情報保護學會論文誌
第14券 第5號, 2004. 10

# MIPv6에서 RR프로토콜 성능개선 방안

이 달 원[a)†], 황 일 선[b)], 손 승 원[c)], 조 인 준[a)‡]

배재대학교[a)], 한국과학기술정보연구원[b)], 한국전자통신연구원[c)]

# Performance Enhancement Scheme for RR Protocol in MIPv6

Dal-won Lee[a)†], Il-sun Hwang[b)], Seung-won Shon[c)], In-june Jo[a)‡]

Paichai University[a)], Korea Institute of Science and Technology Information[b)], Electronics and Telecommunications Research Institute[c)]

## 요 약

IETF mobileip WG에서 MN(Mobile Node)의 위치를 나타내는 '바인딩정보'를 안전하게 CN(Correspondent Node)에게 송신하여 최적경로를 설정하는 RR(Return Routability)프로토콜을 드래프트 문서로 제안하고 있다. 하지만 이 프로토콜의 시작 주체 및 시점이 MN에 의해 이루어짐에 따라 최적경로설정 지연에 따른 홈 네트워크의 부담 및 통신지연을 증가시키고 불필요한 메시지 교환에 따른 통신부담을 문제점으로 지적할 수 있다.

본 논문에서는 상기와 같은 문제점의 해결방안으로 RR프로토콜의 시작 주체 및 시점을 MN에서 HA(Home Agent)로 변경하여 HA가 CN으로부터 첫 번째 패킷을 수신했을 때 최적경로설정을 시작하도록 개선된 RR프로토콜을 제안하였다. 이를 통해서 최적경로설정에 소용되는 시간을 단축하고 교환되는 메시지 수를 감소시켜 통신부담을 경감시키는 효과를 얻을 수 있다. 이럼에도 불구하고 기존의 RR프로토콜과 동일한 보안수준을 제공한다.

## ABSTRACT

An Internet draft, named RR(Return Routability) protocol, proposed to IETF mobileip WG, in order to establish an optimal path to MN(Mobile Node) by securely sending the BU(Binding Update) message to CN(Correspondent Node). However, it has some problems with initiating the protocol by the MN: it causes to increases in communication load in the home network, to increases communication delay between MN and CN, and increases in communication load due to unnecessary message exchanges.

To resolve the problems, this paper proposes an alternative scheme for the RR protocol in MIPv6. The proposed scheme is devised to start the protocol by HA on receiving the first packet from CN. It decreases the route optimization overhead by reducing the number of BU messages as well as the communication time. Beside these advantages, this scheme provides the same security grade as the original RR protocol.

**Keywords** : *MIPv6, Return Routability, Binding Update*

접수일 : 2004년 3월 17일 ; 채택일 : 2004년 8월 30일

† 주저자 : munhee@mail.pcu.ac.kr

‡ 교신저자 : injune@mail.pcu.ac.kr

## Ⅰ. 서 론

현재 국내 *ISP(Internet Service Provider)*들은 *IPv6* 시험 네트워크를 구축하여 다양한 *IPv6* 기능을 테스트 중에 있고 이를 기반으로 *IPv6* 상용서비스가 이루어질 것으로 판단된다. 그리고 *IPv6* 상용망에서 이윤 창출을 위하여 적극적인 도입이 예상되는 분야가 바로 이동 무선인터넷 분야로 전망된다. 국내에서 현재 이동 인터넷 서비스는 각각의 무선단말에 고유의 전화번호를 부여하여 서비스가 제공됨에 따라 서비스의 내용과 품질이 낮다. 이러한 문제점을 해결하고 급격하게 증가되고 있는 이동단말의 *IP*화를 위해 *MIPv6 (Mobile IPv6)*가 대안으로 부상되고 있다. *MIPv6*에서는 *MIPv4*와는 다르게 *MN*과 *CN*간에 최적경로설정을 기본기능으로 제안하고 있다. 최적경로설정방법은 *MN*의 위치정보를 *CN*에게 등록함으로써 이루어진다. 하지만 *MN*의 위치정보를 *CN*에 등록하는 과정에서 위치정보를 불법적으로 활용할 수 있는 보안 위협요소가 존재한다. 이러한 보안 위협에 대응하여 안전하게 위치정보를 보호하면서 최적경로를 설정할 수 있는 여러 방안들이 연구되었다[1,2,3]. 이들 결과물 중에 *IETF mobileip WG*에서 제안한 *RR*프로토콜[4]이 인터넷 *RFC* 표준 후보로 관심의 대상이 되고 있다.

참고문헌 [4]에 의하면 *MN*과 *HA*간에는 안전한 *IPsec(Internet Protocol security) ESP(Encapsulation Security Payload)* 채널 설정을 전제로 하고 있다. 따라서 *MN*이 외부 네트워크로 이동을 하면 항상 자신의 위치정보를 안전한 채널을 사용하여 *HA*에 등록한다. 이러한 전제하에서 참고문헌 [4] *RR*프로토콜의 시작 주체 및 시점은 *MN*이 된다. 즉, *MN*이 *CN*으로부터 첫 번째 패킷을 *HA*를 경유하여 수신하면 *MN*이 *RR* 프로토콜을 구동시킴을 의미한다. 여기에서 문제점은 *MN*의 위치정보를 안전한 *IPsec ESP* 채널을 통해 *HA*가 유지하고 있음에도 불구하고 *MN*이 *RR*프로토콜의 시작 주체 및 시점이 된다는 점이다. 본 논문에서는 *RR*프로토콜의 시작 주체 및 시점을 *MN*에서 *HA*로 변경함으로써 참고문헌 [4]의 프로토콜보다 성능이 개선된 *RR*프로토콜을 제안하였다. 즉, 제안한 *RR*프로토콜은 *CN*으로부터 *MN*으로 향하는 첫 번째 패킷을 *HA*가 수신하면 *HA*가 바로 *RR*프로토콜을 구동하도록 하여 참고문헌 [4]의 *RR*프로토콜보다 최적경로설정시간을 단축시키고 교환되는 메시지 수를 감소시켜 통신부담 경감효과를 얻을 수 있는 개선된 *RR*프로토콜을 의미한다. 이럼에도 불구하고 기존의 *RR*프로토콜과 동일한 보안수준을 제공한다.

본 논문의 구성은 본론의 1절에 참고문헌 [4]의 *RR*프로토콜의 동작절차와 분석 내용을 기술하였고, 2절에 개선된 *RR*프로토콜을 제안하고 기존 *RR*프로토콜과 개선된 *RR*프로토콜을 비교하였다. 마지막으로 결론을 맺었다.

## Ⅱ. 본 론

### 1. MIPv6에서 RR프로토콜의 개요

*MIPv6*에서 보안은 크게 3가지로 분류한다. (1) *MN*과 *HA*, *MN*과 *CN*간에 전송되는 *BU(Binding Update)*메시지 보호, (2) 서브넷 프래픽스 발견 메시지 보호, (3) 데이터 패킷 전송메커니즘의 보호 등이다. 현재 *BU*메시지 보호방법으로는 참고문헌 [4]의 *RR*프로토콜, 서브넷 프래픽스 발견 메시지 보호방법으로는 *IPsec ESP*[5,6], 데이터 패킷 전송메커니즘 보호방법으로는 공격을 제한하는 다양한 방법 등이 제안되고 있다[7]. 본 논문에서는 *MN*과 *CN*간에 교환되는 *BU*메시지 보호방법 개선을 목적으로 하기 때문에 참고문헌 [4]의 *RR*프로토콜만을 설명한다.

*RR*프로토콜은 *MIPv6*에서 최적경로설정 시 *BU*메시지 보호를 위해 참고문헌 [4]에서 제안한 프로토콜이다. 이는 *MN*과 *CN*간에 어떤 보안 인프라 구조도 존재하지 않음을 전제로 한다. 이 프로토콜은 *CN*이 수신한 *BU*메시지가 적법한 *MN*으로부터 제공된 것임을 보장한다. 이점은 첫째, 인터넷 어느 곳에서나 위조된 *BU*메시지를 *CN*에게 전송하는 행위를 제한하며, 둘째, *CN*에게 보내진 *BU*메시지의 무결성 및 인증 보안서비스를 제공한다.

*RR*프로토콜의 전체적인 개요는 다음과 같다. *MN*이 *BU*메시지를 직접 *CN*에게 전송하기 전에 4개의 메시지(*HoTI, HoT, CoTI, CoT*)를 서로 다른 경로를 통해서 교환하여 *BU*메시지 보호에 필요한 데이터를 *MN*이 얻는다. *MN*은 얻어진 정보를 활용하여 *BU*메시지를 생성함으로써 *MN*과 *CN*사이에 존재하는 공격자가 불법적으로 *MN*의 위치정보를 활용할 수 없도록 보호한다.

#### 1.1 RR프로토콜 동작절차

참고문헌 [4] *RR*프로토콜의 전체적인 동작절차를 살펴보면 그림 1과 같다.

그림 1에서 ①과 같이 *MN*이 *CN*으로부터 *HA*를 경

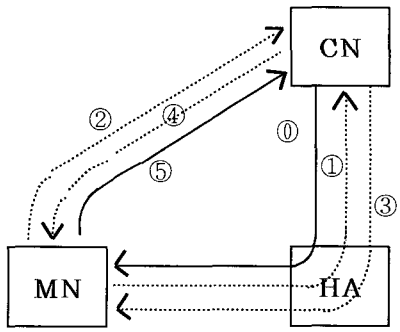


그림 1. 참고문헌 [4]의 RR프로토콜
Fig. 1 RR protocol in Reference [4]

유하여 첫 번째 패킷을 수신했을 때 안전한 최적경로 설정을 위해 *RR*프로토콜이 시작된다.

**(Step1)** *MN*은 다음의 ①과 ②와 같은 두개의 메시지를 생성하여 *CN*에게 보낸다.

① *MN* → *CN*(*HA* 경유): *HoTI*
② *MN* → *CN*: *CoTI*

*MN*은 먼저 *HA*를 경유하여 *CN*에게 *HoTI*(*Home Test Init*) 메시지를 송신한다. 이 메시지에는 자신이 생성한 *64bit* 쿠키(*Home Init Cookie, HIC*)가 포함된다. 이때 *MN*과 *HA*간에는 *IPsec ESP*로 역 터널링 경로설정이 주어지기 때문에 이 메시지는 안전하다. 다음으로 *MN*이 직접 *CN*에게 *CoTI*(*Care-of Test Init*) 메시지를 송신한다. 이 메시지에는 자신이 생성한 *64bit* 쿠키(*Care-of Init Cookie, CIC*)가 포함된다.

**(Step2)** *CN*이 상기의 ①과 ② 메시지를 각각 수신하면 다음과 같이 ③과 ④의 메시지를 생성하여 *MN*에게 송신한다.

③ *CN* → *MN*(*HA* 경유): *HoT*
④ *CN* → *MN*: *CoT*

먼저 *HoTI* 메시지를 수신한 *CN*은 *HA*를 경유하여 *HoT*(*Home Test*) 메시지를 *MN*에게 송신한다. *HoT*메시지는 {*HIC*, *HNI*(*Home Nonce Index*), *HKT*(*Home Keygen Token*)}로 구성된다. 여기에서 *HIC*는 *MN*으로 부터 받은 *HoTI* 메시지에 포함된 것이고, *HNI*는 자신이 생성하여 유지하고 있는 넌스 색인이다. 그리고 *HKT*는 *first*(*64, HMAC_SHA1*(*Kcn, (HoA|nonce|0)*))로 구성되며 *CN*이 *HoTI*로부터 추출한 *HoA*와 *HNI*에 해당되는 넌스값 및 넌스 색인값을 자신의 기밀 키 *Kcn*로 계산한 *MAC*(*Message Authentication Code*)[8]값이다.

다음으로 *CoTI* 메시지를 수신한 *CN*이 직접 *CoT*(*Care-of Test*) 메시지를 *MN*에게 송신한다. *CoT*메시지는 {*CIC, CNI*(*Care-of Nonce Index*), *CKT*(*Care-of Keygen Token*)}로 구성된다. 여기에서 *CIC*는 *MN*으로 부터 받은 *CoTI* 메시지에 포함된 것이고, *CNI*는 자신이 생성하여 유지하고 있는 넌스 색인이다. 그리고 *CKT*는 *first*(*64, HMAC_SHA1*(*Kcn, (CoA|nonce|1)*))로 구성되며 *CN*이 *CoTI*로부터 추출한 *CoA*와 *CNI*에 해당되는 넌스값 및 넌스 색인값을 자신의 기밀 키 *Kcn*로 계산한 *MAC*값이다.

**(Step3)** *MN*이 *HoT*와 *CoT*를 수신하면 다음의 *BU* 메시지 생성하여 *CN*에게 송신한다.

⑤ *MN* → *CN*: *BU*메시지

*BU*메시지는 {*HoA, seq#, HNI, CNI, HMAC_SHA1*(*kbm, (CoA|CNA|BU*메시지)))}로 구성된다. *HoA*는 *BCE*(*Biding Cache Entry*) 구성에 필요한 *MN*의 홈 주소이고, *seq#*는 이 *BU*메시지에 대응한 *BA*(*Binding Acknowledgement*) 메시지를 전달받기 위함이다. 그리고 *HNI*와 *CNI*는 이 메시지가 *CN*에 전달되었을 때 *kbm*(*binding management key*) 생성에 필요한 *CN*의 넌스 색인들이다. 마지막으로 *MAC*값은 *kbm*으로 {*CoA, CNA, BU*메시지}를 해쉬한 것이다. 여기에서 *kbm*은 *CN*으로부터 수신한 {*HKT, CKT*}의 해쉬값(*kbm:= SHA1*(*HKT|CKT*))이다. 따라서 *kbm*은 *CN*의 기밀 요소인 *Kcn*, 넌스 색인값, 넌스값, *MN*의 *HoA*와 *CoA*가 결합되어 만들어진 것이다.

**(Step4)** *CN*이 *MN*으로부터 *BU*메시지를 수신하면 다음의 절차에 따라 *MN*의 위치정보를 *CN*의 *BCE*에 등록한다.

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

*HKT*와 *CKT*로부터 *kbm*(*kbm*:= *SHA1*(*HKT*|*CKT*))을 계산한다. 이를 이용하여 *HMAC_SHA1*(*kbm*, (*CoA*|*CNA*|*BU* 메시지))을 계산한다. 계산된 이 *MAC*값이 *BU*메시지에서 전송된 *MAC*값과 동일하면 *MN*으로부터 받은 위조되지 않은 메시지로 판단하여 {*HoA*, *CoA*}로 구성된 *BCE*를 생성한다.

### 1.2 RR프로토콜 분석

*BU*메시지 보호를 위해 *IETF mobileip WG*에서 드래프트 문서로 제안한 기존 *RR*프로토콜의 주 목적은 *CN* 입장에서 정당한 *MN*이 *BU*메시지를 보냈는지를 검증하는데 있다. 이 방법은 *HA*와 *CN* 사이의 경로에 위치한 공격자에 대해서는 보안 취약성이 존재하지만 인터넷의 어떤 위치에서나 행할 수 있는 위조된 *BU* 메시지 사용을 제한할 수 있다[4]. 본 논문과 관련하여 *RR*프로토콜의 특징을 요약하면 다음과 같다.

(1) *MN*이 *CN*으로부터 *HA*를 경유하는 첫 번째 패킷을 수신했을 때 안전한 최적경로설정을 위해 *RR*프로토콜이 구동된다.

(2) 최종적인 *BU*메시지 전달을 위해 총 4개의 메시지(*HoTI, HoT, CoTI, CoT*)가 교환되며 이들 메시지가 통과되는 경로는 총 8경로(*MN*과 *CN* 간 직접 2경로, *MN*과 *HA*간 3경로, *HA*와 *CN*간 3경로)이다.

(3) *CN*과 *MN*간 직접 그리고 *HA*를 경유하는 서로 다른 두 경로를 통해서 메시지가 송수신되는 이유는 *CN*에서 *MN*으로 송신하는 메시지가 *MN*의 *HoA*와 *CoA*로 전달이 가능함을 확인하기 위해서이다.

(4) 쿠키(*HIC, CIC*)의 사용은 첫째, *HoTI*와 *HoT* 그리고 *CoTI*와 *CoT*쌍의 일치성 검증에 사용되며, 둘째, *HoTI*와 *CoTI* 메시지를 수신하지 않은 노드에 의해 보내진 위장된 응답을 추출하기 위한 것이다.

(5) 넌스 색인(*HNI, CNI*)을 사용하는 이유는 *CN*의 넌스값을 노출시키지 않으면서 최종 메시지인 *BU*메시지를 받을 때 까지 비상태유지(*Stateless*) 방식으로 수행됨을 의미한다.

(6) *HKT*와 *CKT*의 역할은 *CN*과 *MN*간에 형성된 직접경로와 *HA*를 경유하는 경로를 사용하여 *CN*으로부터 두 메시지(*HoT, CoT*)를 수신한 *MN*만이 *kbm* 생성을 통해 *BU*메시지를 작성할 수 있음을 의미한다. 또한 *BU*메시지에 포함된 *MAC*값을 통해 무결성 보안 서비스를 제공하며, *BU*메시지를 받은 *CN*이 *HoA*와 *SA*(*Source Address*)인 *CoA*를 이용하여 *MAC*값을 생성한 후 *BU*메시지에 포함된 *MAC*값과 비교함으로서 메시지 인증 보안 서비스를 제공한다.

## 2. 개선된 RR프로토콜 제안

제안 동기는 다음과 같다. *MN*이 외부네트워크로 이동하면 *MN*은 자신의 현 위치정보를 *BU*메시지를 통해 *HA*의 *BCE*에 등록한다. 이때 참고문헌 [4] *RR*프로토콜과 마찬가지로 *MN*과 *HA*간에는 안전한 *IPsec ESP* 채널이 사용된다. 따라서 *HA*가 유지하는 *MN*의 위치정보는 위조되지 않은 정확한 정보이다. 따라서 본 논문에서 제안한 기본 아이디어는 *RR*프로토콜의 시작 주체 및 시점을 기존의 *MN*에서 *HA*로 변경하는 것이다. 이러한 변경이 가능한 이유는 *HA*가 *MN*의 현 위치정보를 *IPsec ESP* 채널을 통해 항상 안전하게 유지하기 때문이다. 이렇게 함으로써 참고문헌 [4]와 동일 수준의 보안서비스를 제공하면서 최적경로설정 시간을 단축시킬 수 있다. 또한 하나의 메시지만을 *CN*에게 전달하여 *HKT*와 *CKT*를 생성한 후 이를 *MN*에게 전달함으로써 4개의 메시지를 2개로 줄일 수 있다. 메시지가 통과되는 경로는 총 8 경로에서 6 경로로 줄어들게 되어 네트워크 부담을 경감시킨다.

### 2.1 개선된 RR프로토콜 동작절차

개선된 *RR*프로토콜은 참고문헌 [4]의 *RR*프로토콜과 마찬가지로 *MN*과 *CN*간에 어떤 보안 인프라 구조도 존재하지 않음을 전제로 하며, *CN*이 수신한 *BU*메시지가 적법한 *MN*으로부터 제공된 것임을 보장한다. 그림 2에 개선된 *RR*프로토콜을 보여주고 있다. 그림 2에서 ⓪과 같이 *HA*가 *CN*으로부터 *MN*으로 향하는

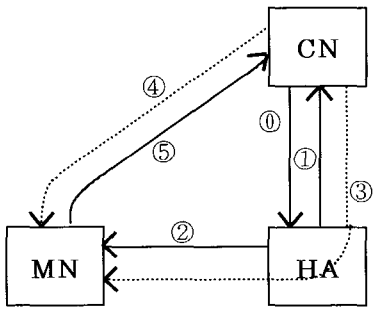


그림 2. 개선된 RR프로토콜
Fig. 2 proposal RR proocol

첫 번째 패킷을 수신하면 최적경로설정이 시작된다.

**(Step1)** *HA*는 다음의 ①과 ②와 같은 2개의 메시지를 생성하여 각각 *CN*과 *MN*에게 송신한다.

① *HA* → *CN*: *HoCoTI*
② *HA* → *MN*: *HoCoTI*플래그, *HoCoIC*

첫 번째 메시지는 *HA*가 *CN*에게 보내는 *HoCoTI* (*Home & Care-of Test Init*)이다. 이 메시지는 *HA*에 저장되어 있는 *MN*의 *BCE* 정보로 {*HoA*, *CoA*}를 참조하여 (*SA*(*HoA*), *DA*(*CNA*): *HoCoIC*, *CoA*)로 구성된다. 여기에서 *SA*는 발신지 주소, *DA*는 목적지 주소, *CNA*(*Correspondent Node Address*)는 *CN*의 주소를 나타낸다. *HoCoIC*(*Home & Care-of Init Cookie*)는 *MN*이 *CN*으로부터 수신할 *HoT*와 *CoT* 메시지에 대한 일치성 검증을 위한 것이다. 두 번째 메시지는 *MN*으로 송신되는 ⓘ 패킷에 *HoCoTI*플래그와 *HoCoIC*를 피기백시켜 보낸다. *HoCoTI*플래그는 *MN*에게 개선된 *RR* 프로토콜이 *HA*에 의해 시작되었음을 알리기 위함이다. *HoCoIC*는 *MN*이 수신한 *HoT*와 *CoT*가 *HoCoTI*메시지를 수신한 *CN*에 의해 보내진 것임을 검증하는데 사용된다. 이때 *MN*은 *HoCoIC*와 *CNA*를 *BU*목록에 저장한다.

**(Step2)** *HoCoTI* 메시지를 수신한 *CN*은 ③과 ④와 같은 두개의 메시지를 생성하여 *MN*에게 송신한다.

③ *CN* → *MN*(*HA* 경유): *HoT*
④ *CN* → *MN*: *CoT*

첫 번째 *HoT* 메시지는 *HA*를 경유하여 *MN*에게 송신한다. 이 메시지는 (*SA*(*CNA*), *DA*(*HoA*): *HoCoIC*, *HNI*, *HKT*(*first*(64, *HMAC_SHA1*(*Kcn*, (*HoA*|*nonce*|0))))로 구성된다. 이 메시지 구성 요소들의 기능 및 의미는 1.2절에서 설명한 참고문헌 [4] *RR*프로토콜과 동일하다. 두 번째 *CoT* 메시지를 *MN*에게 직접 송신한다. 이 메시지는 (*SA*(*CNA*), *DA*(*CoA*): *HoCoIC*, *CNI*, *CKT*(*first*(64, *HMAC_SHA1*(*Kcn*, (*CoA*|*nonce*|1))))로 구성된다. 역시 이 메시지 구성 요소들의 기능 및 의미는 참고문헌 [4] *RR*프로토콜과 동일하다.

**(Step3)** *MN*이 *HoT*와 *CoT*를 수신하면 다음과 같은 처리 후 *BU*메시지를 생성하여 *CN*에게 송신한다.

*HoT*와 *CoT*를 수신한 *MN*은 메시지의 발신지 주소로부터 *CNA*를 추출하여 *BU*목록에 저장된 *CNA*와 비교하여 일치성을 검사하고 저장된 *HoCoIC*와 ③ 그리고 ④ 메시지의 *HoCoIC*를 비교하여 일치하면 *HoCoTI*를 수신했던 정당한 *CN*이 보낸 메시지임을 알게 된다. 그리고 참고문헌 [4] *RR*프로토콜에서와 같이 *kbm*을 계산하고 이를 통해 *BU*메시지를 생성하여 *CN*에게 송신한다.

⑤ *MN* → *CN*: *BU*메시지

**(Step4)** *CN*이 *MN*으로부터 *BU*메시지를 수신하면 다음의 절차에 따라 *MN*의 위치정보를 *CN*의 *BCE*에 등록한다.

*BU*메시지를 수신한 *CN*은 참고문헌 [4] RR프로토콜에서와 같은 방법으로 *HKT*와 *CKT* 생성 후 *kbm*을 생성하여 *MAC*값을 계산한다. 그리고 계산된 *MAC*값을 *BU*메시지내의 *MAC*값과 비교하여 동일하면 적법한 *MN*으로부터 받은 위조되지 않은 *BU*메시지로 판단하여 *MN*의 위치정보를 나타내는 {*HoA*, *CoA*}로 구성된 *BCE*를 생성한다.

### 2.2 참고문헌 [4]의 RR프로토콜과 개선된 RR프로토콜의 비교

비교평가를 위해서 참고문헌 [4] *RR*프로토콜과 개선된 *RR*프로토콜의 상세한 동작절차를 그림 3과 그림 4에 각각 보였다. 두 그림을 바탕으로 두 프로토콜의 성능을 다음과 같이 3가지 측면에서 비교할 수 있다.

첫째, 최적경로설정에 필요한 메시지가 네트워크를 통과하는 경로 수를 비교할 수 있다. 이는 네트워크 부하에 영향을 주는 요소이다. 그림 3과 그림 4에서 보듯이 *BU*메시지를 포함하면 참고문헌 [4] *RR*프로토콜은 총 9개인데 반해 개선된 *RR*프로토콜은 7개이다. 이는 개선된 *RR*프로토콜이 전체적인 네트워크 부담을 경감시킴을 의미한다.

둘째, *CN*이 그림에서 '*first packet*' 전송 후 *CN*에서 *MN*의 *BCE* 생성까지 소요되는 시간을 비교할 수 있다. 이는 *BCE*가 생성되기 전에 *MN*으로 보내지는 패킷들(*first packet*, *HoTI*, *HoT*)은 *HA*를 경유하기 때문에 이 패킷들에 대한 소요시간이 단축될수록 홈 네

트워크 및 HA의 부하를 경감시키기 때문이다. 그림 3과 그림 4에서 보듯이 참고문헌 [4]의 *RR*프로토콜과 제안 프로토콜의 *BCE* 생성시간은 다음 식 ①과 ② 같이 계산할 수 있다.

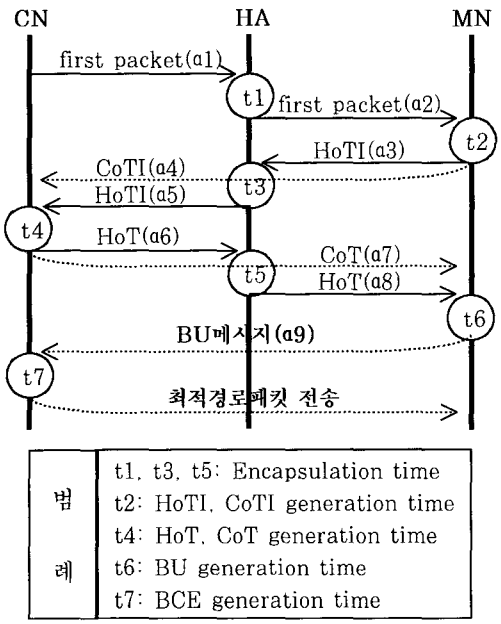


그림 3. 참고문헌 [4] RR프로토콜의 BCE 생성시간
Fig. 3 BCE generation time in Reference [4] RR protocol

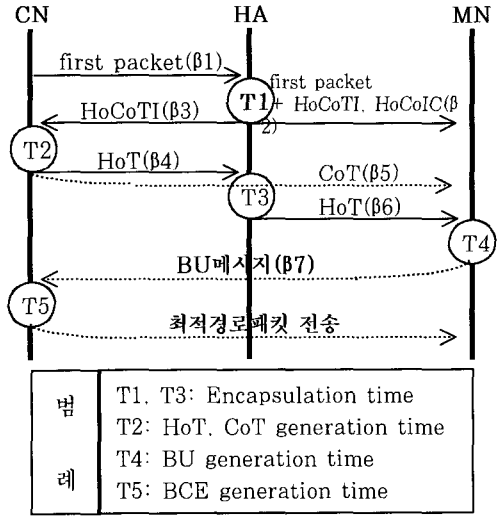


그림 4. 제안된 RR프로토콜의 BCE 생성시간
Fig. 4 BCE generation time in proposal RR protocol

*MN*의 *BCE* 생성시간 =
*P*(노드에서 메시지 처리 및 생성시간) +
*T*(메시지 전송시간)

참고문헌 [4]에서 *BCE* 생성시간 =
$P(t1 + t2 + t3 + t4 + t5 + t6 + t7) +$
$T(a1 + a2 + a3 + a5 + a6 + a8)$ ····· ①

제안방안에서 *BCE* 생성시간 =
$P(T1 + T2 + T3 + T4 + T5) +$
$T(\beta1 + \beta3 + \beta4 + \beta6)$ ····· ②

먼저 식 ①과 ②에서 메시지 처리 및 생성시간 *P*를 살펴보면 다음과 같다. 여기에서 인캡슐레이션(*Encapsulation*) 시간은 기존 방안과 제안방안 모두 같다고 가정한다. 즉, 그림 3에서 *t1*, *t3*, *t5* 각각은 그림 4에서 *T3* 시간과 같다. 또한 *CN*에서의 *HoT*와 *CoT* 생성시간, *BCE* 생성시간도 같다. 그리고 *MN*에서의 *BU*메시지 생성시간 역시 같다. 즉 그림 3에서 *t4*, *t6*, *t7*은 그림 4에서 *T2*, *T4*, *T5*와 각각 같다. 또한 참고문헌 [4] *RR*프로토콜에서 *t1*은 순수한 인캡슐레이션 시간이고 *t2*는 *HoTI* 메시지를 생성하고 이를 인캡슐레이션하는 시간이다. 제안 프로토콜에서 *T1*은 *HoCoTI* 생성하여 그림 2의 ⓪ 패킷에 피기백시켜 인캡슐레이션하는 시간이다. 따라서 *t2*와 *T1*은 근접한 소요시간이 된다. 이를 반영하여 각 프로토콜의 메시지 처리 및 생성시간 *P*를 계산하면 식 ①과 ②가 다음 식 ③과 ④ 처럼 정리된다.

참고문헌 [4]에서 $P$시간 $= t1 + t5$ ····· ③
제안방안에서 $P$시간 $= 0$ ····· ④

식 ③과 ④가 의미하는 것은 메시지 처리 및 생성시간 *P*가 제안 프로토콜이 참고문헌 [4]의 *RR*프로토콜보다 $(t1 + t5)$ 시간만큼 빠르다는 것을 나타낸다.

다음으로 메시지 전송시간을 살펴보면 다음과 같다. 참고문헌 [4] *RR*프로토콜에서 *MN*과 *CN*간의 메시지 전송은 두 방향으로 이루어진다. 한 방향은 *MN*과 *CN*간에 직접 이루어지고, 다른 하나의 방향은 *HA*를 경유하여 이루어진다. 전자의 메시지 전송시간은 후자의 메시지 전송시간보다 빠르다. 따라서 메시지 전송시간의 비교를 위해서는 후자의 전송시간을 고려할 수 있다. 이를 반영하여 생성한 식이 참고문헌 [4]에서 *T*시간과 제안방안에서 *T*시간이다.

상기의 두 프로토콜의 각 단계별 전송시간을 비교하면 $\alpha 1 = \beta 1$, $\alpha 5 = \beta 3$, $\alpha 6 = \beta 4$, $\alpha 8 = \beta 6$ 관계가 성립된다. 따라서 위 식에서 동일한 전송시간을 소거하면 다음과 같은 식 ⑤와 ⑥을 얻을 수 있다.

참고문헌 [4]에서 $T$시간 = $\alpha 2 + \alpha 3$ …… ⑤
제안방안에서 $T$시간 = $0$ …… ⑥

따라서 데이터 전송시간은 참고문헌 [4]가 제안방안 보다 ($\alpha 2 + \alpha 3$)만큼 데이터 전송시간이 느리다. 즉 제안 프로토콜이 기존 프로토콜보다 *HA*와 *MN*간에 메시지를 왕복전송에 걸리는 시간만큼 빠르다.

위에서 두 프로토콜을 비교를 위해 최종적인 메시지 처리 및 생성 시간 $P$와 메시지 전송시간 $T$를 원식에 반영하면 다음과 같은 *MN*의 *BCE* 생성시간을 식 ⑦과 ⑧ 처럼 계산할 수 있다.

참고문헌 [4]에서 *BCE* 생성시간 =
($t1 + t5$) + ($\alpha 2 + \alpha 3$) …… ⑦
제안방안에서 *BCE* 생성시간 = 0 …… ⑧

위의 식 ⑦과 ⑧에서 본바와 같이 제안 프로토콜이 참고문헌 [4]의 *RR*프로토콜보다 *MN*의 *BCE*을 {($t1 + t5$) + ($\alpha 2 + \alpha 3$)} 시간만큼 빠르게 생성함을 의미한다.

셋째, 제안방안에서 *HA*의 부하 비교이다. 기존방안에서는 *HA*가 단순히 인캡슐레이션 기능만을 담당하는데 반해 제안방안에서는 *HoCoTI* 생성과 *HoCoTI* 플래그 및 *HoCoIC*를 추가하여 인캡슐레이션하는 부담을 안고 있다. 즉, 제안방안에서는 *HoCoTI* 생성시간이 추가적 부담이다. 그러나 이는 단순한 난수(*HoCoIC*) 생성과 이를 데이터로 하여 패킷을 생성하기 때문에 소요시간이 짧다. 그리고 둘째 비교분석에서 본 바와 같이 제안방안이 *HA*를 경유하는 패킷수가 감소하기 때문에 이러한 *HA* 부담을 상쇄할 수 있다.

상기의 비교분석 결과를 정리하면 다음과 같은 이점이 있다. 첫째, *HA*가 *MN*으로 향하는 첫 번째 패킷 수신 시점에서 개선된 *RR*프로토콜이 시작되기 때문에 *CN*에서 *MN*으로 전송되는 패킷의 최적경로설정 확률을 높인다. 이는 *HA*를 경유하는 패킷을 줄임으로써 통신지연 현상 및 네트워크 부하를 경감시킴을 의미한다. 둘째, *HA*가 *HoCoTI*를 *CN*에게 직접 보냄으로써 *MN*에서 *HA*로 전송되는 *HoTI* 메시지와 *MN*에서 *CN*으로 전송되는 *CoTI* 메시지가 제거되어 *RR*프로토콜에 의한 네트워크 부하를 줄인다. 셋째, 기존 *RR*프로토콜과 개선된 *RR*프로토콜의 보안 수준은 동일하다. 이는 두 프로토콜 모두 *MN*이 *BU*메시지 생성 시 필요한 *Kbm*을 *CN*과 *MN*간에 형성된 직접경로와 *HA*를 경유하는 경로를 통해서 도착한 *HoT*와 *CoT* 메시지 내의 *HKT*와 *CKT*를 이용하여 생성하기 때문이다.

## Ⅲ. 결 론

본 논문에서는 참고문헌 [4] *RR*프로토콜의 보안수준은 동일하게 유지하고 성능만을 개선하는 방안을 제안하였다. 개선된 *RR*프로토콜의 동작환경은 참고문헌 [4] *RR*프로토콜과 마찬가지로 *MN*과 *CN*간에 사전에 설정된 보안 인프라 구조를 정의하지 않는다. 다만 참고문헌 [4]의 *RR*프로토콜과 마찬가지로 *MN*과 *HA*간에는 *IPsec ESP* 보안 인프라 구조 정의를 전제로 한다.

이러한 환경을 전제로 개선된 *RR*프로토콜이 *BU*메시지 전송 전에 교환되는 메시지 수 및 경로 수를 감소시킴으로써 네트워크 부하 및 최적경로설정 확률이 개선되었음을 보였다. 이와 더불어 보안수준은 참고문헌 [4] *RR*프로토콜과 동일하다.

## 참 고 문 헌


[1] P. Nikander, C. Perkins, "Binding Authentication Key Establishment Protocol for Mobile IPv6," ⟨draft-perkins-bake-01.txt⟩, July 2001.

[2] S. Bradner, A. Mankin, J. Schiller, "A Framework for Purpose Built Keys(PBK)," ⟨draft-bradner-pbk-frame-00.txt⟩, February 2001.

[3] Stefano M. Faccin, Franck Le, "Dynamic Diffie Hellman based Key Distribution for Mobile IPv6," ⟨draft-le-mobileip-dh-00.txt⟩, October 2001.

[4] C. Perkins, D. Johnson, "Mobility Support in IPv6," ⟨draft-ietf-mobileip-ipv6-21.txt⟩, Fe- bruary 2003.

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

[6] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents," <draft-ietf-mobileip-mipv6-ha-ipsec-03.txt>, February 2003.
[7] M. Roe, T. Aura, G. O'Shea, J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments," <draft-roe-mobileip-updateauth-02.txt>, February 2002.
[8] National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180-1, April 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

## 〈著者紹介〉

**이 달 원 (Dal-won Lee)**
1996년 : 충남대학교 화학과 이학사
2000년 : 배재대학교 컴퓨터공학과 공학석사
2001년~현재 : 배재대학교 컴퓨터공학과 박사과정
<관심분야> 정보보호, 컴퓨터네트워크

**황 일 선 (Il-sun Hwang)**
2001년 : 호원대학교 전자계산학과 공학사
2004년 : 성균관대학교 컴퓨터공학과 공학석사
2004년~현재 : 성균관대학교 컴퓨터공학과 박사과정
1981년~현재 : 한국과학기술정보연구원, 초고속연구망사업실 실장
<관심분야> Grid 네트워킹, 멀티미디어 스트리밍

**손 승 원 (Seung-won Shon)**
1984년 : 경북대학교 전자공학과 공학사
1994년 : 연세대학교 전자공학과 공학석사
1999년 : 충북대학교 컴퓨터공학과 공학박사
1996년 : 정보통신기술사
1991년~현재 : 한국전자통신연구원 책임연구원, 정보보호연구단장
<관심분야> IC Card, Biometry, Active Network

**조 인 준 (In-june Jo)**
1982년 : 전남대학교 계산통계학과 공학사
1985년 : 전남대학교 전자계산학과 공학석사
1999년 : 아주대학교 컴퓨터공학과 공학박사
1983년~1994년 : 한국전자통신연구원 선임연구원
1994년~현재 : 배재대학교 컴퓨터공학과 교수
<관심분야> 정보보호, 컴퓨터네트워크, 전산조직응용