Journal of The Korea Society of Computer and Information
Vol. 17 No. 9, September 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.9.057

네트워크 이동성 환경에서 안전한 Seamless 핸드오버 지원을 위한 인증 프로토콜

김 종 영*, 윤 용 익**, 이 강 호***

Authentication Protocol Supporting Secure Seamless Handover in Network Mobility (NEMO) Environment

Jongyoung Kim, Yong-ik Yoon, Kang-ho Lee

요 약

네트워크 이동성 환경에서 기존에 제안된 프로토콜들은 많은 계산비용을 필요로 하거나 바인딩 갱신의 지연을 초래 할 수 있다. 이를 해결하기 위해 본 논문에서는 네트워크 이동성 환경에서 안전한 seamless 핸드오버를 지원하기 위한 경량화된 인증 프로토콜을 제안한다. 이 방식은 바인딩 갱신 지연 시간을 최대한 줄이기 위해 접속 라우터간의 그룹키와 키 발행 서버로부터 발행된 마스터키를 이용하여 이동 라우터와 접속 라우터 간에 빠른 상호인증을 수행한다. 분석 결과 기존의 제안된 프로토콜보다 적은 계산량으로 빠른 바인딩 갱신을 수행할 수 있었으며 기존의 공격에도 강건함을 보였다.

▸ Keywords : 경량화된 상호 인증, 네트워크 이동성, 끊김 없는 핸드오버

Abstract

The existing protocols proposed in network mobility (NEMO) environment can require many computational costs and can bring about a delay of binding update. To solve these problems, in this paper we propose an authentication protocol supporting secure seamless handover in NEMO environment. The proposed protocol can handle quickly mutual authentication between a mobile router (MR) and an access router (AR), which uses group key among ARs and a master key (MK) issuing from key issuing server (KIS) for reducing the time of binding update as much as possible. In performance, the proposed protocol can process quickly binding update with little computational cost comparison with the existing binding update protocols and it results in robustness against

* 제1저자 : 김종영, 교신저자 : 김종영
* 김종영 입체영상 문화기술 공동연구센터
** 윤용익 숙명여자대학교멀티미디어과학과
*** 이강호 국립한국복지대학교컴퓨터정보보안과
• 투고일 : 2011. 07. 12, 심사일 : 2012. 08. 20, 게재확정일 : 2012. 09. 24.

existing attacks.

▸ Keywords : Lightweight mutual authentication, Network mobility (NEMO), Seamless handover

I. 서 론

이동 네트워크는 무선 네트워크 분야에서 상당한 주목을 받고 있다. 이동 네트워크 환경에서 사용자들은 스마트폰과 PDA를 이용하여 언제 어디서나 인터넷에 접속하여 데이터 전송, VoIP, 동영상 검색과 같은 서비스를 이용한다. 이동 네트워크는 선박이나 비행기뿐만 아니라 기차와 같은 운송 수단에 구성될 수 있다. 이동 네트워크가 다른 네트워크로 이동하게 되면 이동 네트워크 안에서 인터넷 서비스를 이용하는 많은 사용자들의 인터넷 서비스가 끊기게 된다.

IETF(Internet Engineering Task Force)에서는 이런 문제점을 해결하기 위해 NEMO Basic Support[1]를 제안하였다. 이는 기존의 모바일 IPv6[2]를 확장한 것으로 이동 네트워크가 다른 네트워크로 이동하게 되면 외부 네트워크의 접속 라우터(AR: Access Router)로부터 네트워크 프리픽스를 포함한 네트워크 정보를 획득하여 이동 라우터(MR: Mobile Router)는 주소 자동 설정 방법에 의해 의탁주소(CoA: Care-of Address)를 구성한다. 그런 후에 이동 라우터는 자신의 홈 에이전트(HA: Home Agent) 및 대응노드(CN: Correspondent Node)와 바인딩 갱신(binding update)을 수행하여 의탁주소를 등록한다. 이를 통해 이동 네트워크에 있는 노드들에게 투명한 인터넷 접속을 제공한다.

하지만 이동 네트워크는 무선 접속 방법으로 인터넷 서비스를 제공하기 때문에 링크 신뢰성이 떨어질 수 있다. 더욱이 하나의 이동 라우터가 처리해야 하는 사용자의 수는 증가할 수 있다. 이런 문제점을 개선할 수 있는 방법이 이동 네트워크에 다수의 이그레스(egress) 인터페이스를 제공하거나 다수의 이동라우터 및 글로벌(global) 인터페이스를 제공하는 것일 수 있다[3-4]. 이런 개념이 멀티호밍(multi-homing)이다. 더욱이 이런 과정이 안전하게 수행되지 않을 경우 이동 네트워크에서 인터넷 서비스를 제공받는 많은 사용자들에게 중요한 정보의 누출과 같은 치명적인 위험을 초래할 수 있다. NEMO Basic Support는 충분한 인증 메커니즘을 제공하지 않고 있다.

[5]와 [6]은 AAA(Authentication, Authorization, Accounting) 모델을 이용하여 NEMO Basic Support의 안전성을 지원하기 위한 방법을 제안했다. H. Fathi외 5명[5]은 공개키 기반 구조(PKI)에 기반한 LR-AKE(leakage resilient-authentication key establishment) 기법을 제안했다. 일반적으로 PKI는 다양한 공격자들로부터 강력한 인증을 제공하지만 대부분의 모바일 장치들에게는 많은 부담을 줄뿐만 아니라 바인딩 갱신 시간도 지연될 수 있다. Shi외 1명[6]은 인증 과정에 대한 RTT(Round trip time)을 줄이기 위한 로컬 인증 기법을 제안했다. 그러나 모바일 라우터의 홈 AAA가 모바일 라우터가 최초 다른 네트워크로 이동했을 경우 인증 절차를 수행해야 한다. 만일 다른 네트워크가 홈 네트워크와 상당한 거리에 있을 경우에는 인증 지연이 발생할 수 있다.

본 논문에서는 안전한 seamless 핸드오버를 지원하기 위한 경량화된 인증 프로토콜을 제안한다. 제안하는 기법은 바인딩 갱신 지연 시간을 최대한 줄이기 위해 접속 라우터간의 그룹키를 생성하고 키 발행 서버로부터 발행된 마스터키를 이용하여 이동 라우터와 접속 라우터 간에 빠른 상호인증을 수행한다. 이는 빠른 바인딩 갱신을 수행하므로 seamless 핸드오버를 지원할 수 있고 기존의 공격에 강건함을 보이며 각 노드에서 처리해야 할 계산량 역시 적다.

본 논문은 다음과 같이 전개된다. 2장에서는 관련연구에 대해 기술하며, 3장에서는 제안하는 프로토콜에 대해 설명한다. 4장에서는 제안하는 프로토콜의 안전성 및 효율성을 분석한다. 마지막으로, 5장에서는 결론과 향후 계획에 대해서 논의한다.

II. 관련 연구

1. NEMO Basic Support[1]

NEMO[1]은 이동네트워크에 존재하는 많은 사용자들에게 투명한 네트워크 이동성을 지원하기 위해 제안되었다. 이동 라우터가 홈 네트워크에서 외부 네트워크로 이동했을 때 먼저 외부 네트워크에서 프리픽스 정보를 획득하여 의탁주소를 생성한다. 그런 다음 이동 라우터는 새롭게 구성한 의탁주소를 자신의 홈 에이전트에게 등록한다. 이때, NEMO는 구체적인 AAA를 이용한 인증 방법을 제시하지 않고 있다. 따라서 IETF는 이런 문제점을 해결하기 위해 이동 네트워크가 다른 네트워크로 이동하는 동안 이동 라우터부터 요청이 왔을

때 AAA 문제를 해결하기 위한 AAA 모델을 제안했다. 하지만 이동하고 있는 이동 라우터와 로컬 AAA 서버 간에 사전에 어떤 비밀 정보를 공유할 수 없다. 왜냐하면 이동 라우터와 로컬 AAA 사이에는 직접적인 SA(Security Association)가 부족하기 때문이다.

2. LR-AKE[5]

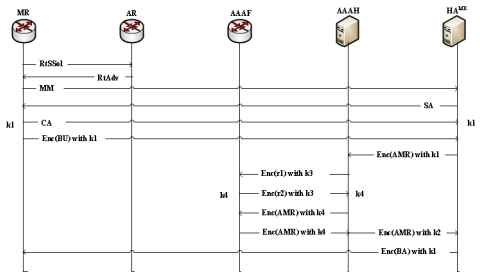

그림 1. LR-AKE
Fig. 1. LR-AKE

H. Fathi외 5명은 NEMO를 위한 인증 기법 LR-AKE 기법을 제안했다. 구체적인 홈 에이전트와의 인증 방법은 그림 1과 같다. 먼저 이동 라우터는 MM(Masked message) 메시지를 자신의 홈 에이전트 HA^{MR}에게 전송한다. 이에 대한 응답으로 HA^{MR}은 SA(Sever authenticator) 메시지를 전송한다. 이동 라우터는 SA 메시지를 수신한 후에 HA^{MR}를 인증하고 CA(Client authenticator)메시지를 전달하고 세션키 k1을 생성한다. HA^{MR}역시 MR를 인증하고 같은 세션키 k1을 생성한다. 다음으로, 이동 라우터는 세션키 k1으로 암호화한 바인딩 갱신 메시지 Enc(BU)를 HA^{MR}에게 전송한다. HA^{MR}은 AAAH와 미리 공유한 비밀키 k2로 AMR(AAA message request) 암호화한 Enc(AMR) 메시지를 AAAH에게 전달하면 AAAH는 핸드오버 이전의 AAA인 AAAF에게 미리 공유한 비밀키 k3로 암호화한 Enc(r1) 메시지를 전송한다. 여기서 r1은 임의 수(random number)이다. AAAH와 AAAH가 상호 인증이 끝나면 각각은 k4를 다음과 같이 생성한다.

$$k4=h6(r1||r2||AAAH\_addr||AAAF\_addr)$$

이 키는 두 노드 간의 재생 공격을 방지하기 위해 사용된다. AAAF는 k4로 AMR 메시지를 암호화하여 AAAH에게 전달한면 AAAH는 HA와 미리 공유한 비밀키 k2로 암호화해서 전달한다. 그런 후에 이동 라우터와 공유한 비밀키로 HA^{MR}은 바인딩 응답(binding acknowledgement) 메시지를 이동 라우터에게 전달한다. 이로서 전체 바인딩 갱신 과정이 종료한다. 이 방법은 앞서 설명한 바와 같이 공개키 기반의 인증 기법으로 계산량이 다소 많다는 점과 인증된 바인딩 갱신을 위해 많은 절차가 필요하여 바인딩 갱신 지연을 초래할 수 있다.

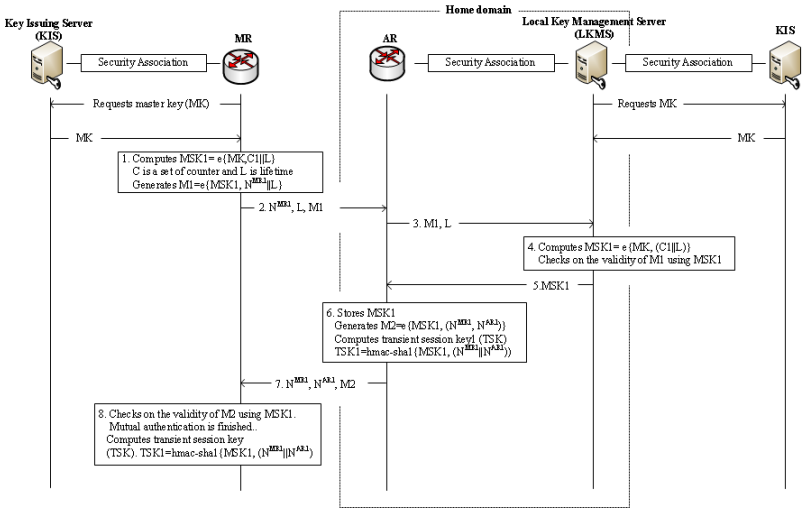

그림 2. Home 도메인에서의 최초 인증 과정
Fig. 2. Initial authentication process in home domain

3. Shi외 1명[6]

Shi외 1명은 인증 과정에 대한 RTT를 줄이기 위한 로컬 인증 기법을 제안했다. 그러나 모바일 라우터의 홈 AAA가 모바일 라우터가 최초 다른 네트워크로 이동했을 경우 인증 절차를 수행해야 한다. 만일 다른 네트워크가 홈 네트워크와 상당한 거리에 있을 경우에는 인증 지연이 발생할 수 있다. 또한 이동 라우터와 LAAA 간에 미리 세션키를 공유할 수 있다는 가정을 하고 있으나 이는 일반적인 AAA 모델에서는 쉽지 않다.

4. Koo외 2명[7]

Koo외 1명은 이종 네트워크에서 네트워크 이동성을 지원하기 위해 CGA(Cryptographically Generated Address) 기반의 인증된 경로 최적화 기법을 제안하였다. 이 기법은 이동 라우터와 AR는 각 1번의 암·복호화와 해쉬연산을 수행하여 빠른 바인딩 갱신을 수행 할 수 있지만 홈 에이전트에서 처리해야 할 계산량이 다소 많다는 단점이 있다.

III. 제안하는 프로토콜

본 절에서는 제안하는 프로토콜에서 사용할 표기법과 가정에 대해 기술한 후 프로토콜에 대한 상세한 설명을 하도록 한다. 표기법과 가정은 다음과 같다.

1. 표기법 및 가정

- KIS(Key issuing server) : 키 발행 서버로서 MR와 LKMS(Local key management server)에게 마스터 키 MK(Master key)를 발행한다.
- LKMS : 로컬 키 관리 서버로서 홈 도메인에 있는 AR 간에 그룹키를 생성하고 이동 라우터와의 인증을 위한 마스터 세션 키 MSK(Master session key)를 발행한다.
- MK : 마스터 키로서 이동 라우터와 AR간에 상호 인증 시 메시지 암호화를 위한 MSK를 생성하는데 사용된다. 전체 세션이 종료되면 갱신된다.
- MSK : 마스터 세션키로 이동 라우터와 AR간에 인증하기 위한 메시지 암호화에 사용되며 TSK를 생성하는데 사용된다. 홈 도메인에서 외부 도메인으로 이동 라우터가 이동시에 갱신된다.
- TSK : 일시적 세션키로 이동 라우터와 AR간에 안전한 바인딩 갱신 및 패킷 전송에 사용되며, AR간에 핸드오버가 발생시 갱신된다.
- C : 키 생성 노드 간에 동기화된 카운터이다. 마스터 세션키 생성에 사용된다.
- e(K,M) : 비밀키 K로 메시지 M을 암호화한다.
- hmac-sha1(K,M) : 키 K로 메시지 M을 계산한 MAC(Message authentication code)이다.
- N/L : nonce와 lifetime이다.
- M1||M2 : 메시지 M1와 메시지 M2의 비트 결합이다.

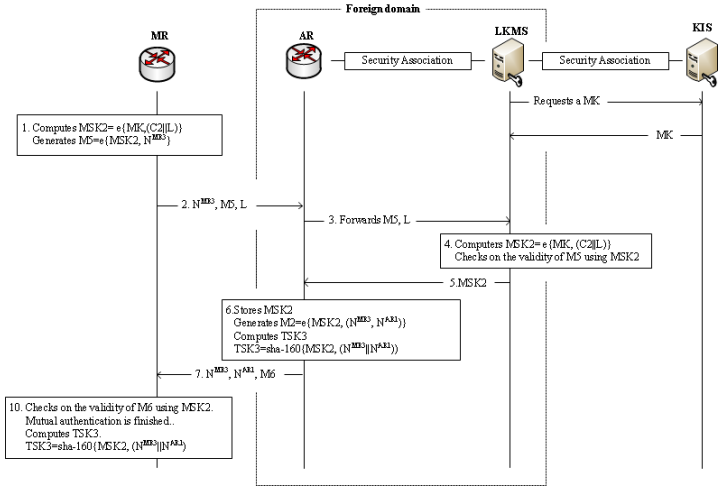

그림 3. Home 도메인에서 Foreign 도메인으로 핸드오버시 인증 과정
Fig. 3. Authentication process on handover from home domain to foreign domain

본 인증 기법에서는 다음과 같은 사항들을 가정한다.

- 이동 라우터 및 LKMS는 미리 SA를 맺을 수 있다.
- LKMS는 핸드오버 전에 미리 그룹키를 생성하여 AR에게 전달 할 수 있다.

2. 프로토콜

홈 도메인에서 최초 MR와 AR간의 인증 과정은 그림 2와 같다. 이동 라우터와 LKMS는 미리 KIS로부터 MK를 안전한 채널을 이용하여 획득한다.

MK를 획득한 이동 라우터는 최초 AR과의 인증을 위해 MSK1=e{MK, (C1||L)}를 생성한다. 그런 후에 AR와 상호 인증을 위해 MSK를 이용하여 메시지 M1=e{MSK1, (N^{MR1}||L)}를 생성하고 AR에게 L와 N^{MR1} 메시지와 함께 전송한다. AR는 메시지를 수신한 후에 자신의 LKMS에게 전달하면 LKMS는 정당한 사용자로부터 수신한 메시지인지 확인하기 위해 먼저 MK를 이용하여 MR와 같은 방법으로 MSK1을 생성하고 메시지 M1을 인증한 후 그룹키를 이용하여 안전하게 생성한 MSK1을 AR에게 전송한다. AR는 안전하게 MSK1을 저장하고 M2={MSK1, (NMR1, NAR1)}를 생성하여 이동 라우터에게 전송한다. 이동 라우터는 M2 메시지를 검증하여 AR를 인증한다. 그런 후에 이동 라우터와 AR는 TSK=hmac-sha1{MSK1, (NMR1||NAR1)}를 생

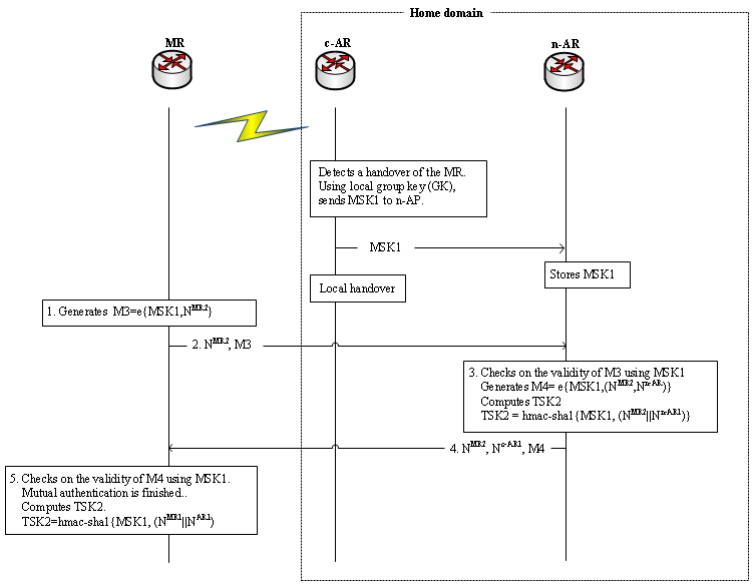

그림 4. 홈 도메인에서 핸드오버시 인증 과정
Fig. 4. Authentication process on handover in home domain

표 1. 각 프로토콜의 연산량 비교
Table 1. Comparision of Protocol Computations

	계산량								
	MR				AR				합계
	해시함수	암호화	복호화	공개키 연산	해시함수	암호화	복호화	공개키 연산	
[5]	3×0.026K	2×3028K	2×3028K	1×62000K(서명) 1×3019K(복호화)	3×0.026K	2×3028K	2×3028K	1×62000K(서명) 1×3019K(복호화)	154262.156K
[6]	4×0.026K	2×3028K	2×3028K	0	4×0.026K	2×3028K	2×3028K	0	24224.208K
[7]	1×0.026K	1×3028K	1×3028K	0	1×0.026K	1×3028K	1×3028K	0	12116.052K
Proposed method	3×0.026K	1×3028K	1×3028K	0	1×0.026K	1×3028K	1×3028K	0	12116.078K

성한다. 이로서 홈 도메인에서 이동 라우터와 AR간에 최초 인증 과정이 종료된다.

그림 3은 이동 라우터가 홈 도메인에서 외부(foreign) 도메인으로 핸드오버시 인증과정을 나타낸다. 외부 도메인에 있는 LKMS 역시 홈 도메인에 있는 LKMS와 같이 KIS로부터 MK를 획득한다. 이동 라우터는 외부 도메인으로 핸드오버시 먼저 도메인이 변경되었기 때문에 MSK2=e{MK, (C2||L)}를 새로 생성한다. 이를 이용하여 M5=e{MSK2, N^{MR3}}를 생성하여 AR에게 전달하면 홈 도메인의 AR와 같이 LKMS에게 전달한다. LKMS는 MSK2를 이동 라우터와 동일하게 생성하고 MSK2를 외부 도메인에 있는 AR간의 그룹키를 이용하여 AR에게 전송한다. AR는 MSK2를 안전하게 저장하고 M6=e{MSK2, (NMR3, NAR1)}를 생성하고 이동 라우터에게 전송한다. 이동 라우터는 MSK2로 M6메시지를 인증하고 TSK3=sha-160{MSK2, (N^{MR3}||N^{AR1})}를 AR와 같이 생성한다. 이로서 이동 라우터가 외부 도메인으로 이동했을 경우에도 홈 도메인에 있을 때와 같이 간단한 방법으로 AR를 인증하고 키를 생성할 수 있다. 이동 라우터는 자신의 홈 에이전트와 대응노드에게 자신의 의탁주소를 등록하여 빠른 바인딩 갱신을 수행한다.

그림 4는 이동 라우터가 동일한 홈 도메인에서 핸드오버가 발생했을 시 인증 과정을 나타낸다. 이때는 이동 라우터가 외부 도메인으로 이동을 한 경우가 아니기 때문에 자신의 홈 에이전트와 바인딩 갱신을 수행할 필요는 없다. 다른 도메인으로 핸드오버가 발생했을 경우와 달리 간단하고 빠른 인증을 수행할 수 있다. 먼저 AR는 이동 라우터의 홈 도메인 핸드오버 조짐을 미리 감지하고 인접 AR인 n-AR에게 로컬 그룹키를 이용하여 MSK1을 전송한다. n-AR은 MR로부터 수신한 M3=e{MSK1, NMR2}를 MSK1을 이용하여 검증하고 M4=e{MSK1, (N^{MR2}, N^{n-AR})}를 생성한 후 MR에게 전송한다. 이동 라우터 역시 MSK1을 이용하여 n-AR을 인증하고 안전한 패킷 전송을 위한 TSK2=hmac-sha1{MSK1, (N^{MR1}||N^{n-AR})}를 n-AR와 같은 방법으로 생성한다.

IV. 분 석

1. 안전성 분석

- 재생 공격(Replay attack) : 최초 인증 과정에서 재생 공격이 발생할 수 있는 구간은 이동 라우터와 AR사이의 전송 메시지 구간이다. 다른 구간은 미리 확립된 비밀키를 이용하여 SA를 확립하고 있기 때문에 불가능하며 이동 라우터와 AR간 역시 Nonce를 이용하고 있기 때문에 이 공격에 강인함을 보인다.
- 중간자 공격(Man-in-the middle attack) : 이동 라우터와 AR간에 전송되는 메시지는 비밀키 MSK로 암호화 되어 있기 때문에 중간자가 공격에 안전하다.
- 리소스 고갈 공격(DoS, denial of service) : 이동 라우터와 AR간에 인증 절차시 공개키와 같은 계산량이 많은 지수 연산을 수행하지 않기 때문에 리소스 고갈 공격에 강인함을 보인다.

2. 계산량 분석

효율성은 프로토콜에 참여하는 각 단말의 계산량과 통신량을 통해 분석할 수 있는데 통신량은 일정하다고 가정하고 각 노드의 계산량만으로 프로토콜을 분석한다[7]. 분석 결과는 표 1과 같다.

LR-AKE[5] 프로토콜은 공개키 기반의 인증 방법으로 MR과 AR은 인증 및 키 동의를 위해 각각 한번의 서명과 검증을 수행하며 2번의 암·복호화 과정을 수행하여 대략 154262Kbyte의 계산량이 요구된다. Donghai 외 1명[6]의 프로토콜은 공개키 기반이 아니기 때문에 LR-AKE 프로토콜과는 달리 공개키 연산이 요구되지는 않지만 이동 라우터와 AR가 각각 2번의 암·복호화과정을 수행하기 때문에 대략 24224Kbyte의 계산량을 필요로 한다. 이와 달리 [7]은 각 1번의 암·복호화와 해쉬연산을 수행하여 제안하는 프로토콜과 거의 비슷한 계산량인 12116Kbyte의 계산량이 요구된다. 하지만 [7]의 경우에는 각 라우터의 홈 에이전트에서 처리해야할 계산이 많다. 마지막으로 제안하는 프로토콜은 이동 라우터와 AR에서각각 1번의 암·복호화 과정과 3번의 해쉬연산을 수행하여 12116Kbyte의 계산량이 필요하다. 이는 [7]과 달리 홈에이전트에서 처리해야할 계산이 없다.

V. 결론

본 논문에서는 네트워크 이동성 환경에서 안전한 seamless 핸드오버를 지원하기 위한 인증 기법을 제안하였다. 기존에 제안된 프로토콜들은 각 노드에서 처리해야할 계산적 부담이 있거나 이동 라우터와 AR간의 인증 지연으로 인해 신속한 바인딩 갱신을 수행하기 힘들었다. 해당 기법은 각 노드에서 처리해야할 계산량을 줄이기 위해 해쉬기반의 경량화된 인증기법을 사용하였고, 이동 라우터와 AR들간의 빠른 상호인증을 위해 같은 도메인에 있는 AR들 간에 그룹키와 키 발행 서버의 마스터키를 이용하였다. 이는 기존에 제안된 기법들과 비교 분석한 결과 기존 공격에 강건함을 보였고 계산량 역시 가장 적었다. 이를 통해 빠른 바인딩 갱신을 수행 할 수 있음을 보였다. 향후에는 MR의 중첩된 환경에서 경량화된 인증 프로토콜에 대해 연구할 것이다.

참고문헌

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, Jan. 2005.

[2] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6", Internet Engineering Task Force (IETF) Request for Comment (RFC) draft-ietf-mext-rfc3775bis-13 (work in progress), Mar. 2011.

[3] Wallaace D. T. and Shami A., "Review of Multihoming Issues Using the Streaming Control Transmission Protocol", IEEE Communications Survey & Tutorials, vol.13, pp.1-14, June 2011.

[4] Mase K., "Layer 3 wireless mesh networks: mobility management issues", IEEE Communications Magazine, vol.49, pp.156-163, July 2011.

[5] H. Fathi, S. Shin, K. Kobara, S. Chakraborty, H. Imai, and R. Prasad, "LR-AKE-Based AAA for Network Mobility (NEMO) Over Wireless Links", IEEE Journal on Selected Area in Communications (JSAC), vol.24, pp.1725-1737, Sept. 2006.

[6] Donghai Shi and Chojing Tang, "A Fast Handover Shame Based on Local Authentication in Mobile Network", 6th IEEE International Conference on ITS Telecommunications Proceedings (ITST), pp.1025-1028, June 2006.

[7] Jung-Doo Koo, Seong-Hoon Oh, and Dong-chun Lee, "Authenticated Route Optimization Scheme for Network Mobility (NEMO) Support in Heterogeneous Networks", International Journal of Communication Systems (IJCS), vol.23, pp.1252-1267, Sept. 2010.

저 자 소 개

김 종 영

1996 : 한양대학교
전자계산학과 공학사
1998 : 한양대학교
전자계산학과 공학석사
현 재 : 입체영상 문화기술 공동연구센터
관심분야 : 컴퓨터 보안, 모바일 컴퓨팅
Email : kim.jongyoung@gmail.com

윤 용 익

1983 : 동국대학교 통계학과 이학사
1985 : 한국과학기술원
전산공학과 공학석사
1994 : 한한국과학기술원
전산공학과 공학박사
현 재 : 숙명여자대학교
멀티미디어과학과 교수
관심분야 : 스마트사이니지, 스마트 클라우드 컴퓨팅, 모바일 멀티미디어 시스템, 분산시스템, 실시간 처리시스템, 미들웨어, 실시간 OS/DBMS, 상황인지 서비스, N-Screen 표준화, 모바일 클라우드
Email : yiyoon@sookmyung.ac.kr

이 강 호

1986 : 중앙대학교
전자공학과 공학석사
1991 : 중앙대학교
전자공학과 공학박사
현 재 : 국립한국복지대학교
컴퓨터정보보안과 교수
관심분야 : 정보보안, 디지털영상처리, 컴퓨터 네트워크 보안
Email : lkh@hanrw.ac.kr