네트워크 이동성 지원을 위한 인증된 경로 최적화(ATRO) 프로토콜

구중숙*, 김진근*, 박종혁** 구중두***, 이기성***
*경기대학교 정보보호학과
**고려대학교 컴퓨터정보통신공학과
***호원대학교 컴퓨터게임학부
e-mail:ygslee@howon.ac.kr

Authenticated Route Optimization (ATRO) Protocol for Network Mobility Support

Jung-Sook Koo*, Jin-Geun Kim*, Jong Hyeok Bak**,
Jung-Doo Koo***, Gi-Sung Lee***
*Dept. of Information Security, Kyonggi University
**Dept. of Computer and Information Communication Engineering, Korea University
***School of Computer Game, Howon University.

요 약

NEMO 기본 지원 (NEMO-BS, NEMO Basic Support) 프로토콜에서 MNN(Mobile Network Node)가 CN(Correspondent Node)과 통신을 하기 위해서는 항상 MR(Mobile Router)과 HA(Home Agent) 사이의 양방향 터널을 이용해야 한다. 그러나 NEMO-BS 방식은 노드 간 데이터 전송 지연과 부분 구간에 대한 공격 가능성이 존재한다.

따라서 본 논문에서는 NEMO를 위한 인증된 경로 최적화(ATRO) 프로토콜을 제안한다. MR은 홈 링크로부터 멀어졌다고 판단되면 MNN으로부터 위임 권한을 얻기 위해 권한 위임 프로토콜을 수행한다. 그런 후에 MR과 CN은 공개키 암호 방식을 이용하여 자신의 의탁주소(CoA, Care-of Address)를 MNN의 홈 주소(HoA, Home-of Address)와 매핑하기 위한 등록 과정을 수행한다. 이때 각 노드의 주소 소유권 증명을 위해 암호학적으로 생성한 주소(CGA, Cryptographically Generated Address)를 이용한다. 성능분석에서는 구간별 안전성과 종단간 패킷 전송 지연 시간을 통해 프로토콜을 분석한다.

1. 서론

이동 네트워크에 네트워크 이동성을 지원하기 위해 Internet Engineering Task Force (IETF)의 NEMO 워킹 그룹에서는 2005년에 모바일 IPv6에 기반한 네트워크 이동성 지원 프로토콜을 발표했다[1]. 하지만 NEMO-BS 프로토콜에서는 매번 MR과 HA 사이에 IPsec 양방향 터널을 통해서 통신을 수행해야 하기 때문에 삼각 경로 문제(tringle routing problem)가 발생할 수 있다. 특히, 이런 문제는 중첩 이동 네트워크 환경에서는 더욱 치명적이다. 왜냐하면 항상 중첩 MR들의 HA들을 경유해서 데이터를 전송해야 하기 때문이다. 이를 가리켜 핀볼 경로 문제(pinball routing problem)라고 한다. 다시 말해서, 두 통신 노드 간에 패킷 전송 지연이 크다. 따라서 경로 최적화 과정을 수행해야 한다. 하지만 이런 과정을 안전하게 수행하지 않을 경우 여러 공격으로부터 위협받을 수 있다.

따라서 본 논문에서는 경로 최적화와 전체 구간에 대한 안전성을 제공하기 위한 ATRO 프로토콜을 제안한다. ATRO 프로토콜을 수행하기 전에 MR은 MNN과 권한 위임 프로토콜을 선행해야 한다. 이때 두 노드 간에 IPsec 터널을 사용한다. 이에 대한 이용은 정당하다[2]. 성능 분석에서는 구간별 안전성 분석과 종단간의 패킷 지연 시간 비교를 통해 효율

성을 분석한다.

이 논문의 구성은 다음과 같다. 2장에서는 본 연구를 위한 연구배경에 대해서 살펴보고, 3장에서는 제안하는 ATRO 프로토콜에 대해 구체적으로 기술한다. 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 끝으로 5장에서는 결론과 향후 연구방향을 제시한다.

2. 관련연구

본 절에서는 네트워크에 이동성을 지원하기 위해 IETF NEMO 워킹 그룹에 의해 표준화된 NEMO-BS 프로토콜에 대해서 알아본다.

■ NEMO-BS 프로토콜[1]

네트워크 이동성이란 임의의 이동 네트워크가 외부 링크로 이동하여 인터넷에서의 접속점이 변경되었을 경우, 그 네트워크 내 단말은 이동과 무관하게 자신의 주소를 변경하지 않고 인터넷과 접속이 가능하도록 하는 기술이다. 또한 네트워크 내 단말이 인터넷 상의 임의의 대응 노드와 통신 중인 경우에도 단말과 대응노드 사이의 통신이 단절되지 않고 계속 서비스되어야 한다. RFC 3963[2]으로 표준화 된 네트워크 이동성 기본 지원 프로토콜은 MIPv6를 기반으로 하여 개개의 단말에 대한 이동 투명성을 제공하면서 네트워크 이동성을 관리하기 위한 프로토콜이다. HA는 MNN와 MR에 대한 이동성 관리 및 패킷 전달 기능을 수행하며 이동성 관리를 위해서 MR의 위치가 변경될 때마다 등록 과정을 통해서 현재의 주소 정보를 유지하게 된다. 이 정보를 기반으로 홈 네트워크에서 외부 네트워크로 터널을 생성하여 외부 망으로 이동한 노드에게 패킷을 전달한다. 그림 1은 기본적인 이동 네트워크에서의 NEMO-BS 과정을 보여준다. 이동 네트워크가 홈 링크에 있을 때 MNN은 MR을 통해 CN과 통신 중이다. 이 때, 이동 네트워크가 홈 링크를 떠나서 외부 링크로 이동하면 MR은 CoA를 주소 자동 설정 과정을 통해 생성하고 자신의 HA에게 이 주소를 등록한다. 이런 과정을 끝나고 나면 새로운 경로가 생성된다. 하지만 이 경로를 이용할 경우 항상 HA와 MR 간의 양방향 터널을 지나야 하기 때문에 삼각 라우팅 문제가 발생할 수 있다.

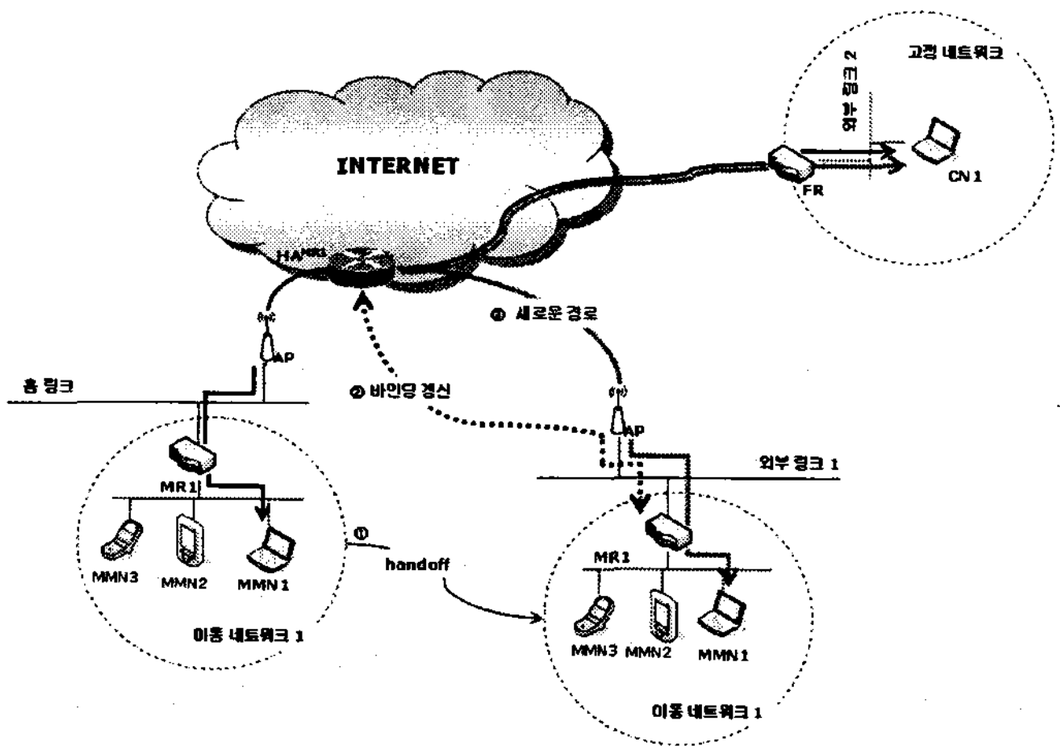

그림 1. NEMO 기본 지원 프로토콜

3. 프로토콜

본 ATRO 프로토콜은 MNN과 CN사이의 구간별 안전성 제공을 통한 전체 프로토콜의 안전성을 제공하고자 한다. 구간을 분류해보면, MNN와 MR 구간, MR와 HA 구간 그리고 MR와 CN구간으로 나뉜다. MNN과 MR구간은 MR과 HA 구간과 같이 IPsec을 이용한 양방향 터널을 이용한다. 이를 통해 데이터의 무결성뿐만 아니라 재생공격 방지 및 기밀성을 보장할 수 있다. 그림 2는 제안하는 ATRO 프로토콜의 전체 구조를 보여준다.

3.1. 시스템 설정

제안하는 프로토콜에서 MNN1과 MR1 그리고 MR1과 HA 사이에는 IPsec SA가 미리 확립되어 있다고 가정한다. 또한, CGA를 이용한 주소 생성 시에 각 노드의 HoA와 CoA에 들어가는 공개키는 같아야 한다. MR1과 CN은 전력 및 계산 능력에 제한을 받지 않는 노드이다. 마지막으로 제안하는 프로토콜은 표 1과 같은 시스템 파라미터를 가지며 이후부터는 다음에서 정의한 표기법을 사용한다.

표 1. 표기법

표기	의미
HoA_X/CoA_X	X 노드의 홈 주소와 의탁주소
K_{X-Y}	X 노드와 Y 노드 사이의 세션키
$+K_X/-K_X$	X 노드의 공개키와 세션키
procuration	MNN의 위임서
$sig(-K_X,M)$	X노드의 개인키로 생성한 서명
$hmac(K,M)$	비밀키 K를 이용한 메시지 M의 hmac 값
N_X	X 노드가 생성한 난스
L_{BU}/T_X	BU의 수명 및 X 노드의 타임 스탬프
$S^{\#}$	일련번호
m1||m2	메시지 m1과 m2의 비트 결합

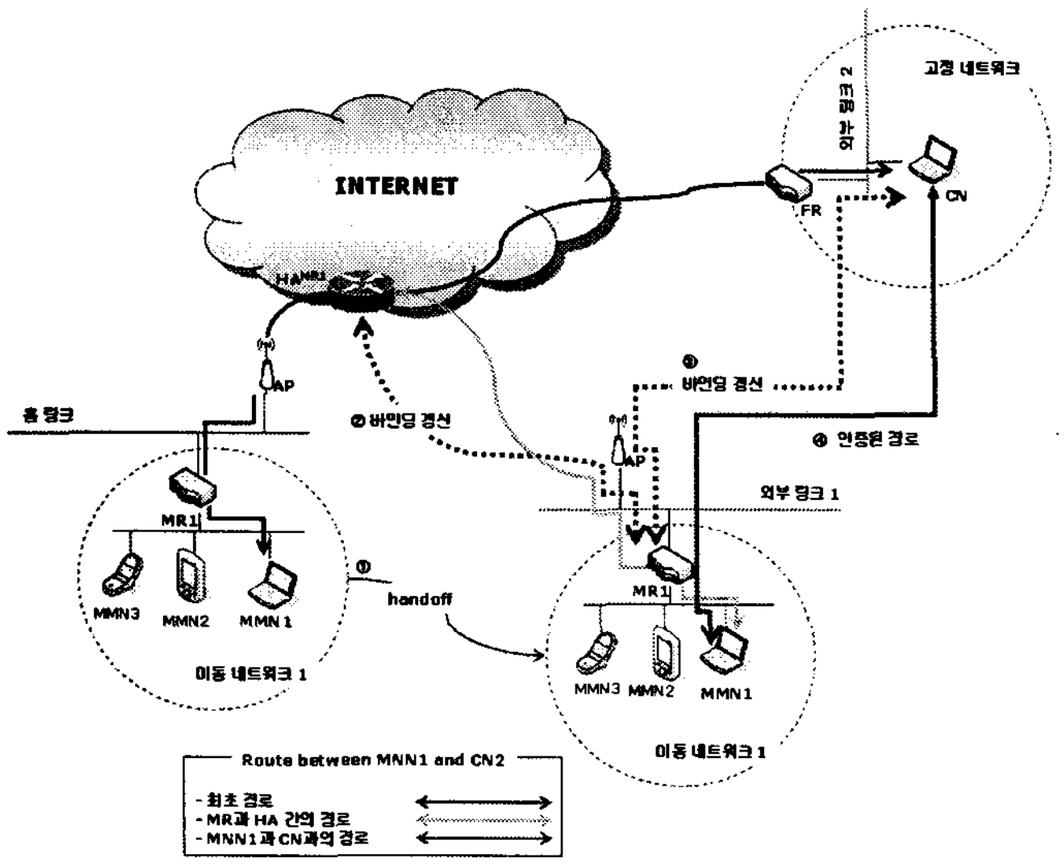

그림 2. MNN1과 CN사이의 인증된 경로 최적화

3.2. 권한 위임 프로토콜

위임 프로토콜은 IPsec을 이용한 양방향 터널을 통해서 전송된다. MR1과 MNN 사이의 프로토콜은 다음과 같다.

M1(MR1→MNN1): N_{MR}

M2(MNN1→MR1): N_{MR}, procuration, F=1

procuration은 MNN1이 MR1에게 부여한 위임 권한 증명서로서 자신의 홈 주소를 포함한 위임 승인을 인정하는 보안 파라미터가 포함되어있다. 이는 차후 MR1이 CN과 BU를 수행할 때 이용된다. F는 위임 권한 증명서에 대한 상태 정보다. 예를 들어, 다른 악의적인 노드가 위임 권한 증명서 발행 요청을 할 경우 이 값을 통해 증명서 발행 상태를 확인하고 발행 여부를 결정한다. MR1이 CN과 BU를 수행한 후에 MR1은 MNN1에게 위임 권한을 반환한다. MNN1은 플래그 F의 값을 0으로 설정한다.

3.3. ATRO 프로토콜

위임 프로토콜을 통해 위임 권한을 획득한 MR1은 먼저 자신의 HA와 양방향 터널을 통해 BU를 수행한다. 하지만 그림 1에서와 같이 이 단계에서 끝날 경우 MNN1은 CN과 통신하거나 인터넷에 접속하여 다른 서비스를 받을 경우 항상 MR1과 HA 사이의 양방향 터널을 통해 통신을 수행해야 한다. 이른 안전성과 효율성 측면에서 많은 단점을 갖는다.

따라서 본 ATRO 프로토콜에서는 그림 3과 같이

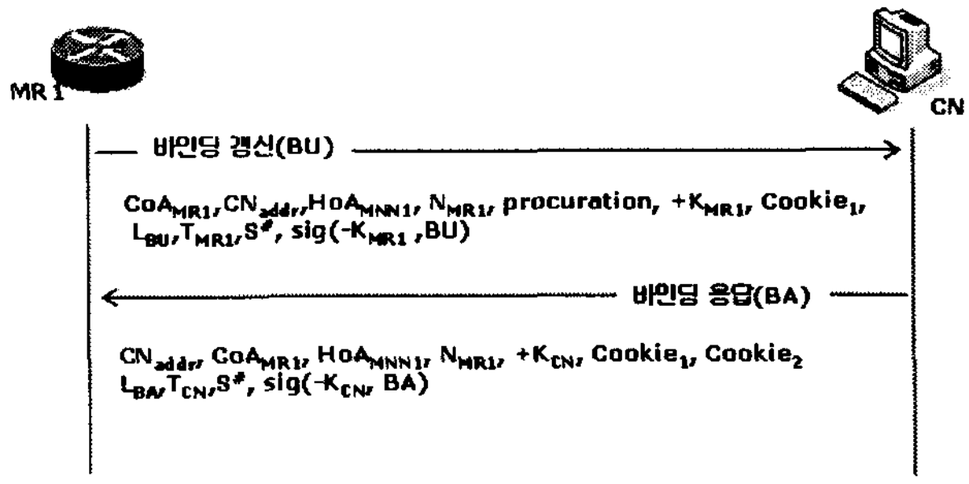

그림 3. BU/BA 전송 메시지

위임 권한을 획득한 MR이 MNN을 대신해서 CN과 BU를 수행한다. 먼저, MR1은 BU 메시지를 CN에게 전송한다. $+K_{MR1}$은 MR1의 공개키로서 MR1의 주소 소유권을 증명하기 위해 포함된다[3]. $Cookie_1$은 두 노드 사이에서 리소스 고갈 공격 및 연결 고갈 공격을 할 수 있는 공격자의 위험을 줄이기 위해 사용된다.

그런 후에 전체 BU 메시지에 서명함으로서 공개키에 대한 인증을 한다. 이 메시지를 수신한 CN은 먼저 $Cookie_1$을 검증하여 이 구간에 공격자가 있는지 확인한 후에 MR1의 주소를 검증하고 MR1이 생성한 서명 값을 확인한다. 모든 검증 과정이 끝나면 CN은 MNN1의 홈 주소와 MR의 의탁주소를 바인딩하고 이 정보를 자신의 바인딩 캐시에 안전하게 저장한다. CN은 MR1에게 BU에 대한 응답 메시지 BA를 전송한다. MR1 역시 CN이 생성한 $Cookie_2$값을 검증하고 서명을 확인한다. 안전한 바인딩 과정이 끝난 후에 MR1은 자신의 이동 네트워크에 있는 MNN1에게 위임 권한을 안전한 양방향 터널을 통해서 반환한다.

4. 성능분석

이번 절에서는 앞서 제안한 ATRO 프로토콜의 안전성과 효율성을 NEMO-BS 프로토콜[1]과 비교 분석한다. 안전성 분석은 구간별 안전성을 검증을 통해서 수행되고 효율성 분석은 종단간의 패킷 전송 지연 시간을 통해 비교한다.

4.1. 안전성 분석

NEMO-BS 프로토콜과 제안하는 ATRO 프로토콜을 구간별 공격 가능성 분석을 통해 비교한다.

4.1.1. NEMO-BS 프로토콜

NEMO-BS 프로토콜이 전체 경로에 안전성을 제

공하기 위해서는 다음과 같은 구간에 안전성을 제공해야 한다.

- MNN1→MR1 • MR1→HA_{MR1}
- HA_{MR1}→CN

먼저 MNN1과 MR1구간을 살펴보면 어떠한 보안 메커니즘을 제공하고 있지 않기 때문에 다양한 공격이 발생할 수 있다. 이 구간에 대한 안전성을 제공하고 있지 않기 때문에 전제 구간에 대한 안전성은 낮다. 다음으로, MR1과 HA_{MR1}구간을 살펴보면 IPsec을 통한 양방향 터널을 통해서 패킷을 전송하기 때문에 메시지의 무결성 및 인증된 패킷을 전송할 수 있다. 따라서 이 구간은 안전하다고 볼 수 있다. 마지막으로 HA_{MR1}과 CN사이의 안전성이다. 이 구간 역시 MNN1과 MR1 구간과 같이 어떠한 안전성도 제공하고 있지 않다.

4.1.2 ATRO 프로토콜

제안하는 ATRO 프로토콜에서 MNN1과 CN사이의 통신은 MR의 HA를 경유하지 않기 때문에 전체 패킷 전송 경로는 다음과 같다.

- MNN1→MR1 • MR1→CN

MNN1과 MR1구간을 살펴보면 NEMO 지원 프로토콜에서의 MR1과 HA 구간과 같이 IPsec을 이용한 양방향 터널을 통해서 데이터 패킷을 전송한다. 따라서 이 구간은 안전하다.

다음으로 MR1과 CN구간이다. 이 구간은 MR1과 CN이 전력이나 계산 능력에 제한을 받지 않는 노드이므로 안전성이 증명된 공개키 방식을 사용한다. 다시 말해서, 각 노드의 공개키로 주소 소유권을 증명하고 MR1과 CN이 생성한 서명을 확인함으로서 각 노드를 인증한다. 따라서 이 구간 역시 안정성을 제공한다.

결과적으로 NEMO-BS 프로토콜은 MNN1과 CN사이의 통신에 있어 부분 구간에 대한 안전성을 제공하지 못해 전체 통신 구간에 대한 안전성을 제고하지 못하는데 반해 제안하는 ATRO 프로토콜은 모든 구간별 안전성을 제공함으로 전체 통신 구간에 대한 안전성을 제공하고 있다.

4.2. 효율성 분석

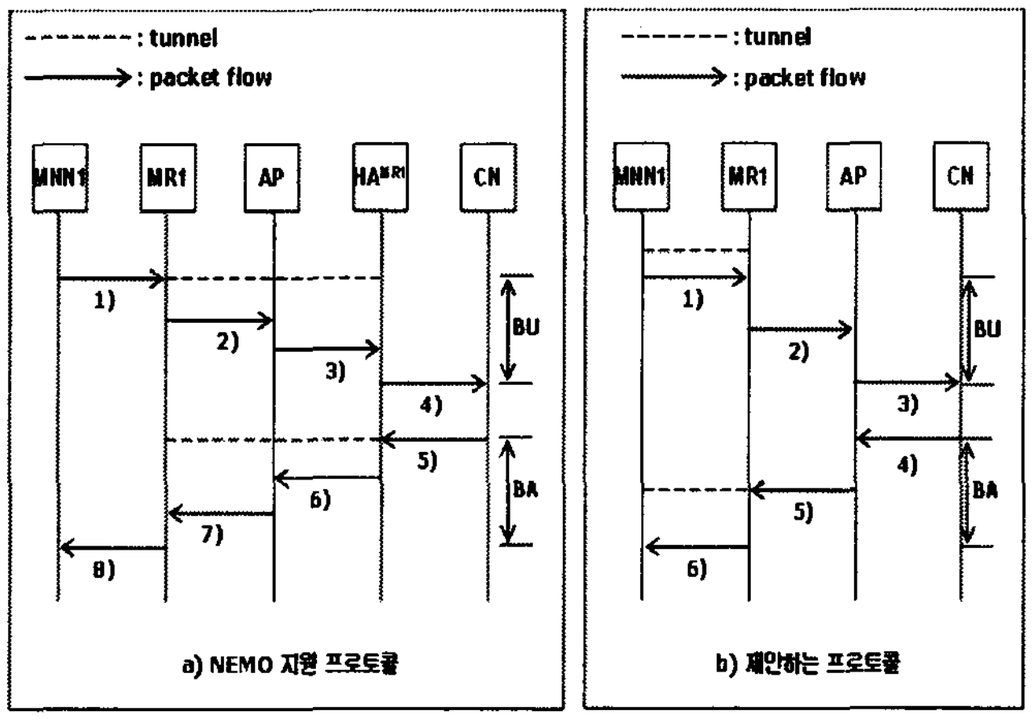

그림 4. BU 메시지 전송 과정

효율성 분석은 MNN1과 CN사이의 종단간의 패킷 전송 지연 시간을 통해 NEMO-BS 프로토콜과 제안하는 ATRO 프로토콜을 비교한다.

4.2.1. NEMO-BS 프로토콜

그림 4는 제안하는 ATRO 프로토콜과 NEMO-BS 프로토콜의 패킷 전송 과정을 보여준다. 이를 통해 종단간 패킷 전송에 요구되는 시간을 계산한다. 먼저 NEMO 지원 프로토콜의 종단간 패킷 지연시간 D_N^{total}을 구하면 수식 (1), (2)와 같다.

$$
\begin{aligned}
D_N^{total} = 2\times[1]\,D_{td} &= \frac{S_{ps}+S_{hao}}{B_{ts}^{wl}},\\
D_{pcd} &= \frac{D_{dn}^{ws}}{PS},\ D_{pd}=T_{tp}]\\
+\,2\times[2]\,D_{td} &= \frac{S_{ps}+S_{hao}+S_{ts}}{B_{ts}^{wl}},\\
D_{pcd} &= \frac{D_{dn}^{wl}}{PS}]\\
+\,2\times[3]\,D_{td} &= \frac{(S_{ps}+S_{hao}+S_{ts})\times H_{avg}}{B_{ts}^{w}},\\
D_{pcd} &= \frac{D_{dn}^{wl}\times H_{avg}}{PS}]\\
+\,2\times[4]\,D_{td} &= \frac{(S_{ps}+S_{hao})\times H_{avg}}{B_{ts}^{w}},\\
D_{pcd} &= \frac{D_{dn}^{wl}\times H_{avg}}{PS},\ D_{pd}=T_{tp}].
\end{aligned}
\tag{1}
$$

$$D_N^{total} = 2\times\frac{2\times(S_{ps}+S_{hao})+S_{ts}}{B_{ts}^{wl}} + 2\times\frac{2\times((S_{ps}+S_{hao})\times H_{avg}+(S_{ts}\times H_{avg})}{B_{ts}^{w}} + 4\times\frac{D_{dn}^{wl}+(D_{dn}^{wl}\times H_{avg})}{PS}+2T_{tp}. \quad (2)$$

수식 (1)에서 D_{td}, D_{pcd}와 D_{pd}는 각각 전송 지연 시간, 처리 지연 시간과 전파 지연 시간을 뜻한다. PS는 전파 속도(m/sec)를 뜻하며 B_{ts}^{w}와 B_{ts}^{wl}는 각각 유선과 무선 상의 전파 속도(bit/sec)이다. 또한 D_{dn}^{w}와 D_{dn}^{wl}는 각각 유선과 무선 상의 평균 거리(m)를 가리킨다. 마지막으로 S_{ts}, S_{hao}, S_{ps}, H_{avg}와 T_{tp}는 각각 터널 헤더 크기(bit), 홈 주소 옵션 크기, 일반적인 패킷 크기(bit), 유선 상에서의 평균 홈 증가 수와 터널 출입구에서의 처리 시간(sec)이다.

4.2.2. ATRO 프로토콜

제안하는 ATRO 프로토콜의 종단간 패킷 지연시간 D_P^{total}을 구하면 수식 (3), (4)와 같다.

$$D_P^{total} = 2\times[1]\,D_{td}=\frac{S_{ps}+S_{hao}+S_{ts}}{B_{ts}^{wl}},\quad D_{pcd}=\frac{D_{dn}^{wl}}{PS}] +2\times[2]\,D_{td}=\frac{S_{ps}+S_{hao}}{B_{ts}^{wl}},\quad D_{pcd}=\frac{D_{dn}^{wl}}{PS},\ D_{pd}=T_{tp}] +2\times[3]\,D_{td}=\frac{S_{ps}+S_{hao}+S_{ts}}{B_{ts}^{wl}},\quad D_{pcd}=\frac{D_{dn}^{wl}}{PS}]. \quad (3)$$

$$D_P^{total} = 2\times\frac{3\times(S_{ps}+S_{hao})+2S_{ts}}{B_{ts}^{wl}} + \frac{6D_{dn}^{wl}}{PS}+T_{tp}. \quad (4)$$

제안하는 ATRO 프로토콜과 NEMO-BS 프로토콜의 대략적인 전체 지연 시간을 계산하기 위해 [4]와 같은 성능 평가 파라미터들을 사용한다. 두 프로토콜의 계산 결과는 수식 (5), (6)과 같이 계산된다.

$$D_N^{total}\approx 9.7\times10^{-3}. \quad (5)$$

$$D_P^{total}\approx 7.3\times10^{-3}. \quad (6)$$

이런 결과를 통해 제안하는 ATRO 프로토콜이 NEMO-BS 프로토콜보다 종단간 패킷 지연시간이 적게 소요되는 것을 볼 수 있다. 특히 중첩된 NEMO 환경일 경우에 NEMO-BS 프로토콜은 종단간 패킷 지연 시간은 더욱 커진다.

5. 결 론

본 논문은 NEMO-BS 지원 프로토콜의 안전성과 효율성을 개선한 프로토콜이다. 이동 네트워크 내의 노드들과 MR 간에는 장기간의 연결 세션을 유지하기 때문에 IPsec을 이용한 양방향 터널을 이용하고 MNN으로부터 BU에 대한 위임 권한을 획득한 MR은 CN과 인증된 키 동의 프로토콜을 통해 안전한 BU를 수행한다. 성능 분석에서 안전성은 부분적 구간에 대한 안전성을 분석하고 효율성은 핸드오프 지연 시간과 종단간 패킷 지연 시간을 계산하였다.

결과적으로 제안하는 ATRO 프로토콜이 NEMO-BS 프로토콜보다 안전성이나 효율성 측면에서 우월하다는 결과를 얻었다. 향후에는 멀티호밍(multihoming)을 고려한 안전하고 효율적인 경로 최적화 기법에 대한 연구를 진행할 것이다.

참고문헌

[1] V. Devarapalli, R. Wakikawa, A. Petresuc, and P. Thubert, "NEMO Basic Support Protocol," IETF RFC 3963, Jan. 2005.

[2] J. Arkko, V. Devarapalli, and F. Dupont, "Usin g IPsec to Protect Mobile IPv6 Signaling Betw een Mobile Nodes and Home Agents," IETF R FC 3776, Jun. 2004.

[3] T. Aura, "Cryptographically Generated Address es (CGA)," IETF RFC 3972, Mar. 2005.

[4] Y. Ahn, T. Lee, and H. Choo, \Lightweight Bi ndings for Mobile Routers," ICCSA 2006, LNC S, vol.3981, pp.661-670, 2006.