MVPN 서비스 제공을 위한 효율적이고 안전한 핸드오버 메커니즘

(An Efficient and Secure Handover Mechanism for MVPN Services)

우 현 제 † 김 경 민 † 이 미 정 ††
(Hyunje Woo) (Kyoungmin Kim) (Meejeong Lee)

요 약 MVPN(Mobile Virtual Private Network)은 이동단말을 사용하는 이동근무자가 지역적 제한 없이 VPN 서비스를 제공받을 수 있도록 하는 기술이다. 이동 VPN 사용자에게 지속적인 VPN 서비스를 제공하기 위해서는 이동성을 제공하기 위한 MIP(Mobile IP) 프로토콜과 IPsec 기반 VPN 기술의 공존이 필요하다. 그런데 MIP와 IPsec 기반 VPN GW(Gateway)를 함께 사용하게 되면 등록 실패나 빈번한 IPsec 터널 재 설립과 같은 문제가 발생한다. IETF에서는 이와 같은 문제를 해결하기 위해 VPN GW의 외부에 홈 에이전트(x-HA)를 사용하는 방안을 제시하였고, 이를 기반으로 동일한 외부네트워크 내에서의 이동에 대한 핸드오버 지연을 줄이기 위한 방안으로 MN(Mobile Node)이 위치한 외부네트워크 내에 x-HA를 동적으로 할당하는 방안도 제안되었다. 그러나 동적으로 x-HA를 할당하는 방안은 세션 키의 노출이나 네트워크 간 이동 시의 긴 핸드오버 지연 발생과 같은 문제를 가진다. 이에 본 논문은 이동 VPN 사용자의 핸드오버 지연시간을 최소화하고 핸드오버로 인한 데이타 손실을 줄이면서 보안을 강화하는 새로운 MVPN 프로토콜을 제안하고, 시뮬레이션을 통해 기존에 제안된 방안과 비교하였다.

키워드 : 이동 가상사설망, 디피-헬만 키 합의 알고리즘, Diameter MIPv4 응용

Abstract Mobile Virtual Private Network (MVPN) provides VPN services without geographical restriction to mobile workers using mobile devices. Coexistence of Mobile IP (MIP) protocol for mobility and IPsec-based VPN technology are necessary in order to provide continuous VPN service to mobile users. However, Problems like registration failure or frequent IPsec tunnel re-negotiation occur when IPsec-based VPN Gateway (GW) and MIP are used together. In order to solve these problems, IETF proposes a mechanism which uses external home agent (x-HA) located external to the corporate VPN GW. In addition, based on the IETF proposal, a mechanism that assigns x-HA dynamically in the networks where MN is currently located was also proposed with the purpose to reduce handover latency as well as end-to-end delay. However, this mechanism has problems such as exposure of a session key for dynamic Mobility Security Association (MSA) or a long latency in case of the handover between different networks. In this paper, we propose a new MVPN protocol in order to minimize handover latency, enhance the security in key exchange, and to reduce data losses cause by handover. Through a course of simulation, the performance of proposed protocol is compared with the existing mechanism.

Key words : Mobile Virtual Private Network (MVPN), Diffie-Hellman Key Agreement Algorithm, Diameter MIPv4 Application

· 본 논문은 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성사업 (ITAC1090060300350001000100100)의 지원에 의 수행되었음
† 학생회원 : 이화여자대학교 컴퓨터학과
hjwoo@ewhain.net
kkm@ewhain.net
†† 정 회 원 : 이화여자대학교 컴퓨터학과 교수
lmj@ewha.ac.kr
논문접수 : 2006년 5월 20일
심사완료 : 2006년 11월 21일

1. 서 론

MVPN(Mobile Virtual Private Network) 서비스는 VPN 사용자에게 이동성을 제공해야 한다. 이를 위해 IETF MIP(Mobile IP) WG(Working Group)에서는 인터넷에서 이동성을 제공하기 위한 표준프로토콜인 MIP 프로토콜을 MVPN을 위해 사용하는 방안을 제시하였

다. 이동 VPN 사용자가 IP 기반 VPN 기술을 사용하여 보안을 유지하는 홈네트워크와 통신을 원하는 경우 MIP와 IPsec 프로토콜이 함께 동작해야 한다. 그런데 MIP가 IPsec 기반 VPN GW(Gateway)와 동작하는 경우에는 사용자 이동에 의해 빈번하게 IPsec 터널을 재설정하거나 MIP 등록 자체가 불가능해지는 문제가 발생한다. MIP에서 MN(mobile Node)은 외부네트워크로 이동한 후 새롭게 얻은 CoA(Care of Address)를 자신의 HA(Home Agent)에게 등록해야 하고, VPN에서는 MN이 HA와 등록 관련 메시지를 주고 받기 위해 우선 VPN GW와 IPsec 터널을 설립해야 하는데, MN이 FA-CoA 모드로 동작할 경우에는 MN의 MIP 등록요청(Registration-Request) 메시지가 IPsec에 의해 암호화되어 있기 때문에, FA(Foreign Agent)가 암호화된 IPsec 패킷을 MIPv4 메시지로 복호화 할 수 없어 결과적으로 MN이 HA에게 새로운 CoA를 등록하는 과정 자체를 실패하게 된다. MN이 Co-located 모드로 동작하는 경우에는 MN이 새로운 CoA를 획득할 때마다 IPsec 터널 SA(Security Association)를 식별하는 파라미터 중 하나인 MN의 목적지 주소가 변경되므로 VPN GW와 MN간에 IPsec 터널을 새롭게 설정해야 하는 문제가 발생한다. MN이 FA-CoA 모드로 동작하는 경우에도 HA와 성공적으로 등록을 완료할 방법이 있다고 가정한다면 역시 이와 유사한 문제가 발생한다. 자원이 제한된 무선환경에서 IPsec 터널을 자주 설정할 경우, 긴 지연의 발생으로 인해 실시간 서비스가 원활히 제공되지 못하는 등의 성능 저하를 초래한다.

이러한 문제점을 해결하기 위해 IETF MIP WG에서는 외부네트워크에 x-HA(external Home Agent)를 두는 방안을 제안하였다[2]. [2]에서는 MN이 외부네트워크로 이동한 경우 홈네트워크 외부에 있는 x-HA에 현재 위치를 등록하도록 함으로써, IPsec에 의해 암호화되지 않은 등록 메시지로 등록이 수행되도록 하여 FA가 암호화된 MIP 등록 메시지를 해독하지 못함으로 인한 등록 실패 문제를 해결하고, VPN GW와는 x-HA로부터 할당 받은 고정된 주소인 x-HoA (external Home Address)를 사용하여 IPsec 터널을 설정하도록 함으로써 MN이 새로운 CoA를 획득할 때마다 IPsec 터널이 재설정되어야 하는 문제를 해결하였다. 그러나 [2]에서 제시한 방안에서는 모든 외부네트워크를 대상으로 하나의 x-HA를 정적으로 할당하기 때문에 MN이 x-HA와 위치상 멀리 이동하거나 인터넷 지연시간이 긴 경우 핸드오버 지연시간이 길어지고, 홈네트워크 외부에 위치한 x-HA을 어떻게 신뢰할 것인가가 분명히 정의되지 않았다. 이와 같은 문제점을 해결하기 위해 MN의 현재 위치한 외부네트워크 내에 x-HA를 동적으로 할당하는 방안이 제시되었으나, 이 방안은 MN과 x-HA 간의 동적인 MSA(Mobility Security Association)를 설립하기 위한 세션키가 노출될 위험성이 있다는 보안상 취약점이 있고, 네트워크 간 이동이 일어날 때는 긴 핸드오버 지연이 발생할 수 있다는 문제를 지닌다[3].

이에 본 논문에서는 MVPN 환경에서 보다 효율적이고 안전한 핸드오버 방안을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 1장의 서론에 이어서 2장에서는 관련 연구에 대하여 좀 더 자세히 설명하고, 3장에서는 본 논문에서 제안하는 방안에 대하여 소개한다. 4장에서는 제안한 방안의 효율성을 살펴보기 위한 시뮬레이션 결과를 제시하고 마지막으로 5장에서는 이 논문의 결론을 맺는다.

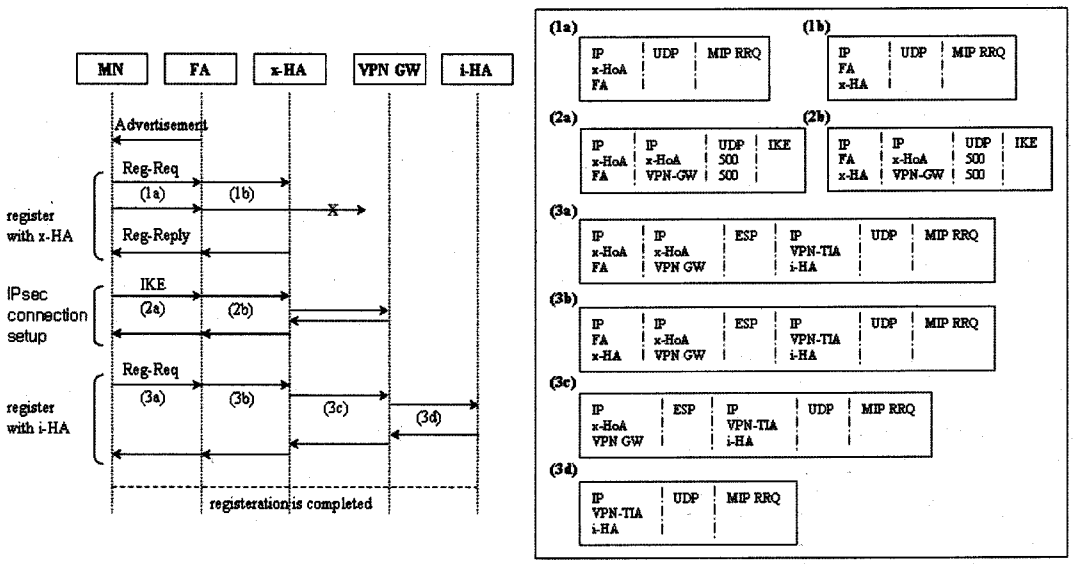
2. 관련연구

이 장에서는 MVPN 서비스를 위해 기존에 제안된 두 가지의 방안을 살펴보고, 이들 방안이 가지는 비효율성이나 취약점을 설명한다.

2.1 외부네트워크를 대상으로 하나의 정적인 x-HA를 할당하는 IETF 방안

VPN 사용자에게 이동성을 제공하기 위해 MIP가 IPsec 기반 VPN GW와 동작할 경우, FA-CoA 모드로 동작하는 MN은 새롭게 획득한 CoA를 FA를 통해 i-HA에게 등록하는 과정 자체를 실패하고, MN이 Co-located 모드로 동작하는 경우에는 등록 과정 자체를 수행하는데는 문제가 없으나 새로운 CoA를 획득할 때마다 VPN GW와 MN간에 IPsec 터널을 새롭게 설정해야 한다는 문제는 여전히 존재한다. MN이 FA-CoA 모드로 동작하는 경우에도 FA를 통한 등록이 성공했다고 가정하더라도 역시 이와 유사한 문제가 발생한다. IETF에서는 이와 같은 문제점을 해결하기 위해 홈네트워크와 외부네트워크를 위해 각각 i-HA(internal Home Agent)와 x-HA를 두는 방안을 제안하였다. 그림 1은 FA-CoA로 동작하는 MN이 외부네트워크로 이동했을 경우에 홈네트워크와 connection을 설립하기 위한 메시지 흐름과 패킷 포맷을 보여준다.

그림 1과 같이 MN은 FA로부터 새로운 CoA를 받으면 자신의 새로운 위치를 HA에게 등록하기 위해 i-HA와 x-HA에게 MIP 등록요청 메시지를 보낸다. 홈네트워크는 IPsec 터널을 통해서 들어오는 패킷 만을 허용하므로 IPsec 터널이 설정되기 전의 MIP 등록요청 메시지는 오직 x-HA에게만 전달된다. MN은 x-HA에게 새로운 CoA에 대한 등록을 완료한 후, 홈네트워크의 VPN GW와 IPsec 터널 설정을 위한 IKE 절차를 실행한다. 그림 1(b)의 (2a)는 MN이 VPN GW와 IPsec 터널 설정을 위한 IKE 절차를 실행할 때의 패킷 포맷을



(a) 메시지 흐름 (b) 패킷 포맷

그림 1 외부네트워크에 위치한 MN의 connection 설립 과정

보여준다. MN은 VPN GW와의 IPsec 터널 SA (Security Association)를 식별하는 요소인 자신의 목적지 주소를 x-HA로부터 획득한 x-HoA를 사용한다. x-HA는 MN이 외부네트워크에 있는 한 이동과 관계없이 일정하므로, x-HoA를 이용하여 VPN GW와 IPsec 터널을 설정함으로써 MN이 새로운 서브넷으로 이동하더라도 IPsec 터널 재설정을 하지 않아도 된다. 임의의 CN(Correspondent Node)이 MN의 i-HoA(internal Home Address)로 보낸 패킷이 자신의 현재 주소로 배달될 수 있도록 하기 위해서는 홈네트워크에 도착한 패킷이 자신의 현재 주소를 가지고 있는 x-HA로 전달되도록 해야 한다. 이를 위해 MN은 i-HA에게 자신을 서브하는 x-HA를 등록한다. 이동 VPN 사용자가 홈네트워크와 통신을 원하는 경우, VPN GW와 설정한 IPsec 터널을 통해서만 홈네트워크에 패킷이 주입될 수 있으므로 MN은 i-HA에게 보내는 MIP 등록요청 메시지를 ESP 암호화 하여야 한다. MIP 프로토콜에서는 FA가 ESP 암호화된 MIP 등록요청 메시지를 복호화 할 수 없으므로 등록이 실패했지만, IETF가 제시한 [2]에서는 그림 1(b)의 패킷 (1a)와 같이 x-HA에게 MN의 CoA를 등록하도록 함으로써 FA가 IPsec에 의해 암호화되지 않은 MIP 등록 메시지로 등록을 수행하도록 하였다. 또한, 그림 1(b)의 패킷 (3a)와 같이 MN이 i-HA에게 보내는 MIP 등록요청 메시지를 ESP 암호화를 한 후 x-HA로부터 VPN GW로 터널링 되도록 IP 헤더를 붙여 FA를 통해 x-HA에게 전달하고, 마지막으로 x-HA가 i-HA에게 전달되도록 함으로써 i-HA로의 등록도 성공적으로 수행된다.

MN이 Co-located 모드로 동작하는 경우에도 FA-CoA 모드로 동작하는 경우와 마찬가지로 x-HA로부터 획득한 x-HoA를 이용하여 IPsec 터널을 설정함으로써 MN의 CoA가 변경될 때마다 VPN GW와 MN간의 IPsec 터널을 재설정해야 하는 문제를 해결하였다.

2.2 외부네트워크에 x-HA를 동적으로 할당하는 방안

[2]에서 IETF가 제시한 방안은 MIP 프로토콜이 IPsec 기반 VPN과 함께 동작하면서 발생하는 문제점들은 해결하였지만 모든 외부네트워크를 대상으로 하나의 x-HA만을 정적으로 할당하기 때문에 핸드오버 지연시간이나 종단간 지연이 길어지는 문제와 외부네트워크에 위치한 x-HA를 어떻게 신뢰할 것인가에 대한 해결책을 제시하지 못했다. 이와 같은 문제점들에 대한 보안으로 [3]에서는 Diameter 프로토콜을 사용하여 AAA(Authentication, Authorization, Accounting) 서버를 통해 동적으로 x-HA를 할당하는 방안을 제안하였다. AAA는 로밍 등 도메인 간 서비스에서의 안전하고 신뢰할 수 있는 인증, 권한 부여, 과금 등의 서비스를 제공하기 위한 기술이며, 현재 IETF AAA WG에서 MIP 외의 여러 WG과 3GPP, 3GPP2로부터 요구 사항을 수용하여 표준을 진행 중이다. Diameter는 유무선 이동인터넷 환경에서 AAA 서비스를 제공하기 위한 IETF의 표준 프로토콜로서 로밍에 필요한 도메인간 이동성 지원, 강화된 보안 제공 등의 특징을 가진다. 또한, Diameter는 HA의 동적 할당뿐 만 아니라 키 분배 센터 역할도 수행함으로써 MIP 에이전트와 MN 간의 동적 MSA 설립도

지원한다. [3]에서 제안한 방안은 Diameter MIPv4 응용[4]을 기반으로 MN이 현재 위치한 네트워크에 x-HA를 할당함으로써 MN이 동일 외부네트워크 내에서 이동하는 경우의 핸드오버 지연시간을 최소화하였고, Diameter 기반 프로토콜의 AA(Authentication, Authorization)를 통해 외부네트워크에 존재하는 x-HA의 신뢰성 문제를 해결했다. 그림 2는 동적으로 x-HA를 할당하는 MVPN의 기본 구조를 보인다. 그림 2에서 외부네트워크1을 위해서는 x-HA1이 외부네트워크2를 위해서는 x-HA2가 각각 존재한다.

그림 3은 FA-CoA 모드로 동작하는 MN이 네트워크 간 이동을 했을 경우에 [3]에서 제안한 방안의 메시지 흐름을 보여준다. MN은 외부네트워크로 이동한 후 FA로부터 새로운 CoA를 획득하면(그림 3의 1), 자신의 새로운 위치를 홈네트워크에 등록하기 위해 인증 정보를 포함한 MIP 등록요청 메시지를 생성한다(그림 3의 2). 동적 x-HA 할당을 위해 MN은 MIP 등록요청 메시지의 확장 필드에 x-HA의 할당과 x-HA와의 동적 MSA 설립을 요구하는 내용을 포함해야 한다. FA는 MN을 위해 Diameter 클라이언트 역할을 수행하는데, 이를 위해 MN으로부터 MIP 등록요청 메시지를 받으면 x-HA의 할당을 요청하는 Diameter 메시지인 AMR(AA-Mobile-Node-Request)를 생성하여 AAAF에게 보낸다(그림 3의 3). FA로부터 AMR 메시지를 받은 AAAF는 외부네트워크에 x-HA를 할당하도록 AAAH에게 지시하기 위해 후보 x-HA의 NAI(Network Access

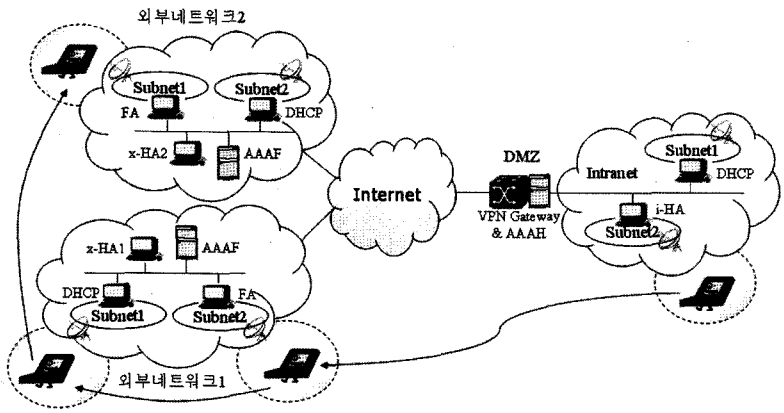


그림 2 동적으로 x-HA를 할당하는 MVPN 네트워크

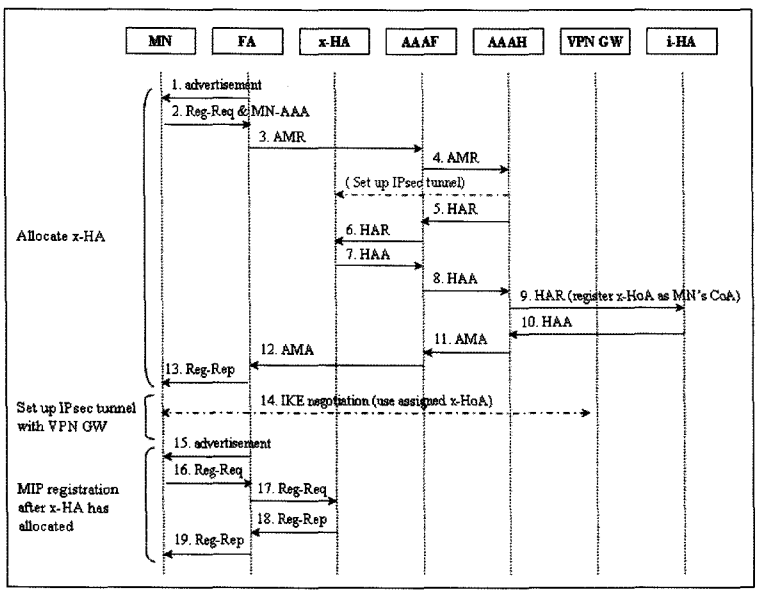


그림 3 메시지 흐름

Identifier)를 포함한 AMR 메시지를 AAAH에게 전송한다(그림 3의 4). AAAH는 AMR 메시지를 통해 우선 MN을 인증한 후에 MN이 외부네트워크에 x-HA를 요구한 경우, AAAF가 AMR 메시지에 포함하여 알려준 후보 x-HA나 자신이 직접 선택한 x-HA를 MN의 x-HA로 결정하고 MN과 x-HA 사이의 동적 MSA를 설립하기 위한 세션키를 생성한다. AAAH는 세션키와 세션키를 유도하기 위한 Nonce 값, 그리고 x-HA가 MN의 x-HoA를 할당하도록 지시하는 정보를 포함한 HAR(Home-Agent-MIP-Request) 메시지를 생성하여 x-HA에게 전송한다(그림 3의 5~6). AAAH는 자신과 비밀키를 공유하는 MN에게는 세션키 유도값만 전달하고 SA가 미리 설립되지 않은 x-HA에게는 세션키 자체를 전달하는데, 이 경우 x-HA가 외부 네트워크에 존재하므로 세션키가 외부에 위치한 공격자에게 노출될 수 있어 MN과 x-HA이 동적 MSA를 설립하는데 있어 보안이 위협받을 수 있다. AAAH로부터 HAR 메시지를 받은 x-HA는 MN의 x-HoA를 할당하고 AAAH가 보낸 HAR메시지에 대한 응답으로 HAA(Home-Agent-Answer) 메시지를 생성하는데, 여기에는 i-HA에게 MN의 현재 x-HoA를 등록하기 위한 MIP 등록응답(Registration-Reply) 메시지가 포함된다(그림 3의 7~8). 이 MIP 등록 메시지에는 x-HoA 주소와 x-HA 주소, MN이 x-HA와 동적 MSA를 설립하는데 사용될 세션키를 유도하는 Nonce 값 그리고 세션키를 이용하여 생성한 MIPv4 Authentication 확장 필드가 포함된다. AAAH는 x-HA가 전송한 HAA 메시지를 통해 MN의 x-HoA를 획득하고 이를 i-HA에게 등록한 후(그림 3의 9~10), MN에게 MIP 등록응답 메시지를 전달하기 위한 AMA(AA-Mobile-Node-Answer) 메시지를 생성하여 FA에게 전송한다(그림 3의 11~12). FA는 AMA 메시지를 통해 MIP 등록응답 메시지를 생성하여 최종적으로 MN에게 전달하고, MN은 MIP 등록응답 메시지로부터 x-HA주소, x-HoA 주소 그리고 x-HA와의 동적 MSA 설립에 사용될 세션키를 유도하기 위한 Nonce 값을 획득한다(그림 3의 13). MN이 이 Nonce 값과 AAAH와 공유한 비밀키를 이용하여 x-HA와의 인증을 위한 세션키를 생성하고 MIP 등록응답 메시지의 MIPv4 인증 확장 필드를 검증함으로써 x-HA 동적 할당이 완료된다. x-HA을 할당 받은 MN은 x-HA가 할당한 x-HoA를 이용하여 홈네트워크에 존재하는 VPN GW와 IPsec 터널을 설정한다(그림 3의 14).

이 방안에서는 MN이 새로운 외부네트워크로 이동할 때마다 동적으로 x-HA를 할당 받기 위한 프로세싱을 해야 하기 때문에 인해 IETF에서 제안한 [2]에 비해 오버헤드가 증가하나, 그림 3의 15~19와 같이 MN이 동일한 외부네트워크 내에서 이동하는 경우 가까운 곳에 위치한 동일 지역 내의 x-HA에게 등록을 하기 때문에 동일 외부네트워크 내에서의 이동에 대한 핸드오버 지연시간을 줄이고 총 종단 간 지연시간을 줄였다. 그러나 MN이 네트워크 간 이동을 할 경우 핸드오버 지연시간이 크게 증가하므로, 이 제안은 네트워크 간 이동이 빈번한 상황이나 심리스한 서비스 제공을 위해서는 미흡한 면이 존재한다. 또한 앞에서 지적했듯이 AAAH로부터 외부네트워크에 위치한 x-HA에게 세션키 자체가 전달되기 때문에 세션키가 노출되어 AAAH와 x-HA 사이의 보안에 취약점(security hole)이 발생할 수 있다. Diameter MIPv4 응용에서는 이를 방지하기 위해 x-HA와 AAAH 사이에 TLS(Transport Layer Security) 또는 IPsec 암호화를 사용하도록 제시하였다. 그러나 이와 같이 [3]의 보안을 강화한다면 x-HA가 변경되어야 하는 네트워크 간 이동이 발생하는 경우에 대한 핸드오버 지연시간은 훨씬 증가할 것으로 예상된다.

2.3 MIP와 MOBIKE 프로토콜을 활용하는 방안

MIP에 IPsec을 적용할 경우 MN의 IP 주소가 변경될 때마다 IP 주소에 의존하는 IPsec SA를 변경되어 빈번하게 IPsec 터널을 재 설립해야 하는 문제를 해결하기 위해 MOBIKE(IKEv2 Mobility and Multihoming Protocol) 프로토콜을 사용하는 방안이 제안되었다[9]. MOBIKE는 키 변경 없이 IP 주소 변경이 가능하도록 IKEv2를 확장한 프로토콜이다.

MN이 이동하여 IP 주소가 변경되는 경우, MN은 우선 현재의 네트워크가 홈네트워크인지 외부네트워크인지를 인지하기 위해 VPN GW와 IKE mobility를 교환함과 동시에 홈네트워크에 위치한 홈에이전트에게 VPN 캡슐화 없이 MIP 등록요청 메시지를 보낸다. 만일 MN이 홈에이전트로부터 MIP 등록응답 메시지를 수신할 경우 자신이 홈에 위치했음을 인지하게 되며 그렇지 않을 경우에는 VPN GW와 IPsec 터널을 설립하기 위한 과정을 수행하게 된다. 홈네트워크에서 이미 VPN GW와 VPN 연결을 설립한 경우에는 자신의 현재 위치를 갱신하기 위한 IKE mobility exchange를 시작하고, VPN 연결이 설립 안 된 경우에는 VPN GW와 VPN 터널을 설립한다. 기존의 IPsec SA가 종단 간의 IP 주소가 변경되는 경우 SA를 재 설립해야 하는 반면에 MOBIKE는 키 변경 없이 종단 간의 IP 주소만을 변경할 수 있으므로 MN이 이동하여 IP 주소가 변경되더라도 IPsec SA는 재 설립 할 필요가 없다. MN이 VPN GW와 VPN 터널 설립을 성공적으로 마친 이후에는 VPN 터널을 통해 자신의 홈에이전트에게 MIP 등록 과정을 수행한다. 이 때 홈에이전트에 등록되는 MN의 현재 위치는 VPN GW로부터 할당 받은 VPN TIA 주소

를 사용함으로써 MN의 이동을 투명하게 한다.

이 방안에서는MIP에 IPsec을 적용하기 위해 x-HA를 활용하는 [2], [3] 방안에 비해 MOBIKE 프로토콜을 통해 IPsec 터널 재 설립 문제를 해결함으로써 MIP 터널 오버헤드를 줄였으나, FA-CoA 모드로 동작하는 경우 MIP 등록 자체가 실패하는 문제점을 여전히 가지고 있다. 또한, 아직까지는 IPsec 터널 모드에만 적용 가능하다는 한계점을 지닌다.

3. MVPN을 위한 안전하고 심리스한 핸드오버 처리

본 논문에서는 [3]에서 AAAH가 외부네트워크에 위치한 x-HA에게 세션키 자체를 전송함으로 인해 세션키가 노출될 수 있는 취약해진 보안을 강화하기 위해, x-HA와 AAAH간에 Diffie-Hellman (이하 D-H) 키 합의 알고리즘을 사용하여 AAAH가 x-HA에게 암호화된 세션키를 전송하는 방안을 제안한다. 이 방안은 세션키 분배 송·수신자인 AAAH와 x-HA 간에 안전한 세션키 전달을 위해 IPsec 터널을 형성하는 [4]에 비해 종단간 핸드오버 지연시간을 크게 감소시킬 수 있다. 또한, 제안하는 방안에서는 [3]에서 이동 VPN 사용자가 외부네트워크 간 이동을 했을 때 긴 핸드오버 지연시간으로 인해 다량의 패킷 손실이 발생하는 것을 보완하기 위해, 새로운 네트워크로부터 CoA를 할당 받은 이후로부터 새 네트워크로부터 할당 받은 x-HoA를 i-HA에 등록하고 새로운 x-HoA로 홈네트워크 VPN GW와의 IPsec 터널 재설정을 완료할 때까지, 이전 x-HA와 FA 사이에 터널을 설정하여 MN에게 패킷을 전송하는 방안을 제안하였다. 본 방안에서는 MN이 VPN을 사용할 수 있는 합법적인 사용자라면 MN과 홈네트워크에 존재하는 AAAH와 i-HA 사이에 필요한 SA는 미리 설립되었다고 가정한다.

그림 4는 제안하는 방안에서 FA-CoA 모드로 동작하는 MN이 외부네트워크로 이동한 경우의 메시지 흐름을 보여준다.

3.1 Diffie-Hellman 키 합의 알고리즘을 활용한 세션키 암호화 방안

[3]은 AAAH가 MN과 x-HA 간의 동적 MSA를 설정하는데 사용될 세션키를 외부네트워크에 위치한 x-HA에게 직접 전달함으로 인해 MN과 x-HA 사이의 보안이 위협을 받으며, 이를 보완하기 위해 [4]에서는 x-HA와 AAAH간의 IPsec 터널 설정을 제시하였다. 그러나 이와 같이 [3]의 보안을 강화한다면 네트워크 간 이동이 발생하는 경우에 새로운 x-HA와 AAAH 간 IPsec 터널 설정이 이루어져야 하기 때문에 핸드오버 지연시간은 훨씬 증가할 것이다. 이에 본 장에서는 MN이 x-HA가 변경되어야 하는 네트워크 간 이동을 하는 경우, MN과 x-HA 간의 동적 MSA를 안전하게 설립하고 핸드오버 지연시간을 줄이기 위해 두 통신 개체가 비밀키를 공유할 수 있는 공개키 암호화 알고리즘인

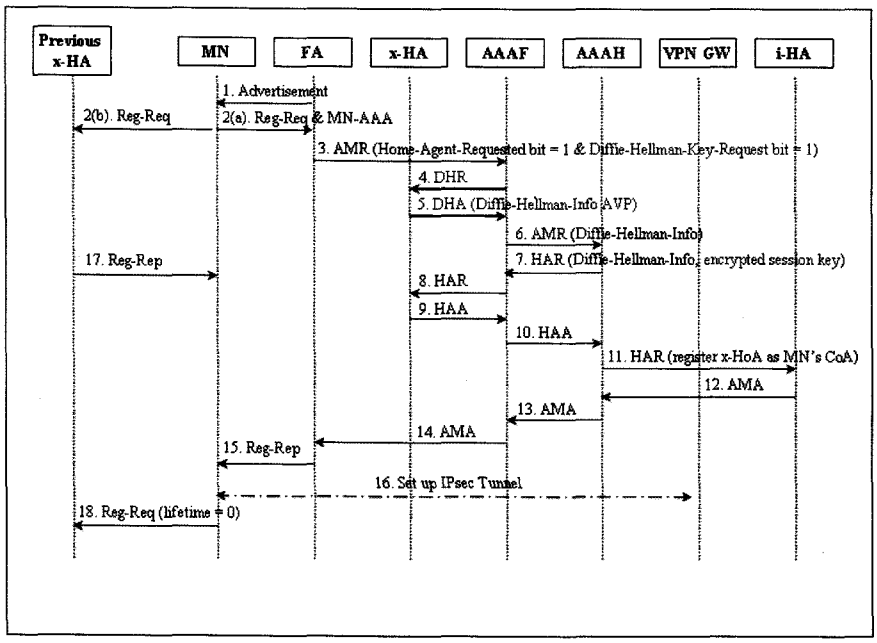


그림 4 FA-CoA 모드에서의 메시지 흐름

D-H 키 합의 알고리즘[6]을 이용하는 방안을 제안한다. 제안한 방안에서는 MN과 x-HA 간의 동적 MSA를 설립하는데 사용될 세션키를 AAAH가 x-HA에게 암호화하여 전달하도록 하였고, 이를 위해 AAAH가 x-HA에게 세션키를 전달하기 전에 x-HA와 AAAH는 D-H 기법에 따라 D-H 공개정보를 교환하고 서로 교환한 D-H 공개정보와 자신의 D-H 비밀정보를 조합하여 공유된 비밀키를 생성해낸다. AAAH는 공유된 비밀키로 세션키를 암호화하여 x-HA에게 전달함으로써 안전하게 키 분배를 수행하고, x-HA는 공유된 비밀키를 통해 세션키를 복호화할 수 있다.

D-H 키 합의 알고리즘은 IKE 프로토콜에서 세션키를 설정하는데 사용되는 알고리즘이므로 IPsec 암호화 기반 구조와 호환성에 문제가 없다. 또한, D-H 키 합의 송·수신자인 x-HA와 AAAH는 D-H 키 합의 알고리즘의 취약점인 중간자 공격(middleperson attack)으로부터 안전하다. 중간자 공격이란, D-H 키 송수신자의 데이타를 가로챈 공격자가 송신자에게는 자신이 수신자인 것처럼, 수신자에게는 자신이 송신자인 것처럼 D-H 공개정보를 전달하여 D-H 송수신자 사이의 암호화된 메시지를 복호화하여 데이타를 읽는 공격 방법인데, 이러한 취약성은 D-H 키 교환 참가자들이 서로간에 인증을 하지 않기 때문에 발생한다. Diameter 기본 프로토콜[5]에서는 Diameter 노드 간의 인증을 제공하기 위해 pre-shared key 방식의 IKE를 지원하므로, 메시지 교환에 참여하는 모든 Diameter 노드는 pre-shared key를 이용하여 서로를 인증할 수 있고, 따라서 x-HA와 AAAH의 공개키가 위조되는 것을 방지할 수 있다. 따라서 본 방안에서 D-H 키 합의 알고리즘이 적용되는 x-HA와 AAAH 간에는 중간자 공격을 피할 수 있다고 볼 수 있다.

제안하는 방안에서는AAAH와 x-HA가 세션키를 암호화, 복호화하기 위해 필요한 공유된 비밀키를 생성하기 위해 D-H 공개정보를 교환해야 한다. 이를 위해 D-H 키 합의 프로세싱을 x-HA가 시작하도록 명시하기 위해 AMR 메시지에 Diffie-Hellman-Key-Request 비트를 추가하였다. MN이 x-HA와의 동적 MSA 설립에 사용할 세션키 할당을 요구한 경우, FA는 AMR 메시지에 Diffie-Hellman-Key-Request 비트를 설정하여 AAAF(Foreign AAA Server)가 x-HA에게 DHR(Diffie-Hellman-Key-Exchange-Request) 메시지를 보내도록 유도한다(그림 4의 3). FA로부터 x-HA 할당을 요청하는 AMR 메시지를 받은 AAAF는 Diffie-Hellman-Key-Request 비트가 설정된 경우, 후보 x-HA를 선택하여 D-H 키 합의 프로세싱을 시작하도록 유도하기 위해 해당 x-HA에게 DHR 메시지를 보낸다(그림 4의 4). DHR 메시지를 받은 x-HA는 D-H 키 합의 알고리즘에 기반하여, AAAH가 공유된 비밀키를 생성하는데 필요한 자신의 D-H 공개정보와 자신의 공유된 비밀키를 생성하기 위한 D-H 비밀정보를 생성해야 한다.

x-HA는 AAAH에게 제공할 D-H 공개정보를 DHA (Diffie-Hellman-Key-Exchange-Answer) 메시지의 Diffie-Hellman-Info AVP에 포함하여 AAAF에게 보낸다(그림 4의 5). DHA 메시지를 받은 AAAF는 FA로부터 받은 AMR 메시지에 DHA 메시지로부터 얻은 x-HA의 D-H 공개정보를 추가하여 AAAH에게 전송한다(그림 4의 6). AAAH는 MN이 x-HA 의 할당과 동시에 x-HA와의 MSA를 설립하기 위한 세션키를 요구한 경우, 세션키를 생성한 후에 세션키의 암호화 여부를 판단하기 위해 AMR 메시지의 Diffie-Hellman-Key-Request 비트를 확인하고 이 비트가 설정된 경우에는 AMR 메시지의 Diffie-Hellman-Info AVP로부터 x-HA와 공유된 비밀키를 생성하기 위한 x-HA의 D-H 공개정보를 획득한다. 또한, AAAH는 x-HA와 마찬가지로 공유된 비밀키를 생성하는데 필요한 자신의 D-H 비밀정보를 생성하고, x-HA가 공유된 비밀키를 생성하는데 사용할 자신의 D-H 공개정보를 생성한다. AAAH는 AMR 메시지에 포함된 x-HA의 D-H 공개정보와 자신의 D-H 비밀정보를 조합하여 x-HA와 공유할 비밀키를 생성하고 이 비밀키를 사용하여 x-HA에게 전달할 세션키를 암호화한다. AAAH는 x-HA에게 MN을 서브하도록 지시하기 위해 HAR(Home-Agent-MIP-Request) 메시지를 생성하고 이 메시지에 암호화된 세션키와 x-HA가 이를 복호화 하는데 필요한 공유된 비밀키를 생성할 수 있도록 자신의 D-H 공개정보를 포함하여 x-HA에게 전송함으로써 MN과 x-HA가 안전하게 동적 MSA를 설립할 수 있도록 한다(그림 4의 7~8). 표 1은 암호화된 세션키를 전달하기 위해 확장된 MIP-HA-to-MN-MSA AVP의 포맷이다.

표 1 확장된 MIP-HA-to-MN-MSA

```
MIP-HA-to-MN-MSA ::= < AVP Header: 332 >
                     { MIP-HA-to-MN-SPI}
                     { MIP-Algorithm-Type}
                     { MIP-Replay-Mode}
                     { Encryption-Algorithm-Type}
                     { MIP-Encrypted-Session-Key}
                    * [ AVP ]
```

AAAH로부터 HAR 메시지를 받은 x-HA는 암호화된 세션키를 복호화하기 위해 Diffie-Hellman-Info AVP로부터 AAAH의 D-H 공개정보와 세션키를 암호화한 알고리즘을 확인한 후, AAAH의 D-H 공개정보와

자신의 D-H 비밀정보를 조합하여 비밀키를 생성한다. D-H 키 합의 알고리즘에 근거하여 x-HA와 AAAH는 동일한 비밀키를 공유하며, x-HA는 공유된 비밀키로 복호화한 세션키를 MN과 동적 MSA를 설립하는데 사용한다. MN을 서브할 x-HA의 할당이 완료된 후에, 새롭게 할당 받은 x-HA를 i-HA에게 등록하는 과정과 x-HA로부터 할당 받은 x-HoA를 사용하여 VPN GW와 MN간의 IPsec 터널을 형성하는 과정은 [3]과 동일하다. 자세한 메시지 흐름은 그림 4의 11~16을 참조한다.

종합적으로 보면, 제안한 방안은 AAAH가 x-HA에 안전하게 세션키를 전달하도록 하기 위해 그림 4의 메시지 4, 5와 같이 동일 지역 내에 가까이 위치하는 x-HA와 AAAF 간에 2번의 추가적인 Diameter 메시지 교환만을 요구한다. 이에 반하여 [3]의 방안에서 AAAH가 x-HA에게 안전하게 세션키를 전달하도록 하기 위해 [4]에서 제시한 대로 x-HA와 AAAH 간에 IPsec 터널을 설정한다면, x-HA가 변경되는 네트워크 간 이동이 발생할 때마다 새로운 x-HA와 AAAH 간에 IKE SA와 IPsec SA의 설정이 이루어져야 한다. D-H는 IKE SA 협상 과정에서 세션키를 생성하기 위한 알고리즘이므로 전체 IPsec 터널 설정에 비해 프로세싱 오버헤드가 적다. 따라서 제안한 방안은 [3]에 비해 MN의 종단간 핸드오버 지연 시간을 줄였으며 AAAH가 x-HA에게 세션키를 안전하게 전달하기 위한 x-HA와 AAAH의 프로세싱 오버헤드도 줄였다.

3.2 이전 x-HA 활용 방안

이 절에서는 동적으로 MN이 이동한 네트워크 내에서 x-HA를 할당하는 경우에, 네트워크 간 이동 시 긴 핸드오버로 인해 성능 저하가 발생하는 문제를 보안하기 위해 MN이 이동하기 바로 직전의 네트워크에서 MN을 서브한 x-HA(이후로 이전 x-HA라 부름)를 활용하는 방안에 대해서 설명한다. 그림 5는 제안하는 방안에서 MN이 네트워크 간 이동 시 이전 x-HA에게 등록을 하는 메시지 전달 과정을 보여주고 있다.

임의의 외부네트워크에 위치한 MN이 또 다른 외부네트워크로 이동하는 경우 MN은 FA로부터 받은 광고 메시지 또는 DHCP(Dynamic Host Configuration Protocol) 서버로부터 받은 CoA를 통해 네트워크 간 이동을 감지하면, 3.1절에서 설명된 새로운 외부네트워크를 위한 등록과정을 시작함과 동시에 그림 4의 메시지 2(b)와 같이 이전 x-HA에게 새로운 CoA의 등록을 위한 MIP 등록요청 메시지를 보낸다. 이전 x-HA와의 인증을 위해 MN은 이 MIP 등록요청 메시지의 홈주소를 이전 x-HA에게 받은 x-HoA 주소로 계속 사용하고 이전 x-HA와의 세션키로 생성한 Mobile-Home Authentication Extension 필드를 그대로 포함한다. 따라서 이전 x-HA는 MIP 등록요청 메시지에 포함된 Mobile-Home Authentication Extension 필드를 통해 MN을 성공적으로 인증하게 된다. 인증이 성공하면, 이전 x-HA는 MN에 대한 Mobility Binding을 MN의 현재 위치로 갱신한 후 MN에게 MIP 등록응답 메시지를 보낸다(그림 4의 17). 이와 같이 이전 x-HA와의 등록이 완료되면, 목적지가 MN의 x-HoA인 패킷은 이전 x-HA로 전달된 후 FA로의 터널링을 통해 또는 직접 MN에게 계속 전달되어 핸드오버로 인한 패킷 손실을 줄일 수 있다. 한편, 외부네트워크를 위한 등록이 완료되어 새로운 x-HA를 할당 받고 VPN GW와 MN 간의 IPsec 터널이 설정되면, MN은 새로운 x-HA를 통해서 데이타를 전송 받게 되며 이전 x-HA에 대한 바인딩은 해제한다(그림 4의 18). 이와 같이 MN이 외부네트워크 간 이동 시에 이전 x-HA를 활용하도록 함으로써, 새로운 외부네트워크를 위한 등록 과정과 새로운 x-HoA를 사용한 VPN GW와의 IPsec 터널 설립이 이루어지는 동안 발생하게 되는 핸드오버로 인한 다량의 패킷 손실을 피할 수 있다.

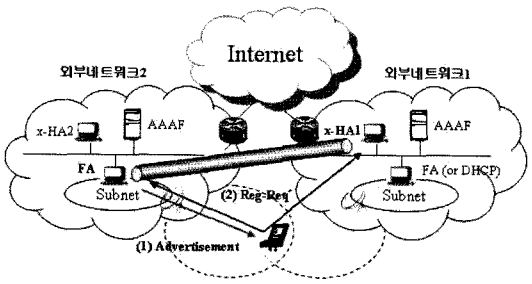


그림 5 이전 x-HA을 활용하기 위한 등록 메시지 전달 과정

4. 시뮬레이션

제안된 D-H 키 합의 알고리즘을 활용한 세션키 암호화 및 이전 x-HA 활용 방안을 사용하였을 경우 얻을 수 있는 효과에 대해 검토하기 위해 OPNET Modeler 11.0를 이용하여 시뮬레이션을 수행하였다.

제안된 방안의 구현을 위해 OPNET Modeler의 MIP 프로세서 모델을 수정하였으며, 여기에는 새로운 에이전트인 x-HA의 추가 및 x-HA와 i-HA, x-HA와 FA 간의 터널링 그리고 MN과 이전 x-HA와의 등록 메시지 전송과 이전 x-HA의 등록메시지 처리 과정이 포함된다. 또한 Diameter MIPv4 응용에 기반하여 외부네트워크에 x-HA를 동적으로 할당하는 과정과 AAAH의 키 분배 기능을 구현하였다. 제안된 방안의 성능 평가를 위해서 [3]에서 이동 VPN 사용자가 외부 네트워크 간 이동을 하는 경우 보안을 강화하기 위해 x-HA와

AAAH간에 IPsec 터널 설정을 하는 방안과 본 논문에서 제안한 D-H 키 합의 알고리즘 활용 방안을 비교하였다. 또한 제안된 방안의 성능에는 이전 x-HA를 활용하는 방안도 포함된다.

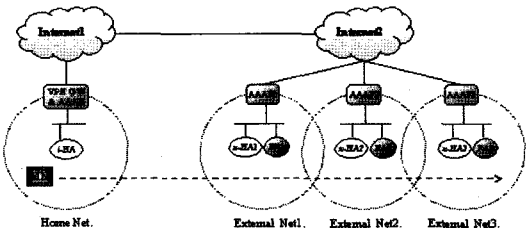


그림 6 시뮬레이션 네트워크 모델

그림 6은 시뮬레이션을 위한 네트워크 모델을 보여주고 있다. 시뮬레이션 네트워크 모델에서는 한 개의 홈네트워크와 3개의 외부네트워크가 존재하며 각 네트워크에는 MIP 에이전트와 AAA 서버가 존재한다. 홈네트워크는 VPN GW와 CN(Correspondent Node), 이동 단말인 MN으로 구성되어 있다. 무선접속망은 802.11b이며, 에이전트 간의 거리는 2km이고 안테나의 전송 파워는 0.005W로 하였다. MN은 홈네트워크에서 외부네트워크를 차례로 거치면서 일정시간을 외부네트워크 내에서 머무른 후 이동을 하며 CN은 128Kbps의 CBR 트래픽을 MN에게 전송한다. 각 노드에서 IPsec 터널 설정과 D-H 키 합의 알고리즘을 수행하기 위한 프로세싱 시간은 [7]에 따라 각각 215ms과 35ms으로 설정하였다.

그림 7은 MN이 외부네트워크2에서 외부네트워크3으로 이동하는 시점에서의 MN의 패킷 처리량 변화를 보여주고 있다. MN은 시속 60km로 이동하며 홈네트워크까지의 인터넷 지연시간은 0.1초라고 가정하였다. 시뮬레이션에서 MN은 하드 핸드오버를 하며 이동 후 등록 과정이 완료되기까지 데이타 손실이 발생되어 그림 7에서 보듯이 동적 x-HA 할당 방안과 제안 방안이 각각 약 10초와 20초간 패킷 수신이 0인 것을 볼 수 있다.

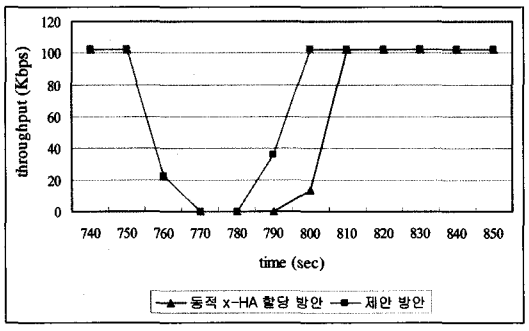


그림 7 처리량

제안한 방안에서는 MN이 네트워크 간 이동 후 새로운 x-HA와 AAAH 간에 IPsec 터널을 설정하는 과정을 수행하지 않기 때문에 등록 완료 시간이 더 짧을 뿐만 아니라, 이전 x-HA에게 자신의 현재 위치를 등록하여 데이타를 수신하는 방법으로 통신의 세션 재개 시간을 앞당겼다. 즉, 새로운 x-HA 등록 과정과 MN과 VPN GW와의 IPsec 터널 설정이 완료되는 시점까지 데이타 수신을 못하는 동적 x-HA 할당 방안에 비해 제안 방안은 더 빨리 새로운 위치에서 패킷 수신을 시작한다. 홈네트워크에 위치한 i-HA와의 등록 과정이 완료된 시점부터는 두 방안이 동일하게 동작하므로 두 경우의 처리량이 동일함을 볼 수 있다.

그림 8과 9는 인터넷 지연시간 변화에 따른 평균 처리율과 패킷 손실률을 보여주고 있다. 이 실험에서는 MN이 시속 60km로 외부네트워크1의 임의 지점으로부터 외부네트워크3의 임의 지점까지 반복적으로 이동하는 상황에서 홈네트워크와 연결된 인터넷의 지연시간을 증가시키면서 성능을 평가해 보았다.

동적 x-HA 할당 방안과 제안 방안은 MN이 외부네트워크 간 이동을 하는 경우에 홈네트워크에 위치한 홈 에이전트에게 등록 과정을 수행해야 하므로, 두 방안 모두 홈네트워크와 연결된 인터넷 지연시간이 증가함에 따라 처리율이 감소하고 패킷 손실률은 증가하는 경향

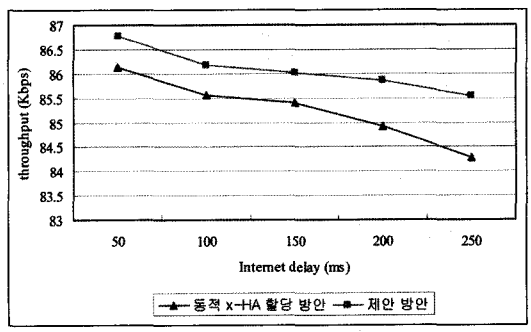


그림 8 처리율

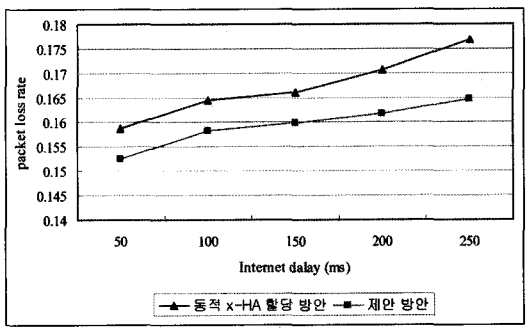


그림 9 패킷 손실률

을 보인다. 특히, 동적 x-HA 할당 방안은 MN이 네트워크 간 이동을 한 경우에 새로운 외부네트워크를 위한 등록 과정에 x-HA와 AAAH 그리고 MN과 VPN GW 간의 두 번의 IPsec 터널을 설정해야 한다. IPsec 터널 설정은 터널 종단 간에 6번의 IKE 메시지를 교환해야 하므로 MN과 홈네트워크와의 거리가 증가하거나 인터넷의 혼잡 등의 이유로 인터넷 지연시간이 증가할수록 동적 x-HA 할당 방안은 새로운 외부네트워크를 위한 등록완료 시간이 길어져 데이타 처리율이 급격히 감소하고 패킷 손실이 증가한다. 반면에 제안 방안은 MN이 새로운 외부네트워크를 위한 등록을 완료하기 전까지 이전 x-HA를 통해 데이타를 수신하므로 패킷 손실을 줄일 수 있으며, 이전 x-HA는 MN이 이동하기 직전의 네트워크에 위치하므로 MN과 i-HA와의 거리에 비해 상대적으로 가깝게 위치하므로 MN과 이전 x-HA와의 등록완료 시간은 인터넷 지연에 거의 영향을 받지 않아 동적 x-HA 할당 방안과 비교하여 좋은 성능을 나타낸다. 또한 제안 방안은 D-H 키 합의 알고리즘을 사용하여 AAAH가 x-HA에게 IPsec 터널 설정 없이 안전하게 세션키를 전달하므로 동적 x-HA 할당 방안에 비해 새로운 외부네트워크를 위한 등록이 빠르게 완료된다.

그림 10과 그림 11은 MN의 이동속도에 따른 평균 처리율과 패킷 손실률을 보여주고 있다. 이 실험에서는

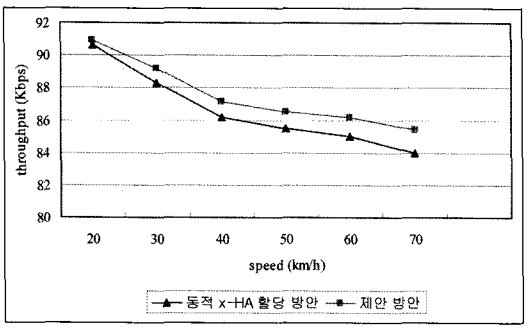


그림 10 처리율

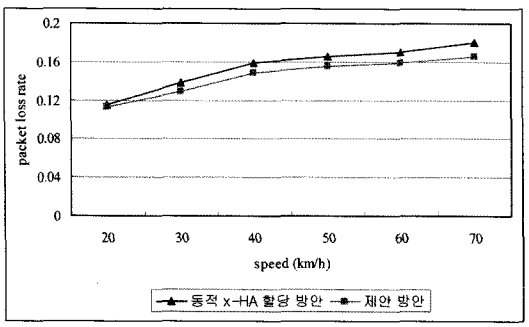


그림 11 패킷 손실률

MN의 이동속도를 시속 20km에서 시속 70km까지 10km 단위로 증가시켜 보았고, MN이 네트워크의 특정 장소에서 일정 시간을 머무르는 일 없이 외부네트워크1의 임의 지점으로부터 외부네트워크3의 임의 지점까지 반복적으로 4000초 동안 지속적으로 왕복 이동하는 상황을 실험했다. 홈네트워크와 연결된 인터넷의 지연시간은 0.1초로 하였다.

MN이 핸드오버를 완료하는데 걸리는 시간은 이동속도와 관계없이 거의 일정하지만, MN의 이동속도가 느릴수록 동일 시간 내의 핸드오버 횟수가 적으므로 핸드오버로 인한 데이타 손실이 적다. 따라서 두 방안 모두 이동속도가 증가함에 따라 처리율이 감소하고 패킷 손실률은 증가하는 경향을 보인다. 그런데 네트워크 간 이동이 발생하였을 때, 제안 방안에서는 새로운 외부네트워크에 대한 등록 완료 및 새롭게 획득한 x-HoA를 사용하여 VPN GW와 IPsec 터널을 설립하는 등 핸드오버 처리가 완료되기 전에 MN이 이전 x-HA를 통해 데이타를 수신하므로 모든 경우에 대해 동적 x-HA 할당 방안보다 좋은 성능을 나타낸다.

특히 이동속도가 빠를수록 제안 방안과 동적 x-HA 할당 방안의 성능차가 더 큰 경향이 있는데, 이는 MN의 이동속도가 느린 경우에는 제안하는 방안에서 이전 x-HA와 등록하는 시점이 MN이 새로운 FA의 안정적인 데이타 수신 범위에 도달하는 시점보다 더 빨라서 이전 x-HA가 전달해주는 데이타를 MN이 받지 못하는 경우가 발생하여 제안 방안의 장점을 충분히 활용치 못하기 때문이다. MN의 이동속도가 빨라지면 이와 같은 문제가 없어지기 때문에 동적 x-HA 할당 방안과의 성능 차가 좀 더 커지게 된다.

5. 결 론

본 논문에서는 MN과 x-HA가 안전하게 동적 MSA를 설립할 수 있도록 하기 위해 D-H 키 합의 알고리즘을 이용하여 세션키를 암호화하는 방안과 네트워크 간 이동에 대한 핸드오버 시의 데이타 손실을 줄이기 위해 이전 x-HA를 활용하는 방안을 제안하였다.

제안하는 방안에서는 MN과 x-HA가 동적으로 MSA를 설립하기 위해 사용할 세션키를 AAAH가 D-H 키 합의를 통해 생성한 비밀키로 암호화하여 x-HA에게 전달하도록 제안하였다. 이를 위해 x-HA와 AAAH에서 D-H 키 합의 알고리즘을 수행하는 프로세싱 오버헤드와 동일 네트워크에 존재하는 x-HA와 AAAF 간에 D-H 키 합의를 위한 메시지를 주고 받는 전송 오버헤드가 추가적으로 발생한다. 그러나 D-H 키 합의 알고리즘 프로세싱은 IPsec 터널을 설정하기 위한 IKE 협상 절차에 비해 간단하므로 [4]에서 제시한 방안에 비해

프로세싱 오버헤드가 적고, IKE 협상을 위해 여러 번의 IKE 메시지가 인터넷을 경유해야 하는 시간적 오버헤드를 제거하기 때문에 핸드오버 지연시간도 크게 감소시킨다. 한편, D-H 키 합의 알고리즘의 취약점으로 알려진 중간자 공격은 서로 간의 인증 절차 없는 키 교환이 원인이나, Diameter 기반 프로토콜은 pre-shared key 방식의 IKE를 통해 Diameter 노드 간 인증을 제공하므로 본 방안에서 사용하는 D-H 키 합의 알고리즘은 중간자 공격에 안전하다. 또한 본 방안은 MN이 외부네트워크 간 이동을 하는 경우 이전 x-HA를 활용하여 빠르게 세션을 재개함으로써 이동으로 인한 데이타 손실률을 최소화 하도록 하였다. 시뮬레이션을 통하여 제안한 방안의 성능을 평가해 본 결과, 이동 VPN 사용자가 외부네트워크 간 이동을 하는 경우에 안전하게 x-HA를 할당 받고 핸드오버 시 빠르게 세션을 재개함으로써 패킷 손실을 줄여 성능을 향상시킴을 볼 수 있었다.

참 고 문 헌

[1] Adrangi, F., "Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways," RFC4093, 2005.

[2] Vaarala, S., "Mobile IPv4 Traversal Across IPsec-based VPN Gateways," draft, 2005.

[3] Yi-Wen Liu, "dynamic external Home Agent Assignment in Mobile VPN," Vehicular Technology Conference, 2004.

[4] Calhoun, P., "Diameter Mobile IPv4 Application," RFC4004, 2005.

[5] Calhoun, P., "Diameter Base Protocol," RFC3588, 2003.

[6] Rescorla, E., "Diffie-Hellman Key Agreement Method," RFC2631, 1999.

[7] Craig Shue, "Analysis of IPsec Overheads for VPN Servers," 1st IEEE ICNP Workshop, 2005.

[8] P. Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)," draft, 2006.

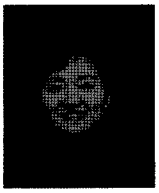
[9] V. Devarapalli, P. Eronen, "Secure Connectivity and Mobility using Mobile IPv4 and MOBIKE," draft, 2006.

우 현 제

1999년~2004년 이화여자대학교 컴퓨터학과 학사. 2004년~2006년 이화여자대학교 대학원 컴퓨터학과 석사. 관심분야는 MVPN, NEMO, VPN QoS

김 경 민

2001년~2005년 이화여자대학교 컴퓨터학과 학사. 2005년~현재 이화여자대학교 대학원 컴퓨터학과 석사. 관심분야는 Mobile VPN, VPN, 인터넷 QoS 지원, 무선 네트워크



이 미 정

1983년~1987년 이화여자대학교 전자계산학 학사. 1987년~1989년 University of North Carolina at Chapel Hill 컴퓨터학 석사. 1990년~1994년 North Carolina State University 컴퓨터공학 박사. 1994년~현재 이화여자대학교 공과대학 컴퓨터학과 교수. 관심분야는 고속 통신 프로토콜 설계 및 성능 분석, 멀티미디어 전송을 위한 트래픽 제어, 인터넷에서의 QoS 지원, 무선 이동 네트워크, Ad-hoc 네트워크, 광대역통합망, 가상사설망