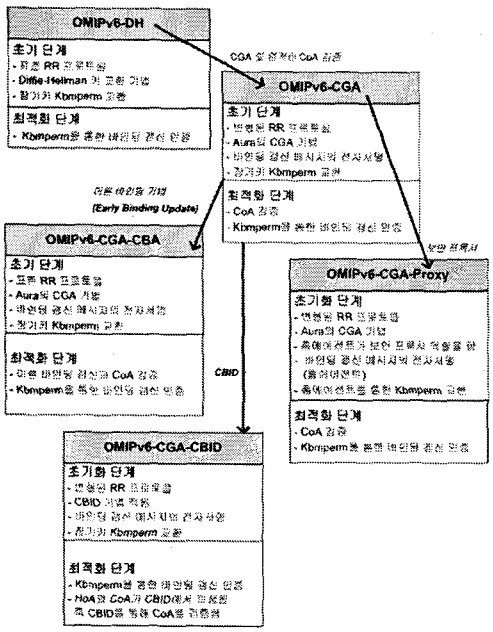

그림 2. OMIPv6 프로토콜 시리즈 요약
Fig. 2. Summary of OMIPv6 Protocol Series

III. OMIPv6 시리즈의 프로토콜별 후속 단계 개선 전략

OMIPv6 시리즈에서는 초기 단계 이후에 주로 후속 단계가 실행되기 때문에 후속 단계의 효율성을 극대화 하는 것이 매우 중요하다. 이를 위해 OMIPv6 시리즈는 초기 단계에서 생성된 강력한 장기키를 바탕으로 이후에 발생하는 후속 단계를 개선하기 위해 노력을 집중하였다. 본 장에서는 이러한 노력을 각각의 프로토콜별로 분석한다.

본 장에서 사용되는 표기법은 다음과 같다.

- *MN* : 이동노드
- *CN* : 대응노드 (주소의 의미로도 사용됨)
- *BU* : 바인딩 갱신 메시지
- *BA* : 바인딩 응답 메시지
- *CNI*: Care-of nonce index
- *HNI*: Home nonce index
- PrK_X : X의 개인키
- PuK_X : X의 공개키
- $P_X(m)$: 메시지 m이 공개키 X에 의해 암호화 됨
- $P_X^{-1}(m)$: 메시지 m이 개인키 X에 의해 암호화 됨- K_X : X의 비밀키
- | : 결합연산자
- *SHA1(m)*: 메시지 m의 *SHA1* 해쉬값
- *HMAC_SHA1(k, m)*: k 키를 사용하여 계산된 메시지 m의 *HMAC* 값 (*SHA1* 사용됨)
- *First(n,m)*: 메시지 m의 첫 번째 n비트

OMIPv6 시리즈의 첫 번째 프로토콜인 OMIPv6-DH는 후속 단계에서 HoA 검증과 함께 CoA 검증을 생략하고 오직 바인딩 갱신만 실행되도록 하였다. 비록 이와 같은 방법이 최고의 성능을 보장하지만 그림 3에서 설명된 악의적인 이동노드에 의한 반사공격에 취약하다.

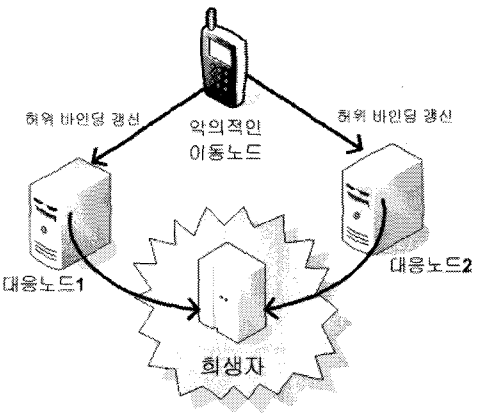

그림 3. 악의적인 이동노드에 의한 반사공격
Fig. 3. Redirect Attack by a Malicious MN

악의적인 이동노드에 의한 반사공격을 방어하기 위해 OMIPv6-CGA는 OMIPv6-DH와는 대조적으로 바인딩 갱신이전에 메시지 수신여부를 테스트하는 엄격한 CoA 검증을 실행한다. 비록 엄격한 CoA 검증이 악의적인 이동노드에 의한 반사공격을 효과적으로 봉쇄함에도 불구하고 그림 4와 같이 바인딩 갱신 메시지를 전송하기 이전에 *COTI*와 *COT*를 교환해야 하기 때문에 1 *RTT*(Round Trip Time)의 핸드오버 지연을 발생시킨다.

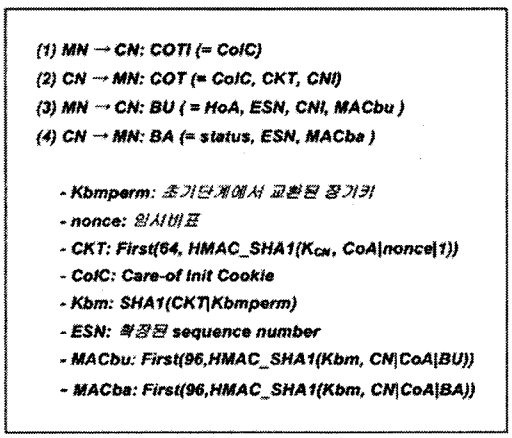

그림 4. OMIPv6-CGA의 후속 단계
Fig. 4. Subsequent Phase of OMIPv6-CGA

OMIPv6-CGA-CBA는 그림 5와 같이 이른 바인딩 갱신(Early Binding Update) 기법을 적용하여 엄격한 CoA 검증을 개선하였다.

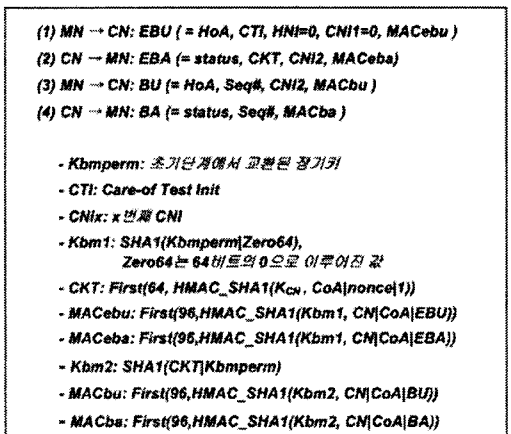

그림 5. OMIPv6-CGA-CBA의 후속 단계
Fig. 5. Subsequent Phase of OMIPv6-CGA-CBA

OMIPv6-CGA-CBA는 (1)과 (2)에 해당하는 이른 바인딩 갱신 과정에서 *CTI*와 *CKT*를 통해 CoA 검증을 함과 동시에 데이터 전송을 시작하여 1 *RTT*의 핸드오버 지연 문제를 해결하였다. 즉 이동노드는 *CTI*를 포함하는 *EBU*를 보낸 직후에 바로 데이터를 전송하고 대응노드는 *EBU* 검증과 함께 데이터를 수신하고 *CKT*를 포함한 *EBA*를 보낸 직후에 바로 데이터를 전송한다. 이때 대응노드는 이동노드를 위한 데이터 전송을 무제한 허용하는 것이 아니라 이동노드가 그동안 대응노드에게 전송한 데이터양으로 한정한다. 따라서 데이터 전송량의 한계를 넘어서면 이동노드는 대응노드로부터 직접 데이터를 받을 수 없게 된다. 이러한 한계는 (3)과 (4) 과정의 완전 바인딩 갱신(complete binding update)이 실행되기 전까지 적용된다.

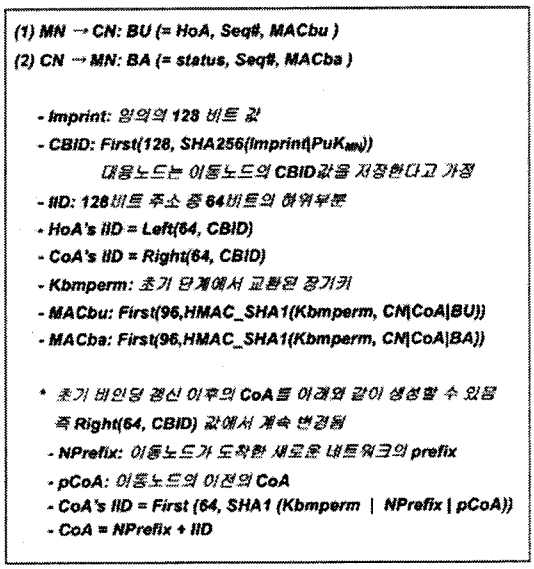

그림 6. OMIPv6-CBID의 후속 단계
Fig. 6. Subsequent Phase of OMIPv6-CBID

OMIPv6-CBID는 초기 RR 프로토콜 과정에서 발생가능한 세션 가로채기(Session Hijacking) 공격을 방어하기 위해 제안되었다. 세션 가로채기공격은 대응노드가 이동노드의 CoA 소유를 증명할 수 없기 때문에 발생하며 OMIPv6-CBID는 CGA 대신 CBID 기법을 적용함으로써 이 문제를 해결하였다. 즉 그림 6과 같이 이동노드의 HoA와 CoA가 CBID로부터 파생되기 때문에 대응노드는 CBID를 통해서 이동노드의 두 주소를 검증할 수

있다. 이러한 특성은 메시지 수신여부를 테스트하지 않고 CoA 검증을 하기 때문에 핸드오버 지연 시간 및 이동 시그날 메시지 양을 최적화 하였다. 또한, OMIPv6-CBID는 이동노드에게 오직 CBID에 근거한 CoA만을 선택하도록 하기 때문에 이동노드가 스스로 주소를 선택할 수 없는 네트워크 환경(예를 들어 이동노드가 네트워크 환경으로부터 주소를 부여 받거나 정해진 주소범위에서 주소를 선택해야 하는 경우)에서는 적용하기 어렵다. 또한, CGA 기법과 달리 만일 이동노드와 HoA의 하위 64비트 주소가 동일한 다른 노드가 존재한다면 반사공격이 가능하다.

Ⅳ. OMIPv6 후속 단계 개선 전략 비교 분석 및 개선 제안

본 장에서는 앞서 언급되었던 OMIPv6 시리즈의 CoA 검증 방법을 성능과 보안 측면에서 비교 분석하고 후속 단계를 위한 개선안을 제안한다.

4.1 성능

본 절에서는 핸드오버 지연 시간과 암호화 연산량 및 이동 시그날 메시지 전송량을 기준으로 각 프로토콜의 성능을 비교 분석한다.

핸드오버 지연 시간은 성능에서 가장 중요한 요인으로 후속 단계의 성능개선 노력 또한 주로 핸드오버 지연 시간에 중심을 두었다. 각 프로토콜별 핸드오버 지연 시간은 아래와 같이 구할 수 있다.

- *N*: 이동노드의 대응노드 개수
- *M*: 핸드오버 횟수
- *RTTcot*: 엄격한 CoA 테스트를 위한 시간 (=1 *RTT*)
- *RTTbu*: 바인딩 갱신을 위한 시간 (=1 *RTT*)
- *P*: 이른 바인딩 갱신에서 이동노드가 대응노드로부터 데이터를 전송받지 못할 확율
- *RTTmn*: 대응노드에서 이동노드의 HoA로 데이터를 전송할 때 데이터가 도착하는데 걸리는 시간 (= 1 *RTT*)
- *Lsend(X)*: 프로토콜 *X*에서 이동노드가 데이터를 전송하기까지의 지연시간
- *Lrecv(X)*: 프로토콜 *X*에서 이동노드가 데이터를 수신하기까지의 지연시간

$$Lsend(OMIPv6\text{-}DH) = 0\ RTT \quad (1)$$
$$Lrecv(OMIPv6\text{-}DH) = M\times N\times RTTbu = M\times N\times RTT \quad (2)$$
$$Lsend(OMIPv6\text{-}CGA) = M\times N\times RTTcot = M\times N\times RTT \quad (3)$$
$$Lrecv(OMIPv6\text{-}CGA) = M\times N\times(RTTcot+RTTbu) = 2\times M\times N\times RTT \quad (4)$$
$$Lsend(OMIPv6\text{-}CGA\text{-}CBA) = 0\ RTT \quad (5)$$
$$Lrecv(OMIPv6\text{-}CGA\text{-}CBA) = M\times N\times(RTTbu+P\times RTTmn) \quad (6)$$
$$Lrecv(OMIPv6\text{-}CGA\text{-}CBA) \geqq M\times N\times RTT \quad (7)$$
$$Lrecv(OMIPv6\text{-}CGA\text{-}CBA) \leqq 2\times M\times N\times RTT \quad (8)$$
$$Lsend(OMIPv6\text{-}CBID) = 0\ RTT \quad (9)$$
$$Lrecv(OMIPv6\text{-}CBID) = M\times N\times RTTbu = M\times N\times RTT \quad (10)$$

위의 결과를 보면 메시지 수신여부를 테스트하여 CoA를 엄격하게 검증하는 OMIPv6-CGA가 최소의 핸드오버 지연을 보이는 OMIPv6-DH와 OMIPv6-CBID에 비해 1 *RTT*의 오버헤드를 갖는 것을 볼 수 있다.

표 1. OMIPv6 시리즈의 연산량 및 메시지 전송량
Table. 1. Computational Overhead and the Amount of Mobility Signaling Messages of OMIPv6 Series

프로토콜	암호화 연산량	메시지 전송량
①	*4×HMAC-SHA1*	*BU+BA*
②	*6×HMAC-SHA1* *2×SHA1*	*COTI+COT* *BU+BA*
③	*10×HMAC-SHA1* *4×SHA1*	*2×(BU+BA)*
④	*4×HMAC-SHA1* *(1×SHA1)*	*BU+BA*

① OMIPv6-DH ② OMIPv6-CGA
③ OMIPv6-CGA-CBA ④ OMIPv6-CBID

표 1에서 OMIPv6 시리즈의 연산량과 이동 시그날 메시지 전송량을 비교하였다. 핸드오버 지연 시간의 결과처럼 CoA 검증을 전혀 하지 않거나 혹은 CBID를 통해 CoA를 검증하는 OMIPv6-DH와 OMIPv6-CBID가 우수한 결과를 보인 반면 이른 바인딩 갱신과 완전 바인딩 갱신을 모두 실행하는 OMIPv6-CGA-CBA는 암호화 연산과 메시지 전송 오버헤드가 가장 큰 것을 알 수 있다.

4.2 보안

후속 단계의 가장 큰 보안 위협은 악의적인 이동노드에 의한 반사공격이고 이를 방어하는 가장 확실한 방법은 실제로 이동노드가 주장하는 이동노드의 CoA에 메시지를 보내고 그 주소로부터 응답을 확인하는 방법이다. OMIPv6-CGA는 메시지 수신여부 테스트에 의한 엄격한 CoA 검증을 하기 때문에 가장 보안성이 뛰어나며 OMIPv6-CGA-CBA는 이른 바인딩 갱신과 완전 바인딩 갱신 사이에서 제한적인 반사공격을 허용한다. 한편, OMIPv6-CBID는 메시지 수신여부 테스트를 사용하지 않고 CBID에 의한 효과적인 CoA 검증을 하지만 다음과 같은 보안위협을 갖는다. 첫째로, 이동노드의 모든 CoA 오른쪽 하위 64비트를 CBID의 오른쪽 하위 64비트로 사용할 경우, 공격자의 공개키쌍이 주어질 때 공격대상의 주소가 CoA가 되도록 적절한 *Imprint*를 발견하는 전사공격에 취약하다. (단, CoA의 하위 64비트가 계속 변경되는 방법을 사용하면 이 공격에 취약하지 않다.) 둘째로, CBID 붕괴를 위한 전사공격의 비용이 $O(2^{64})$이기 때문에 $O(2^{59+16\times Sec})$의 비용을 갖는 CGA기법에 비해 보안성이 떨어진다. 이것은 OMIPv6-CBID의 전체적 보안성에 영향을 주는 요소가 된다.

4.3 개선 제안

표 2는 성능과 보안성 측면에서 각 프로토콜의 비교를 요약하였다. 표 2를 보면 알 수 있듯이 OMIPv6 시리즈의 후속 단계에는 성능과 보안이라는 트레이드오프(trade-off)가 존재한다. OMIPv6-DH와 OMIPv6-CGA는 성능 혹은 보안에 극단적으로 치우친 전략을 선택하였고 이들과 달리 OMIPv6-CGA-CBA와 OMIPv6-CBID는 성능과 보안사이의 적절한 절충점을 선택하여 후속 단계를 개선하였다. OMIPv6-CBID의 경우, CBID에 의한 효과적인 CoA 검증을 통해 전혀 CoA 검증을 하지 않는 OMIPv6-DH에 근사한 성능을 보인다. 그러나 보안성과 적용성은 OMIPv6-CGA와 OMIPv6-CGA-CBA에 비해 뛰어 나지 않음을 알 수 있다. 특히, 적용성의 경우 CBID 기법으로 인해 CoA 선택의 제약을 요구하기 때문에 네트워크 환경에 영향을 받는 한계를 갖는다.

본 논문에서는 OMIPv6-CGA-CBA의 이른 바인딩 갱신 및 CGA 기법을 OMIPv6-CBID에 적용하여 OMIPv6-CBID의 문제를 해결하고자 한다. 개선방안은 다음과 같다. 첫째로, 이동노드가 새로운 네트워크에 도착하였을 때 CoA를 자유롭게 선택할 수 있다면 OMIPv6-CBID의 CoA 검증기법을 적용하고 반대의 경우에는 OMIPv6-CGA-CBA의 이른 바인딩 갱신 기법을 적용하여 다양한 네트워크 환경에서 최적의 성능을 (특히, 핸드오버 지연 시간에서) 보장할 수 있도록 한다. 둘째로, CBID 대신 CGA 기법을 선택하여 보안성을 강화한다. 이를 위해 그림 7과 같이 CGA 기법을 수정하였다. 즉 CGA 기법에서 이동노드의 HoA 생성을 위해 계산되는 *Hash1*값으로부터 초기 CoA의 하위 64비트 값을 추출한다. 이후의 CoA는 OMIPv6-CBID와 유사하게 초기 CoA으로부터 파생된다.

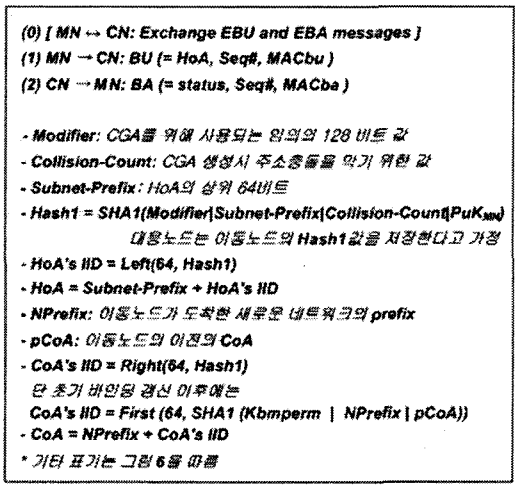

그림 7. 후속 단계 개선안
Fig. 7. Proposed Method for Subsequent Phase

개선안은 OMIPv6-CBID의 성능이점에 적용성과 보안성을 강화하여 성능과 보안 트레이드오프의 최적점을 찾으려 하였다. 개선안의 성능은 주로 이동노드의 방문 네트워크가 CBID를 허용하는 비율 즉 이른 바인딩 갱신을 하는 비율에 좌우한다. 즉 이른 바인딩 갱신을 많이 할수록 개선안의 성능은 OMIPv6-CGA-CBA에 가까워지고 반대일 경우에는 OMIPv6-CGA-CBID에 가까워진다. 표 2를 보면 전체적으로 개선안은 OMIPv6-CBID에 가까운 성능(일반적으로 MIPv6 환경에서는 이동노드가 CoA를 직접 결정함)과 OMIPv6-CGA-CBA와 동일한 보안성과 적용성을 보인다. 단 성능의 경우는 앞서 언급했듯이 이동노드가 방문하는 네트워크 환경에 따라 좌우될 수 있으나 최악의 경우라 할지라도 OMIPv6-

CBID보다 저조하지 않다. 이처럼 개선안이 성능과 보안성, 적용성을 전체적으로 고려할 경우, 다른 프로토콜들에 비해 우수함을 알 수 있다.

표 2. 개선안과 OMIPv6 프로토콜 시리즈의 비교
Table. 2. Comparison of the Proposed Method and Subsequent Phases of OMIPv6 Protocol Series

프로토콜		①	②	③	④	⑤
CoA 검증기법		×	메시지 수신 테스트	이른 바인딩 갱신 (EBU)	CBID	EBU+ CBID
성능	1회 핸드오버 지연시간 (RTT)	(송신) 0	1	0	0	0
		(수신) 1	2	1과2 사이	1	③과④ 사이
	암호화 연산량	적음	중간	많음	적음	③과④ 사이
	메시지 전송량	적음	중간	중간	적음	③과④ 사이
	전체적	좋음	나쁨	중간	좋음	③과④ 사이
보안성	반사공격	취약	강함	중간	중간	중간
	공개키와 주소의 연관성	나쁨	좋음	좋음	중간	좋음
적용성		좋음	좋음	좋음	중간	좋음

주) ① OMIPv6-DH ② OMIPv6-CGA
③ OMIPv6-CGA-CBA ④ OMIPv6-CBID
⑤ 개선안

V. 결 론

본 논문에서는 OMIPv6 프로토콜 시리즈의 후속단계를 성능과 보안성, 적용성의 측면에서 비교 분석하였다. 비교 분석 결과를 보면 OMIPv6 시리즈의 후속 단계에는 성능과 보안이라는 트레이드오프가 존재한다. 즉 OMIPv6-DH와 OMIPv6-CGA는 성능 혹은 보안에 극단적으로 치우친 전략을 선택하였고 이들과 달리 OMIPv6-CGA-CBA와 OMIPv6-CBID는 성능과 보안사이의 적절한 절충점을 선택하여 후속 단계를 개선하였다. 특히, OMIPv6-CBID의 경우 CBID에 의한 효과적인 CoA 검증을 통해 전혀 CoA 검증을 하지 않는 OMIPv6-DH에 근사한 성능을 보인 반면에 보안성과 적용성은 뛰어 나지 않음을 알 수 있다. 본 논문에서는 이른 바인딩 갱신 및 CGA 기법을 통해 OMIPv6-CBID 기법을 개선하였다. 개선안은 성능과 보안성, 적용성을 전체적으로 고려할 때 다른 프로토콜들에 비해 우수함을 보였다.

향후연구로 시뮬레이션을 통해 이동 패턴별 OMIPv6 시리즈의 성능분석과 이를 바탕으로 이동노드의 프로파일에 따른 성능최적화 연구가 요구된다.

참고문헌

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

[2] I. You, J. Lim, "Advanced Agent-Delegated Route Optimization Protocol for Efficient Multimedia Services at Low-Battery Devices," UMS 2007, Springer-Verlag LNCS 4352, Part II, pp. 479 - 486, Jan. 2007

[3] W. Haddad, F. Dupont, L. Madour, S. Krishnan and S. Park, "Optimizing Mobile IPv6 (OMIPv6)," draft-haddad-mipv6-omipv6-01.txt, Feb. 2004 (Work in progress)

[4] W. Haddad, L. Madour, J. Arkko and F. Dupont. "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)," draft-haddad-mip6-cga-omipv6-04, May 2005 (Work in progress)

[5] J. Arkko, C. Vogt and W. Haddad, "Applying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6," draft-arkko-mipshop-cga-cba-04.txt, June 2006 (Work in progress)

[6] F. Dupont and W. Haddad, "Optimizing Mobile IPv6 (OMIPv6)," draft-dupont-mipshop-omipv6-00.txt, Feb. 2006 (Work in progress)

[7] I. You, "Improving the CGA-OMIPv6 Protocol for Low-Power Mobile Nodes," ICCSA 2006, Springer-Verlag LNCS 3938, pp. 336-343, May 2006

[8] S. Bradner, A. Mankin and J. Schiller, "A Framework for Purpose-Built Keys (PBK)," draft-bradner-pbk-frame-06.txt, Oct. 2003 (Work in progress)

[9] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972, March 2005

[10] R. Deng, J. Zhou, and F. Bao, "Defending Against Redirect attacks in Mobile IP," Proceedings of the 9th ACM Conference on Computer and Communications Security, Nov. 2002

저자소개

유 일 선(Ilsun You)

1995년 단국대학교 전산통계 학과 학사 졸업
1997년 단국대학교 전산통계학과 석사 졸업
2002년 단국대학교 전산통계학과 박사 졸업
2005년~현재 한국성서대학교 정보과학부 전임강사
※관심분야 : MIPv6, 인터넷 보안, 접근통제

김 흥 준(HeungJun Kim)

1989년 단국대학교 전자계산학과 졸업(학사)
1993년 단국대학교 대학원 전산통계학과 (석사)
1999년 단국대학교 대학원 전산통계학과 (박사)
1999년~현재 진주산업대학교 컴퓨터공학부 부교수
※관심분야 : 컴퓨터구성, 모바일 네트워킹, etc.