모바일 PKI 기반한 인증 구조

The Authentication Structure Based Mobile PKI

김미혜
충북대학교 전기전자컴퓨터공학부

서세영
충북대학교 컴퓨터공학과

중심어 : 공개키 기반구조, 인증구조, 위임티켓

요 약

본 논문은 공개키 기반구조(PKI-Public Key Infrastructure)에서 중추적인 역할을 담당하는 공개키 인증시스템을 설계하고 구현한다. 본 논문에서는 인증기관의 역할을 수행할 수 있는 공개키 인증시스템의 요구사항 및 특징을 분석하여, 실제 인증 서비스가 제공 가능한 인증과정은 HA 및 FA한테 위임하고 설계한다. 인증 구조는 Root CA와 Home agent 및 Foreign agent로 구성되어 있고, 필요할 때 CA은 위임권을 HA나 FA한테 전송한다.

Mi-Hye Kim (mhkim@chungbuk.ac.kr)
School of Electronic & Computer Eng., Chungbuk National University
Shi-Ying Xu (xushiying690503@hotmail.com)
Dept. of Computer Engineering., Chungbuk National University

Keyword : PKI, Authentication Model, Delegation Ticket

Abstract

In this paper, we design an authentication model based mobile PKI (Public Key Infrastructure). The authentication model consists of Root-CA, Home-network agent and Foreign-network agent. CA will going to gave the delegation ticket to Home-Agent or Foreign-Agent when they request. The authentication model information security is various characteristic : more then high speed, mobile network, and low cost more then previous structure of assure information security.

I. 서론

오늘날 개방형 네트워크인 인터넷의 급속한 발전으로 인하여 그 동안 오프라인으로 처리되었던 많은 업무들이 온라인 처리로 전환되어 가고 있다. 하지만 개방형 네트워크인 인터넷에서의 업무처리는 개인 정보의 누출, 개인 정보의 위조 및 변조 등과 같은 위협요소를 항상 내포하고 있으며 이러한 개인 정보 노출에 대한 위협요소를 해결하기 위해서 PKI(Public Key Infrastructure) 기반에 인증서 검증 방식이 제안되었고 현재도 연구가 계속 되어지고 있다[1].

현재 Mobile IP의 보안성을 증대시키기 위해서는 강력한 인증 절차와 데이터의 보호를 위한 암호화기능이 필요하다. 유선네트워크의 보안문제와는 별개로 Mobile IP에서는 호스트들의 이동성 지원을 위해 무선환경을 사용하게 되므로 무선환경에 적합한 보안 및 인증 프로토콜이 구축되어져야 한다. 그러나, 무선환경 자체의 단점은 낮은 대역폭, 이동 단말기의 연산 능력, 그리고 이동 단말기의 짧은 전지 수명 등이 Mobile IP의 보안 문제를 해결하는데 많은 어려움으로 작용하고 있다[2],[3],[4],[5].

본 논문에서는 이러한 문제점을 보완하기 위한 개선된 무선 PKI 기반의 보안구조를 제안한다. 이 새로운 보안구조에 따라서 상위 계층 참가자로부터 하위 계층 참가자로 이루어지고, 위임티켓(Delegation Ticket)[5]을 통해 실질적인 권한 위임이 수행된다, 인증기관 CA가 생성한 위임티켓은 비밀분산법[5]에 의해 대리인증자와 공유하고, 이렇게 공유된 정보를 위임티켓 공유정보라고 한다. 특히, 제안하는 방법에서는 Diffie-Hellman 문제[6]를 해결하여 가정 없이 안전한 비밀터널을 이용하여 대리인증자한테 안전하게 위임티켓 정보를 전송할 수 있다.

접수번호 : #040107-001
접수일자 : 2004년 1월 7일, 심사완료일 : 2004년 2월 1일

*교신저자 : 김미혜, e-mail : mhkim@chungbuk.ac.kr

II. Diffie-Hellman 문제

Diffie-Hellman 공개키 교환 프로토콜은 두 사용자가 사전에 어떠한 비밀교환 없이 안전하지 않은 매체상에서 공통키를 교환하도록 한다. 프로토콜은 두 시스템 파라미터 p와 g를 갖는다. 그것들은 모두 공개되고 시스템 안의 모든 사용자들에 의해 사용될 수 있다. 파라미터 p는 소수이고 파라미터 g (일반적으로 생성자(generator)로 불리는)는 p보다 작은 정수이며, g는 그 자신이 어떤 횟수만큼 소수 p의 법으로 곱해질 때 1부터 p-1까지의 모든 요소들을 생성할 수 있다. A와 B가 Diffie-Hellman 키 교환 프로토콜을 이용해서 다음과 같이 공통키를 나눈다.

첫 번째로, A는 랜덤한 비밀키 a를 생성하고 B은 랜덤한 비밀키 b를 생성한다. 그리고 나서 파라미터 p, g 그리고 비밀키들을 이용해서 그들의 공개키들을 만든다. A의 공개키는 ga mod p이고 B의 공개키는 gb mod p이다. 그리고 나서 서로 공개키를 교환한다. 마지막으로, A는 kab = (gb)a mod p를 계산하고, B은 kba = (ga)b mod p를 계산한다. kab = kba = k이므로, A와 B은 공통의 비밀키 k를 갖는다.

프로토콜의 안전에 대해서 이산 대수 문제를 기반으로 한다. 이것은 소수 p가 충분히 클 때 주어진 두 개의 공개 값들 ga mod p와 gb mod p를 가지고 공유된 비밀키 k = gab mod p를 계산하는 것이 불가능하다고 가정한다.

Diffie-Hellman 키 교환은 중간자 공격(middleperson attack)에 취약하다. 이 공격에서, 공격자 C는 A의 공개 값을 가로채고 C자신의 공개 값을 B에게 보낸다. B는 그의 공개 값을 전달할 때, C는 자신의 값으로 대체하고 A에게 그 값을 전달한다. C와 A는 하나의 공유된 키를 합의하고 C와 B은 다른 공유된 키를 합의한다. 이러한 교환 후에, C는 A나 B에 의해서 만들어진 어떤 메시지를 단순히 복호화하고, 복호문을 읽고 나서 읽고 적당한 키로 다시 암호화하고 그것들을 변경한 후에 적당한 상대방에게 전달한다. 이러한 취약성은 Diffie-Hellman 키 교환이 참가자들을 인증하지 않기 때문이다. 이를 막기 위해서 전자 서명과 같이 사용한다.

III. 무선 PKI

유선 인터넷 환경과 마찬가지로 무선 인터넷이 안전한 서비스를 제공하기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 서비스를 제공하기 위한 무선 PKI가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소한으로 변화시킨 것이다. 즉, WAP게이트웨이를 통한 무선 PKI 서비스에서는 기존의 유선 환경에서 사용하는 X.509 인증서에 비해 부피가 작고 간단한 구조로 구성되어 있는 WTLS(Wireless Transport Layer Security) 인증서를 사용한다. 이는 무선 환경에서 사용하는 소용량 단말기에서 암호화 및 인증 업무를 효율적으로 수행 할 수 있도록 구성되었다.

1. 모바일 PKI 모델

무선 PKI 모델에서는 기본적으로 무선용 X.509 인증서를 사용하지만, 무선 CA 서버는 단말기의 검증능력을 고려하여 Short-lived 인증서인 WTLS 인증서를 사용하며, 단말기의 경우 저장공간의 문제로 인증서를 발급 받을 경우 인증서의 URL을 이용한다.

단말기에서 무선용 X.509 서버 인증서의 검증메커니즘으로는 CRL이나 OCSP를 사용하도록 한다. 또한 무선에서는 CRL를 잘게 쪼개서 최근 CRL를 가져와서 검증할 수 있는 메커니즘인 Delta CRL이 옵션으로 사용된다.

무선단말에서 RSA를 사용하여 키 생성이 용이하지 않아 ECDSA를 사용하여 키를 생성할 수 있는 기능이 무선에서 추가되었으며, 서명 알고리즘으로는 RSA, ECDSA가 사용되며, 키 분배용으로는 RSA, ECDH가 사용된다.

무선에서는 무선환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 사용한다.

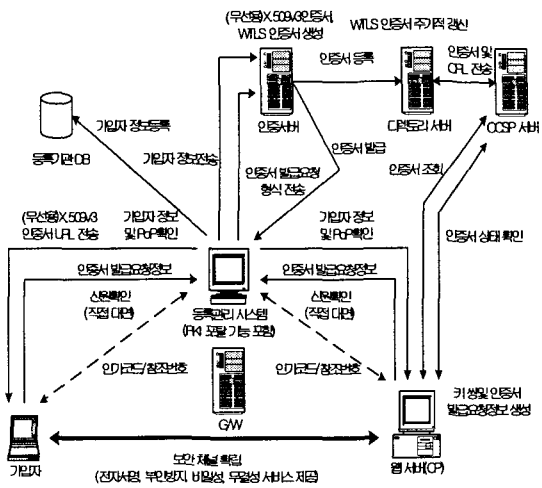


그림 1. 모바일 PKI 서비스 시나리오

○ 인증서 등록절차

① 등록기관이 직접대면을 통해 사용자 신원확인을 함

② 등록기관이 사용자의 신원확인 후 참조번호와 인가코드를 사용자에게 전달한다.

③ 등록기관은 자신의 DB에 가입자를 등록하며 인증기관에 가입자의 정보를 전송한다.

○ 인증서 발급절차

① 가입자는 인증서 발급에 필요한 전자 서명키 쌍, 무선 인증서 발급요청형식을 생성한다.

② 가입자는 자신의 전자 서명 생성키로 무선 인증서 발급 요청형식을 서명한 후 등록기관에 전송한다.

③ 전자서명된 무선 인증서 발급요청형식을 받은 등록기관은 가입자의 전자서명 검증을 통해 실제로 전자서명 검증키에 대응하는 전자서명 생성키의 소유여부를 확인한 후 요청형식을 인증기관에 전송한다.

④ 인증기관은 무선 전자서명용 X.509v3 인증서를 생성하여 자신의 디렉토리에 등록한 후 등록기관에 인증서 또는 인증서 URL을 전송한다.

⑤ 등록기관은 인증기관으로부터 받은 인증서 또는 인증서 URL 정보를 가입자에게 전송한다.

○ 인증서 확인절차

등록기관으로부터 인증서를 받은 가입자는 자신이 받은 인증서의 이상유무를 확인한다.

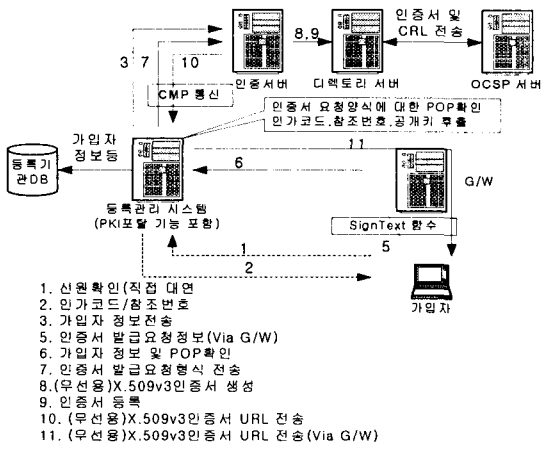


그림 2. 무선 전자서명용 X.509v3 인증서 발급신청 및 등록과정

○ 인증서 검증과정

인증서 검증과정은 가입자가 서버로부터 전송 받은 인증서의 검증 과정과 서버가 가입자로부터 전송 받은 인증서 또는 URL의 검증의 두 종류가 있다.

① 가입자가 서버로부터 전송 받은 인증서의 검증

서버는 자신의 인증서 (무선 전자서명용 X.509v3)를 가입자에게 전송한다. 그리고, 가입자는 서버로부터 받은 인증서의 상태검증을 해야한다. 이때 디렉토리에 있는 인증서 폐지목록(X.509v2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인 할 수 있다.

② 서버가 가입자로부터 전송 받은 인증서 또는 URL의 검증

가입자는 자신의 인증서(무선 전자서명용 X.509v3) 또는 인증서 URL을 서버에게 전송한다. 그리고, 서버는 가입자로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서 폐지목록을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인 할 수 있다. URL을 받은 경우는 디렉토리로부터 인증서를 받아서 검증에 이용할 수 있다[7],[8],[9].

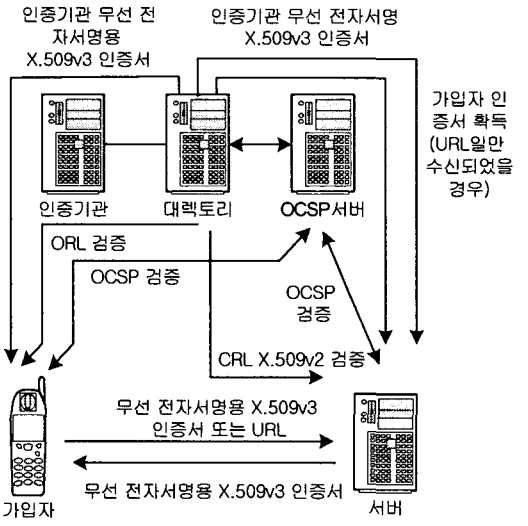


그림 3. 무선 전자서명용 X.509v3 인증서 검증과정

2. 모바일 PKI 구성요소 [10]

무선 PKI를 구성하는 요소로는 인증서를 발행하고 효력정지 및 폐지 기능을 수행하는 인증기관, 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관, 인증서 및 인증서 폐지목록을 저장하는 디렉토리, 그리고 인증서를 신청하고 인증서를

사용하는 사용자로 분류될 수 있으며 각각의 특징은 다음과 같다.

○ 인증기관(CA : Certification Authority)

인증기관은 공개키 기반구조를 구성하는 가장 핵심 객체로 사용자의 공개키 인증서의 발급·효력정지 및 폐지와 등록기관의 요청에 따라 인증서를 발급하는 기능을 수행한다. 또한, 인증서와 인증서 소유자의 정보의 관리 인증서와 그 소유자의 정보를 관리하는 데이터 베이스의 관리, 인증서 효력정지 및 폐지목록, 감사 파일을 보관 등의 업무를 수행하는 핵심 기관이다.

○ 등록기관(RA : Registration Authority)

등록기관은 인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 설치하여 인증기관을 대신하여 사용자들의 인증서 신청 시 그들의 신분과 소속의 확인, 인증기관에 인증서 요청서 전송, 디렉토리로부터 인증서와 인증서 효력정지 및 폐지 목록 검색, 인증서 효력정지 및 폐지 요청 등의 기능을 수행한다.

○ 디렉토리(Directory)

디렉토리란 인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 폐지목록의 저장 및 검색 장소로. 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol) 또는 LDAP(Lightweight DAP v2, v3)를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간 동안 디렉토리에 저장된다.

○ 사용자(End entity)

공개키 기반구조내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 말하며, 자신의 비밀키/공개키 쌍을 생성하고 검증, 공개키 인증서의 요청/획득, 전자 서명의 생성 및 검증, 특정 사용자의 인증서 획득 및 검증, 자신의 인증서 취소 등의 기능을 수행한다.

IV. 무선 PKI 기반의 이동 보안 구조

1. 모바일 환경에서 기존 인증 메커니즘 및 문제점

공개키를 사용하는 '사용자'는 공개키를 사용하기 전에 키에 대한 신뢰성을 확립하기 위해서 인증서 검증을 수행한다. 사용자가 인증서 검증은 사용자의 트러스트 도메인으로부터 인증서 소유자까지의 경로에 해당하는 모든 인증서를 검증하는 과정을 거쳐야 한다. 이러한 과정은 많은 리소스를 사용하므로 시스템 성능에 영향을 미치게 된다. 특히, 이동통신 시스템과 같이 사용 가능한 리소스의 양이 상대적으로 적은 경우에는 큰 부담이 될 수 있다. 또한, 외부 에이전트가 직접 이동노드를 인증할 수 없도록 설계되어있다.

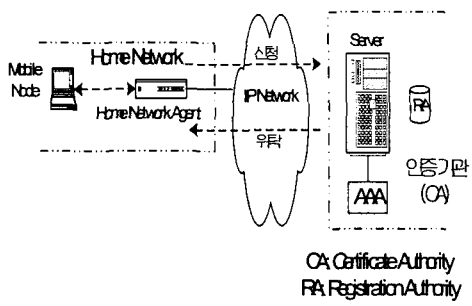
2. 위임 티켓을 기반으로 이동통신 보안 시스템

본 논문에서는 제안된 기존 알고리즘의 단점을 해결하기 위한 새로운 무선 PKI 기반으로 보안구조를 제안한다. 제안한 보안구조는 에이전트에게 위임 티켓을 위임한 방식을 사용하기 때문에 인증 시간을 최대한도로 줄였으며, 위임티켓을 이용한 위탁인증 방식으로 에이전트들과 이동 노드간의 직접적인 인증이 이루어지도록 한다.

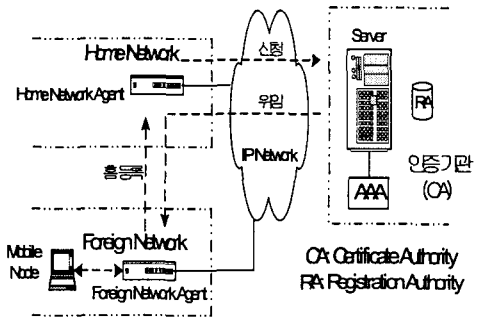
3. 제안한 알고리즘

모바일 노드를 MN(Mobile Node)이라고 부르며, 모바일 노드는 홈 주소 HoA(Home Address)라고 불리는 고유한 IP주소를 갖는데, 이 주소는 모바일 노드의 현재 위치와 무관하다. HoA를 포함하는 서브네트워크를 그 모바일 노드의 홈 네트워크를 HN(Home Network)이라고 하며, HN안에 있는 라우터인 홈 에이전트 HA(Home Agent)는 모바일 노드가 홈 네트워크를 떠나 있을 때 모바일 노드에게 보내진 패킷들을 전달하는 역할을 수행한다. 모바일 노드가 홈 네트워크에 위치할 때는 모바일 노드는 일반 노드와 전혀 차이가 없다. 모바일 노드가 홈 네트워크를 떠나 다른 곳에서 인터넷에 연결될 때, 접속 위치의 네트워크를 외지 네트워크를 FN(Foreign Network)이라고 하며, FN의 라우터를 외지 에이전트 FA (Foreign Agent), FN에서 임시로 부여받은 IP주소를 CoA (Care of Address)라고 부른다. MN는 HA에게 현재 위치를 알려주는 것을 홈 등록HR(Home Registration)이라고 부른다. 알고리즘을 구현하기 전에 HA, FA과 CA 사이에 항상 신뢰한다고 가정한다. MN가 통신망에 초기 가입 할 때 위치에 따라 각각의 위탁 인증 신청 과정을 수행하고, CA는 이 신청을 허락하면 CA가 위임티켓 또는 저장한 인증 정보를 HA나 FA에게 전달한다. 이 때 HA나 FA가 CA의 역할을 수행 할 수 있다.

그림 4는 MN이 위치에 따라 HN 또는 FN 영역 안에 있는 경우 초기 가입위탁 인증 신청 과정을 나타낸 것이다.



(a) MN가 HN 영역 안에 있는 경우의 위탁 인증 신청 과정



(b) MN가 FN 영역 안에 있는 경우 위탁 인증 신청 과정

그림 4. 위탁 인증 신청 과정

○ 대리 인증을 위한 위임티켓 생성

새로이 제안한 알고리즘에 사용된 표기는 표 1과 같다.

표 1. 알고리즘의 표기법

표기법	
p, q	q|(p-1)을 만족하는 큰 소수
g	위수가 q인 Z_p상의 원소
x_i	각 대리자의 비밀키
y_i	각 대리자의 공개키
h	해쉬함수
pc	위임 인증서 (proxy certificate)
I_0	원 인증기관 CA 의 인증 정보

MN는 Home Network 내에 있는 경우: CA는 HA에게 원 인증기관 CA의 인증 기능을 위임하고자 한다면 다음 단계를 수행한다.

원 인증기관 CA는 아래와 같이 위임티켓을 생성하여 대리 인증자 HA에게 전송한다.

1. CA는 난수 $a_{CA} \in Z_{p-1}$ 을 선택한 후 $k_{CA} \equiv g^{a_{CA}} \pmod p$을 계산.
2. CA는 자신의 정보와 대리 인증자의 정보가 포함된 위임 인증서 pc_{CA} 와 k_{CA} 을 가지고 $e_{CA} \equiv h(pc_{CA}, k_{CA}) \pmod q$를 계산한다.
3. CA는 위임티켓 $S_{CA} \equiv x_{CA} e_{CA} + a_{CA} \pmod q$를 계산한다.
4. CA는 I_{CA} , S_{CA} , e_{CA} , pc_{CA} 을 안전한 채널을 통해 HA에게 전송.

MN가 Foreign Network내에 있는 경우 : CA는 FA에게 원 인증기관 CA의 인증 기능을 한다면 FA에서 HA을 통하여 CA에게 인증신청을 하고 MN과 FA의 모든 정보를 CA에게 전송하고 나면 CA에세 인증위임 절차는 HA를 통하여 FA으로 모든 인증 정보를 보낸다.

원 인증기관 CA는 아래와 같이 위임티켓을 생성하여 대리 인증자 FA에게 전송한다

1. HA는 난수 $a_{HA} \in Z_{p-1}$ 을 선택한 후 $k_{HA} \equiv g^{a_{HA}} \pmod p$를 계산한다.
2. HA는 $e_{HA} \equiv h(pc_{CA} \| pc_{HA}, k_{HA}) \pmod q$를 계산한다. 이 때 이전에 받은 pc_{CA}의 내용과 pc_{HA} 를 연결하여 해쉬 함수를 적용한다.
3. HA는 위임티켓 $S_{HA} \equiv S_{CA} + x_{HA} e_{HA} + a_{HA} \pmod q$를 계산한다.
4. HA는 $I_{CA}, S_{HA}, (e_{CA}, e_{HA}), (pc_{CA}, pc_{HA})$를 FA에게 전송한다.

위임티켓 검증 (U_0 : CA, U_1 : HA, U_2 : FA)

대리 인증자 U_i 는 U_{i-1}(i=1,2) 에게 받은 정보와 U_{i-1}의 공개키 y_{i-1} 와 대리 인증용 공개키를 이용하여 다음과 같이 위임티켓을 검증한다.

1. $e_{i-1}' \equiv h(pc_0 \| pc_1 \| ... \| pc_{i-1}, K_{i-1})$을 계산한 후 e_{i-1}과 같은지 확인한다.
2. 위 식이 성립하면, $g^{S_{i-1}} \equiv y_0^{e_0} y_1^{e_1} ... y_{i-1}^{e_{i-1}} K_0$

$K_1 \cdots K_{i-1}$ (mod p)을 확인한다.

위 식이 검증되면, U_i 는 U_{CA} 의 대리 인증 티켓 s_i , r_i 를 생성할 수 있다. 여기에서 r_i 는 인증키이고, s_i 는 다른 대리인에게 보내는 위임티켓이다.

$$r_i \equiv s_{i-1} + e_{i-1} \quad x_i \text{ (mod q)}$$

4. 성능비교

새로운 인증 구조와 기존의 인증 구조의 성능 비교는 다음과 같다.

표 2. 인증모델의 성능 비교

	Jacobs 인증모델	K.Lam 인증모델	새로운 인증모델
상호인증	지원	지원	지원
신뢰도	높음	높음	높음
상호인증 시간	길다	길다	짧다
공개키의 신뢰정점	Root CA	Root CA	Root CA, HA, FA
신뢰경로 구축	어려움 (Root부터)	어려움 (Root부터)	용이 (HA또는 FA로부터)
적용 환경	유선환경	유선환경 무선환경	유선환경 무선환경
모델의 확장성	낮음	중간	높음
핸드오프시간	길다	중간	짧다
인증 시간	길다	중간	짧다
관리 용이성	어려움	어려움	용이
오버헤드 길이	크다	중간	짧다
처리효율	낮음	중간	높음
자원 사용량	낭비	중간	절약
복잡도	높음	중간	낮음
핸드오프시 CRL 검색	필요	필요	불필요 (OCSP사용)

V. 실험 및 결과분석

1. 실험환경

본 논문에서 제안한 무선PKI 기반의 보안구조의 성능을 평가하기 위해 이미 제안된 Jacobs 공개키 기반 인증 알고리즘, Sufatrio.K.Lam 인증 알고리즘들 비교하고 CRL을 검색하는 시간 관점에서 성능을 분석하였으며 각각의 알고리즘과 제안한 보안구조를 비교하여 그래프로 나타내었다.

실험은 Intel Pentium III 1G PC에서 Visual C#.NET 언어를 이용하여 수행하였으며, 제안 보안구조의 성능 향상 정도를 알아보기 위하여 특정 Agent에 핸드오프를 요구하는 무선 단말기의 도착률은 λ_1이고, 초기 인증을 요구하는 무선 단말기의 도착률이 λ_2일 때에 utilization 변화에 따른 핸드오프 시 인증 대기시간을 알아보았다. 핸드오프 시에 무선 대역폭은 2Mbps, 유선 대역폭은 10Mbps, 인증서 크기가 1KB, 공개키 암호/복호 처리 속도를 1.6Mbyte/s, 인증서 검증 시간을 32ms로 가정하였다.

그림 5 은 성능 분석을 위한 실험환경을 나타낸 것이다. 그림에서 볼 수 있듯이 초기 인증을 요청하는 단말기가 도착율 λ_2로 발생되고, 핸드오프를 요청하는 단말기는 도착율 λ_1로 발생된다. 특징 에이전트에게 초기 인증을 요청하는 무선 단말기와 핸드오프를 요구하는 무선 단말기의 요청이 모두 존재하는 경우, 에이전트는 우선 순위 큐잉에 의해서 핸드오프시 인증 서비스를 우선적으로 수행하게

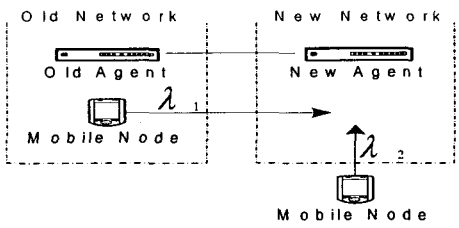


그림 5. 분석을 위한 시나리오

그림 5 에서 각 에이전트의 큐잉모델은 그림 6 와 같이 Q_1, Q_2 두 개의 큐로 구성된다. Q_1는 Q_2보다 높은 우선 순위를 가지는 큐로써 핸드오프시 인증 서비스를 처리한다. Q_1에서 도착율은 λ_1으로 나타낸다. Q_2는 초기 로그인과정의 인증 서비스를 처리하는 큐로 나타낸다. Q_2에서 도착율은 λ_2로 나타내며 Q_2의 처리 순위는 Q_1보다 낮은 우선 순위를 갖는다. Q_1, Q_2는 FIFO(First In First Out)방식을 적용하며, Q_2에서 초기 인증 서비스가 처리중인 경우에 핸드오프 요청이 발생하면 현재 처리 중인 초기 인증 서비스가 끝난 후에 핸드오프를 위한 인증 서비스를

수행하는 비 선점 방식이 적용된다.

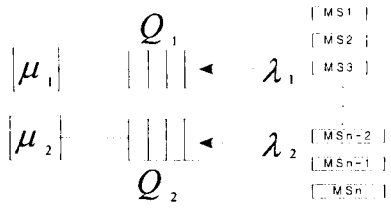


그림 6. 큐잉 모델

이와 같은 큐잉 모델에서 각 큐에서의 평균대기시간은 다음 식과 같이 표현할 수 있다.

$$E(W_k) = \frac{\sum_{i=1}^{2} \lambda_i E(q_i^2)}{2(1-\sum_{i=1}^{k-1} p_i)(1-\sum_{i=1}^{k} p_i)} \quad (k=1, 2)$$

위의 식에서 W_1, W_2는 각각 Q_1, Q_2 에서의 평균대기시간이고, q_1, q_2는 Q_1, Q_2에서 하나의 인증에 대하여 소요되는 처리시간을 나타내는 랜덤변수이다. p_1, p_2는 각각 초기 인증 및 핸드오프시 인증으로 인한 서버의 이용율을 나타내는 변수로서 $p_1 = \lambda_1 E(q_1)$, $p_2 = \lambda_2 E(q_2)$의 값을 갖는다. 여기서 E(·)는 대기치를 나타낸다.

핸드오프 시 인증을 위한 인증 대기시간 $E(W_1)$을 구하면 다음과 같다.

$$E(W_1) = \frac{\lambda_1 E(P_1^2) + \lambda_2 E(P_2^2)}{2(1-\rho_1)}$$

또한 초기 인증 시 대기시간 $E(W_2)$을 구하면 다음과 같다.

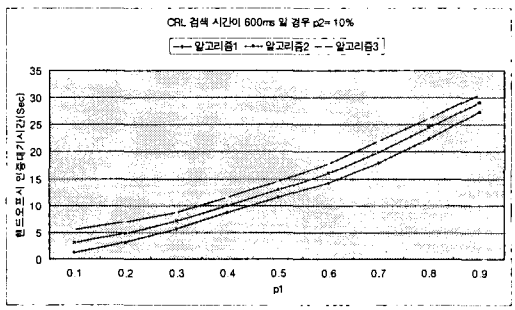
$$E(W_2) = \frac{\lambda_1 E(P_1^2) + \lambda_2 E(P_2^2)}{2(1-\rho_1-\rho_2)(1-\rho_1)}$$

위의 식에서 W_1, W_2 는 각각 Q_1, Q_2 에서의 평균대기시간이고, P_1, P_2 는 Q_1, Q_2 에서 하나의 인증에 대하여 소요되는 처리시간을 나타내는 랜덤변수이다. ρ_1, ρ_2는 각각 초기 인증 및 핸드오프 시 인증으로 인한 서버의 utilization을 나타내는 변수로서 $\rho_1 = \lambda_1 E(P_1)$, $\rho_2 = \lambda_2 E(P_2)$의 값을 갖는다. 여기서 E(*)는 대기치를 나타낸다.

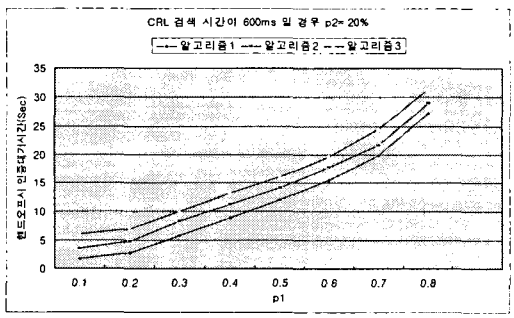
2. 결과분석

첫 번째 실험은 CRL을 검색하는 시간을 각각 600ms와 900ms로 구분하여 분석한 것이다. 핸드오프 시 인증을 처리하는 Q_1의 이용률이 ρ_1, 초기인증을 처리하는 Q_2의 이용률이 ρ_2이므로, 전체 큐의 이용률 ρ는 $\rho = \rho_1 + \rho_2 < 1$의 관계를 갖는다.

그림 5은 CRL 검색에 600ms가 소요되는 경우이다. Agent의 초기 인증 과정을 처리하는 ρ_2의 비율이 각각 10%, 20%를 차지할 경우에 핸드오프 시 인증 서비스를 수행하는 ρ_1의 비율을 변화시켜 가면서 핸드오프 시 인증 대기시간을 구하였다.



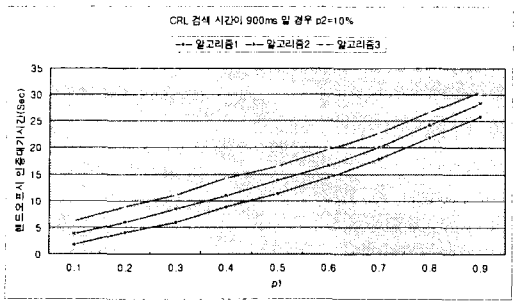
(a) CRL 검색 시간이 600ms & p2=10%일 경우



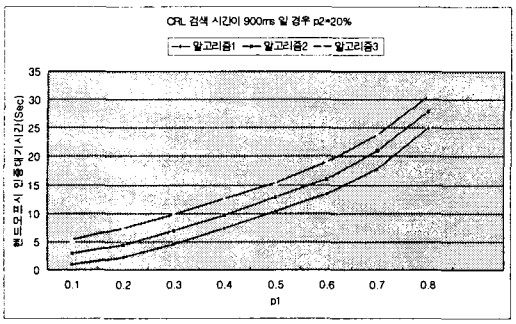
(b) CRL 검색 시간이 600ms & p2=20% 일 경우

그림 7. 핸드오프 시 인증 대기시간

그림 6은 CRL 검색에 900ms가 소요되는 경우이다. Agent의 초기 인증 과정을 처리하는 ρ_2의 비율이 각각 10%, 20%를 차지할 경우에 핸드오프 시 인증 서비스를 수행하는 ρ_1의 비율을 변화시켜 가면서 핸드오프 시 인증 대기시간을 구하였다.



(a) CRL 검색 시간이 900ms & p2=10%일 경우



(b) CRL 검색 시간이 900ms & p2=20%일 경우

그림 8. 핸드오프 시 인증 대기시간

그림 5와 그림 6를 통해서 다음과 같은 결과를 볼 수 있다. 초기 인증 과정 처리 시간이 일정할 경우 제안구조의 핸드오프 인증 서비스 대기 시간이 일반 구조의 경우에 비해 작음을 알 수 있다. 또한 CRL 검색 시간이 클수록 성능 향상 정도가 더욱 확연해 짐을 알 수가 있다. 즉 가입자가 많은 경우, CRL 사이즈가 커지게 되므로 본 논문에서 제안한 구조가 더욱 유용하게 된다.

V. 결론

본 논문에서는 무선환경에서 통신의 보안취약점, 무선 PKI 구조 및 무선 PKI를 기반한 보안알고리즘에 대해 분석하고, 기존의 공개키 기반 보안 알고리즘을 보완하는 새로운 알고리즘을 제시하였다.

무선환경에서 CRL 검색과 인증서 검증 할 때 큰 오버헤드를 최소한으로 사용함으로써, 무선환경에서 적합한 공개키 기반 구조가 되도록 하였다. 또한, 공개키를 사용함으로써 재사용 공격과 서비스 거부 공격을 방지할 수 있도록 하였으며, 메시지와 사용자의 인증, 무결성, 부인 봉쇄 등의 서비스를 지원할 수 있도록 설계하였다.

기존의 프로토콜에서는 외부 에이전트가 단순히 이동노드와 홈 에이전트의 메시지를 전송하는 수동적인 기능만을 수행하였으나, 제안 알고리즘에서는 외부 에이전트가 이동노드와 홈 에이전트를 직접 인증할 수 있도록 하였기 때문에, 위장된 홈 에이전트와 이동노드의 재사용 공격으로부터 보호될 수 있다. 또한 HA, FA가 이동노드의 위탁인증기관 역할을 수행하기 때문에 인증 할 때 빠른 속도로 진행한다.

공개키 기반구조는 무선 데이터 통신 환경에서도 중요한 기반기술로서 작용할 것이다. 정보보호 기술은 과거 응용 서비스의 요소기술 정도로 생각되었지만, 이제는 안전하고 신뢰할 수 있는 통신환경 구축에 있어서 핵심적인 역할을 하고 있으며, 이는 향후 정보통신 산업이 발전함에 따라 더욱 더 강조될 것이다. 또한 모바일 인터넷의 계속적인 발전은 유·무선 통합 환경의 등장으로 이어질 것이다. 유·무선 통합 환경에서는 기존의 인터넷이나 무선통신 환경에서의 정보보호 서비스와는 다른 새로운 패러다임이 적용될 것이며, 이에 대한 연구 및 개발이 계속 진행되어야 할 것이다.

참 고 문 헌

[1] 이용, 무선인터넷을 위한 PKI 구축, 제6회 정보보호 심포지엄, 한국정보보호진흥원, 2001. 7.

[2] C.E. Perkins. ed., "IP Mobility Support," IETF RFC 2002, Network Working Group, October 1996.

[3] C. E. Perkins, D. B. Johnson, "route Optimization in Mobile IP," IETF Mobile IP Working Group Internet Draft, November 2000.

[4] C. E. Perkins, "Mobile IP Local Registration with Hierarchical Foreign Agent Approach," IETF Draft, February 1996.

[5] RFC 2002bis, IP Mobility Support (RFC 2002).

[6] S. jacob, "Mobile IP Public Key Based Authentication," Internet Draft, <draft -jacobs- mobileip - pki-auth-00.txt>, August 1998.

[7] Internet X.509 Public Key Certificate Infrastructure and CRL Profile (RFC 2459), http://www.ietf.org/rfc/rfc2459.txt

[8] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560),

http"//www.ietf.org/rfc/rfc2560.txt
[9] IETF RFC 2459(1999), Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
[10] "Wireless PKI," 한국정보보호진흥원, 2001. 5.

김 미 혜(Mi-Hye Kim) 종신회원

1992년 2월 : 충북대학교 수학과 (이학사)
1994년 2월 : 충북대학교 수학과 (이학석사)
2001년 2월 : 충북대학교 수학과 (이학박사)
2001년 4월 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 초빙교수
<관심분야> : 퍼지이론, 정보이론, 금융수학

서 세 영(Shi-Ying Xu) 정회원

2000년 2월 : 충북대학교 컴퓨터공학과 대학원(공학석사)
2004년 2월 : 충북대학교 컴퓨터공학과 대학원(공학박사)
현재 : (주)덱트론 연구원
<관심분야> : 멀티미디어통신, Mobile PKI, VoIP, QoS