MIPv6에서 RR프로토콜 성능개선 방안

나재훈*, 이달원**, 손승원*, 조인준**
*한국전자통신연구원, **배재대학교

Performance Enhancement Scheme for RR Protocol in MIPv6

jae-hoon na, seung-won shon*, dal-won lee**, in-june jo**,*
**ETRI, **Paichai University*

요 약

*IETF mobileip WG*에서 *MN(Mobile Node)*의 위치를 나타내는 '바인딩정보'를 안전하게 *CN(Correspond Node)*에게 송신하여 최적경로를 설정하는 *RR(Return Routability)*프로토콜을 드래프트 문서로 제안하고 있다[1]. 하지만 이 프로토콜은 최적경로설정이 *MN*에 의해 시작됨에 따라 최적경로설정 지연에 따른 최적경로설정 확률의 저하와 불필요한 메시지 교환에 따른 통신부담을 문제점으로 지적할 수 있다.

본 논문에서는 상기와 같은 문제점 해결방안으로 *HA(Home Agent)*가 *CN*으로부터 첫번째 패킷을 수신했을 때 최적경로설정을 시작하도록 개선된 *RR*프로토콜을 제안하였다. 이를 통해서 최적경로 설정에 소용되는 시간을 단축하고 교환되는 메시지 수를 감소시켜 통신부담 경감효과를 얻을 수 있다. 이럼에도 불구하고 기존의 *RR*프로토콜과 동일한 보안수준을 제공한다.

I. 서론

현재 국내 *ISP*들은 *IPv6* 시험 네트워크를 구축하여 다양한 *IPv6*기능을 테스트 중에 있고 이를 기반으로 2003년에 *IPv6* 상용서비스가 이루어질 것으로 예측된다. 그리고 *IPv6* 상용망에서 이윤창출을 위해 적극적인 도입 예상분야가 이동 무선인터넷 분야로 전망된다. 국내에서 현재의 이동 인터넷 서비스는 각각의 무선단말에 고유의 전화번호를 부여하여 서비스가 제공됨에 따라 서비스의 내용 및 품질이 낮다(즉, *IP*기반 이동인터넷이 아님).

이러한 문제점을 해결하고 급격하게 증가되고 있는 이동단말의 *IP*화를 위해 *MIPv6*가 대안으로 부상되고 있다. 하지만, *MIPv6*의 취약한 보안문제 때문에 *MIPv6 RFC* 표준이 지연상태에 있다[2].

본 논문에서는 *IETF mobileip WG*에서 이동인터넷 보안기술로 제시한 RR프로토콜의 문제점 개선방안을 제안한다.

II. 본론

1. MIPv6 보안[1][2]

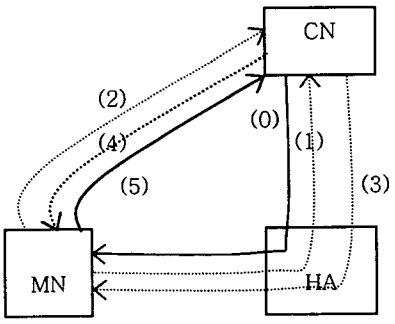
MIPv6 보안은 3 가지로 분류한다. (1) *MN*과 *HA*, *MN*과 *CN*간에 전송되는 *BU*메시지 보호, (2) 서브넷 프래픽스 발견메시지 보호, (3) 데이터 패킷 전송메커니즘의 보호 등이다. 현재 *BU*메시지 보호로 *RR*프로토콜, 서브넷 발견메시지 보호로 *IPsec*, 데이터 패킷 전송메커니즘 보호로 공격을 제한하는 방법 등이 제안되고 있다[1]. 본 논문에

서는 *BU*메시지 보호방법 개선을 목적으로 하기 때문에 참고문헌[1]에 제안된 RR프로토콜만을 설명한다.

1) *RR*프로토콜 동작절차

이는 *MIPv6* 최적경로설정시 *BU*메시지 보호를 위해 참고문헌[1]에서 제안한 프로토콜이다. 이는 *MN*과 *CN*간에 어떤 보안 인프라구조도 존재하지 않음을 전제로 한다. 이 프로토콜은 CN이 수신한 BU메시지가 적법한 *MN*으로부터 제공된 것임을 보장한다. 이점은 (1) 인터넷 어느 곳에서나 위조된 *BU*메시지를 *CN*에게 전송하는 행위를 제한한다. (2) *CN*에게 보내진 *BU*메시지의 무결성과 인증서비스를 제공한다.

이 프로토콜의 개요는 다음과 같다. *MN*이 *BU* 메시지를 직접 *CN*에게 전송하기 전에 4개의 메시지(*HoTI/HoT, CoTI/CoT*)를 서로 다른 경로를 통해서 송수신하여 보안에 필요한 데이터를 *MN*이 얻는다. 이와 같이 서로 다른 경로를 통해서 메시지가 송수신되는 이유는 *CN*에서 *MN*으로 송신하는 패킷이 최소한 *MN*의 *HoA* 혹은 *CoA*로 전달이 가능함을 확인하기 위한 것이다. *RR*프로토콜의 전체적인 메시지 흐름을 [그림 1]에서 보여주고 있다.



[그림 1] 참고문헌[1] *RR*프로토콜

[그림1]에서 본 바와 같이 *RR*프로토콜은 *MN*이 *CN*으로부터 첫번째 패킷을 수신했을 때 시작된다([그림 1]에서 (0)). *MN*은 먼저 *HA*를 경유하여 *CN*에게 *HoTI(Home Test Init)*메시지를 송신한다([그림 1]에서 (1)). 이 메시지에는 자신이 생성한 *64bit* 쿠키(즉, *HIC, home init cookie*)가 포함된다. 이때 *MN*과 *HA*간에는 *IPsec ESP*[3,5]로 역 터널링 경로설정 된다. 다음으로 *MN*이 직접 *CN*으로 *CoTI(Care of Test Init)*메시지를 송신한다([그림 1]에서 (2)). 이 메시지에는 자신이 생성한 *64bit* 쿠키(즉, *CIC, care of init cookie*)가 포함된다. 이와 같이 2개의 메시지에 각각 포함된 쿠키의 용도는 첫째, *HoTI*와 *HoT, CoTI*와 *COT*쌍의 일치성 검증에 사용된다. 둘째, *HoTI*와 *CoTI*메시지를 수신하지 않은 노드에 의해 보내진 위장된 응답의 추출을 위한 것이다.

*HoTI*메시지를 수신한 *CN*은 *HA*를 경유하여 *HoT(Home Test)*메시지를 *MN*에게 송신한다([그림 1]에서 (3)). 이 메시지는 *{HIC, HNI(Home Nonce Index), HKT(home keygen token)}*로 구성된다. 여기에서 *HIC*는 *MN*이 *HoTI*메시지에 포함된 것이고, *HNI*는 자신이 생성하여 유지하고 있는 넌스 색인이다. 그리고 *HKT*는 *first(64, HMAC_SHA(Kcn, (HoA|nonce|0))*[4]이다. *HKT*계산에서 사용된 *Kcn*은 *CN*이 유지하는 기밀 키이다. 이렇게 구성함으로써 *HIC*는 *HoTI* 요구에 *HoT*로 응답함을 *MN*에게 알리고, *HNI*는 *CN*의 넌스값을 노출시키지 않고 *MN*에 전달하고 이를 다시 *BU*메시지를 통해서 전달 받음으로써 *CN*이 유지하고 있는 넌스값을 추출할 수 있다. 이는 *CN*이 최종적인 *BU*메시지를 수신할 때까지 "비 상태유지*(Stateless)*"로 수행됨을 의미한다. 마지막으로 *HKT*는 *CN*이 *HoTI*로부터 추출한 *HoA*와 이에 대응한 넌스값 및 인덱스을 자신의 기밀 키(*Kcn*)로 계산된 *MAC(Message Authentication code)*[4]값이다. 이는 *MN*에 전달되어 *Kbm*생성에 사용된다.

*CoTI*메시지를 수신한 *CN*은 직접 *CoT(Care of Test)*메시지를 *MN*에게 송신한다([그림 1]에서 (4)). 이 메시지는 *{CIC, CNI(Care of Nonce Index),*

*CKT(Care of keygen token)}*로 구성된다. 여기에서 *CIC*는 *MN*이 *CoTI*메시지에 포함된 것이고, *CNI*는 자신이 생성하여 유지하고 있는 넌스 색인이다. 그리고 *CKT*는 *first(64, HMAC_SHA(Kcn, (CoA|nonce|1))*이다. *CKT*계산에서 사용된 *Kcn*은 *CN*이 유지하는 기밀 키이다. 이렇게 구성함으로써 *CIC*는 *CoTI* 요구에 *CoT*로 응답함을 *MN*에게 알리고, *CNI*는 *CN*의 넌스값을 노출시키지 않고 *MN*에 전달하고 이를 다시 *BU*메시지를 통해서 전달 받음으로써 *CN*이 유지하고 있는 넌스 값을 추출할 수 있다. 이는 *CN*이 최종적인 *BU*메시지를 수신할 때까지 "비 상태유지*(Stateless)*" 로 수행됨을 의미한다. 마지막으로 *CKT*는 *CN*이 *CoTI*로부터 추출한 *CoA*와 이에 대응한 넌스 값 및 인덱스을 자신의 기밀 키*(Kcn)*로 계산된 *MAC(Message Authentication code)*값이다. 이는 *MN*에 전달되어 *Kbm*생성에 사용된다.

*HoT*와 *CoT*를 수신한 *MN*은 *BU*메시지를 *CN*에게 송신한다([그림 1]에서 (5)). 이 메시지는 *{HoA, seq#, HNI, CNI, HMAC_SHA1(Kbm, (CoA|CNA|BU))}*로 구성된다. *HoA*는 *BCE(Biding Cache Entry)* 구성에 필요한 *MN*의 홈 주소이고, *seq#*는 이 *BU*에 대응한 *BA(Binding Acknowledgement)*를 전달 받기 위함이다. 그리고 *HNI*와 *CNI*는 이 메시지가 *CN*에 전달되었을 때 이 *MAC* 검증에 필요한 *CN*의 넌스 값 지시를 위한 것이다. 마지막으로 *MAC*은 바인딩 키(즉 *Kbm)*로 *{CoA, CAN, BU메시지}*를 해쉬한 것이다. 여기에서 *Kbm*은 *CN*으로부터 수신한 *{HKT, CKT}*의 해쉬 값(즉, *Kbm := SHA1(HKT|CKT))*이다. 따라서 *Kbm*에는 *CN*의 기밀 요소인 *Kcn*, 넌스, 넌스 인덱스 인자와 *MN*의 *HoA*와 *COA* 인자가 결합되어 만들어진 바인딩 키이다. 이러한 의미를 가진 *Kbm*으로 *{CoA|CNA|BU}*의 *MAC*값을 계산한 이유는 *MN*이 *BU*메시지를 보낼 때 *SA(Source Address)*로 사용하는 *CoA, DA(Destination Address)*로 사용하는 *CNA*, 그리고 *BU*메시지 자체의 위조 방지를 위한 것이다.

*BU*메시지를 수신한 *CN*은 다음과 같이 이를 검증한다. 메시지로부터 *HoA, HNI*를 추출하고, 자신이 소유하고 있는 넌스를 *HNI*로부터 획득하여 이들에게 자신의 기밀 키 *Kcn*으로 *HKT*를 생성한다. 다음으로 메시지의 SA로부터 *CoA*, 메시지 내용으로부터 *CNI*를 추출하고 자신이 소유하고 있는 넌스를 *CNI*로부터 획득하여 이들에게 자신의 기밀 키 *Kcn*으로 *CKT*를 생성한다. 이들 *HKT*와 *CKT*로부터 *Kbm*(즉, *Kbm := SHA1(HKT|CKT))*을 계산한다. 이를 이용하여 *HMAC_SHA1(Kbm, (CoA|CNA|BU))}*을 계산한다. 계산된 이 값이 *BU*메시지에서 전송된 값과 동일하면 *MN*을부터 위조되지 않은 *BU*메시지로 판단하여 *{HoA, CoA}*로 구성된 *BCE(Biding Cache Entry)*를 생성한다.

2) *RR*프로토콜 분석 및 문제점

*BU*메시지 보호를 위해 *IETF draft[1]*에서 제안한 *RR*프로토콜의 주 목적은 *CN*입장에서 정당한 *MN*이 *BU*메시지를 보냈는지를 검증하는데 있다. 이 방법은 *HA*와 *CN* 패스에 위치한 공격자에 취약성이 있다. 따라서 *RR*은 인터넷의 어떤 위치에서나 행할 수 있는 위조된 *BU* 메시지 제한에 있다.

이 프로토콜의 문제점은 (1) 최적경로설정 시기의 지연이다. 즉 *RR*프로토콜이 *MN*이 *CN*으로부터 첫번째 메시지를 HA 경유하여 수신했을 때 시작된다. (2) 네트워크 과부하가 문제이다. 최종적인 *BU*메시지 전달을 위해 총 4개의 메시지 *(HoTI/HOT, CoTI/COT)*가 교환된다. 이들 메시지가 통과되는 경로는 총 8경로(*MN*과 *CN*간에 2경로, *MN*과 *HA*간에 3경로, *HA*와 *CN*간에 3경로)이다. 이는 네트워크 부담요소이다. 결론적으로 최적경로설정시기의 지연 및 다수개의 메시지 전

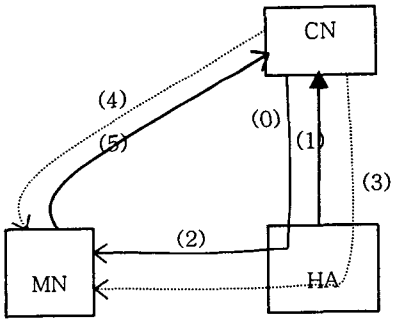
달에 따른 네트워크 부담으로 최적경로설정 확률이 낮아진다. 이의 개선을 위한 방안을 제 2 절에서 제안한다.

2. 개선된 *RR* 프로토콜 제안

상기의 2) 항에서 제기한 문제점 개선을 위해 다음과 같은 수정된 *RR*을 제안한다. 제안동기는 (1) *MN*이 홈을 이동했을 때 *MN*은 직접 *BU*메시지를 통해 *HA*에 바인딩정보를 등록한다. 이때 *MN*과 *HA*간에는 *IPsec ESP*[2]에 의해 안전한 채널을 기반으로 한다. 따라서 *MN*의 위치를 나타내는 바인딩정보가 안전하게 *HA*에 유지된다. 따라서 *RR*프로토콜 시작시점을 *HA*가 행하도록 함으로써 최적경로설정 시간을 단축시킬 수 있다. 또한 하나의 메시지만을 *CN*에게 전달하여 *HKT*와 *CKT*를 생성하여 *MN*에게 전달함으로써 4개의 메시지를 2개로 줄일 수 있다. 메시지가 통과되는 경로는 총 8 경로에서 6경로로 줄여 네트워크 부담을 경감시킨다. 이럼에도 불구하고 기존의 RR과 동일한 수준의 보호를 이룩할 수 있다.

1) 개선된 RR프로토콜의 동작절차

이는 [그림 2]에서 본 바와 같이 4개의 메시지와 5개의 경로를 통해 메시지가 교환된다.



[그림 2] 개선된 *RR*프로토콜

*HA*가 *CN*으로부터 *MN*으로 향한 첫번째 패킷을 수신하면([그림 2]에서 (0)) 2개의 메시지를 생성하여 *CN*과 *MN*에게 송신한다. 첫째, *HA*에 저장된 바인딩정보 *{HoA, CoA}*를 참조하여 *HoCoTI(Home & Care of Test Init)*메시지를 *CN*에게 보낸다([그림 2]에서 (1)). 이는 *(SA(HOA), DA(CNA) : HoCoIC, COA)*로 구성된다. *HoCoIC(Home & Care of Init Cookie)*는 *HoCoTI*메시지와 다음에 수신할 *HoT*와 *CoT*가 각각 쌍으로 일치성 검증을 위한 것이다. 둘째, *MN*으로 향한 패킷에 *HoCoTI* 플래그와 *HoCoIC*를 피기백시켜 보낸다([그림 2]에서 (2)). *HoCoTI* 플래그는 *MN*에게 RR프로토콜이 *HA*에 의해 시작되었음을 알리기 위함이고 *HoCoIC*는 *MN*이 수신한 *CoT*가 *HoCoTI*와 쌍임을 검증하는데 사용된다. 이때 *MN*은 *HoCoIC*와 *CNA*를 *BU*목록에 저장한다.

*HoCoTI*메시지를 수신한 *CN*은 2개의 메시지를 생성하여 *MN*에게 송신한다. 첫째, *HOT*메시지를 *HA*를 경유하여 *MN*에게 송신한다([그림 2]에서 (3)). 이 메시지는 *(SA(CNA), DA(HOA) : HoCoIC, HNI, HKT(first(64, HMAC_SHA(Kcn, (HOA|nonce|0))*로 구성된다. 둘째, *COT*메시지를 *MN*에게 직접 보낸다([그림 2]에서 (4)). 이 메시지는 *(SA(CNA), DA(COA) : HoCoIC, CNI, CKT(first(64, HMAC_SHA(Kcn, (COA|nonce|1))*로 구성된다. 이 메시지의 구성요소들의 기능 및 의미는 기존의 *RR* 프로토콜과 동일하다.

*HoT*와 *CoT*를 수신한 *MN*은 메시지에서 *DA*를 추출하여 저장된 *CNA*와 비교하여 일치성을 검사하고 저장된 *HoCoIC*와 메시지의 *HoCoIC*를 비교하여 일치하면 *HoCoTI*요구에 의한 응답으로 처리한다. 그리고 나서 기존의 *RR*에서와 같이 *Kbm*을 계산하고 이를 통해 *BU*메시지를 생성하여 *CN*에게 보낸다([그림 2]에서 (5)).

*BU*메시지를 수신한 *CN*은 다음과 같이 이를 검증한다. 메시지로부터 *HoA*, *HNI*를 추출하고, 자신이 소유하고 있는 넌스를 *HNI*로부터 획득하여 이들에게 자신의 기밀 키 *Kcn*으로 *HKT*를 생성한다. 다음으로 메시지의 SA로부터 *CoA*, 메시

지 내용으로부터 *CNI*를 추출하고 자신이 소유하고 있는 넌스를 *CNI*로부터 획득하여 이들에게 자신의 기밀 키 *Kcn*으로 *CKT*를 생성한다. 생성된 *HKT*와 *CKT*로부터 *Kbm*(즉, *Kbm := SHA1(HKT|CKT)*)을 계산한다. 이를 이용하여 *HMAC_SHA1(Kbm, (CoA|CNA|BU))*을 계산한다. 계산된 이 값이 *BU*메시지에서 전송된 값과 동일하면 *MN*을부터 위조되지 않은 *BU*메시지로 판단하여 *{HoA, CoA}*로 구성된 *BCE*를 생성한다.

2) 기존 RR프로토콜과 제안 프로토콜 비교

상기와 같이 RR프로토콜을 개선하면 다음과 같은 이점이 있다. 첫째, *HA*가 *MN*으로 향하는 첫번째 패킷 수신 시점에서 *RR*프로토콜이 시작되기 때문에 *CN*에서 *MN*으로 전송되는 패킷의 최적경로설정확률을 높인다. 둘째, *HA*가 *HoCoTI*를 *CN*에게 직접 보냄으로써 *MN*에서 *HA*로 전송되는 *HoTI*메시지와 *MN*에서 *CN*으로 전송되는 *CoTI*메시지지가 제거되어 네트워크 부하를 줄인다. 세째, 그럼에도 불구하고 기존의 *RR*프로토콜의 보안수준은 그대로 유지된다. 비교 내용은 [표 1]과 같다.

[표 1] 비교표

	참고문헌[1] RR 프로토콜	제안된 RR 프로토콜
최적경로 시작시점	첫번째 패킷이 MN에 도착 시	첫번째 패킷이 HA에 도착 시
BU메시지 전송전에 교환되는 메시지 수	5개	4개
BU메시지 전송전에 교환되는 메시지의 경로 수	8개	6개
보안수준	동일	동일
최적경로 설정 확률	낮음	높음

III. 결론

본 논문에서는 참고문헌[1]의 *RR*프로토콜의 성능개선방안을 제안하였다. 제안된 프로토콜의 동작환경은 참고문헌[1]의 *RR*프로토콜과 마찬가지로 *MN*과 *CN*간에 사전에 설정된 보안인프라구조를 정의하지 않는다. 다만 *MN*과 *HA*간에는 *IPsec ESP*보안 인프라구조정의를 전제로 한다.

이럼에도 불구하고 *BU*메시지 전송전에 교환되는 메시지 수 및 경로 수를 감소시킴으로써 네트워크 부하 및 최적경로설정 확률을 크게 개선되었음을 보였다. 이와 더불어 보안수준은 참고문헌[1]의 *RR*프로토콜과 동일하다.

참고문헌

[1] Perkins, C. and D. Johnson, "Mobility Support in IPv6", Internet-Draft http://www.ietf.org/internet-rafts/draft-ietf-mobileip-ipv6-21, February, 2003.

[2] Roe, M., Aura, T., O'Shea, G. and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", draft-roe-mobileip-updateauth-02.txt, February 2002.

[3] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, November 1998.

[4] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

[5] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling betweenMobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-03, February 2003.