한국산학기술학회논문지
Vol. 8, No. 4, pp. 781-787, 2007

네트워크 이동성 지원을 위한 인증된 경로 최적화 프로토콜

구중두[1], 이기성[1*]

Authenticated Route Optimization Protocol for Network Mobility Support

Jung-Doo Koo[1] and Gi-Sung Lee[1*]

요 약 NEMO(Network Mobility) 기본 지원 프로토콜은 경로 최적화 과정을 수행하고 있지 않으며 MR(Mobile Router)과 HA(Home Agent) 사이의 양방향 터널 구간을 제외한 다른 구간에서는 특별한 보안 메커니즘을 제시하고 있지 않다. 따라서 본 논문에서는 MR과 MNN(Mobile Network Node) 사이의 양방향 터널을 통해 위임 권한 프로토콜을 수행하고 위임 권한을 획득한 MR과 CN (Correspondent Node) 사이에 인증된 바인딩 갱신 프로토콜을 통해 경로를 안전하게 최적화한다. 각 노드의 주소는 주소 소유권 증명을 위해 CGA(Cryptographically Generated Address)방식을 통해 생성한다. 끝으로 NEMO에서의 보안 요구사항과 기존에 알려진 공격을 통해 안전성을 분석하고 NEMO 지원 프로토콜과 연결성 복구력(connectivity recovery)과 종단간 패킷 전송 지연 시간율(end-to-end packet transmission delay time)을 비교하여 효율성을 분석한다.

Abstract Network Mobility (NEMO) basic support protocol doesn't execute the process of route optimization and has not presented the particular security mechanism in other blocks except bi-directional tunnel between Mobile Router (MR) and its Home Agent (HA). Therefore in this paper we process secure route optimization courses through authenticated binding update protocol between MR and its Correspondent Node (CN) and the protocol of the competency of mandate between MR and its Mobile Network Node (MNN); its block also uses an bi-directional tunnel as the block between MR and its HA. The address of each node are generated by the way of Cryptographically Generated Address (CGA) for proving the ownership of address. Finally we analyze the robustness of proposed protocol using security requirements of MIPv6 and existing attacks and the efficiency of this protocol using the connectivity recovery and end-to-end packet transmission delay time.

Key Words : 네트워크 이동성, 경로 최적화 프로토콜, CGA

1. 서론

노트북, PDA, 휴대폰과 같은 이동 단말기 보급의 확산과 4G 셀룰러 망과 같은 All-IP 네트워크의 필요성이 대두되면서 Infrastructure에 구애받지 않는 IP 기반의 이동성 지원 기술의 개발이 필요하게 되었으며 이동 단말기 사용자는 인터넷 접속 및 사용에 있어 끊김없는 한 차원 높은 QoS (Quality of Service)에 대한 요구가 대두되었다. 이런 요구를 만족하기 위해서 Internet Engineering Task Force (IETF)의 NEMO 워킹 그룹에서는 2005년에 모바일 IPv6에 기반한 네트워크 이동성 지원 프로토콜을 발표했다. 하지만 NEMO 표준은 MNN과 CN 사이에 경로 최적화 과정을 수행하지 않고 이기 때문에 삼각 경로 문제를 비롯해 중첩 환경일 경우에는 핀볼(pinball) 경로 문제를 유발할 수 있다[1]. 또한 MNN과 CN 사이의 통신에서 안전성은 단지 MR과 HA의 사이의 양방향 터널에 의지하고 있다. 이는 다시 말해서 HA과 CN 사이의 구간 및 MNN과 MR사이의 구간은 안전하지 않을 수 있다. 따라서 NEMO 기본 지원 프로토콜 역시 경로 최적화 과정을 수행해야 하며 모든 구간에 대한 안전성을 제공해야 한다.

본 논문에서는 MNN과 CN 사이의 경로 최적화 과정

이 논문은 2007년 호원대학교 교내연구비의 지원에 의하여 연구되었음
[1]호원대학교 컴퓨터게임학부
*교신저자: 이기성(ygslee@howon.ac.kr)

을 안전한 바인딩 갱신을 통해 수행하며 모든 구간에 대한 안전성을 제공하기 위해 MNN과 MR사이에는 양방향 터널을 이용하며 MNN으로부터 위임 권한을 획득한 MR은 CN과 보안 프로토콜을 수행하여 안전한 바인딩 갱신을 수행한다. 본 프로토콜에서 각 노드의 주소는 주소 소유권 증명을 위해 암호학적으로 생성한 주소(CGA, Cryptographically Generated Address)[2] 방식을 통해 생성한다. 성능 분석에서는 핸드오프 후의 연결 복구 시간 평가와 종단간의 패킷 지연 시간 분석을 통해 제안하는 프로토콜과 NEMO 지원 프로토콜을 비교 분석한다.

이 논문의 구성은 다음과 같다. 2장에서는 NEMO 기본 지원 프로토콜에 대해서 살펴보고 3장에서는 제안하는 NEMO 환경에 적합한 인증된 경로 최적화 프로토콜에 대해 자세히 기술한다. 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 끝으로 5장에서는 결론과 향후 연구방향을 제시한다.

2. NEMO 기본 지원 프로토콜

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 대응노드와 통신 중인 경우에도 단말과 대응노드 사이의 통신이 단절되지 않고 계속 서비스되어야 한다. RFC 3963[1]으로 표준화 된 네트워크 이동성 기본 지원 프로토콜은 MIPv6(Mobile IPv6)[3]를 기반으로 하여 개개의 단말에 대한 이동 투명성을 제공하면서 네트워크 이동성을 관리하기 위한 프로토콜이다. 네트워크 이동성 관련 용어를 살펴보면 먼저 이동네트워크(Mobile Network)는 네트워크 이동성 지원 프로토콜을 구현하여 네트워크 단위로 이동하는 네트워크이며 HA(Home Agent)는 MNN(Mobile Network Node)와 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. MR(Mobile Router)는 자신의 하부에 접속한 호스트에게 이동성을 지원하고 인터넷 연결을 유지시켜주는 이동 가능한 라우터로서 동작한다. MNN는 특징에 따라 지역 고정노드(Local fixed router)와 지역 이동 노드(Local mobile node) 및 방문 이동노드(Visiting mobile node)로 나눌 수 있다. 먼저 지역 특정노드는 이동 네트워크 내에서 접속 지점을 변경하지 않는 노드로서 홈 네트워크를 이동 네트워크로 설정하는 노드이며 지역 이동 노드는 홈 네트워크를 이동 네트워크로 하면서 세션이 유지되는 동안 이동 가능한 노드이다. 마지막으로 방문 이동 노드는 홈 네트워크를 이동 네트워크 외부에 갖는 노드로서 세션을 유지하면서 이동하는 노드이다. 그림 1은 NEMO 기본 지원 프로토콜의 동작 과정을 보여준다. 이동 네트워크가 홈 링크에 있을 때 이동 네트워크 노드는 이동 라우터를 통해 대응노드와 통신 중이다. 이 때, 이동 네트워크가 홈 링크를 떠나서 외부 링크로 이동하면 이동 라우터는 의탁주소를 자동 설정 과정을 통해 생성하고 자신의 HA에게 이 주소를 등록한다. 이런 과정을 끝나고 나면 새로운 경로 생성된다. 하지만 이 경로를 이용할 경우 항상 HA와 MR 간의 양방향 터널을 지나야 하기 때문에 삼각 라우팅 문제가 발생할 수 있다.

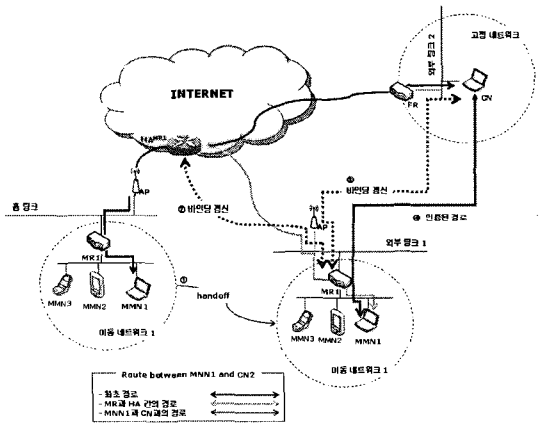


그림 1. MNN과 CN사이의 인증된 경로 최적화

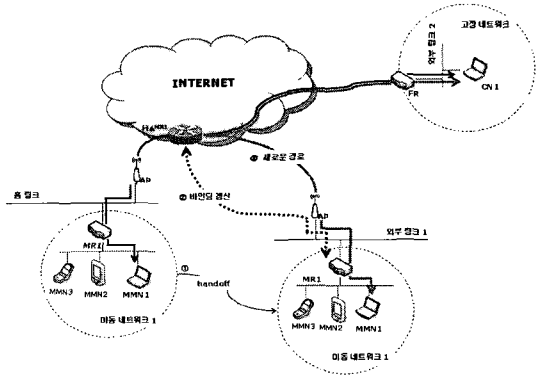


그림 2. NEMO 기본 지원 프로토콜

3. 제안하는 프로토콜

본 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[1],[3],[4]. 이를 통해 데이터의 무결성뿐만 아니라 재생공격 방지 및 기밀성을 보장할 수 있다. 다음으로 MR과 CN구간은 인증된 키 교환 프로토콜을 통해 생성된 세션키를 이용하여 통신한다.

그림 2는 제안하는 프로토콜의 전체적인 경로 최적화 과정을 보여준다. 먼저 이동 네트워크가 외부 링크로 이동하면 이동 네트워크에 있는 MR이 자신의 HA에게 외부 링크에서 획득한 CoA를 등록한다. 그런 후에, MR은 MNN1으로부터 경로 초적화 위임 권한을 획득한 후에 CN과도 바인딩 갱신을 안전하게 수행함으로써 종단간 패킷 지연 시간 및 핸드오프 지연 시간을 줄일 수 있다.

3.1 시스템 설정

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
LBU/T_X	BU의 수명 및 X 노드의 타임 스탬프
$S^{\#}$	일련번호
m1||m2	메시지 m1과 m2의 비트 결합

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.

3.2 메시지 형식

경로 최적화를 위해 수행하는 바인딩 갱신에 필요한 BU 메시지와 BA 메시지의 형식은 그림 3, 4와 같다.

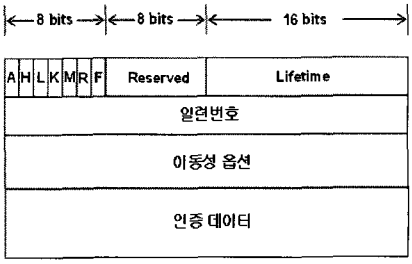


그림 3. BU 메시지 형식

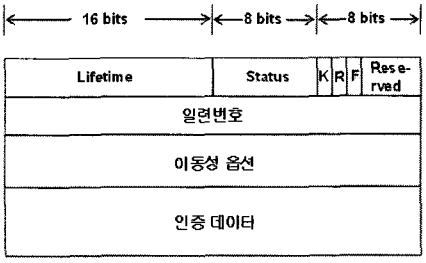


그림 4. BA 메시지 형식

이 형식은 NEMO 기본 지원 프로토콜을 변형한 형태이다[1]. 큰 차이점은 F 필드의 추가이다. 이는 MR이 MNN 으로부터 획득한 위임권한을 설정하기 위한 필드이다. 이를 통해 CN은 MR을 정당한 권한이 있는 노드라고 판단하여 BU를 수행한다.

3.3 인증된 바인딩 갱신 프로토콜

MR1과 CN사이에 BU를 수행하기 전에 MR1은 먼저 자신의 이동 네트워크에 있는 MNN1 으로부터 BU를 수행하기 위한 권한을 획득한다. 그런 후에 획득한 권한을 이용하여 CN과 BU를 수행한다.

가. 위임 프로토콜

위임 프로토콜은 MR과 MNN 사이에 IPsec을 이용한 양방향 터널을 통해서 전송된다. MR1과 MNN1 사이의 전송 메시지는 수식 (1)과 같다.

$$M1(MR1 \rightarrow MNN1):N_{MR}$$
$$M2(MNN1 \rightarrow MR1):N_{MR},procuration,F=1 \quad (1)$$

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 수해한 후에 MR1은 MNN1에게 위임 권한을 반환한다. MNN1은 플래그 F의 값을 0으로 설정한다.

나. 바인딩 갱신 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 프로토콜에서는 그림 5와 같이 위임 권한을 획득한 MR이 MNN을 대신해서 CN과 BU를 수행한다.

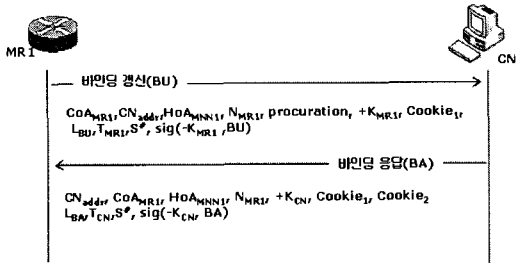


그림 5. BU/BA 전송 메시지

먼저, MR1은 BU 메시지를 CN에게 전송한다. $+K_{MR1}$은 MR1의 공개키로서 MR1의 주소 소유권을 증명하기 위해 포함된다. $Cookie_1$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 비로서 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 프로토콜의 안전성과 효율성을 NEMO 지원 프로토콜[2]과 비교분석한다. 안전성 분석은 구간별 안전성을 통해 전체 통신 경로의 안전성을 보인다. 효율성 분석은 연결성 복구 가능성과 종단간의 전송 지연 시간을 계산한 결과를 통해 확인한다.

4.1 안전성 분석

가. NEMO 지원 프로토콜의 안전성

본 프로토콜의 안전성 분석에 앞서 먼저 NEMO 지원 프로토콜의 구간별 안전성을 분석한다. 이 프로토콜이 전체 경로에 안전성을 제공하기 위해서는 수식 (2)와 같은 구간에 안전성을 제공해야 한다.

- MNN1→MR1
- MR1→HA_{MR1}
- HA_{MR1}→CN (2)

먼저 MNN1과 MR1구간을 살펴보면 어떠한 보안 메커니즘을 제공하고 있지 않기 때문에 다양한 공격이 가능하다. 이 구간에 대한 안전성을 제공하고 있지 않기 때문에 전제 구간에 대한 안전성은 취약하다. 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.

나. 제안하는 프로토콜의 안전성

제안하는 프로토콜에서 MNN1과 CN사이의 통신은 MR의 HA를 경유하지 않기 때문에 전체 패킷 전송 경로는 수식 (3)과 같다.

- MNN1→MR1
- MR1→CN (3)

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

은 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 지원 프로토콜은 MNN1과 CN사이의 통신에 있어 부분 구간에 대한 안전성을 제공하지 못해 전체 통신 구간에 대한 안전성을 제고하지 못하는데 반해 제안하는 프로토콜은 모든 구간별 안전성을 제공함으로 전체 통신 구간에 대한 안전성을 제공하고 있다.

4.2 효율성 분석

효율성 분석은 MNN1과 CN사이의 연결 복구력과 종단간의 패킷 지연 시간을 통해 NEMO 지원 프로토콜과 비교한다. 연결 복구력은 MR이 외부 링크로 이동한 후에 얼마나 빨리 즉 바인딩 갱신을 통해 얼마나 끊김없는 통신을 제공하느냐 이므로 핸드오프 지연 시간에 달려 있다고 볼 수 있다. 따라서 연결 복구력은 핸드오프 지연 시간을 통해 분석하도록 한다.

가. 연결 복구력(Reachability Recovery)

$$D_N = \begin{cases} T^f_{addr} + T_{MR_1 - HA^{MR_1}}, & \text{if } x = 1, \\ T^f_{addr} + 2 \times (T_{rMR-rHA} + \sum_{i=2}^{x} T_{MR_1^{i-1} - MR_1^i} + T_{HA^{i-1}_{MR_1} - HA^i_{MR_1}}, & \text{if } x \geq 2. \end{cases} \quad (4)$$

$$D_P = \begin{cases} T^f_{addr} + T_{MR_1 - CN}, & \text{if } x = 1, \\ T^f_{addr} + 2 \times (T_{rMR-rHA} + \sum_{i=2}^{x} T_{MR_1^{i-1} - MR_1^i}, & \text{if } x \geq 2. \end{cases} \quad (5)$$

NEMO의 핸드오프 지연 시간량과 제안하는 프로토콜의 핸드오프 지연 시간량은 각각 수식 (4), (5)와 같다. 핸드오프 지연시간은 중첩되지 않은 NEMO와 중첩일 경우를 고려하여 계산한다. 먼저 T^f_{addr} 는 MR1이 외부 링크로 이동하여 새로운 의탁주소를 얻는데 걸리는 시간이다. $T_{MR_1 - HA^{MR_1}}$는 MR1과 HA사이에 바인딩 갱신을 수행하는데 걸리는 시간이다. $T_{MR_1^{i-1} - MR_1^i}$는 중첩된 MR간의 핸드오프 지연 시간이다. 마지막으로 $T_{HA^{i-1}_{MR_1} - HA^i_{MR_1}}$ 는 중첩된 MR의 HA간의 핸드오프 지연 시간이다. 핸드오프 지연 시간량을 통해 제안하는 프로토콜이 NEMO 지원 프로토콜보다 중첩된 환경에서 적은 핸드오프 지연 시간을 보인다. 왜냐하면 중첩된 MR1의 HA들 간에 바인딩 갱신 메시지를 전송하지 않기 때문이다.

나. 종단간 패킷 지연 시간

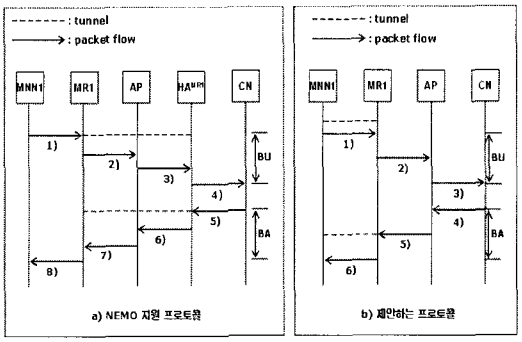


그림 6. BU 메시지 전송 과정

그림 6은 제안하는 프로토콜과 NEMO 지원 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 (6)과 같다.

$$D_N^{total} = 2 \times [1] D_{td} = \frac{S_{ps} + S_{hao}}{B_{ts}^{wl}}, \quad D_{pcd} = \frac{D_{dn}^{ws}}{PS}, D_{pd} = T_{tp}] + 2 \times [2] D_{td} = \frac{S_{ps} + S_{hao} + S_{ts}}{B_{ts}^{wl}}, \quad D_{pcd} = \frac{D_{dn}^{wl}}{PS}] + 2 \times [3] D_{td} = \frac{(S_{ps} + S_{hao} + S_{ts}) \times H_{avg}}{B_{ts}^{w}}, \quad D_{pcd} = \frac{D_{dn}^{wl} \times H_{avg}}{PS}] \quad (6)$$

$$+2\times[4]\,D_{td}=\frac{(S_{ps}+S_{hao})\times H_{avg}}{B_{ts}^{w}},$$
$$D_{pcd}=\frac{D_{dn}^{wl}\times H_{avg}}{PS},D_{pd}=T_{tp}],$$

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

수식 (6)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. 다음은 제안하는 프로토콜의 종단간 패킷 지연 시간 D_P^{total}으로 수식 (7)과 같다.

$$D_P^{total}=2\times[1]\,D_{td}=\frac{S_{ps}+S_{hao}+S_{ts}}{B_{ts}^{wl}},$$
$$D_{pcd}=\frac{D_{dn}^{wl}}{PS}]$$
$$+2\times[2]\,D_{td}=\frac{S_{ps}+S_{hao}}{B_{ts}^{wl}},$$
$$D_{pcd}=\frac{D_{dn}^{wl}}{PS},D_{pd}=T_{tp}]$$
$$+2\times[3]\,D_{td}=\frac{S_{ps}+S_{hao}+S_{ts}}{B_{ts}^{wl}},\qquad(7)$$
$$D_{pcd}=\frac{D_{dn}^{wl}}{PS}].$$

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

제안하는 프로토콜과 NEMO 지원 프로토콜의 대략적인 전체 지연 시간을 계산하기 위해 [5]와 같은 성능 평가 파라미터를 사용한다. 두 프로토콜의 계산 결과는 수식 (8)와 (9)와 같이 계산된다.

$$D_N^{total}\approx 9.7\times10^{-3}.\qquad(8)$$

$$D_P^{total}\approx 7.3\times10^{-3}.\qquad(9)$$

이런 결과를 통해 제안하는 프로토콜이 NEMO 기본 지원 프로토콜보다 종단간 패킷 지연시간이 적게 소요되는 것을 볼 수 있다.

5. 결 론

본 논문은 NEMO 지원 프로토콜이 갖고 있는 안전성과 효율성의 취약성을 분석하여 안전하고 효율적인 기법을 제시했다. 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 프로토콜이 NEMO 지원 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.

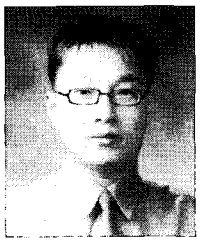
[2] T. Aura, "Cryptographically Generated Addresses (CGA)," IETF RFC 3972, Mar. 2005.

[3] D. Johnshon, C. Perkins, J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, Jun. 2004.

[4] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," IETF RFC 3776, Jun. 2004.

[5] Y. Ahn, T. Lee, and H. Choo, "Lightweight Bindings for Mobile Routers," ICCSA 2006, LNCS, vol.3981, pp.661-670, 2006.

구 중 두(Jung-Doo Koo) [정회원]



- 2003년 2월 : 호원대학교 컴퓨터공학과 (공학사)
- 2006년 8월 : 한양대학교 컴퓨터공학과 (공학석사)
- 2007년 3월 ~ 현재 : 호원대학교 컴퓨터게임학부 시간강사

<관심분야>
암호 이론, 모바일 통신 및 센서 네트워크 보안

이 기 성(Gi-Sung Lee) [종신회원]

- 1993년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

<관심분야>
이동통신, 멀티미디어 통신, 네트워크 보안