PKI 기반 이동 네트워크에서의 안전한 보안 구조

김수정°, 김미희, 채기준
이화여자대학교, 컴퓨터학과
{iris1993°, mihui, kjchae}@ewha.ac.kr

A Secure Security Architecture on the PKI-based Mobile Network

Soojeong Kim°, Mihui Kim, Kijoon Chae
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

MIPv6(Mobile IPv6)를 확장한 새로운 이동통신 기술인 이동 네트워크 (NEtwork MObility, NEMO)는 여러 개의 노드와 하나 이상의 이동 라우터(Mobile Router, MR)로 구성되어 네트워크 단위로 이동성을 지원한다. NEMO의 경우 여러 네트워크들이 계층적으로 이루어진 형태를 가지고 있기 때문에, 상위 네트워크와 하위 네트워크의 긴밀한 관계가 유지되어야 한다. 따라서 이동 네트워크와 자신에게 서비스를 제공해 줄 방문 네트워크상에서 상위 네트워크와의 상호인증이 보안상 무엇보다 중요하다. 본 논문은 PKI와 challenge-response를 사용한 상호인증을 제안한다. 또한, 이러한 인증에 필요한 인증서를 받기 위해서는 기존의 중앙 집중화된 인증기관의 인증서 서비스는 이동 환경에 적합하지 않으므로, secret-share 기법을 이용하여 분산화된 환경에서 인증서 서비스를 제공하는 안전한 보안 구조를 제안한다.

1. 서 론

최근 무선 네트워크의 기술 발달로 많은 기기들이 이동성 지원을 요구하고 있다. 그러나 기존의 Mobile IPv6는 이동성 지원을 위한 시그널 양이 단말과 비례한다는 점에서 대역폭 낭비가 심하다. 이동 네트워크 기술[1]은 Mobile IPv6를 바탕으로 여러 이동 단말과 하나 이상의 이동 라우터를 이동 네트워크라는 단위로 묶어 이동성을 제공한다. 이때 노드들은 이동 라우터를 통해 인터넷에 접속하기 때문에 이동과 관련된 아무런 작업이 필요 없고 그만큼 바인딩(binding) 시그널이 줄어 인터넷 접속 비용 절감과 여러 노드가 동시에 바인딩 업데이트를 하여 발생하는 바인딩 스톰 문제를 해결할 수 있다. 이동 라우터는 이동시 자신의 홈 에이전트(Home Agent, HA)에 바인딩 하여 생성된 양방향 터널을 통해 패킷을 주고받으면서 통신을 이어가게 된다. 그러나 그림 1에서 보듯이 NEMO의 경우 여러 네트워크들이 계층적으로 이루어져 있어, 이동 네트워크가 방문 네트워크로 이동한 경우 자신과 연결된 상위 네트워크를 통해서만 인터넷 서비스를 받을 수 있고, 또한 이동 네트워크 역시 방문 네트워크의 구성원이 되어 향후 자신이 하위 계층으로 연결될 새로운 이동 네트워크에게 서비스를 제공해야 한다. 따라서 방문 네트워크와 이동 네트워크의 상호인증이 필수적이다. 또한 인증 후 PKI구조를 위한 X.509와 같은 중앙 인증기관 방식은 하나의 서버가 서비스를 담당하므로 서비스 에러나 공격에 분산구조보다 취약하고, 확장성이 떨어져 네트워크의 구조가 가변하는 이동 네트워크 환경에 맞지 않고 무선이라는 환경상 에러률이 높아 원격 서버로부터의 서비스 에러가 증가할 수 있다.

이 논문에서는 우선 이동 네트워크 환경에서 적합한 보안 구조를 제안하기 위해 적용될 관련 연구들과 이동 네트워크 구조를 위한 기본 가정 설명하고자 한다. 이를 바탕으로 보안을 위한 별다른 기반 구조가 필요 없는 challenge-response와 PKI 방식을 혼합한 상호 인증 방식을 제안하고, 현재의 중앙 인증기관 방식의 문제점을 해결할 수 있는 분산화된 인증서 서비스 메커니즘으로서 secret-share를 이용한 인증서 서비스 방식을 제안하고자 한다.

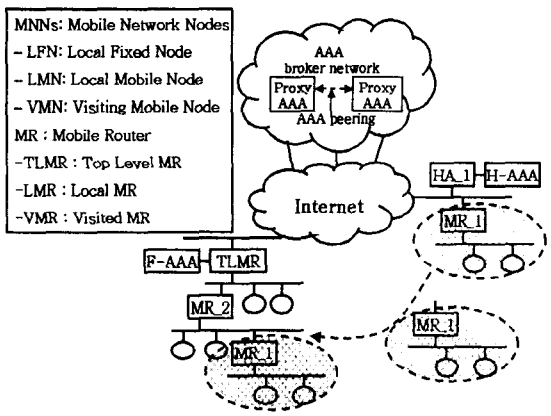

그림 1. 기본적인 이동 네트워크 구조

2. 관련연구 및 가정

2.1 AAA (Authentication, Authorization and Accounting) 구조

본 논문에서는 EAP (Extensible Authentication Protocol)구조를 따른다. MR의 HA가 홈 네트워크의 AAA 서버(Home AAA sever, H-AAA)로 방문 네트워크의 TLMR를 방문 네트워크의 AAA 서버(Foreign AAA server, F-AAA)로 가정한다. 두 AAA 서버를 따로 두어도 무방하다. 그리고 두 AAA간에 secure association을 맺었거나(복잡도 $O(N^2)$), 중간에 AAA broker를 두어(복잡도 $O(N)$) 두 서버 간의 통신은 안전하게 이루어진다고 가정한다[2].

2.2 PKI(공개키 기반구조)

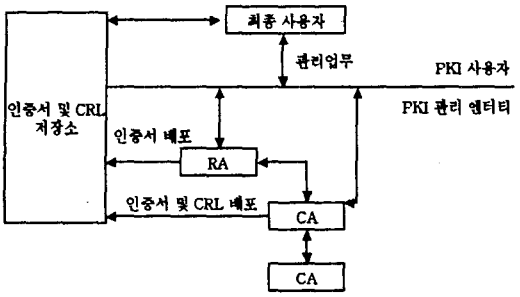

그림 2. X.590를 이용한 인증 시스템

그림 2는 PKI 기반의 인증서 처리 기반 기술인 X.509의 구조이다. X.509는 중앙의 인증기관(CA)이 인증서를 발급, 관리, 폐지, 감사하는 구조를 가진다[3].

다음은 인증서와 전자 서명을 사용한 인증 절차를 보여준다[4].

1)단방향 사용자 인증 :

$A \leftarrow B$: r_B (1)

$A \rightarrow B$: $cert_A$, r_A, ID_B, $S_A(r_A, r_B, ID_B)$ (2)

2)상호 인증 :

$A \leftarrow B$: r_B (1)

$A \rightarrow B$: $cert_A$, r_A, ID_B, $S_A(r_A, r_B, ID_B)$ (2)

$A \leftarrow B$: $cert_B$, ID_A, $S_A(r_B, r_A, ID_A)$ (3)

r_i : 난수, $cert_i$: 사용자 i의 인증서, ID_i : i의 아이디
S_i : 사용자 i의 비밀키를 이용한 전자 서명

난수를 대신하여 타임스탬프를 사용할 경우 메시지 수는 한개 감소하나, 두 사용자간 동기화가 필요하다[4].

2.3 secret-share 메커니즘[5]

secret-share 메커니즘은 비밀 다항식(secret polynomial)을 근본으로 한다. 방정식 f(x)가 (K-1)차 방정식일 때, K개의 (x, f(x))의 쌍을 알면, 이 방정식은 구할 수 있다. 이 아이디어를 바탕으로 일정 K개의 노드로부터 부분 정보가 모이면 RSA의 비밀키인 SK=<d,n>의 정보를 유추할 수 있게 된다.

secret-share 방식은 우선 네트워크에 새로 참가할 노드가 자신의 공개키 정보(X)를 브로드캐스트하면, 그것을 받은 네트워크의 노드들은 자신이 가지고 있는 부분 정보(partial information)를 수신한 공개키 정보에 서명하여 새로이 참가할 노드에게 보내주게 된다. 서명된 부분 정보(X^{SK_i})는 다음과 같다.

$f(x) = d + f_1 \cdot x + \cdots + f_K \cdot x^{K-1}$, $f(0) = d$

$P_{vi} = f(v_i) \bmod n$, v_i는 노드i의 고유 아이디

$SK_i = P_{vi} \cdot l_{vi}(0) \bmod n$, $l_{vi}(0)$은 Lagrange 계수

일정 K개의 노드로부터 부분 정보로 서명된 값을 다중-시그네이처(multi-signature) 프로토콜을 사용하여 정보를 결합한다.

$$X^{SK_1} \cdot X^{SK_2} \cdots X^{SK_K} = X^{SK_1 + SK_2 + \cdots + SK_K} = X^{t \cdot n + d}$$

결합한 정보로 K-Bounded Coalition Offsetting을 이용하여 네트워크의 비밀키(기존에 CA의 비밀키)로 서명된 자신의 인증서를 추출한다. 즉, 노드들이 보내준 정보는 네트워크에서 사용되는 비밀키의 부분정보이다. 물론 비밀키가 노출되는 것은 아니며 단지 받은 정보들의 결과가 네트워크의 비밀키에 의해 서명된 자신의 인증서가 되는 것이다. 이 방식은 중앙에 인증기관 없이 네트워크 구성원에 의해 인증서 서비스를 받는 안전하고, 유비쿼터스적인 보안 구조를 제공해준다. 적은 수의 K에서도 보안의 강도는 저하되지 않는다는 장점을 가진다.

3. 제안하는 방법

상위 계층의 네트워크가 하위 계층의 네트워크를 인증하는 식의 계층적 인증이 이루어진다면 전체 네트워크를 구성하는 모든 네트워크들을 신뢰할 수 있게 될 것이다. 그리고 네트워크의 이동성을 관장하는 것이 이동 라우터이므로 이동 라우터에게 인터넷 서비스를 제공하는 것도 결국은 이동해온 방문 네트워크의 한 이동 라우터이다. 따라서 이 논문에서는 그림 1과 같이 MR_1을 가진 이동 네트워크가 TLMR를 최상위 이동 라우터로 하는 방문 네트워크로 이동 시, MR_2의 라우터 광고 메시지를 통해 이동을 감지하여 MR_2에 연결 될 때 MR_2가 방문 네트워크를 대표해 challenge-response를 이용해 MR_1을 인증한다. 그리고 MR_1은 MR_2의 인증서를 통해 MR_2를 인증한다. 양방향 인증이 이루어지고 나면, MR_1은 secret-share를 통해 이웃 노드들로부터 분할된 정보를 받아 인증서를 발급 받는다.

3.1 인증서를 가지고 있는 경우

MR_1이 이동한 네트워크에서 사용 가능한 인증서를 가지고 있다면, 2.1의 방식으로 상호 인증을 수행한다.

3.2 인증서가 없는 경우

그림 1에서 MR_1을 가진 이동 네트워크가 이동을 감지한 후 시행되는 양방향 인증 과정은 그림 3과 같다.

① K_{MR_1,HA_1}는 MR_1과 HA_1이 공유하는 비밀키이다. MR_1은 response 값을 암호화 하여 보냄으로써 비밀성을 유지한다. 난수 r_1은 되풀이 공격(replay attack) 방지에 쓰인다.

② MR_2는 challenge와 자신의 인증서를 TLMR로 전송한다. 이 둘 사이에 거쳐야 할 MR가 더 있을 수 있다.
③ TLMR는 2.1의 가정에 따라 안전한 채널을 이용하여 HA_1에게 메시지들을 보낸다.

④ HA_1은 challenge에 맞는 response'를 계산해서 암호화 하여 보내주고, 되풀이 공격을 막기 위한 난수 r_2를 함께 보낸다. 이 통신 역시 2.1의 가정을 따른다.
⑤ TLMR는 암호화된 response'와 난수 r_2를 MR_2에게 보내준다. 이 때 난수 r_2의 도청을 막기 위해 ②에서 받은 인증서에서 추출한 MR_2의 공개키로 암호화 한다.

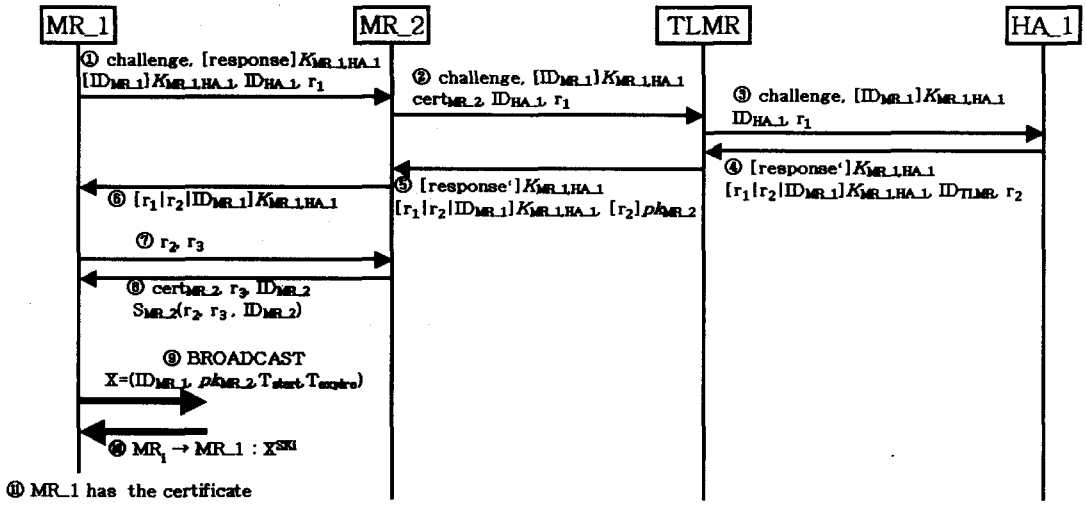

그림 3. 제안하는 보안구조

⑥ MR_2는 ⑤에서 받은 [response']K_{MR_1,HA_1}와 ①에서 받았던 [response]K_{MR_1,HA_1}를 비교한다. 같다면, MR_2는 [r_1|r_2|ID_{MR_1}]K_{MR_1,HA_1}을 MR_1에게 보낸다. 이것은 MR_1의 시기적절함(timeliness)을 평가하여 되풀이 공격을 막기 위해서이다.

⑦ MR_1은 ⑥에서 받은 메시지를 복호화 하여 얻은 난수 r_2를 MR_2에게 보내준다. MR_2는 이 난수와 ⑤에서 얻은 난수 r_2를 비교한다. 같다면 MR_2는 MR_1의 인증이 완료한다. 그리고 MR_1는 MR_2를 인증하기 위해 난수 r_3을 함께 MR_2에게 전송한다.

⑧ MR_2는 2.1의 1)의 전자 서명 방식으로 MR_1에게 자신을 인증시킨다. 이것으로 상호 인증은 완료된다.

상호 인증이 완료되면, MR_1은 자신이 이동한 네트워크에서 쓰이는 인증서를 받아야 한다. 이 과정은 액세스 라우터의 역할을 하는 MR_2를 통해 K개의 네트워크 구성원으로부터 얻은 정보를 통합함으로써 이루어진다. 그 과정은 다음과 같다[4].

⑨ MR_1은 자신의 공개키 정보를 네트워크 내로 브로드캐스트한다. 이때 MR_2가 액세스 라우터가 된다.

⑩ MR_1은 네트워크내의 K개의 MR로부터 각각 분할된 정보를 얻게 된다.

$X^{SK_1} \cdot X^{SK_2} \cdot \cdots X^{SK_K} = X^{SK_1+SK_2+\cdots+SK_K} = X^{t \cdot n + d}$

⑪ MR_1은 K-Bounded Coalition Offsetting을 통해 $X^{t \cdot n+d}$에서 RSA singing key, SK=<d, n>으로 서명된 인증서를 추출한다[5].

이 과정이 끝나면, MR_1이 이끄는 이동 네트워크는 방문 네트워크에서 인터넷에 접근할 수 있는 자격이 주어진다.

4. 결론

제안하는 방법은 challenge-response 방식과 PKI 기반의 전자 서명 방식을 이용하여, 이동 네트워크가 홈 네트워크를 벗어나 방문 네트워크로 이동시 홈 네트워크와의 메시지 교환을 한번으로 하여 간단하고 빠르게 양방향 인증을 제공할 수 있게 하였다. 또한 적절한 난수의 사용으로 네트워크간 동기화가 이루어지지 않아도 되풀이 공격을 피할 수 있다.

네트워크에 이동성이 주어지게 되면 한 네트워크는 여러 개의 이동 네트워크들이 계층적 구조를 이루는 네트워크의 집합이 될 것이다. 이때 중앙에 인증기관을 두어 인증서를 관리하는 기존의 X.509의 PKI 방식 보다는 이미 인증 받은 네트워크 내의 다른 구성체들로부터 정보를 받아 인증서를 만들어주는 것이 빠르게 변하는 네트워크 환경에 적합할 것이다. 또한 금융권이 통합되어 하나의 인증서를 사용하는 것과 같이 여러 개의 인증서를 각 사용에 맞게 통합되어 가는 추세에서 본 논문이 제안한 분산화된 인증서 발급은 기존 중앙 집중화된 인증서 발급보다 더 큰 효율성을 기대할 수 있을 것이다.

5. 참고문헌

[1]Ryuji Wakikawa, Alexandru Petrescu and Pascal Thubert, "Nemo Basic Support Protocol.txt," Internet draft, IETF, Dec. 2003. Work in progress.

[2]Luca Salgarelli et al., "Efficient Authentication and Key Distribution in Wireless IP Networks," IEEE Wireless Communications, Dec. 2003.

[3]이만영, 손승원, 조현숙, 정태명, 채기준, "차세대 네트워크 보안기술", 생능출판사, Nov. 2002.

[4]A. Menezes, P. van Oorschot, and S. Vanstone "Handbook of Applied Cryptography," CRC Press, http://www.cacr.math.uwaterll.ca/hac, 1996.

[5]Jiejun Kong et al., "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," IEEE ICNP 2001, Nov. 2001.