AAA 기반 Mobile IP 등록을 위한 키 관리기법

강현선*, 박창섭*
*단국대학교 전자계산학과
e-mail : sshskang@dankook.ac.kr

A Key Management Scheme for Mobile IP Registration Based on AAA

Hyun-Sun Kang*, Chang-Seop Park*
*Dept. of Computer Science, Dan-Kook University

요 약

Mobile IP 는 모바일 노드(MN)의 이동성을 지원하기 위한 프로토콜로, 등록 프로토콜을 통해 이동 중에도 지속적인 서비스를 제공받게 된다. 등록 프로토콜은 무선 환경에서 다양한 MN 을 대상으로 수행되기 때문에, 반드시 인증절차가 필요하며, 인증을 위한 키 관리를 위해 AAA 를 도입하는 것이 일반적인 접근방식이다. 본 논문에서는 AAA 도입한 기본적인 Mobile IP 모델에 본 논문에서 새롭게 제안하는 계층적 키 관리기법을 도입하고, AAA 지연을 최소화하는 효율적이고 안전한 등록 프로토콜을 제안한다. 또한 제안 프로토콜은 해쉬체인을 이용하여 차후 MN 의 네트워크 서비스 사용에 대한 부인방지 서비스도 제공된다.

1. 서론

Mobile IP(MIP)는 모바일 노드(MN)에게 현재 진행중인 전송계층의 중단함이 없이 이동성을 제공하기 위해 제안되었다. MIP 에서는 MN 에게 두 가지 유형의 IP 주소가 제공된다. 하나는 MN 의 홈 도메인(home domain)에서 제공된 HOA(home address)이고, 다른 하나는 MN 이 외부 도메인(foreign domain)으로 이동하였을 경우 외부 에이전트(FA)에 의해 동적으로 할당 받게 되는 COA(care-of address)이다. MN 은 등록 프로토콜을 통해 현재 COA 를 자신의 홈 에이전트(HA)에 등록함으로써 이동중에도 패킷전달(packet forwarding) 서비스를 받게 된다. 기본적인 MIP 는 재생공격 방지와 메시지 무결성을 보장을 위해 난수와 MAC(Message Authentication Code)을 사용하는 방식을 제공한다. 난수를 사용하는 방식은 마지막 등록 과정에서 HA 가 선택한 난수를 현재의 등록요청 메시지에 포함하게 된다.

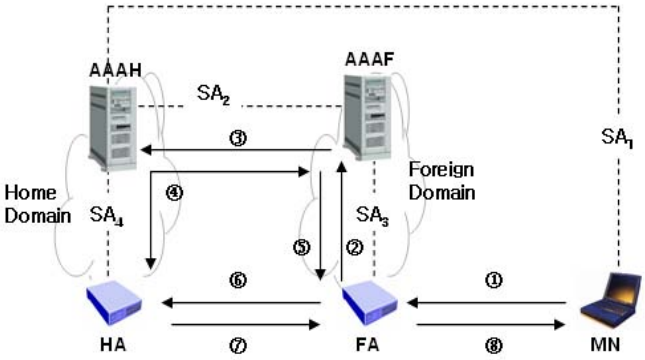
인증 서비스의 실제적인 구현을 위해서는 MIP 각 개체들 간에 세션키가 사전에 공유되어야 한다. MIP 에 참여하는 임의의 두 개체간에 세션키를 공유하기 위한 방식으로는 PKI 기반의 공개키 암호 시스템[9]과 키 분배센터의 역할을 하는 AAA 서버를 이용하는 방식[1][8]이 있다. 하지만, 현재의 상황에서 전 세계적인 규모의 PKI 구축을 가정하기에는 무리가 있으며 또한 하드웨어에 제약적인 MN 이 계산 복잡도가 높은 공개키 관련 작업을 수행하는 데에도 한계가 있다. 결론적으로, 대칭키 암호에 기반을 둔 AAA 프로토콜을 통해서 세션키를 설정/분배하는 것이 보다 현실적인 접근방법이 된다.

본 논문에서는 안전한 Mobile IP 등록을 위해 새로운 계층적 키 관리기법을 도입하고, 기본적인 AAA 방식에 해당 키 관리기법을 도입하여 등록지연을 최소화하는 효율적인 MIP 등록 프로토콜을 제안한다. 또한 제안 프로토콜에서는 해쉬체인을 이용하여 차후 MN 의 네트워크 서비스 사용에 대한 부인방지 서비스도 제공한다. 2 장에서는 제안 프로토콜과 관련하여 AAA 를 도입한 기본적인 MIP 모델과 등록 프로토콜을 살펴보고, 3 장과 4 장에서는 본 논문에서 새롭게 제안한 계층적 키 관리기법과 이를 도입한 AAA 기반의 안전

한 MIP 등록 프로토콜을 제안한다. 5 장과 6 장에서는 제안기법의 분석 및 평가와 결론에 대해 논의한다.

2. 관련연구

AAA 를 도입한 기본적인 MIP 에는 AAA 서버로 AAAH(AAA server in home domain)와 AAAF(AAA server in foreign domain)가 존재한다. 그림 1 은 AAA 를 도입한 기본적인 MIP 모델과 등록 프로토콜을 나타내고 있다. 점선으로 표시된 부분은 MIP 두 개체간에 설정되어있는 SA(Security Association)를 나타낸다.



[그림 1] AAA 를 도입한 기본적인 MIP 모델

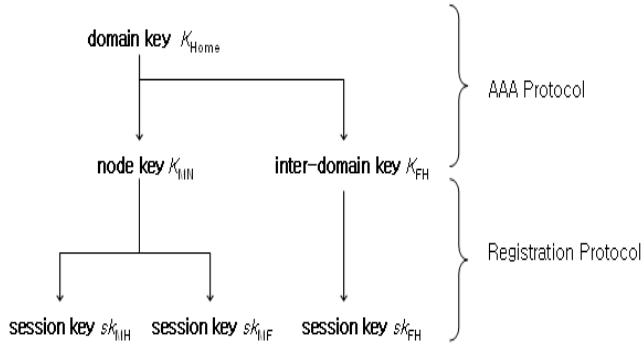
위의 모델에서 등록 프로토콜은 MN 과 FA, FA 와 HA, MN 과 HA 사이의 세션키 공유를 위한 AAA 프로토콜과 결합되어있다. 특히, AAAH 는 이미 설정되어 있는 SA 를 기반으로 각 개체간의 공유키를 생성/분배하는 역할을 수행한다. 만약 현재 각 개체간의 세션키가 분배되었다면, MN 의 FA 를 통한 MIP 등록과정은 ①, ⑥, ⑦, ⑧단계로 구성되고, 분배되지 않았다면, MIP 등록 프로토콜은 키 생성/분배로 구성된 키 분배 프로토콜을 수행할 것이다. AAAH 는 키 생성 단계에서 임의의 난수 r_1, r_2 와 AAAH 와 MN 사이의 사전에 공유된 키 AAA-key 를 일방향 해쉬함수 $h(\ )$에 적용하여 두 개의 세션키 $ks_1 = h(r_1, \text{AAA-key})$, $ks_2 = h(r_2, \text{AAA-key})$를 생성한다. 키 분배단계 ④, ⑤에서 AAAH 는 MN 에게 세션키를 유도할 수 있도록 r_1, r_2를 전송하고, FA 와 HA 에게는 직접 전송한다. 또한, AAAH 와 AAAF 는 HA 와 FA 간에 세션키 ks_3 의 공유를 위해 서로 협력한다. 만약 MN 이 현재의 FA 에서 또 다른 FA 로 이동할 경우, 새로운 등록 프로토콜과 함께 또 다른 키 생성/분배과정이 반복 수행되고, 매 등록요청에 대해 AAAH 와 AAAF 의 메시지 교환이 발생하고 AAAF 와 상대적인 거리를 감안할 때 MN 의 등록과정에 대해 상당한 지연이 발생하게 된다.

본 논문에서는 AAAH, AAAF 의 메시지를 최소화하여 등록지연을 감소시키는 새로운 세션키 설정방법을 소개하며, 이로써 등록과정에서의 발생하는 지연을 줄일 수 있게 된다. domain key 개념의 도입으로써, MIP 등록 프로토콜로부터 AAA 프로토콜을 분리하고 MIP 등록과정에서 AAA 프로토콜과의 상호작용으로 인한 지연을 최소화한다.

3. 안전한 MIP 등록 프로토콜을 위한 키 관리기법

AAA 를 도입한 기본적인 MIP 모델에서는 MN 이 FA 를 통해 등록을 요청할 때마다, MIP 개체들 간의 세션키 공유를 위해 AAAL 와 AAAH 사이의 메시지 교환이 이루어지게 된다. 본 논문에서는 새로운 키 관리기법은 이용하여 AAAH 와 AAAL 의 교환되는 메시지를 줄임으로써 MIP 등록과정의 지연을 줄이고자 한다. 새로운 키 관리기법의 이해를 위해 다음과 같이 몇몇의 용어를 정의한다. *MN*, *FA*, *HA* 는 각각 MN, FA, HA 의 IP 주소를 의미하고, *Foreign* 은 NAI(network access identifier)와 같은 외부 도메인의 ID 를 의미하며 $h()$는 일방향 해쉬함수이다. 관련연구와 같이 MN 과 AAAH, AAAH 과 HA, AAAF 과 FA, AAAH 과 AAAF 간에는 SA 가 사전에 설정되어 있음을 가정한다.

본 논문에서는 동일한 관리 도메인 하의 AAA 서버와 에이전트 사이에 공유된 domain key 를 정의한다. 즉, 홈 도메인 내의 AAAH 와 HA 들은 사전에 설정된 SA 를 기반으로 그룹키 개념의 domain key K_{Home} 를 공유한다. 홈 도메인에 속한 각 MN 에게는 MIP 서비스를 제공받기 위한 가입시에 노드키 $K_{\text{MN}} = h(K_{\text{Home}}, MN)$와 HOA 를 할당 받는다. AAAH 와 AAAF 간에는 SA 가 존재함을 가정하기 때문에, AAAH 는 해당 SA 를 이용하여 inter-domain key $K_{\text{FH}} = h(K_{\text{Home}}, Foreign)$를 AAAF 에게 전달한다. AAAF 는 inter-domain key 를 인증캐쉬(authentication cache)에 유지한다. domain key, inter-domain key, 노드키는 비교적 장기간의 키로 사용되며 MIP 등록 프로토콜과는 관계없이 공유된다. 다음의 그림 2 는 안전한 MIP 등록을 위해 AAA 프로토콜과 MIP 등록 프로토콜로 생성/관리되는 다양한 키들의 계층도를 나타낸다.



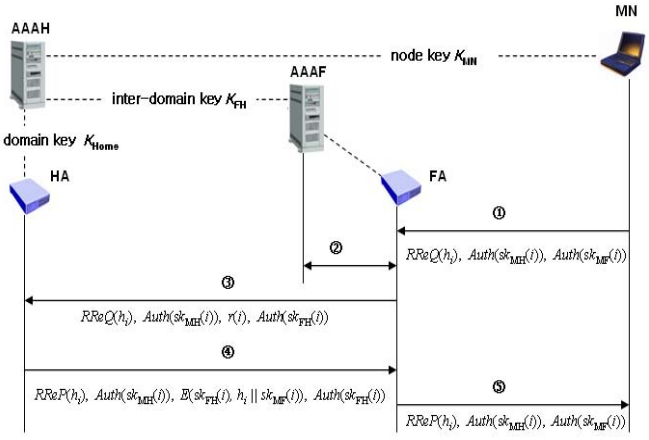
[그림 2] 안전한 MIP 등록을 위한 키 계층도

본 논문에서 해쉬체인[8]은 다음의 두 가지 목적을 위해 사용된다. 하나는 MN 의 등록요청에 대한 부인방지 서비스를 위해서이다. MN 은 MIP 서비스를 제공받기 위한 가입 시에 임의로 선택한 h_n 을 초기값으로 하는 해쉬체인 $\{ h_{i-1} = h(h_i) \mid i = 2, \ldots, n-2, n-1, n\}$을 생성하고, h_1 을 AAAH 에게 전송한다.

AAAH 는 h_1 을 개인키로 서명한 후에 MN 에게 전송한다. AAAH 에 의한 서명값은 홈 도메인의 HA 에 의해 최초의 등록 프로토콜에서 확인되므로, 홈 도메인 내의 모든 HA 는 AAAH 의 공개키를 유지해야 한다. AAAH 의 서명은 생성과 확인이 홈 도메인 내에서만 이뤄지기 때문에 전체적인 PKI 는 필요하지 않게 된다. 다른 한 목적은 해쉬체인을 이용하여 세션키를 유도하기 위해서이다. MN 은 i 번째 등록 세션에서 MN 과 HA 간에 공유되어야 할 세션키 $sk_{MH}(i) = h(K_{MN}, h_i, HA)$와 MN 과 FA 간에 공유되어야 할 세션키 $sk_{MF}(i) = h(K_{MN}, h_i, FA)$를 해쉬체인을 이용하여 유도한다. $r(i)$를 FA 에 의해 새롭게 생성된 난수라고 할 때, HA 와 FA 간의 세션키는 $sk_{FH}(i) = h(K_{FH}, r(i))$로 계산된다. 등록 프로토콜이 수행되는 동안 FA 는 난수를 HA 에게 전달하고 이를 통해 HA 는 $sk_{FH}(i)$를 계산한다.

4. 안전한 MIP 등록 프로토콜

이번 장에서는 앞 장에서 소개된 계층적 키 관리 기법을 기반으로 하는 MIP 등록 프로토콜을 제안한다. 우선 $Auth(k)$는 모든 선행하는 데이터에 대해 대칭키 k 를 기반으로 계산한 MAC 값을 의미한다. $\{m, Auth(k_1), Auth(k_2)\}$의 경우, $Auth(k_2)$는 m 과 $Auth(k_1)$에 대해 k_2 를 기반으로 계산한 MAC 값이다. $E(k, m_1 \| m_2)$은 $m_1 \| m_2$ 에 대해 대칭키 k 를 이용하여 암호화한 값이다. $RReQ(m)$은 MN 의 HOA, COA, HA 의 주소를 포함하는 MN 의 등록요청 메시지이다. 그리고, $RReP(m')$은 MN 의 HOA, HA 의 주소, 등록요청에 대한 결과를 포함한 등록응답 메시지이다. 그림 3 은 계층적 키 관리기법을 기반으로 하여 제안된 MIP 등록 프로토콜을 나타낸다.



[그림 3] 제안된 MIP 등록 프로토콜

현재의 등록이 i 번째라고 가정할 때, ①단계에서 MN 은 우선 자신의 노드키와 i 번째 해쉬체인 값을 기반으로 두 개의 세션키 $sk_{MF}(i) = h(K_{MN}, h_i, FA)$와 $sk_{MH}(i) = h(K_{MN}, h_i, HA)$를 계산한다. 다음으로 h_i 를 포함한 $RReQ$ 를 작성하여 인증 확장값 $Auth(sk_{MH}(i))$, $Auth(sk_{MF}(i))$와 함께 FA 에게 전송한다. 이 단계에서 FA 는 $sk_{MF}(i)$를 모르기 때문에, ④단계가 수행된 후에 $Auth(sk_{MF}(i))$에 대해 확인하게 된다.

②단계에서 FA 는 inter-domain key K_{FH} 를 얻기 위해 AAAF 의 인증캐쉬에 요청하고, 이를 기반으로 세션키 $sk_{FH}(i) = h(K_{FH}, r(i))$를 계산한다. FA 와 AAAF 의 메시지 교환은 AAA 프로토콜 메커니즘을 이용하여 수행된다. inter-domain key 는 lifetime 을 가지며, FA 는 lifetime 이 만료될 때까지 해당 inter-domain key 를 유지하고 사용하게 된다.

③단계에서 FA 는 $RReQ$ 를 $r(i)$과 새롭게 계산된 $Auth(sk_{FH}(i))$와 함께 HA 에게 전달한다. 이 때, HA 는 $RReQ$ 내의 정보를 기반으로 두 개의 세션키를 계산한다. inter-domain key K_{FH} 는 FA 의 도메인 네임과 domain key 로 유도되고, 세션키 $sk_{FH}(i) = h(K_{FH}, r(i))$가 계산되고 $Auth(sk_{FH}(i))$를 확인하게 된다. HA 는 MN 의 노드키 $K_{MN} = h(K_{Home}, MN)$를 유도한 후에 MN 과 공유하는 세션키 $sk_{MH}(i) = h(K_{MN}, h_i, HA)$를 계산한다. 여기서 identification 필드에 포함된 해쉬값에 대한 처리방식에는 두 가지가 있다. 만약 i=1 이면 MN 의 최초 등록요청이며, 이때 사용하는 해쉬체인 값은 AAAH 의 개인키로 서명된 값이므로 HA 는 AAAH 의 공개키로 확인하게 된다. 만약 확인이 성공하면 HA 는 h_1 을 모바일 바인딩 리스트에 저장한다. 만약 $i > 1$ 이면 HA 는 $h(h_i) = h_{i-1}$ 를 계산하고 저장된 값과 비교한다. 만약 동일하다면 MN 의 등록요청은 허가되고 HA 는 MN 의 모바일 바인딩 리스트를 갱신한다.

④단계에서 HA 는 등록응답 메시지 $RReP$ 를 작성하여 인증 필드, $E(sk_{FH}(i), h_i \| sk_{MF}(i))$와 함께 FA 에게 전송한다. HA 는 세션키 $sk_{MF}(i) = h(K_{MN}, h_i, FA)$를 FA 에게 전달한다. $Auth(sk_{FH}(i))$를 확인 후, FA 는 $sk_{MF}(i)$를 복호화하고 ①단계의 $Auth(sk_{MF}(i))$를 확인한다.

⑤단계에서 MN 은 $Auth(sk_{MH}(i))$와 $Auth(sk_{MF}(i))$를 확인한 후에 등록요청이 성공적으로 수행되었는지 검사한다.

5. 분석 및 평가

5.1 등록 프로토콜과 AAA 프로토콜의 분리

기존 기법에는[4,5,7] MIP 개체간 세션키의 생성/분배를 목적으로 AAA 프로토콜이 등록 프로토콜의 한 부분으로 결합되어 있다. AAAH 와 AAAF 에 의한 지연은 매 MIP 등록 프로토콜에서 발생한다. 본 논문의 주요 목적은 AAA 프로토콜과 MIP 등록 프로토콜을 분리하여 AAA 프로토콜에 의한 등록지연을 줄이고자 하는 것이다. 본 논문에서 제안한 계층적 키 관리기법은 MIP 등록 프로토콜에서 AAA 프로토콜을 분리한다. 각 관리 도메인에 대해, 최상위 레벨 domain key 가 정의되고 이를 기반으로 inter-domain key 가 유도된다. 기존 기법과 같이 제안된 기법에서도 AAAH 와 AAAF 간에는 사전에 SA 가

설정되었음을 가정한다. 이는 AAAH 는 AAAF 와 로밍협약의 설정을 의미하기 때문에 로밍협약의 한 부분으로 AAA 프로토콜을 통해 inter-domain key 를 교환할 수 있다. 이를 통해, AAAH 와 AAAF 가 inter-domain key 를 공유하기 때문에 등록 프로토콜에서 AAAH 와 AAAF 간의 지연을 절약할 수 있게 된다.

5.2 부인방지 서비스를 위한 Inter-Domain PKI

전 세계적인 규모의 PKI 를 기반으로 하는 MIP 등록 프로토콜[2,3,4]에서 세션키 분배와 부인방지 서비스가 제공된다. 그러나, 현재 상황에서 전 세계적인 PKI 구축을 가정하기에는 무리가 있으며, 하드웨어 제약적인 MN 이 공개키 관련 작업을 수행하는 데에도 한계가 있다. 하지만, 본 논문에서 제안된 프로토콜에서는 inter-domain PKI 만으로 부인방지 서비스를 제공하고, MN 은 PKI 와 관련된 어떠한 계산도 수행하지 않는다.

MN 의 가입 시에 MN 에 의해 선택된 해쉬체인의 루트를 AAAH 가 서명하고, 최초의 등록과정에서 HA 에 의해 단 한번 확인과정을 거치게 되며, 각각의 해쉬값은 MN 의 성공적인 MIP 등록 프로토콜을 위한 일종의 티켓과도 같다. MIP 서비스 제공자는 해쉬체인을 생성한 MN 에게 서비스를 제공한 증거로 사용할 수 있다.

5.3 재생공격에 대한 방지

MIP 에 대한 기본적인 재생공격은 정당한 MN 에 의한 정상적으로 등록요청 메시지를 기록하였다가 얼마간의 시간이 흐른 후 DOS(denial-of-service)공격을 목적으로 재생하는 방식이다. 이러한 기본적인 재생공격을 방지하기 위해 식별필드에 등록 메시지의 freshness 를 보장하기 위해 난수나 타임스탬프를 포함한다. 하지만, 위의 방식에서 freshness 에 대한 확인이 HA 에서 수행되기 때문에 만약 공격자의 목적이 단지 외부 도메인 상에서의 네트워크 접속이라면 FA 에 대한 다른 유형의 재생공격[9]이 가능하게 된다. 즉, 한 쌍의 $RReQ_{\text{old}}$ 와 $RReP_{\text{old}}$ 를 기록하였다 재생하는 방식이다. 공격자는 $RReQ_{\text{old}}$ 를 FA 에게 전송하고 FA 는 HA 에게 등록요청 메시지를 전송한다. HA 는 해당 요청에 대한 응답 *RReP* 을 FA 에게 전송하는데, 이러한 등록응답 메시지가 FA 에 도착하기 전에 공격자는 $RReP_{\text{old}}$ 를 FA 에게 전송함으로써, 성공적으로 FA 에 접속하게 된다. 이와 같은 공격에 대응하기 위해, 시도-응답(challenge-response)프로토콜이[5][6] 제안되었다. 이 방식은 재생공격에는 대응적이지만 FA 가 생성하여 방송하는 수많은 시도 값을 유지, 관리해야 하는 복잡성의 문제를 안고 있다.

본 논문에서 제안된 등록 프로토콜은 시도-응답 메커니즘을 적용 대신, 각 등록마다 FA 에 의해 새롭게 생성된 HA 와 FA 간의 세션키 $sk_{\text{FH}}(i) = h(K_{\text{FH}}, r(i))$를 사용한다. 따라서 이전에 기록하였던 $RReP_{\text{old}}$ 를 FA 에게 재생할 경우 메시지 인증 검사를 통과하지 못하게 되고, 결국 재생공격은 실패하게 된다.

6. 결론

기존 기법에서는 등록과정에서 개체간에 사용할 세션키의 생성/분배를 위해 AAAH 가 키 분배센터 역할을 한다. 따라서 MN 에 의한 매 등록요청마다 AAAH 와 AAAF 간의 메시지 교환이 요구되며, 이로써 MIP 등록 프로토콜에서 발생하는 지연 이외에도 추가적인 지연이 요구된다. 본 논문에서는 안전한 MIP 등록 프로토콜을 위한 새로운 키 관리기법을 제안하였고, 이 기법을 통해 간단해진 키 생성/분배와 함께 MIP 등록과정의 지연을 감소시킨다. 또한 해쉬체인을 도입하고, 해쉬체인의 루트값을 AAAH 가 서명함으로써 차후 MN 이 제공받은 서비스에 대한 부인방지 서비스를 제공한다.

참고문헌

[1] C. Perkins, Ed., "IP Mobility Support for IPv4," RFC3344, Aug. 2002.

[2] S. Jacobs and S. Belgard "Mobile IP Public Key Based Authentication," Internet Draft, <draft-jacobs-mobileip-pki-auth-03.txt>, July 2001.

[3] J. Zao, J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan, I. Castineyra, S. Kent, “A public-key based secure Mobile IP,” Wireless Networks, vol.5, no.5, pp.373-390, Oct. 1999.

[4] C. Yang, M. Hwang, J. Li, and T. Chang, “A Solution to Mobile IP Registration for AAA,” CIC 2002, LNCS 2524, Springer-Verlag, pp.329-337, 2003.

[5] C. Perkins, “Mobile IP Joins Forces with AAA,” IEEE Personal Communications, vol.7, no.5, pp.59-61, Aug. 2000.

[6] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization and Accounting Requirement," RFC2977, October 2000.

[7] C. Perkins, "AAA Registration Keys for Mobile IP," Internet Draft, <draft-ietf-mobileip-aaa-key-12.txt>, May 2003.

[8] L. Lamport, “Password Authentication with Insecure Communication,” Communication Magazine of ACM, vol.24, no.11, pp. 770-772. 1981.

[9] Sufatrio, Kwok Y. Lam, "Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication," ISPAN'99, June 1999

[10] C.Perkins, "MobileIPv4 Challenge/Response Extensions ," RFC3012, Nov. 2000.