중첩 이동망에서 효율적이고 안전한 경로최적화 프로토콜

유호성*, 오희국*, 김상진**
*한양대학교 컴퓨터공학과
**한국기술교육대학교 인터넷미디어공학부
e-mail: ryuhosung@hanyang..ac.kr

An Efficient and Secure Route Optimization Protocol in Nested Network Mobility

HoSung Ryu*, HeeKuck Oh**, SangJin Kim*
*Dept of Computer Science and Engineering, HanYang University
**School of Internet Media Engineering Korea University of Technology and University

요 약

유비쿼터스 사회에는 도서관, 커피숍과 같은 공공장소와 자동차, 전철, 비행기등과 같은 대중교통에도 인터넷에 접근할 수 있게 될 것이다. 또한 모든 통신은 끊임없는 인터넷이 지원되어야 하고, 세션이 유지되어야 하며, 이동 중에 통신이 끊어지지 않고, 라우팅이 효율적으로 이루어져야 한다. 이러한 요구를 반영할 수 있는 네트워크 이동성 기술은 이동 IPv6이 가지고 있는 근본적이고, 비효율적인 삼각 라우팅 문제와 중첩된 환경에서 삼각라우팅 문제가 반복되는 핀볼 라우팅 문제를 가지고 있다. 본 논문은 중첩환경의 라우팅 문제를 조사하고, 해결하기 위해 이미 제안된 내용들을 분석하고, 효율성과 안전성을 만족할 수 있는 프로토콜을 제안한다.

1. 서론

가까운 미래에 다가올 유비쿼터스 사회에는 도서관, 커피숍과 같은 공공장소와 자동차, 전철, 비행기등과 같은 대중교통에도 인터넷에 접근할 수 있는 인프라를 가지게 될 것이다. 유비쿼터스 사회를 구현하기 위해 이동통신 시스템은 많은 유연성이 요구된다. 또한 많은 이동 통신은 무선 장치들을 허용할 수 있는 확장성이 필요하다.

고정된 노드에 IP주소를 할당할 경우 IP주소는 자신의 신원과 위치를 나타내게 된다. 하지만 이동이 가능한 노드의 경우 끊임없는 통신을 위해 자신이 이동한 위치에 따라서 IP주소를 사용한다. IP주소가 바뀌게 되면 자신의 통신을 지속할 수 있지만, 기존의 신원을 인증할 수 없게 된다. 따라서 이러한 문제를 해결하기 위해 이동 IPv6(MIPv6, mobile IPv6)[1],[2]는 IP주소의 신원과 위치 표현의 기능을 분리하였다. 즉 각 노드는 신원을 표현 하는 홈 주소(HoA, Home Address)와 위치를 표현 하는 보조 주소(CoA, Care of Address)를 사용하여 단말의 이동성을 지원하였다. 그러나 기술의 발전으로 인하여 전체 네트워크의 이동성에 대한 관심과 요구가 확산되었으며, 이러한 요구를 반영하여 IETF(Internet Engineering Task Force)는 네트워크의 모든 노드들의 인터넷 접속점이 변경되더라도 MR(이동 라우터, Mobile Router)를 통해 연속적인 인터넷 접속을 지원하는 망 이동성(NEMO, Network Mobility)기술을 제안하고, 표준화를 진행하고 있다[3].

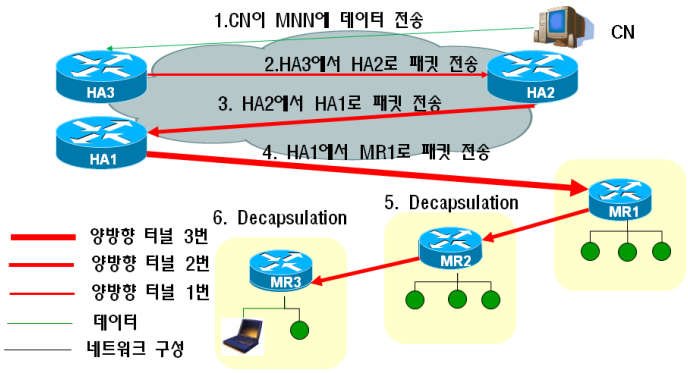
본 논문은 아래와 같이 구성되어 있다. 2절은 망 이동성의 용어와 표준 지원 프로토콜의 비효율적인 삼각 라우팅이 반복되는 핀볼 라우팅을 설명하고, 3절은 경로최적화의 필요성에 대해 이야기 하고, 4절을 통해 기존에 제안된 경로최적화 기법들을 분석한다. 5절에서는 본 논문에서 제안하는 경로 최적화 프로토콜을 설명한다. 그리고 6절은 이미 제안된 프로토콜과 본 논문이 제안하는 프로토콜을 안전성 측면으로 비교 분석한 후, 마지막으로 7절을 통해 결론을 내리고 마치도록 한다.

2. 네트워크 이동성

망 이동성은 비행기, 전철, 자동차와 같은 이동 수단에 이동 가능한 라우터를 설치하여 그에 포함된 많은 노드들

*본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성 지원사업의 연구결과로 수행되었음.

† 주저자, ryuhosung@hanyang.ac.kr
hkoh@hanyang.ac.kr
‡ 교신저자, sangjin@kut.ac.kr



(그림 1) 중첩 구조의 핀볼 라우팅

에게 인터넷 접근성을 지원해주는 기술이다. 이동 네트워크(mobile network)는 망 이동성 지원 프로토콜이 구현되어 있으며 이동 가능한 네트워크를 이야기한다[4].

4세대 이동통신에서는 UMTS, WLAN, Bluetooth와 같은 다양한 유/무선 네트워크가 통합되고, 대역폭과 지연을 고려한 망 연동(Vertical handover)을 지원해야 한다. 이러한 4세대 이동 통신의 요구사항을 만족하기 위한 기술로 망 이동성 기술이 이야기 되고 있다.

중첩된 이동망 환경에서 망 이동성 기본 지원 프로토콜(NEMO Basic Support Protocol)은 그림1과 같이 동작한다[5].

3. 경로최적화

대응 노드와 이동 네트워크에 속한 단말이 통신을 하게 될 때, 이동 네트워크는 항상 홈 대리인을 거쳐서 통신을 진행하게 된다. 이동 네트워크와 이동 네트워크에 속한 단말은 불필요하게 홈 대리인을 경유하는 문제를 가지게 되며 이를 삼각 라우팅 문제라고 이야기 한다. 중첩된 이동 네트워크에서는 삼각 라우팅 문제가 반복적으로 발생하게 된다. 이러한 문제는 아래와 같은 단점을 발생시킨다[6].

홈 대리인, 대응 노드, 이동 네트워크에 속한 단말의 통신 거리가 가까울 경우에는 문제가 많이 되지 않지만, 대응 노드와 이동 네트워크에 속한 단말은 근접하고 홈 대리인이 상당히 먼 거리에 있을 경우에는 통신거리에 비해 라우팅 시간과 지연이 길어지게 된다.

홈 대리인과 이동 라우터 사이에 양방향 터널이 생성되기 때문에, 각 패킷의 헤더 마다 320 bits가 추가되게 된다. 예를 들어 10ms 마다 패킷을 전송하게 될 경우, 32kbps의 헤더 과부하가 걸리게 된다. 캡슐화와 역 캡슐화 과정의 추가 연산이 발생하게 되어 전체적인 연산 지연을 가중 시킨다.

4. 관련연구

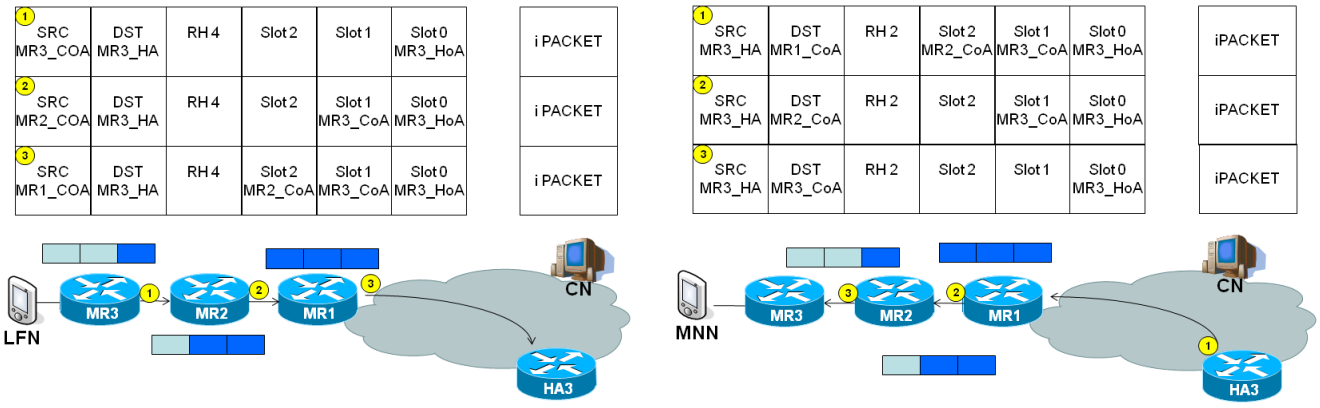
4.1 표기법

표 1. 표기법

표기	의미
MAC	메시지 인증코드 Hash함수를 통하여 계산됨
Nounce	난스
M	전체 메시지, 패킷의 전체
SRC	발신지 주소
DST	목적지 주소
||	비트 결합
K_{MRi}	*i*번째 이동 라우터의 세션키 키
n	중첩 레벨
+K/-K	MR과 HA가 공유하고 있는 공개키 쌍
K	MR과 HA가 공유하고 있는 비밀키
Sn	RRH기법의 사용하는 중첩된 이동 라우터를 기록하는 RRH의 n번째 Slot

4.2 RRH

RRH기법[7]은 기존에 IPv6의 확장헤더로 존재하던 라우팅 헤더에 새로운 헤더 형태를 추가한 기법이다. 그림 2.(a)와 같은 역방향 패킷 전달에는 라우팅 헤더의 타입정보에 4번 타입(RH 4)으로 기록하고 패킷 헤더에 자신이 속한 중첩 이동 네트워크의 모든 라우터 리스트를 기록한다. 그림 2.(b)와 같은 정방향 패킷 전달에는 라우팅 헤더의 타입정보에 2번 타입(RH 2)으로 기록하고, 패킷 헤더



(a) 역방향 패킷 전달 (b) 정방향 패킷 전달

(그림 2) RRH 프로토콜

에 기록된 주소들을 거쳐서 패킷을 전송하게 된다.

그림 2.(a)과 같이 이동 라우터3은 자신의 홈 대리인에게 패킷을 전송할 때, 중첩된 네트워크의 깊이를 Tree Discovery 기법[8]을 이용하여 확인한 후, 그 깊이만큼 라우팅 헤더의 슬롯을 만들어 패킷을 전송한다. 이 패킷을 받은 중간에 위치하고 있는 이동 라우터들은 자신이 받았던 패킷의 발신지 주소를 다음 차례의 슬롯에 넣고, 발신지 주소에 자신의 주소를 넣어 다시 전송한다. 이와 같은 과정을 거치게 되면 홈 대리인이 패킷을 수신할 때에는 모든 슬롯에 패킷이 거쳐 온 이동 라우터의 리스트들이 기록되게 되며, 발신지 주소에는 최상위 라우터의 보조 주소가 기록된다.

RRH 기법은 아래와 같은 보안성의 문제점을 가지고 있다. 첫째, 최상위 라우터와 홈 대리인 사이의 라우터 중

그림3과 같이 중첩구조 속에 있는 중간에 있는 이동 라우터들은 자신이 기록하는 필드들을 다음과 같이 암호화하여 기록한다. 단 최하위 라우터일 경우에는 제외한다.

$$\{\text{Slot } n\text{-}1\}K_{MRn} \quad (1)$$

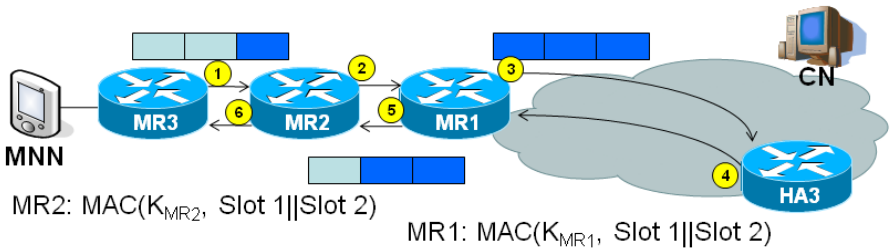
식1과 같이 자신의 개인키로 Slot을 암호화하게 되면 암호화한 자신만 복호화 할 수 있게 되므로, 자신이 아닌 다른 경로로 패킷이 전송될 경우 다음 목적지를 알 수 없게 하여 패킷의 진행을 막는다.

$$MAC(K_{MRn}, \text{Slot } 0 \parallel \ldots \parallel \text{Slot } n\text{-}1) \quad (2)$$

식 2와 같이 자신이 받았던 패킷의 MAC값을 계산하여 가지고 있으므로, 자신 이후에 라우팅 헤더의 변조를 통한 Re-direct공격을 막을 수 있다.

그러나 위 기법은 RRH기법에 안전성을 보완하였지만, 부분적인 라우팅 헤더 Slot들의 기밀성과 무결성과 인증

① SRC MR3_CoA	DST MR3_HA	Slot 2	Slot 1	Slot 0 MR3_HoA	④ SRC MR3_HA	DST MR1_CoA	Slot 2 {MR2_CoA} K_{MR1}	Slot 1 {MR3_CoA} K_{MR2}	Slot 0 MR3_HoA
② SRC MR2_CoA	DST MR3_HA	Slot 2	Slot 1 {MR3_CoA} K_{MR2}	Slot 0 MR3_HoA	⑤ SRC MR3_HA	DST MR2_CoA	Slot 2	Slot 1 {MR3_CoA} K_{MR2}	Slot 0 MR3_HoA
③ SRC MR1_CoA	DST MR3_HA	Slot 2 {MR2_CoA} K_{MR1}	Slot 1 {MR3_CoA} K_{MR2}	Slot 0 MR3_HoA	⑥ SRC MR3_HA	DST MR3_CoA	Slot 2	Slot 1	Slot 0 MR3_HoA



(그림 3) Secure RRH 프로토콜

하나가 라우팅 헤더의 내용을 수정하게 되면 모든 패킷은 수정된 주소를 거쳐 패킷이 전달 되게 된다.

둘째, RRH 기법을 사용한 패킷은 IPSec을 사용하였더라도, 역방향 패킷인 경우 발신지 주소를 위조 할 수 있으며, 정방향 패킷인 경우 목적지 주소와 라우팅 헤더의 정보 등을 바꿀 수 있다. RRH 기법을 사용하게 되면 중첩된 라우터들에 의해 발신지 주소와 목적지 주소가 바뀌게 된다. IPSec은 기본적으로 발신지 주소와 목적지 주소를 인증 헤더와 ESP를 이용하여 보호하지만, 중값에 값들이 바뀌는 항목들은 보안 서비스들이 지원되지 않는다.

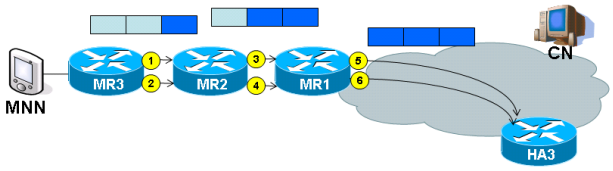
4.3 secure RRH

RRH의 보안상의 문제점을 해결하기 위해 제안되어진 기법으로, 라우팅 헤더의 Slot들의 내용을 보호하기 위해 제안되었다[9].

을 지원한다. 그러나 발신지 주소와 목적지 주소의 무결성은 보장하지 않는다.

5. 제안하는 프로토콜

제안하는 프로토콜은 RRH 기법을 안전하게 동작할 수 있도록 한다. 따라서 기존의 RRH와 Secure RRH가 만족하지 못하던 무결성을 만족한다. 제안하는 프로토콜은 아래와 같이 동작한다.



(그림 4) 제안하는 프로토콜

① {M, SRC, DST}K, {s0}K, +K
② {M, SRC, DST}K, {s0}K

{{s1}K_{MR2i}, K_{MR2i}, N_{MR2i}}+K,{SRC, DST}K_{MR2i}, +K

③ {M, SRC, DST}K, {s0}K,
{{s1}K_{MR2i}, K_{MR2i}, N_{MR2i}}+K, {SRC, DST}K_{MR2i},
{{s2}K_{MR1i}, K_{MR1i}, N_{MR1i}}+K, {SRC, DST}K_{MR1i} ,+K

RRH 기법을 이용하여 상위의 이동 라우터들은 자신들이 기록해야 하는 주소를 MR3가 공개한 공개키 암호화한다. 그리고 임의로 생성한 키로 Slot을 암호화 하고, 차후 자신이 확인할 수 있는 Index의 의미를 가지는 난스와 키를 공개하여 상위의 이동 라우터에게 전달한다. 최종적으로 이 메시지를 전송받은 HA3는 MR3와 공유하고 있는 -K를 이용하여 메시지를 해독화하고, 패킷의 내용의 주소들의 무결성과 Slot들의 무결성을 확인한다. 그리고 안전한 통신을 위해 아래와 같이 이동 라우터들에게 공개할 세션키를 난스를 이용하여 식(3)(4)와 같이 생성한다. 그리고 공개된 키와 난스를 사용하여 4번 메시지를 만들어서 최상위 이동 라우터에게 전달한다.

$K_1 = HMAC(K, N_1||...|| N_n|| Counter\ I)$ (3)

$K_n = HMAC(K, K_{n-1})$ (4)

④ {M}K, {s2}K_n, {s1}K_{n-1}, {s0}K
{SRC, DST, K_n, K_{n-1}}K_{MR1i}, N_{MR1i}
{SRC, DST, K_{n-1}, K_{n-2}}K_{MR2i}, N_{MR2i}

⑤ {M}K, {s1}K_{n-1}, {s0}K
{SRC, DST, K_{n-1}, K_{n-2}}K_{MR2i}, N_{MR2i}

⑥ {M}K, {s0}K

위 메시지를 받은 이동 라우터는 자신이 생성한 난스를 통해 HA가 생성한 세션키($K_{1,2,...,n}$)를 안전하게 해당 MR들에게 전달한다. 모든 과정을 마치게 되면 모든 이동라우터는 자신이 통신해야 하는 이동 라우터와 공유된 세션키를 소유한다. 공유된 세션키를 이용하여 각 이동 라우터간에 지수연산을 사용하지 않는 안전하고 효율적인 통신이 가능하게 된다.

6. 분석

망 이동성 기본프로토콜은 양방향의 터널과 IPSec의 AH[10]와 ESP[11]를 사용하여 안전한 통신을 지원하였다. 하지만 이러한 통신은 이동 네트워크가 중첩되게 되면, 핀볼라우팅 문제가 발생하게 된다. 핀볼 라우팅 문제를 해결하기 위해 제안된 RRH기법은 보안을 고려하지 않아 많은 바인딩 갱신 공격 및 경로변경공격이 가능하다는 단점을 가진다. 때문에 제안하는 프로토콜은 경로를 최적화 하고, 경로변경공격에 강건하도록 제안되었다.

<표 1> 보안 요구사항 분석

	기본+IPSec	RRH	Secure RRH	제안하는 방식
기밀성	O	X	△	O
인증	O	X	X	O
무결성	O	X	△	O

7. 결론

본 논문은 중첩된 이동 네트워크 환경의 안전한 통신 프로토콜에 대해 이야기 하였다. 네트워크 이동성의 기본 프로토콜인 경우 중첩된 이동 네트워크의 레벨이 깊어질수록 핀볼 라우팅 문제가 발생한다. 이러한 문제를 해결하기 위해 제안된 RRH방식인 경우에 적은 Overhead로 핀볼라우팅 문제를 해결하였지만, 보안에 대한 고려가 이루어 지지 않았었다. RRH의 보안요구사항을 만족하기 위해 제안된 Secure RRH 역시 IPSec을 사용하더라도 Slot, 발신지 주소, 목적지 주소의 무결성을 지원하지 못하는 문제를 남기고 있다. 본 논문은 Secure RRH가 만족하지 못하였던 보안 요구사항을 만족함으로, 최소한의 적은 비용으로 안전한 중첩 네트워크의 통신을 지원한다.

참고문헌

[1] C. Perkins, “IP Mobility support for IPv4”, IEFT, RFC 3344, Aug. 2002.

[2] D. Johnson, C. Perkins, J. Arkko, “Mobility support in IPv6”, IETF, RFC 3775, Jun. 2004.

[3] T. Ernst, “Network mobility support goals and requirements”, IETF, RFC 4886, Jul. 2007.

[4] T. Ernst, H-Y. Lach, “Network Mobility Support Terminology”, IETF, RFC 4885, Jul. 2007.

[5] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, “Network Mobility Basic Support Protocol”, IETF, RFC 3963, Jan. 2005.

[6] C. Ng, P. Thubert, M. Watari, F. Zhao, “Network Mobility Route Optimization Problem Statement”, IETF, RFC 4888, Jul. 2007.

[7] Thubert, P. and M. Molteni, “IPv6 Reverse Routing Header and its application to Mobile Networks”, Internet draft, IETF, Feb. 2007.

[8] Thubert, P. “Nested Nemo Tree Discovery”, Internet draft, IETF, Jul. 2007.

[9] Fan Zhao, S. Felix Wu, S.H Jung, H.G. Kim, ”Secure Reverse Routing Header Solution in NEMO”, Internet draft, IETF, Jul. 2004.

[10] S. Kent, R. Atkinson, “IP Authentication Header”, IETF, RFC 2402, Nov. 1998.

[11] S. Kent, R. Atkinson, “IP Encapsulating Security Payload”, IETF, RFC 4303, Dec. 2005.