creative commons

COMMONS DEED

저작자표시-비영리-동일조건변경허락 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

동일조건변경허락. 귀하가 이 저작물을 개작, 변형 또는 가공했을 경우에는, 이 저작물과 동일한 이용허락조건하에서만 배포할 수 있습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:24011-200000232712

2006年　2月

博士學位論文

M-Commerce에서 Mobile-IP를 이용한 효율적인 보안 인증 메카니즘

朝鮮大學校 大學院

電算統計學科

申　　珉　　和

M-Commerce에서 Mobile-IP를 이용한 효율적인 보안 인증 메카니즘

An Efficient Security Authentication Mechanism in Mobile-IP Network on M-Commerce

2006年 2月 日

朝鮮大學校 大學院

電算統計學科

申 珉 和

M-Commerce에서 Mobile-IP를 이용한 효율적인 보안 인증 메카니즘

指導敎授　裵 相 賢

이 論文을 博士學位申請 論文으로 提出함

2005年　10月　日

朝鮮大學校 大學院

電算統計學科

申 珉 和

申珉和의 博士學位 論文을 認准함

委員長　朝鮮大學校 敎授

委員　朝鮮大學校 敎授

委員　順天大學校 敎授

委員　群山大學校 敎授

委員　朝鮮大學校 敎授

2005年　12月　日

朝鮮大學校 大學院

목 차

표목차 ····· iii
그림목차 ····· iv
ABSTRACT ····· v

Ⅰ. 서 론 ····· 1

Ⅱ. *M-Commerce* 보안기술 ····· 3
A. M-Commerce ····· 3
1. M-Commerce의 정의 ····· 3
2. M-Commerce 구성요소 ····· 5
3. M-Commerce 특징 ····· 6
4. M-Commerce 관련 요소 기술 ····· 7
5. 모바일 결제 시스템 ····· 15
B. M-Commerce 보안 기술 ····· 17
1. 암호 시스템 ····· 19
2. 암호 키에 따른 암호화 기법 ····· 20
3. WAP 보안기술 ····· 25
4. WML 전자서명 ····· 29
5. WIM(Wireless Identity Module) ····· 30
6. 종단간 보안(End-to-End Security) ····· 32
7. 무선 PKI ····· 34

Ⅲ. *Mobile-IP*에서의 기존 인증 방식 고찰 ····· 38
A. Mobile-IP ····· 38
1. Mobile-IP의 정의 ····· 38
2. Mobile-IP의 관련 용어 ····· 39

3. Mobile-IP의 동작 구조 ····· 42
B. 기존 인증 메커니즘 고찰 ····· 44
1. 비밀키 기반 인증 메커니즘 ····· 44
2. 공개키 기반 인증 메커니즘 ····· 49
3. 최소 공개키 인증 메커니즘 ····· 51
C. 기존 인증 메커니즘의 문제점 및 분석 ····· 53
1. 인증 참여자 ····· 53
2. 인증 서비스 ····· 54
3. 암호 알고리즘의 분석 ····· 55

Ⅳ. 이동망에서 *Mobile-IP* 인증 및 성능 평가 ····· 57
A. 인증 메카니즘 제시 ····· 57
B. 시뮬레이션 구현 ····· 62
1. 모델링 도구 ····· 62
2. 시뮬레이션 환경 ····· 63
C. 시뮬레이션의 성능 평가 ····· 68
1. 암호화·복호화 횟수 및 인증 평균시간 ····· 69
2. 전체 등록시간과 이동 노드에서의 등록시간 ····· 72
3. 전체 등록시간, 노드프로세스시간 그리고 암호화 시간 ····· 75
4. 이동 노드의 위치 변화에 따른 전체 등록시간 ····· 78
5. 서브넷 크기와 이동 속도에 따른 실제 적용 가능성 ····· 79

Ⅴ. 결론 및 향후 과제 ····· 84

참고문헌 ····· 86

표 목 차

[표 1] 무선 인터넷의 특징 ····· 7
[표 2] 비밀키 암호알고리즘과 공개키 암호알고리즘의 비교 ····· 25
[표 3] 인증 메커니즘의 비교 ····· 62
[표 4] 시뮬레이션 고정 파라미터 값 ····· 64
[표 5] 암호화·복호화 횟수 ····· 70
[표 6] 인증 코드의 평균 시간 ····· 71

그림 목차

[그림 1] M-Commerce 구성요소 ····· 6
[그림 2] 암호 시스템의 구성 ····· 19
[그림 3] 비밀키 암호알고리즘의 암호화 방식 ····· 21
[그림 4] 공개키 암호알고리즘의 암호화 방식 ····· 23
[그림 5] WAP 게이트웨이 모델 ····· 26
[그림 6] WML을 이용한 전자서명 ····· 30
[그림 7] WIM을 이용한 WTLS Handshake ····· 32
[그림 8] Mobile-IP의 동작 구조 ····· 39
[그림 9] Mobile-IP 등록 과정 ····· 43
[그림 10] 비밀키 인증 메카니즘 ····· 49
[그림 11] 공개키 인증 메카니즘 ····· 50
[그림 12] 최소 공개키 인증 메카니즘 ····· 52
[그림 13] 인증 메카니즘의 제시 ····· 59
[그림 14] 망 구성 ····· 63
[그림 15] MAC 동작 ····· 65
[그림 16] 전자서명의 작동 ····· 67
[그림 17] 인증기관을 통한 전자서명 인증절차 ····· 68
[그림 18] 전체 등록 시간 ····· 73
[그림 19] 노드 프로세스 시간 ····· 76
[그림 20] 암호화 시간 ····· 77
[그림 21] 이동 노드의 위치 변화에 따른 등록 시간 ····· 78
[그림 22] 이동 속도에 따른 서브넷 머무는 시간 ····· 80
[그림 23] 서브넷 크기 0.1 km일 때 인증 차지율 ····· 81
[그림 24] 서브넷 크기 0.3 km일 때 인증 차지율 ····· 82
[그림 25] 서브넷 크기 1km일 때 인증 차지율 ····· 83

ABSTRACT

An Efficient Security Authentication Mechanism in Mobile-IP Network on M-Commerce

Shin Min-Hwa
Advisor : Prof. Bae Sang-Hyun, Ph.D.
Department of computer science & statistics,
Graduate School of Chosun University

WAP와 같은 표준에 기초를 둔 휴대 단말기들과 네트워크 상의 데이터 수용 능력의 향상은 이동 네트워크 기기들의 급속한 보급과 더불어 M-Commerce의 영역을 확장해 주고 있다. M-Commerce는 무선 인터넷 서비스 중에서 각종 정보, 서비스, 재화에 대한 유료화된 서비스를 의미한다. 온라인 전자상거래인 E-Commerce는 유선 통신을 이용한다면, M-Commerce는 무선 통신을 통해 이루어지는 상거래이다. M-Commerce를 구성하고 있는 여러 가지 기술 중에서 보안과 지불은 매우 중요한 요소이다. 따라서 M-Commerce가 보다 활성화 되기 위해서는 보안과 지불에 대한 신뢰성을 확보해야 한다. 네트워크 통신의 보안을 위해서는 인증, 비밀성, 무결성, 부인 방지 등과 같은 보안에 관한 핵심적인 사항이 요구된다.

M-Commerce를 하기 위해서는 이동 사용자가 언제 어디에 위치하던간에 다양한 서비스에 자유롭게 접근할 수 있어야 한다. 이동망에서 Mobile-IP는 이와 같은 이동성을 제공하기 위해 제시된 IP 프로토콜이다. 즉, 이동 사용자가 일시적으로 다른 서브넷으로 이동하여도 자유롭게 서비스를 제공 받을 수 있다.

Mobile-IP에서는 이동 사용자가 위치 이동을 하여 새로운 위치 정보를 등록 한

후 모든 데이터그램이 그 경로로 전송 된다. 그러므로 위치 정보의 등록 과정은 매우 중요하며 안전한 데이터 전송을 위한 보안은 필수 사항이다.

본 논문에서는 이동성을 제공하는 Mobile-IP에서의 보안에 관한 인증 메카니즘을 제시하였다. 기존 인증 메카니즘에 관한 분석을 통해 각 메카니즘이 갖는 문제점을 파악하고 이를 위한 대안을 제시하였다.

기존 인증 메카니즘 중에서 비밀키 기반 인증 메카니즘은 이동 노드의 계산시간과 비용에 대한 부담이 적어 전체 인증시간이 짧아 시간적으로 효율적이다. 그러나 많은 사용자가 이용할 때 키 분배에 있어서 확장성이 떨어지며 외부 에이전트의 보안이 제공되지 않는다.

대안으로 제공된 공개키 기반 인증 메카니즘에서는 인증기관을 통한 공개키의 사용으로 비밀키 기반 인증 메카니즘에 비해 확장성을 제공한다. 그러나 공개키 동작이 복잡하다는 점에서 하드웨어의 제한을 갖는 이동 노드에서의 공개키 계산은 매우 큰 부담이다.

이에 공개키 사용의 부담을 줄이기 위해 제시된 최소 공개키 인증 메카니즘에서는 이동 노드에서 비밀키를 사용한 인증을 하여 시간적 측면의 효율을 가져 왔다. 그러나 이동 노드에서 부인 방지 서비스를 제공하지 않아 새로운 위치 등록에 대한 위치 등록 인증 기능이 부족하다.

따라서 본 논문에서는 M-Commerce에서 보안과 지불에 대한 신뢰성 확보를 위해, 공개키를 이용한 전자서명을 통해 Mobile-IP가 이용되기위해 필요한 이동 노드의 부인방지 서비스를 제공 하였고, 공개키의 사용을 최소화 하여 계산 부담을 줄여 시간적 측면의 효율성을 가져왔다.

Ⅰ. 서 론

M-Commerce는 '이동전화나 휴대 단말을 이용한 지불 처리'로 보는 극히 제한적 정의도 있으나 '모바일 전자상거래(Mobile E-Commerce)'를 의미하며 이는 본질적으로 인터넷의 확장이며 기존의 고정된 PC에 의한 전자상거래의 한계를 넘어 액세스 단말에 있어서 이동성(Mobility) 이나 휴대성(Portability)을 부가한 것이다. M-Commerce는 무선 인터넷이 가능한 휴대 단말의 증가에 따라 중요성이 부각되고 있다. 인터넷 접속이 가능한 휴대 단말은 PC의 수를 능가할 것으로 전망되고 있는 실정이다. WAP과 같은 표준에 기초를 둔 단말들과 네트워크 상의 데이터 수용 능력의 향상은 이동 전화의 급속한 보급과 더불어 M-Commerce의 영역을 확장해 주고 있다. M-Commerce는 기본적으로 최종 이용자뿐만 아니라 잠재적으로 정보통신, 금융부분, 그리고 소매부문과 미디어 부문에 이르기까지 산업 전반에 지대한 영향을 미칠 것으로 전망되고 이미 소비자들은 그들의 이동전화를 이용하여 e-Cash 뿐만 아니라 뱅킹, 주식 거래, 극장 예매, 열차표 예매, 게임, 복권 등 실로 광범위한 M-Commerce 서비스를 이용하고 있다. 그리고 M-Commerce를 구성하고 있는 여러 가지 기술 중에서 특히 보안과 지불은 가장 중요시되고 있고, 민감한 요소임에 틀림없다. 재화나 서비스를 구매한 뒤 보안과 지불에 대한 신뢰도가 낮다면 이용자가 서비스를 이용함에 있어 큰 장애가 될 것이기 때문이다[1]. 따라서 M-Commerce가 보다 활성화되기 위해서는 보안과 지불에 대한 신뢰성을 확보하는 것은 중요한 사항이다. 기술적인 측면에서 서로 다른 차원의 수많은 네트워크 보안이 있다. 네트워크 트랜잭션에서 보안을 위해서는 인증(Authentication), 비밀성(Confidentiality), 무결성(Integrity), 부인 방지(Non-Repudiation) 등과 같은 몇 가지 핵심적인 보안 요구들이 요구되어 진다[2]. M-Commerce에서 중요한 것은 어디에 위치하던간에 다양한 서비스에 자유롭게 접근할 수 있어야 한다. Mobile-IP는 이런 이동성을 제공하기 위해 제시된 IP 프로토콜로 이동 사용자가 일시적으로 다른 서브넷으로 이동해도 지속적인 서비스를 제공해줄 수 있다. 그러나 무선 네트워크에서의 시그널 전송은 공격 당하기 쉬워 이동 사용자에게 안전한 데이터를 전송

하는 것이 어렵기 때문에 보안은 Mobile-IP 구조에서 빼놓을 수 없는 중요한 요소이다[3].

Mobile-IP에서는 이동 사용자가 새 위치 정보를 등록한 후 모든 데이터가 그 경로로 전송된다는 점에서 등록 과정은 무척 중요한 과정이 아닐 수 없다. 또한 이동 사용자가 전자상거래와 같은 시스템에서 행한 행동에는 책임이 크기 때문에 이동 사용자가 네트워크에서 한 행동에 대하여 책임을 질 수 있는 서비스가 있어야 한다.

IETF의 RFC2002에서는 Mobile-IP망에서 비밀키 기반 인증 메커니즘을 제시하고 있으나 키 분배에 있어서 확장성이 떨어지며, 이 문제를 해결하기 위하여 제안된 공개키 기반 인증 메커니즘은 공개키 동작이 복잡하다는 면에서 전체적인 인증 시간이 길다는 단점이 있다[4]. 또한 최근의 연구 논문에서는 공개키 사용을 최소로 줄여 효율성을 높인 최소 공개키 기반 인증 메커니즘이 제시되었으나 이동 노드가 공개키를 이용한 전자서명을 하지 않기 때문에 부인방지 서비스가 결여되어 있다. 본 논문의 목적은 이동 사용자가 네트워크를 사용하기 위하여 Mobile-IP 상에서 이동성을 제공하는 것으로, 원활한 네트워크 이용을 위하여 안전하고 효율적인 인증 메커니즘을 제안하는 것이다. Mobile-IP가 이용되기 위해서는 이동 노드에 부인방지 서비스가 제공되어야 하며 부인방지 서비스는 공개키를 기반으로 한 전자서명을 할 때 가능하다. 그러나 공개키 사용에 있어서 공개키 계산이 복잡하여 전체 인증 시간이 증가한다는 점과 공개키 확인을 위하여 인증기관에 접근하는 시간이 길다는 점을 고려하여 전체 인증이 효율적으로 이루어질 수 있도록 해야 한다. 따라서 제안된 인증 메커니즘에서는 공개키 사용을 최소로 하여 인증 시간을 줄이면서도 이동 노드에서 전자서명을 함으로써 부인방지 서비스를 제공하고자한다.

본 논문의 구성은 다음과 같다. 1장 서론에 이어 2장에서는 M-Commerce에 대하여 논하고 M-Commerce의 기존 보안기술에 대하여 기술 하였으며, 3장에서는 이동망에서 Mobile-IP에 관한 기존의 인증 방식에 대하여 기술하였다. 4장에서는 Mobile-IP 인증 메카니즘에 대한 제시와 시뮬레이션을 통한 성능 평가를 통해 공개키를 이용한 전자서명을 하여 이동 노드의 부인방지 서비스를 제공 하였고, 공개키의 사용을 최소화 하여 시간적 측면의 효율성을 가져왔다. 마지막으로 5장에서는 본 논문의 연구 결과와 향후 연구 계획에 대하여 기술한다.

Ⅱ. *M-Commerce* 보안기술

90년대 중반부터 폭발적으로 증가하고 있는 인터넷 서비스는 단기간에 우리들 일상생활 깊숙이 자리잡게 되었지만 근본적인 공간의 한계를 갖고 있다. 따라서 시간과 장소에 구애받지 않고 원하는 정보를 언제 어디서나 통신서비스를 제공 받을 수 있는 무선인터넷의 등장은 필연적인 과정이라 볼 수 있다.

무선인터넷은 언제 어디서나 인터넷 접속이 가능하고, 휴대하기 간편한 이동전화, PDA(개인휴대용단말기) 등을 통한 서비스, 다양한 컨텐츠 등으로 이동성과 편의성을 중시하는 고객을 중심으로 각광받고 있다. 상당수 대기업들과 IT 전문 벤처업체들이 차세대 신시장으로 부상한 M-Commerce를 통해 새로운 수익원을 창출하고 업무 효율성과 영업력을 대폭 강화해 나간다는 전략으로 무선 인터넷 서비스를 중점사업의 하나로 꼽고 무선 인터넷 시대를 준비하는데 바쁜 행보를 보이고 있는 이유도 이러한 무선인터넷 서비스의 낙관적인 전망 때문이다.

그러나 현재 국내 E-Commerce의 열풍이 제대로 자리조차 잡지 못한 상황에서 무선 인터넷 서비스에 대한 관심이 고조되고 있는 상황으로 M-Commerce에 대한 보다 심층적인 연구가 부족한 것 또한 현실이다.

따라서 이 장에서는 M-Commerce에 대해서 살펴보고자 한다.

A. M-Commerce

*1. M-Commerce*의 정의

M-Commerce란 개념이 우리에게 구체적으로 다가온 시기는 일본의 NTT-DoCoMo가 I-Mode 서비스를 시작한 1999년 2월 이후라고 할 수 있다. 이전

에는 서유럽 이동통신사업자들이 무선 인터넷 서비스를 시작하였지만, 유럽의 초기 무선인터넷서비스는 주로 SMS(Short Message Service)에 기반한 단순한 정보이용 수준에 불과하였으나 일본의 I-Mode서비스는 C-HTML 기술언어와 Packet 방식의 과금체계 등을 바탕으로 비즈니스 성격으로 발전하였기 때문이다[5].

M-Commerce는 무선 인터넷서비스 중에서 컨텐츠 및 상거래 등의 영역에서 빠르게 진행되고 있는 유료화 된 서비스를 의미한다.(Durlacher Research. 1999.11)

M-Commerce는 이동통신 단말기와 네트워크를 이용하여 이루어지는 각종정보, 서비스, 재화에 대한 금전적 거래를 의미하는 것으로 M-Commerce는 결국 온라인상의 전자상거래인 E-Commerce에 대응되는 개념으로 기존의 B-to-C, B-to-B 등의 전자상거래가 유선이 아닌 무선을 통해 이루어지는 상거래를 의미한다.

무선통신시장의 급성장과 무선인터넷 가입자수의 증가로 M-Commerce에 대한 관심이 고조되고 있는, M-Commerce의 시장 잠재력은 다음과 같은 측면에서 살펴볼 수 있다.

첫째, 매체로서 이동전화시장의 급성장을 들 수 있다. 전세계 이동전화시장은 그동안 급속한 성장을 거듭해 왔을 뿐 아니라 향후에도 연평균 23.6%의 성장이 전망되고 있다. 전세계 이동전화단말기 수는 98년에 약 2억 9천대로 이미 PC보급대수에 근접하고 있으며 현재에는 PC 보급대수를 크게 상회하고 있는 실정이다. 또한 세계 주요 선진국은 무선 멀티미디어 서비스 제공이 가능한 IMT-2000의 도입을 적극 추진하고 있으며, 이동전화사업자 입장에서도 무선데이터통신이라는 시대적 흐름에 따라 네트워크의 디지털화를 지속적으로 추구하고 있어 향후 이동전화를 통한 M-Commerce가 점차 활성화될 것으로 평가되고 있다.

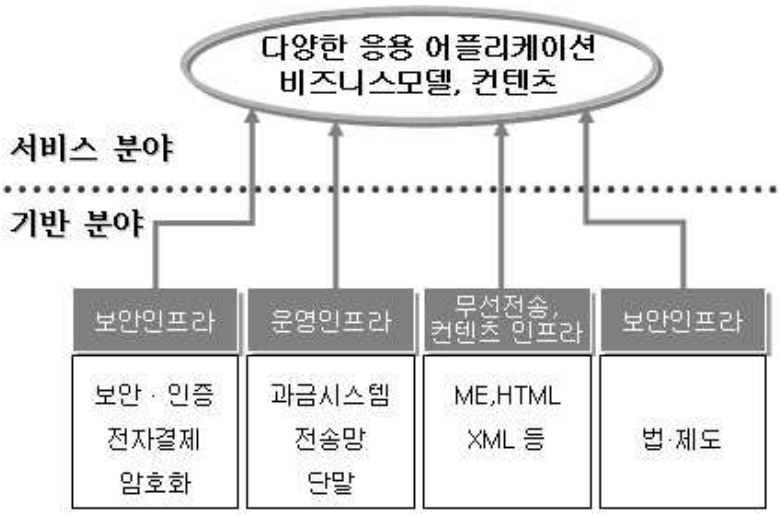
둘째, 인터넷서비스의 폭발적인 성장을 들 수 있다. 인터넷(WWW)은 서비스가 본격화 된 1992년 이후 불과 8년만에 전세계적으로 사용자수가 2억 4천만명에 이르는 폭발적인 성장세를 보이고 있으며, 향후에도 연평균 22.7%씩 증가하여 약 6억 7천만명을 초과할 것으로 전망되고 있다.(ARC Group. 1999.) 또한 인터넷에 접속하는 매개체별 접속 비율 전망을 통하여 무선인터넷 시장의 성장가능성을 엿볼 수 있다. 즉, 현재 유선인터넷에 접속하는 매개체의 98%가 PC이지만 향후에는 인터넷

의 접속수단으로서 PC의 역할은 점차 감소할 것이라는 전망에 꾸준히 제기되고 있으며, 현재는 인터넷 접속수단이 PC라는 단일 플랫폼 중심으로 이루어지고 있지만, 향후에는 이용자의 이용목적과 접속환경에 따라 다양한 매체를 통해 인터넷에 접속할 수 있을 것으로 예상된다.

Dataquest(1999)에 따르면 1999년에 인터넷 접속수단의 98%가 PC이지만 2003에는 전체의 53.5%를 이동통신 단말기가 차지하여 PC의 역할은 34.5%로 축소될 것으로 보인다. 따라서 무선인터넷 서비스 시장은 이동전화의 급속한 보급과 인터넷의 급성장에 힘입어 그 성장가능성이 매우 높다고 할 수 있다. 즉 폭발적인 성장을 거듭한 인터넷은 현재 PC를 통한 접속에만 의존하지 않고 이동전화기, PDA 등 다양한 단말기를 통하여 접속할 수 있게 되었으며, 유 · 무선 통신의 대체현상을 야기할 정도로 보편화된 이동전화 보급률을 감안 할 때 무선인터넷 서비스 시장은 현재의 유선 인터넷 시장에 버금가는 성장잠재력을 가지고 있을 것으로 분석된다.

2. M-Commerce 구성요소

M-Commerce의 구성요소는 [그림 1]과 같이 크게 서비스분야와 기반분야로 구성되어 진다. 서비스 분야는 다양한 응용어플리케이션들이 있으며 기반분야는 보안인프라, 운영인프라, 무선전송 및 컨텐츠 인프라, 제도적 인프라로 나눠진다.



[그림 1] M-Commerce 구성요소

서비스분야는 개인이나 기업이 이동단말을 통해 실제로 구매·관리 등 상거래 행위를 하는 분야로 소비자의 이용을 촉발시키고 사업자가 수익을 올릴 수 있는 비즈니스 모델과 다양한 컨텐츠, 이를 지원하는 응용 어플리케이션 등의 개발이 필요하다. 특히 유선 전자상거래와 마찬가지로 수익성 있는 비즈니스 모델과 컨텐츠 확보가 서비스분야의 성공요인이라 할 수 있다[6].

향후 무선 인터넷 활성화와 IMT-2000 서비스 개시로 많은 사업자가 M-Commerce에 참여할 것으로 예상되며, 시장에서 보다 다양한 아이디어의 창출이 필요하다.

3. M-Commerce 특징

M-Commerce의 환경은 기존의 유선 네트워크와는 환경자체가 다르다. 기존 유선 인터넷과 비교하여 이동성 및 개인화의 장점을 가지고 있다. 무선인터넷 서비스의 장점은 인터넷이라는 네트워크가 가지고 있는 개방성, 양방향성 등의 속성과 이

동통신의 이동성(Mobility), 개인화(Personalization), 위치 기반성(Location Based) 등의 속성을 동시에 지니고 있다[7].

반면 유선 인터넷 서비스와 비교하여 무선 인터넷 서비스가 안고 있는 취약한 면은 전송속도, 화면크기, 통신에러율, 프로토콜의 표준화, 컨텐츠 제작형태, 저장용량 등이 있다. 또한 디스플레이 및 입력장치의 경우에도 유선 인터넷 환경은 대형 화면(17 ~ 21인치)에 편리한 인터페이스를 가지고 있는 반면, 무선 인터넷 환경은 작은 화면(2 ~ 8인치)과 불편한 작은 Keypad를 가지고 있다.

하지만 [표 1] 에서와 같이 M-Commerce가 갖고 있는 유용한 특징들로 인해 M-Commerce 시장에 대한 관심과 기대가 고조되고 있다.

[표 1] 무선 인터넷의 특징

주요특성	의미
Ubiquity	어디에서나 실시간 정보검색 가능
Reachability	언제 어디서나 인터넷 접속 가능
Convenience	통신도구 이용의 편리성
Security	보안 가능
Localization	사용자의 현위치를 보여줌
Instant Connectivity	빠른 시간내에 필요한 정보검색
Personalization	사용자의 개인화

4. M-Commerce 관련 요소 기술

M-Commerce에 관련된 기술들은 무선 접속 기술, 보안기술, 컨텐츠 제작기술, 단말기 제조 기술 등 많은 분야의 복합적인 기술들이 요구되는데 이에 대해 기술

하고자 한다.

a. 무선 접속 기술

이는 단말과 이동통신망을 연결해 주는 무선 구간 기술로 다중 접속 방식, 듀플렉스방식, 채널 코딩, 변조방식, 전력제어기술 등을 말한다[8]. 무선 인터넷을 위한 무선 접속에서의 표준화핵심 기술로는 비대칭 데이터의 효율적인 전송을 위한 시분할 듀플렉스 방식, 다중 대역/다중 모드 지원을 위한 소프트웨어 라디오 기술 등을 들 수 있다. 세계적으로 이동 통신망의 표준은 유럽 표준인 GSM(Global System for Mobile Communication)방식과 미국 표준인 CDMA(Code Divison Mulitple Access)방식으로 크게 나눌 수 있다.

(1) GSM(Global System for Mobile Communication) 방식

1982년 CEPT(Coference of European Posts and Telegraphs)에서 범 유럽용 이동통신 시스템을 개발하기 위해 GSM(Global System for Mobile Communication)을 개발하였다.

GSM은 POTS(Plain Old Telephone Service), ISDN(Integrated Services Digital Network), PSPDN(Packet Switched Public Data Network), CSPDN(Circuit Switched Public Data Network)에 접속되어 최대 9600bps로 통신을 할 수 있으며 이때 X.25 또는 X.32등 다양한 프로토콜을 사용할 수 있다. GSM이 ISDN이나 다른 디지탈 망과 접속시에 별도의 모뎀이 필요치 않지만 아날로그 POTS와 접속 시에는 Audio Modem이 필요하다. 이외 G3 팩스, SMS(Short Message Service) 기능을 지원한다. SMS는 양방향의 단문 전송 서비스로 최대 160byte까지 전송할 수 있으며 실제적으로는 170자까지 전송할 수 있다. SMS는 Point-to-point 서비스나 Cell Broadcasting 서비스로 활용될 수 있으며 SIM에 저장시킬 수도 있다.

GPRS(General Packet Radio Service)는 GSM에서 패킷 전용으로 제시되는 방식으로 9600bps의 낮은 속도를 제공하는 GSM의 데이터 서비스의 단점을 보완하고 있으며, 최대 170kbps 정도를 목표로 하며 실제로 데이터 서비스에 제공되는 데이터 전송 속도는 30kbps ~ 50kbps 정도이다.

EDGE(Enhanced Data Rates for GSM Evolution)는 서비스의 고속화를 위하여 GSM 네트워크에 추가적으로 도입이 가능한 방식이다. GPRS의 진화된 형태로 연구된 망이다. 최고 약 400kbps의 데이터 전송이 가능하다. 이는 3G 서비스 보다 한 발 앞서 데이터 전송 속도를 향상시킬 수 있을 것으로 기대되는 서비스이다.

UMTS(Universal Mobile Telecommunication System)는 IMT-2000을 위하여 제시되는 방식으로 로빙 서비스 및 위성을 사용하여 유럽과 전세계적은 통신 서비스 제공을 목적으로 하고 있다. 이를 위해 셀룰러, 무선 전화기 등의 기존 시스템까지를 통합시킨 시스템으로 구성되는 것이 특징이다.

(2) CDMA(Code Divison Mulitple Access) 방식

코드분할 다중접속방식(CDMA : Code Division Multiple Acess)은 여러 사람이 같은 장소에 모여서 동시에 이야기를 하는 것과 같다. 다만 서로 다른 언어를 사용하기 때문에 자기가 알 수 있는 언어로 이야기하는 내용만 알아 들을 뿐이고, 다른 사람이 이야기 하는 것은 단지 잡음으로만 느끼는 것과 같다. CDMA 기술은 기본적으로 오래전부터 사용해왔던 대역확산 통신기술을 이용한 것으로, 대역확산 기술이 가지고 있는 모든 장점에 주파수 이용 효율을 크게 증가시킨 것이다. 위의 예를 기술적으로 표현해 보면, 모든 서비스 영역에서 같은 주파수 대역을 사용할 수 있기 때문에 셀룰라 개념에서 보면 주파수 재사용 계수가 1이 되어, 주파수 이용 효율이 다른방식에 비해서 월등히 높다는 것과, 모든 서비스 영역에서 같은 주파수 대역을 사용할 수 있기 때문에 소프트 핸드오버가 가능하다는 점, 또한 서로 다른 코드를 사용하여 통신을 하기 때문에 무선 구간의 통신 비밀 보호 특성이 매우 우수하다는 장점이 있다. 또한 CDMA 방식은 여러 사용자가 동일한 주파수를 동시

에 사용하므로 가입자 수용 용량을 그만큼 늘릴 수 있다. CDMA 방식의 디지탈 이동전화 시스템의 상용화 기술은 최근에 나온 기술이지만 CDMA 이론은 1950년대에 이미 정립되었고 1960년대부터는 군통신에서 사용하고 있다. 군통신은 무엇보다도 도청 방지가 중요한데 CDMA 방식의 기술적 근간이 되는 대역확산(Spread Spectrum) 기술이 군통신의 도청 방지에 적용되었던 것이다[9].

예를 들어, IS 95-C는 기존의 IS 95-B에 비하여 패킷 방식의 서비스를 제공하기 때문에 한 차원 높은 서비스의 제공이 가능하다. 속도는 최대 약 144kbps까지 가능하다. 또한 HDR(High Data Rate) 방식은 퀄컴에서 제안한 방식으로 IS 95-C와 같은 1.25MHz의 주파수 대역을 사용하고 IS 95-C와 호환된다. 최대 2.4Mbps의 전송이 가능하나 사용자가 많을 경우 속도가 느려질 수도 있다. MC(Multi Carrier) 방식은 IMT-2000용으로 CDMA쪽으로 제시되는 방식이다. MC 방식에서는 하나의 밴드만을 사용하는 기존의 1X 방식과 달리 3개의 밴드를 사용한다.

(3) CDMA(Code Divison Mulitple Access) 방식의 특징

CDMA 방식의 대표적인 특징은 다음과 같다.

① 대용량이다.

동일한 주파수를 많은 셀에서 사용할 수 있으며 타방식보다 간섭이 적고 통화자가 침묵하고 있는 시간동안 전송을 중지함으로써 아날로그 방식보다 수용 용량을 10배 이상 높일수다.

② 고품질의 서비스 제공이 가능하다.

아날로그 방식에서는 다중 경로로 들어오는 신호들이 통화에 상당히 나쁜 영향을 미친다. 그러나 CDMA에서는 이러한 다중 경로 신호를 각각 분리하여 양호한

신호를 선택 사용하므로 아날로그 방식보다 품질이 우수하고 핸드오프시 통화의 절단이 없는 소프트 핸드오프 방식을 사용하므로 통신의 품질이 양호하다.

③ 보안성이 탁월하다.

아날로그 신호의 디지탈화에 따른 암호화, 광대역 방식에 따른 도청의 한계, 사용자 마다의 PN(Pseudo Noise) 코드 사용에 의한 암호화 등으로 인해 통화 비밀을 유지할 수 있다.

④ 고품질의 데이타 서비스를 제공한다.

디지탈 방식에서는 모든 신호가 디지탈로 처리되므로 이 방식을 이용해 데이타 서비스를 하기가 쉬워진다. 특히 팩스 등의 데이타 서비스에서 통화 절단이 없으므로 데이타 서비스 등에 상당히 우수한 방식이다.

⑤ 이동국의 소비 전력이 적게 들고 소형 경량화가 가능하다.

CDMA 시스템은 인접 셀이나 섹터(Sector)에서도 같은 주파수를 사용하므로 주파수 재배치 같은문제가 발생하지 않아 주파수 계획이 간단하다. 이에 비하여 아날로그 시스템은 C/I를 18dB로 맞추어주기 위해 인접 셀에서는 같은 주파수를 사용할 수 없어(N=7 또는 5) 주파수 계획이 복잡하다

b. 무선 인터넷 전송 프로토콜 기술

무선 응용 서비스의 데이터를 무선 단말기와 유선 인터넷 사이에서 안정적으로 송수신할 수 있드록 해주는 제반 프로토콜 규격을 말한다. 이는 무선 응용 서비스

의 일관된 송수신을 위한 세션 관리 기술, 무선 단말과 인터넷 서버 사이의 데이터 송수신을 위한 데이터 전송기술, 최적의 응용 서비스를 위한 단말과 서버 사이의 프로파일 협상 기술이 있으며, 전송의 효율성을 높이기 위한 데이터의 캐시기술과 푸시기술이 있다.

c. 무선 인터넷 망 기술

이 기술은 무선 인터넷을 구현하기 위하여 이동통신 핵심망 또는 인터넷망에 요구되는 기술로 네트워크 네임(name) 및 주소를 관리하기 위한 네이밍 및 주소기술, 단말의 이동성 관리를 위한 이동성 관리기술, 서비스의 품질을 보장하기 위한 QoS 기술 등을 포함한다.

d. 보안 기술

현재 유선 인터넷에서는 도청, 메시지 변조, 신분 위장 등의 공격에서 기밀성(Confidentiality), 사용자 인증(Authentication), 데이터 무결성(Integrity), 부인봉쇄(Non-Repudiation) 등과 같은 정보보호 서비스를 제공한다. 무선 인터넷에서도 동일한 서비스를 제공해야 하나 무선 환경의 제약사항으로 인하여 기존의 보안 기술을 그대로 사용하기 힘들며, 특히 유·무선 연동을 위한 게이트웨이는 보안에 취약하므로 무선 인터넷 환경에 적합한 새로운 보안 프로토콜의 개발이 필요하다.
무선 인터넷이 유선 인터넷과 다른 점을 크게 자원의 제한과 이동통신 사업자의 개입이라는 측면으로 나누어 살펴보면 다음과 같다.

(1) 제한된 자원

무선 인터넷에서 사용되는 통신 기반은 유선에 비하여 상대적으로 제한된 대역

폭을 갖고 있다. 또한 사용하는 단말기도 휴대성을 확보하고 싼 가격으로 만들어서 대량으로 배포하여야 하는 특성에 따라 상대적으로 약한 CPU 와 더 적은 메모리를 채택하고 전원도 제한된다. 또한 작게 만들어야 하기 때문에 입력에 사용할 수 있는 키보드나 화면의 크기도 제한될 수밖에 없다.

(2) 이동통신사업자의 개입

무선과 유선을 연결하기 위해서는 이동통신사업자가 서비스를 해주지 않고는 불가능하다. 이는 탈 중심적인 기존의 인터넷 구조와는 달리 모든 단말이 이동통신사업자의 게이트웨이를 통하여 서비스를 요청하기 때문에 이동통신사업자는 모든 가입자에 대하여 그들이 어떤 사이트에서 어떤 서비스를 받는 지를 관리할 수 있고 또 관리하여야 하는 상황이 된다.

(3) 느린 응답 속도

단말기와 서버 사이에서 데이터가 오갈 때 유선에 비하여 무선은 시간이 많이 걸릴 수 있다. 이러한 상황에 맞추어 프로토콜을 튜닝하여야 한다.

(4) 낮은 전송률

아직은 무선 인터넷의 대역폭이 크지 않으므로 많은 양의 데이터를 주고받는 형태로 설계되어서는 안 된다.

(5) 낮은 처리 속도와 적은 메모리

단말기에 내장된 마이크로프로세서와 메모리는 처리 속도와 용량 면에서 개인용 컴퓨터에 훨씬 못 미친다. 따라서 복잡하거나 많은 메모리를 차지하는 알고리즘을

채택하기 어려우며 다양한 알고리즘을 지원하는 것도 어렵다.

e. 컨텐츠 기술

컨텐츠에 사용되는 각 미디어를 표현하는데 필요한 데이터 표현 기술과 사용자와 서버간의 서비스를 특성 정보를 협상하는 데 필요한 프로파일 기술을 포함한다. 데이터 표현 기술은 무선 인터넷 환경에서 사용자가 서버로부터 제공받는 서비스가 여러 미디어로 구성되므로, 각 미디어를 표현하고 상호 교환을 위한 기법을 다루며, 프로파일 기술은 인터넷 서비스를 효율적으로 제공받기 위하여 사용자가 이용하는 단말, 네트워크 응용 또는 사용자의 선택사항을 서버와 협상할 수 있도록 하는 기술을 의미한다.

f. 단말기술

무선 데이터 서비스는 기존의 양방향 SMS에 기반 한 무선 데이터 서비스에서 브라우저를 탑재한 무선 인터넷 서비스로 바뀌어 가고 있다. 무선 인터넷을 위하여 무선 단말기는 하드웨어적으로는 빠른 속도 지원, 화면 색상의 다양화, 화면 화소의 증대, 더 많은 배터리 용량, 빠른 CPU 속도 등을 요구하며 소프트웨어적으로 인터넷 서비스를 가능하게 하는 브라우저의 탑재와 각종 서비스를 위한 프로그램이 추가로 필요하다.

최근 휴대 전화는 단말의 고성능화가 진전되고 있으며 많은 단말에 인터넷 접속 기능이 표준으로 탑재되고 있다. 현재 IMT-2000 서비스의 전개에 따른 정보 단말의 발전 방향은 크게 두 가지 흐름을 가지고 있다. 하나는 기존 단말기 업체의 음성 위주 휴대폰이 스마트폰이나 인터넷폰과 같은 화상통화 및 멀티미디어 서비스가 가능하고 복합적인 기능을 가진 정보 단말로 발전하고 있는 것이다. 또 다른 흐름으로는 기존의 PDA가 무선 모뎀을 장착하여 무선 인터넷 시대의 새로운

Post-PC를 대변하는 정보 단말로 변신을 도모하고 있다.

차세대 무선 인터넷 단말기는 무선 LAN 접속이 가능하며, 블루투스(Bluetooth) 기능 등과 같은 많은 무선 인터넷 기능들이 추가될 것이다. 또한 3세대 인터넷 IMT-2000 솔루션을 탑재할 것이므로 음성뿐만 아니라 동영상 처리 기능을 갖춘 멀티미디어 단말기로의 발전이 이루어질 것이다. 그리고 차후의 단말은 국제화 추세를 고려하여 다국어 지원이 이루어져야 하며, 응용 소프트웨어 개발환경에서 다양한 솔루션 확보가 이루어져야 하며, 데이터의 호환성을 확보해야 한다.

5. 모바일 결제 시스템

최근 급증하고 있는 휴대폰 보급률과 함께 이를 활용한 결제서비스들이 잇따라 등장하고 있다. 최근까지만 해도 유료컨텐츠나 온라인쇼핑몰 대금 결제시 휴대폰 SMS(단문메시지전송)를 통해 사용자 인증을 받는 형식의 결제 서비스가 주류를 이루었으나, 최근 들어 모바일 인터넷상의 가상계좌를 충전해 휴대폰으로 결제하거나, 휴대폰에서 바로 신용카드 거래 승인을 받는 서비스, 생체 인증 방식 서비스 등 휴대폰 결제방식이 크게 다양화되고 있다. 또한, IC칩을 휴대폰에 장착하거나, 블루투스와 적외선 전송방식을 이용한 결제서비스도 차츰 대중화될 것으로 보여, 휴대폰 결제의 응용범위가 더욱 확대될 것으로 예측되어진다.

a. 모바일 결제를 위한 인터페이스 국내 기술 개발 동향

국민은행과 LG텔레콤이 합작한 뱅크온 이나 SK텔레콤의 모네타 등 비접촉식 지불 결제도 서비스 제공회사들의 적극적인 마케팅 전략에 힘입어 각광받고 있다. 이와 함께 이마트 등 유통업계에서도 모바일 지불결제 서비스 도입을 서두르고 있어 시장활성화가 기대되고 있다.

비접촉식 무선 기술로는 RF, 적외선, 블루투스 등이 있으나 RF방식이 가장 앞서

가고 있다. RF방식은 카드 등을 삽입하는 시간이 필요없어 빠른 처리가 가능하고 전파를 이용하기 때문에 전파의 전달 범위 안에만 들어오면 방향성 없이 인식할 수 있어 바코드나 적외선과 같이 인위적으로 리더기에 직접 댈 필요가 없어 사람의 개입을 최소화할 수 있는 장점이 있다. 또 유리, 가죽, 종이 등 비금속 재료를 통과할 수 있어 가방에 넣은 상태나 포장된 상태로도 ID를 인식할 수 있고 동시에 여러 개의 태그를 인식할 수 있어 지불결제 서비스는 물론 물류, 공정, 재고, 주차장 관리, 도난방지 등에 많이 이용될 것으로 전망된다[10][11].

b. 모바일 전자지급 결제 표준화

모바일 전자지급 결제 표준화는 전자상거래의 활성화와 관련 산업의 안정적 육성을 보장하고, 나아가서는 국제표준과의 호환성을 사전 확보하여 이 분야 세계시장에서 국가경쟁력 제고를 목적으로 하는 제반 활동이며, 구체적으로는 전자지급결제 시스템을 구성하는 참가주체, 결제수단, 보안프로토콜, 처리흐름 등 시스템 구성요소 전반에 대한 최적의 정의를 통하여 도출된 정형화된 합의(Agreements)로 규정(Rules), 지침(Guidelines) 혹은 특성의 정의(Definitions of Characteristics), 시스템 요구사항을 산출하고,이를 통해 사용자에게 기준모델을 제시하는 일체의 과정과 결과물을 전자 지급결제 표준화라 한다. 또한 정의된 기준 모델은 다수의 사용자를 확보하고 다양한 응용 모델의 제시가 가능한 개방형 모델로 발전함으로써 표준화는 진행된다[12].

c. 모바일 통신카드

최근 정보화 시대를 맞이하여 이동통신 사업이 미래의 핵심 산업으로 급부상 하고, 이동통신 가입자의 폭발적인 증가로 보다 많은 서비스 제공이 요구되고 있다. 이러한 상황에서 IC카드는 뛰어난 보안성과 휴대의 편리성, 응용 확장성으로 인하

여 많은 관심을 집중시키고 있으며, 유럽의 GSM도 응용 범위를 확대하고 있다. 또한, IMT-2000 시스템 사업자가 선정되면서 사용자의 인증과 로밍, 부가서비스 등의 기능을 담당하게 될 사용자 인증 카드(USIM)에 대한 관심이 높아지고 있다. USIM카드는 통신사업자, 사용자 비밀번호, 로밍 정보, 사용자와 관련된 전화번호, 통신사업자 및 컨텐츠 사업자가 개시하고 있는 부가적인 이동통신 서비스를 저장하고 있으며, 이 카드를 장착한 핸드폰을 통해 국제 로밍을 포함한 음성 이동통화 및 텍스트 혹은 브라우저 중심의 M-Commerce 서비스를 제공할 수 있다.

USIM카드는 3세대 비동기식 시스템에 사용되는 사용자 인증카드로 시스템별 응용 서비스를 핸드폰에서 구현하지 않고 카드내 사용자 메모리 공간에 저장함으로써 개인의 정보 보안 및 개인화된 맞춤 서비스 구현이 가능하다.

이에 국내의 통신사업자들은 뉴스, 증권, 게임, 퀴즈 등의 서비스 제공을 준비하고 있으며 이동통신을 이용한 전자상거래와 로얄티 서비스 제공 등 그 사업 영역을 확대하고 있다.

B. M-Commerce 보안 기술

서론에서 언급한 바와같이 정보통신 기술의 급속한 발전과 함께 인터넷의 활용이 다양해져 전자상거래라는 새로운 문화가 생성되고 있다. 또한 이동 통신의 급속한 발전과 함께 개인의 정보통신에 대한 수요가 증가하여 무선 데이터 서비스가 활성화됨에 따라 무선 통신 환경에서 뱅킹서비스, 주식거래, 온라인 쇼핑 등의 전자상거래 서비스가 널리 확대되고 있는 실정이다.

그러나 무선인터넷에서 전자상거래가 원활하게 이루어지기 위해서 보안문제는 시급히 해결해야 할 문제이다. 무선에서의 인터넷은 유선에서의 인터넷과 달리 데이터 전송속도가 느리고, 패킷 오류율이 높으며, 데이터를 전송, 처리하고 사용자에게 그 결과를 보여주는 단말기의 화면, 메모리, 중앙처리장치 등의 자원이 개인용 컴퓨터에 비하여 열악한 환경을 가지는 등의 여러 가지 제약사항을 가지고 있다.

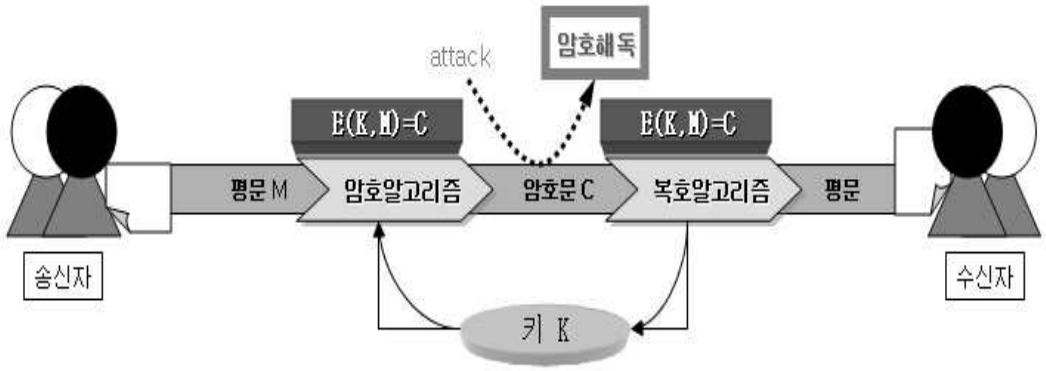
이러한 제약사항으로 인하여 무선인터넷은 휴대 단말과 유·무선 복합 네트워크 환경에 종속적인 프로토콜을 필요로 한다. 따라서 무선인터넷은 기본적으로 기존의 인터넷 환경을 사용하는 만큼, 인터넷이 가지고 있는 보안 취약 요소에 유·무선 복합 네트워크 환경에 따른 프로토콜에 적응적인 기능을 추가로 고려하여야 하며, 휴대 단말의 환경에 적합한 경량의 보안 알고리즘과 메커니즘이 고려되어야 한다.

일반적으로 보안기술은 크게 2가지로 구분할 수 있다. 첫째는 시스템 보안이며, 다른 하나는 네트워크 보안이다. 시스템 보안은 해킹, 바이러스와 같은 공격에 대해서 정보보호 서비스를 제공하며, 주로 운영제체 보안과 관련이 있는데 침입탐지 시스템(IDS : Intrusion Detection System)이 대표적인 예이다. 침임탐지 시스템은 시스템이 네트워크에 대한 침입을 즉각적으로 탐지하고 대처할 수 있는 기술로 침입자에 대한 불법적인 사용을 탐지하고 합법적인 사용자에 의한 오용이나 남용을 탐지하는 것이 목적이다. 네트워크 보안은 네트워크 상에서의 도청, 메시지 변조, 신분 위장 등의 공격에 대해서 정보보호 서비스를 제공한다. 네트워크 보안을 통해 제공되는 정보보호 서비스는 크게 4가지가 있는데, 이는 네트워크를 통해 전송되는 데이터에 대해 권한이 부여된 사람만이 내용을 볼 수 있도록 하는 기밀성(Confidentiality), 메시지를 작성한 사람의 신원을 확인할 수 있도록 하는 사용자 인증(User Authentication), 전송된 데이터가 전송 도중에 변경되었는지 확인할 수 있도록 하는 데이터 무결성(Data Integrity), 송신자가 메시지를 송신한 사실을 부인하거나, 수신자가 메시지 수신 사실을 부인할 수 없도록 하는 부인 봉쇄(Non-Repudiation)가 있다. 이러한 정보보호 서비스는 하나의 메커니즘을 통해서 모두 제공될 수 없으며, 여러 가지 다양한 메커니즘에 의해서 제공되는 것이 일반적이다. 이들 보안 기술 중에서 오래전부터 널리 사용되어온 암호화 기술과 사용자 인증을 제공하여 모바일 전자상거래에서 정보보호 문제해결에 관하여 기술하고자 한다. 또한 현재 무선인터넷으로 서비스 되고 있는 기술로는 기존 유선 인터넷의 프로토콜인 HTTP에 기반하여 서비스를 제공하고 있는 ME(Mobile Explorer)와 I-Mode가 있으며, 무선 네트워크 환경에 적합하도록 새로운 프로토콜을 개발하여 서비스 하고 있는 WAP이 있다. 무선 인터넷에서 정보보호 서비스는 무선인터넷이

어떤 프로토콜을 기반으로 하여 동작하는 지에 따라 제공되는 서비스 형태가 달라진다. 이 장에서는 이들 각각에 대한 보안 기술에 대해 기술 하고자 한다.

1. 암호 시스템

암호(Crytography)란 평문(Plaintext)을 해독 불가능한 암호문(Ciphertext)으로 변형하거나 또는 암호화된 통신문을 복원 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술 또는 과학이다. 암호화(Enctyption)란 데이터의 보호를 위하여 전혀 변화되지 않은 상태의 평문(Plaintext)을 연산자를 이용하여 암호문(Ciphertext)으로 바꾸어 주는 것을 말하며 반면 원래의 평문으로 복원시키는 것을 복호화(Decryption)라 한다[13]. 이 때 사용되는 암호화 키와 함께 암호화와 복호화를 수행하는 시스템을 암호 시스템(Cryptosystem)이라고 하며 [그림 2]와 같이 나타 낼 수 있다. 대부분의 암호 시스템은 암호화·복호화 과정에서 특정한 키를 사용하므로 키를 알고 있는 사람이 암호문을 만들 수 있고 또 암호문을 평문으로 복원시킬 수 있다.



[그림 2] 암호 시스템의 구성

만약, 정보가 제 3자에게 노출될 수 없는 전송 수단을 통해 전달된다면 그 정보는 안전하고, 정보를 보호하기 위한 연구는 필요하지 않을 것이다. 하지만 그러한 전송 수단은 존재하지 않기 때문에 우리는 항상 위험에 대해 대비를 하여야 한다. 즉, 암호는 제 3자가 정보를 훔쳐내더라도 그 의미를 알 수 없도록 하는 것이다.

송신자가 보내고자하는 원래의 데이터를 평문(Plaintext) M 이라 하고, 평문을 암호알고리즘 과정을 거쳐 제 3자가 보더라도 평문의 내용을 쉽게 알지 못하도록 하는 것이 암호화(Encryption)라고 하는데 평문이 암호화과정을 거치면 암호문(Cipertext) C가 된다. 반대로 암호문으로부터 평문으로 바꾸는 과정을 복호화(Decryption)라고 한다.

이러한 암호화, 복호화 과정에서 이용되는 알고리즘을 암호 알고리즘이라 하고 암호 알고리즘에서 평문을 변환하는 주체가 되는 것을 키(Key)라고 한다. 암호화, 복호화 과정에서는 송신자와 수신자가 알고 있는 키(Key)가 사용되는데 제 3자는 송신자와 수진자의 키(Key)를 알지 못함으로 평문의 내용을 쉽게 알 수 없다. 따라서 송신자와 수신자는 서로간의 비밀키의 관리를 중요시해야 한다[14].

이와 같이 암호 시스템의 암호화 과정은 알고리즘과 키로 구성되는데, 키는 알고리즘을 제어하는 평문과 무관하게 독립된 값이며, 알고리즘은 당시 사용된 특정키에 따라 상이한 결과를 생성하게 된다[15]. 키를 바꾸게 되면 그에 따라 알고리즘의 결과도 변하게 된다. 일단 생성된 암호문은 전송되고, 수신된 암호문은 복호화 알고리즘과 복호화키를 사용하여 평문으로 재변환 된다. 암호 시스템은 전통적으로 치환(Substitution)과 전치(Transposition)에 원리를 둔다. 치환은 평문의 비트, 문자, 비트군, 문자군을 다를 원소에 사상시키는 것을 말하며, 전치를 평문의 배열을 재구성함으로서 암호학적 강도를 높이는 것을 말한다.

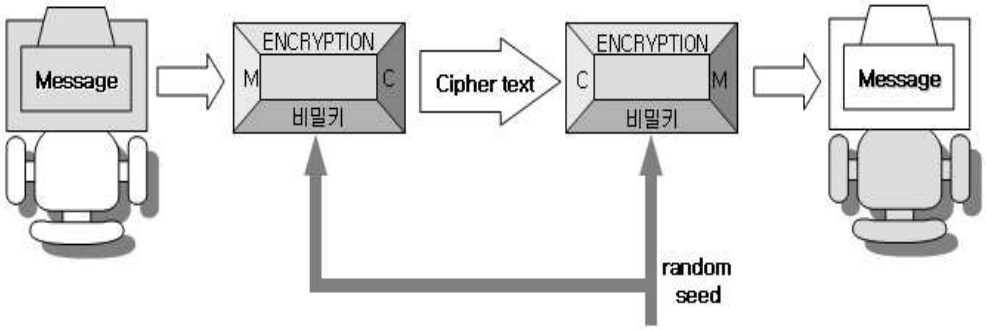
2. 암호키에 따른 암호화 기법

암호방식은 암호키의 사용 방법에 따라 비밀키 암호시스템(Sercret Key

Cryptosystem)과 공개키 암호시스템(Public Key Cryptosystem)으로 나눌 수 있다. 비밀키 암호 시스템은 공개키 암호 시스템이 나오기 전에 주로 사용되던 암호 방식이다. 그 뒤 이 방식의 키 관리 단점을 해결하고자 공개키 암호 시스템이 나오게 되었다.

a. 비밀키 암호 시스템

비밀키 암호 시스템은 대칭 암호 방식(Symmetric Cipher System)이라 부르는데 관용 암호 방식(Conventional Cryptosystem)또는 단일키 암호 시스템(One Key-Cryptosystem)으로도 불리며 암호화와 복호화에 같은 키를 사용하는 방식을 말한다. 송신자는 전송하고자 하는 평문(Plaintext)을 키(Key)와 암호 알고리즘을 통해 암호문(Ciphertext)으로 변환하고, 수신자에게 전송한다. 수신자는 동일한 키를 복호 알고리즘에 사용해서 원래의 평문을 만들어 내게 된다[16]. 이때, 송신자와 수신자는 암호화 통신을 하기전에 안전하게 키를 교환해야 하며, 암호 통신을 도청하려는 제 3자는 송신자와 수신자가 사용한 키가 없으면 원래의 평문을 알 수가 없게 된다. 비밀키 암호 시스템은 [그림 3]과 같이 나타낼 수 있다.



[그림 3] 비밀키 암호알고리즘의 암호화 방식

비밀키 암호 시스템의 보안성은 여러 가지 요소와 관련되지만 가장 중요한점은 안전하게 키를 보관하는 것이다. 즉, 암호화 통신을 하는 송·수신자는 자신들이 가지고 있는 키가 노출이 되지 않도록 비밀로 간직해야 하는데 이것은 암호화·복호화 알고리즘이 공개가 되더라도 키를 알지 못하면 암호문을 해독할 수가 없도록 설계가 되기 때문이다. 이와 같은 특징으로 인하여 암호화 통신을 하고자 하는 상대방이 많으면 그에 따라 관리해야하는 키의 수도증가하게 되며 키 관리상의 문제가 생기게 된다. 그러나 비밀키 암호 시스템은 많은 다양한 알고리즘(DES, IDEA, RC5, RC6 등)이 나와 있으며 암호화·복호화 속도가 공개키 암호 방식 보다 빠르기 때문에 현재에도 평문을 암호화하기 위해 많이 사용되고 있다[17].

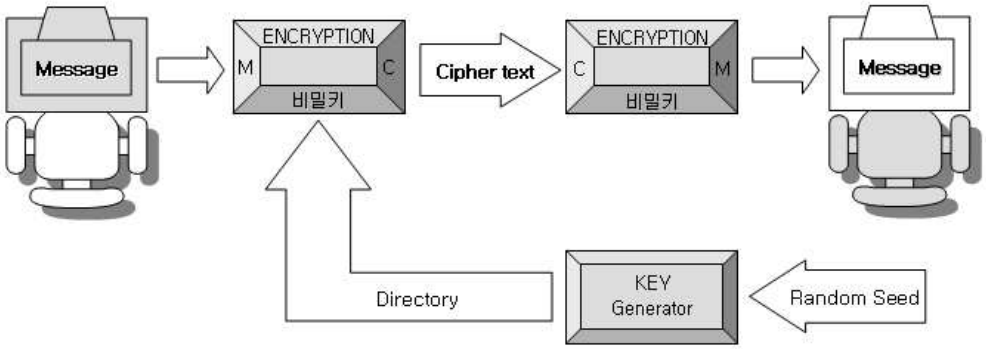
비밀키 암호 시스템은 다시 블록 암호(Block Cipher) 방식과 스트림 암호(Stream Cipher) 방식으로 나눌 수 있다. 블록 암호 방식은 평문을 블록 단위로 암호화시키는 것을 말하여 스트림 암호 방식은 주로 유럽에서 연구 발전된 성형 쉬프트 레지스터를 이용한 이진 수열 발생기를 사용하여 평문을 한 번에 1비트씩(또는 바이트 단위로) 암호화시키는 암호 시스템을 말한다. 블록 암호 방식에서 전형적인 블록 크기는 64bit를 이용하며 경우에 따라 보다 큰 블록을 사용하기도 한다. 그리고 같은 키를 사용하는 블록 암호에서 같은 평문 블록은 언제나 같은 암호문 블록으로 암호화된다. 스트림 암호에서는 주기가 긴 스트림으로 암호화되며, 다른 암호 시스템과 달리 비교적 레지스터의 주기성으로 인해 수학적 분석이 가능하여 여러 가지 중요한 수치에 대하여 이론적인 값을 정확히 계산할 수 있다. 또한 블록 암호 시스템은 쇄도(Avalanche) 효과 때문에 암호화 라운드 수가 증가함에 따라 평문과 키의 확산(Diffusion) 현상이 촉진되어 비도가 높아지는 반면 스트림 암호 시스템은 암호문에 오류가 생길 때 에러 전파 현상이 시스템 구조에 따라 달라진다.

b. 공개키 암호 시스템

공개키 암호 시스템은 비대칭키 암호 시스템(Asymmetric Cryptosystem)이라고

도 불리우며, 수학적 함수를 기반으로 하여 비밀키 암호 시스템과 달리 키 쌍이 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하며 다른 하나는 자신만이 비밀스럽게 보관하는 방식이다. 이때, 공개하는 키를 공개키(Public Key)라고 하며 비밀스럽게 보관하는 키를 개인기(Private Key)라고 한다[18][19].

이러한 방식을 사용함으로써 공개키 암호 시스템은 비밀키 암호 시스템의 키 관리와 분배의 문제점을 해결한다. 즉 n명의 사람들과 암호화 통신을 하기 위해서 비밀키 암호 시스템에서는 n(n-1)/2개의 키가 필요하지만, 공개키 암호 시스템에서는 각 사용자당 2개씩의 키만 필요하게 되므로 전체적으로 2n개의 키가 필요하게 된다. 그러나 이러한 장점 이외에 키 사이즈가 크다는 점과 2진수를 10진수로 변환하는 연산시간이 길다는 단점이 있으며 선택적 평문 공격에 대한 취약성을 가지고 있다. 공개키 암호 시스템은 [그림 4]와 같이 나타 낼 수 있다.



[그림 4] 공개키 암호알고리즘의 암호화 방식

공개키 암호를 이용해서 송신자와 수신자가 암호 통신을 하기 위해서는 다음과 같은 과정을 거친다. 먼저 송신자가 수신자의 공개키로 메시지를 암호화하여 전송하고 수신자는 자신의 개인키로 암호문을 복화화하여 평문을 얻는다. 네트워크 상에서 누군가 암호문을 얻더라도 개인키 없이 암호문을 복화화할 수 없으므로 안전

하게 데이터 전송이 가능하다. 개인키는 언제나 소유자만이 보관하고 있으며, 전송되거나 다른 사람에게 알려질 필요가 없기 때문이다.

이러한 속성은 또한 비밀키 암호 시스템에서 제공할 수 없는 디지털 서명 기능을 제공해준다. 디지털 서명은 송신자 MG가 평문을 자신의 개인키로 암호화한 암호문을 전송하고, 수신자가 암호문을 MG의 공개키로 복호화 함으로써 이루어진다. 이때 개인키를 알고 있는 사람은 오직 송신자 MG밖에 없기 때문에 MG의 공개키로 확인되는 서명을 한 사람이 MG라는 것을 확인할 수 있다. 이러한 과정은 디지털 데이터로 작성된 문서에 작성자나 송신자의 도장을 찍는 것과 마찬가지의 효과를 얻는다. 그러나 이러한 공개키 암호 시스템은 그 역사가 짧으며 현재 나와 있는 알고리즘도 그리 많은 편이 아니다. 또한 비밀키 암호 시스템보다도 데이터 암호화 속도가 매우 느리기 때문에 일반적으로 데이터 암호화에는 사용하지 않으며 키 분배나 디지털 서명 등에 많이 사용되는 편이다. 이러한 공개키 암호 시스템의 대표적은 것으로는 RSA 암호가 있으며 그 밖에 EIGamal, Schnorr, DSA, LUC, ECC 등이 있다[20][21].

다음의 [표 2]에서는 비밀키 암호알고리즘과 공개키 암호알고리즘의 차이점을 비교 하였다.

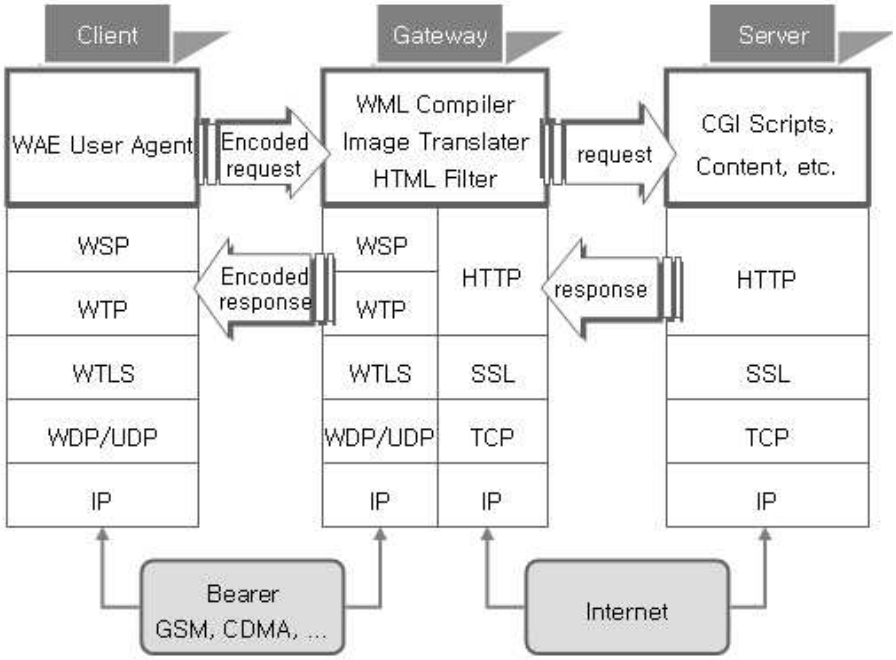
[표 2] 비밀키 암호알고리즘과 공개키 암호알고리즘의 비교

항목 \ 시스템	비밀키 암호 시스템		공개키 암호 시스템
원 리	암호화키 = 복호화키 (비 밀) (비 밀)		암호화키 = 복호화키 (공 개) (비 밀)
비밀키 분배(암호화)	필요		불필요
비밀키의 수 (암호화·복호화)	많다 (통신상대의 수)		적다 (자신의 암호화·복호화키)
안전한 인증	어렵다		쉽다
암호화 속도	빠르다		늦다
암호화 알고리즘	비밀	공개	공개
암호 시스템	Skipjack	DES, FEAL	Rsa, E1Gamal, ECC

3. WAP 보안기술

WAP구조는 무선 단말기를 위한 응용 프로그램 개발을 위해 [그림 5]에서 보는 바와 같이 확장 가능한 프로토콜 환경과 전체 네크워크의 계층화된 구조를 제공한다.

WAE(Wireless Application Environment)는 웹과 무선 단말기 기술의 통합을 기초로 한 일반 목적의 응용 환경이다. WAE의 주요 목적은 서비스 제공자가 효과적이고, 유용한 방법으로 방대한 다른 무선 플랫폼에 접근할 수 있는 응용과 서비스를 만들 수 있는 상호작용 환경을 구축하는 것이다. WAE는 다음의 기능을 포함하는 마이크로브라우저(MicroBrowser) 환경을 포함한다.



[그림 5] WAP 게이트웨이 모델

- WML(Wireless Markup Language) : HTML과 비슷하지만 무선 단말기를 사용하는데 있어 최적화된 경량의 마크업 언어이다.
- WMLScript : Javascript와 유사한 경량의 스크립트 언어이다.
- WTA(Wireless Telephony Application) : 전화 서비스
- WTA(Wireless Telephony Application Interface) : 전화 서비스를 위한 프로그래밍 인터페이스이다.
- 컨텐츠 형식 : 이미지, 전화번호 및 달력 정보를 포함한 데이터 형식을 말한다.

WSP(Wireless Session Protocol)는 두 개의 세션 서비스를 위한 일관된 인터페이스를 가진 WAP의 응용 계층 프로토콜을 제공한다. 첫째는 트랜잭션계층 프로토콜인 WTP(Wireless Transaction Protocol)위에서 동작하는 연결 지향형 서비스이

고, 두 번째는 보안 또는 비보안 데이터그램 서비스인 WDP(Wireless Datagram Protocol)위에서 동작하는 비연결형 서비스이다. WSP는 브라우징 응용인 WSP/B(Wireless Session Protocol-Browsing)에 적절한 서비스들로 구성된다. WSP군에 있는 프로토콜은 상대적으로 긴 지연을 가지고 있으며 낮은 대역폭을 가진 전송 네트워크를 위해 최적화 되어있다.

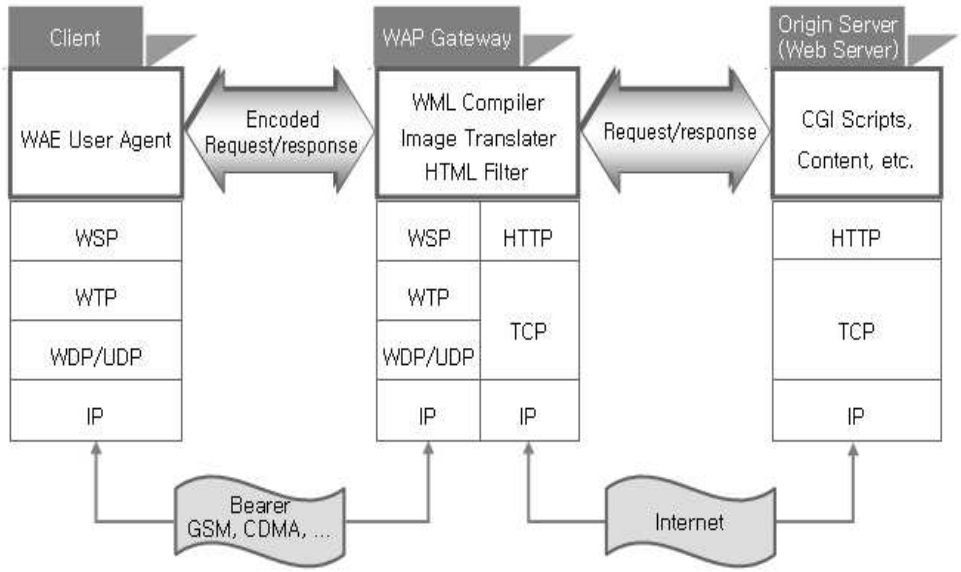
WSP/B는 WAP 프록시가 WSP/B 클라이언트로서 표준 HTTP서버에 연결 할 수 있도록 고안되어 있다. WSP는 현재 브라우징에 적절한 서비스들로 구성되어 있으며, WSP/B는 축소된 인코딩 속에서의 HTTP/1.1 기능, 영구적인 세션 상태 정보, 프로토콜 특징의 상호교환 등과 같은 기능을 제공한다. WTP(Wireless Transaction Protocol)는 데이터 그램 서비스의 상위에서 실행되고 인터넷 접속 전용 컴퓨터에서 실행하기에 적당한 간단한 트랜잭션 지향형 프로토콜이다. 이 WTP는 보안 또는 비보안 무선 데이터 네트워크상에서 모두 효율적으로 동작한다. 트랜잭션 서비스에 있는 3개의 클래스인 신뢰할 수 없는 단방향 요청, 신뢰할 수 있는 단방향 요청, 신뢰할 수 있는 양방향 요청, 응답 트랜잭션에 대해 WTP사용자는 자신이 받은 메시지의 확인을 위해 사용자간의 데이터를 교환함으로써 신뢰성을 유지한다. 또한 대역폭에서 벗어난 데이터가 들어올 때, 선택적으로 승인(Acknowledge)하는 기능, 전송한 메시지의 수를 감소시키기 위한 PDU(Protocol Date Unit)로의 연결과 비동기 트랜잭션을 수행한다. WTLS(Wireless Transport Layer Security)는 WAP 트랜스포트 프로토콜을 사용하며, 좁은 대역폭을 가진 통신 채널을 사용하도록 최적화 된다. WDP(Wireless Data Protocol) 계층은 다양한 네트워크 형태에 의해 지원되는 데이터를 운반하는 능력을 가진 전송 서비스 위에서 동작한다. 일반적인 전송 서비스로서, WDP는 WAP 상위 계층 프로토콜에 일관된 서비스를 제공하며, 이용 가능한 전송 서비스중의 하나를 가지고 통신한다. WDP 프로토콜이 상위 계층 프로토콜의 일반적인 인터페이스를 제공하기 때문에 보안, 세션 그리고 응용계층의 기초를 이루는 무선 네트워크 기능을 독립적으로 수행할 수 있다. WAP 보안은 유선의 SSL(Secure Socket Layer)에 대응하는 WTLS(Wireless Transport Layer Security)에서 담당한다. WTLS는 IETF의

TLS(Transport Layer Security)를 기반으로 무선환경에 적합하도록 개발된 보안 프로토콜 UDP/IP를 적용하고 단말의 성능을 고려하여 여러 가지 관련 파라미터의 길이를 줄였다. TLS를 기본으로 하지만 TLS가 서버 및 클라이언트 인증을 위하여 X.509 V3 인증서를 사용하는데 비해 WTLS는 인증서 규격을 X.509 V3 인증서, WTLS 인증서, ANSI X9.68 인증서로 정의한다. WTLS에서는 Mini Certificate 인증서와 Client/Server 인증서로 정의되어 있는 인증서를 용도에 맞게 사용하여 무결성, 부인방지 등을 제공한다. WTLS는 통신을 하는 두 응용 프로그램 사이에 안전한 채널을 형성하여 통신 내용의 보안을 보장하는 방법이다. WTP와 WDP 사이에서 수행되기 때문에 특정 응용 프로그램에 종속되지 않고, WAP을 사용하는 모든 응용 프로그램들을 지원한다. WTLS는 기밀성, 사용자 인증, 메시지 무결성 등의 보안 서비스를 제공하며, 부인 봉쇄는 제공하지 않는다. 여기서 두 응용간의 기밀성 서비스는 DES, IDEA등과 같은 관용 암호 방식을 사용하여 제공되며, 이 때 사용되는 비밀키는 Handshake 프로토콜을 통해 생성된다. 기밀성을 필요로하는 다수의 어플리케이션 각각에 대해 다양한 암호 알고리즘을 제공할 수 있다. 클라이언트와 서버의 상호 인증은 연결 성절 과정에서 서로간에 신뢰할 수 있도록 클라이언트와 서버가 서로에 대해 인증할 수 있도록 하는데, RSA와 같은 공개키 암호 방식과 X.509 인증서가 사용된다[22][23]. 서버의 인증서는 클라이언트가 신뢰할 수 있는 서버인지 확인하기 위해 사용되며, 반대로 서버는 신뢰할 만한 클라이언트인지 확인하기 위해 클라이언트에게 인증서를 요구할 수도 있다. 또한 메시지 무결성 서비스는 내부적으로 누군가 데이터 전송을 방해 할 수 없도록 하거나 재전송 공격에 이용할 수 없도록 데이터의 무결성을 제공하는데, 키를 사용하는 MAC(Message Authentication Code) 기법을 함께 이용하여 데이터 변조 여부를 확인할 수 있다. WTLS의 문제점은 WTLS로 보안 서비스를 제공할 때 웹서버가 SSL/TLS를 사용하므로 중간의 WAP 게이트웨이에서 암호화된 데이터를 복호화한 뒤 상대편의 프로토콜에 적합하게 다시 암호화하는 과정을 거치므로, 게이트웨이에서 데이터가 평문으로 존재하는 문제점이 발생한다. 단말기의 성능 문제로 Secret 파라미터와 Random Number의 바이트를 약 절반 정도로 축소하므로 빈도의 문제

점이 발생한다. 인증서의 경우 X.509 인증서의 기본필드에 해당하는 부분만 축소되어 있기 때문에 인증서 정책 등의 다양한 인증서 서비스를 제공하는데 어려움이 있다.

4. WML 전자서명

부인 방지는 전송되는 데이터에 대해서 전자서명을 수행함으로써 부인방지 서비스의 제공이 가능하다. 전송되는 모든 데이터에 대해서 전자서명을 수행하는 것은 많은 연산을 필요로 하므로 비효율적이다. 따라서 WTS에서의 부인 봉쇄 서비스는 어플리케이션 계층에서 제공하는데 이를 위해 WAP에서는 WML 전자서명 메커니즘을 제공한다. WMLScript는 JavaScript에 기반에서 설계된 WAP에서의 Script 언어인데, WMLScrip Crypto Library에서 제공하는 Crypto.signText()라는 함수를 이용하여 WML문서에 전자서명 하는 것이 가능하다. WMLScript를 이용한 전자서명은 [그림 6]과 같다.



[그림 6] WML을 이용한 전자서명

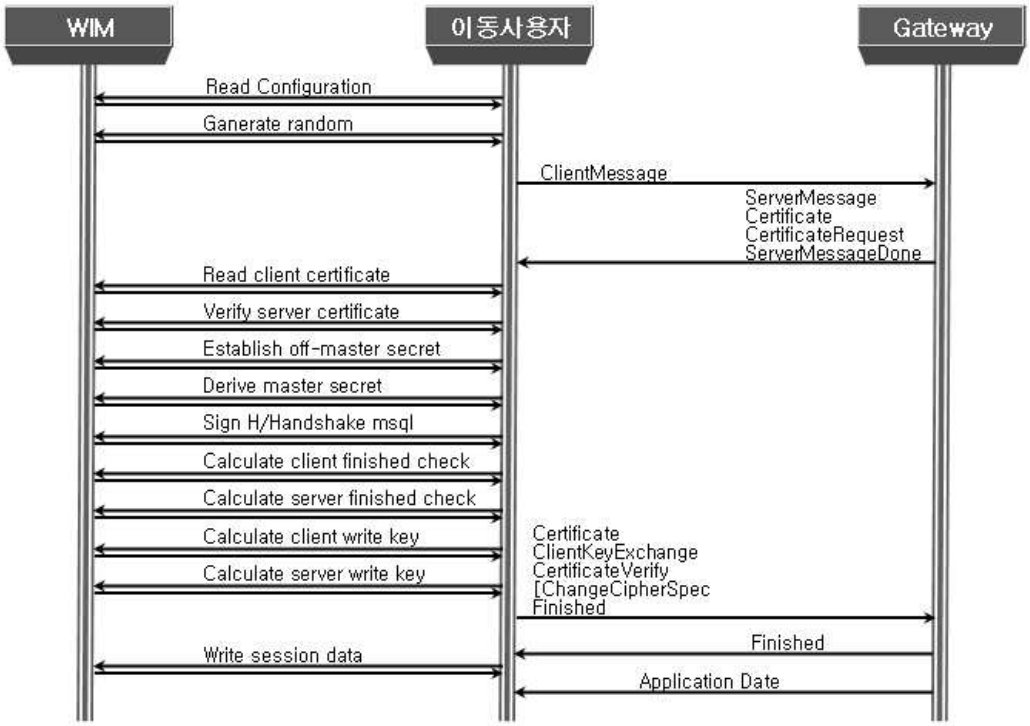
이러한 경우 WML문서 단위로 전자서명이 가능하기 때문에 사용자는 전자서명이 필요로 하는 중요한 문서에 대해서만 전자서명을 수행함으로써 전자서명의 수행 때문에 발생하는 부담을 최소화 할 수 있다. 또한 WTLS와 WMLScript에 의한 전자서명을 함께 운용함으로써 기밀성, 무결성, 사용자 인증, 부인 봉쇄 등 기본적인 정보보호 서비스를 모두 제공할 수 있다. 그러나 전자서명의 수행은 현재 단말기 성능 제한으로 인해 많은 시간이 소요되며, WMLScript에 의해서 생성된 전자서명된 데이터를 WAP 게이트웨이에서 인터넷에 적합한 형식으로 변화시켜야 하므로 보안상 허점이 발생할 수 있는 문제가 있다.

5. WIM(Wireless Identity Module)

전자서명이나 인증서 검증은 시간이 많이 소요되므로 현재 휴대 단말기로 공개키 연산을 단말기 내에서 수행하기는 매우 곤란하다. 또한 메모리의 제한으로 인해

서버의 인증서나 사용자의 인증서를 여러개 보관하는 것도 문제가 있으며, 단말기 분실시 인증서나 비밀키와 같은 중요 정보를 분실할 우려도 있어 안정성 면에서도 문제가 있다[24].

이와 같은 문제 해결을 위해 WTLS 와 WAL 사이의 보안을 담당하는 모듈인 WIM이라는 WAP에서 사용할 수 있는 스마트 카드의 규격과 단말기와 스마트카드 간의 인터페이스를 정의하고 있다. 이는 사용자 식별 및 인증을 위한 정보를 관리하며, WAP 동작에 필요한 센서티브 데이터 및 Authentication Key를 처리한다. WIM은 PKCS#15에 기반하여 설계되었으며, 스마트 카드에 저장되는 정보는 사용자의 비밀키, 인증서등으로 [그림 7]과 같이 인증서 검증, 전자서명 생성 등 많은 시간을 필요로 하는 연산을 스마트카드에서 수행함으로써 단말기의 부담을 덜 수 있다. 또한 비밀키, 인증서 등의 중요 정보를 스마트 카드에 저장함에 따라 안전성 또한 보다 향상된다.



[그림 7] WIM을 이용한 WTLS Handshake

6. 종단간 보안(End-to-End Security)

현재 WTLS을 이용한 보안 솔루션이 갖고 있는 가장 큰 문제는 종단간 보안 문제이다. 무선 네트워크에서는 WTLS를 이용하여 정보 보호 서비스를 제공하고, 유선 네트워크에서는 SSL또는 TLS를 통해 정보 보호 서비스를 제공하게 되는데, 이때 종단간 보안 문제가 발생한다. 즉, 보안 서비스를 운영할 경우에 WAP게이트웨이는 WTLS로 보호되는 데이터를 SSL에 적합하게 변환하거나, SSL로 보호되는 데이터를 WTLS에 적합하게 변환하는 역할을 수행한다.

WAP게이트웨이는 WTLS나 SSL로 보호되는 데이터를 복호화하는 작업을 수행해야하며, 이과정에서 본래 데이터(평문)의 내용을 알 수 있다. 이러한 경우, WAP

게이트웨이 관리자가 불법적으로 사용자의 정보를 사용할 수 있기 때문에 큰 문제가 된다.

현재 종단간 보안 서비스를 제공할 수 있는 방안은 다음과 같은 3가지가 있다.

a. SSL이용

유·무선 전구간에서 SSL을 이용하여 정보보호 서비스를 제공하는 방법이다. 이때 게이트웨이는 무선 네트워크 구간과 유선 네트워크 구간의 중계 역할만을 담당하여, 클라이언트와 웹 서버의 통신에 개입하지 않는다. 따라서 클라이언트와 웹서버 간의 종단간 보안이 가능하며, 클라이언트와 웹서버는 기존 유선인터넷에서와 동일하게 SSL을 통한 정보보호 서비스를 제공받을 수 있다. 또한 정보보호 서비스를 위해서 특별한 수정이 필요하지 않기 때문에 기본에 구축되어 있는 시스템을 그대로 사용할 수 있다는 장점이 있다. 그러나 이 방법의 원활한 운용을 위해서는 단말기에서 SSL을 효율적으로 처리할 수 있는 방법을 개발하는 것이 무엇보다 중요하다. 특히 많은 양의 연산을 필요로 하는 공개키 쌍 생성이나 인증서 관리 등의 처리는 매우 곤란하다고 할 수 있다.

b. Secure WAP 게이트웨이 이용

이는 WAP포럼에서 제안하고 있는 방법으로 종단간 보안 서비스 제공을 위해서 웹서버 바로 앞 단에 또 하나의 WAP게이트웨이를 설치하며, 이 때 Secure WAP 게이트웨이와 웹 서버 사이의 구간은 안전한 것으로 가정한다. 이와 같이 구성함으로써 WAP게이트웨이는 단순히 무선 구간과 유선 구간 사이의 중계 역할만을 담당하여 WTLS와 SSL간의 변환 과정이 필요하지 않게 된다. 따라서 WAP게이트웨이는 클라이언트와 웹 서버 간의 통신 내용을 알 수 없다. 그러나 이와 같은 방법은 인터넷 상에서 서비스를 제공하려는 웹 서버 측에서 추가적으로 Secure WAP

게이트웨이를 설치해야 한다는 부담이 있다. 또한 Secure WAP 게이트웨이와 웹 서버간의 구간을 안전하다고 가정하더라도, 이 부분이 내부 또는 외부의 공격으로부터 노출되어 있다는 문제가 있다.

c. 응용프로그램 이용

정보보호 서비스와 관련된 모든 작업을 응용 프로그램 레벨에서 처리하는 방법이다. 즉, 클라이언트와 웹 서버는 정보보호 서비스를 위한 전용 프로그램을 설치하고 이를 통해서 통신함으로써 종단간 보안 서비스를 제공 받는다. 즉 WAP 게이트웨이는 단순히 유선 구간과 무선 구간사이의 중계 역할만을 수행하여 통신 내용을 알지 못하므로 안전성이 높다. 이 방법 역시 단말기의 성능이 문제가 되지만, 기존의 표준 규격을 따르는 것이 아니고, 새로운 프로그램을 개발하는 것이기 때문에 최적화의 여지가 많으며, 응용분야에 적합하게 프로그램의 수정이 가능하다는 장점이 있다.

7. 무선 *PKI*

무선 인터넷 환경에서 사용하는 전화, 이동장치 등에서 빠른 처리속도를 보이지 못하는 기존의 암호화 기법의 단점을 없애고자 ECC(Elliptic Curve Cryptography)라는 새로운 공개키 암호 알고리즘이 대두되고 있다. 이는 RSA와 같은 기능을 수행할 수 있으며 적은 CPU 리소스만을 요구하며 통신하거나 저장하는 데에 적은 데이터 용량이 사용된다[25].

a. 가입자 전자 서명키 생성

인증서를 생성하기 위해서는 키 쌍의 생성이 필수적이다. 이 때 키를 생성하는

방법으로 주로 사용되는 것으로 가입자가 직접 생성하는 방법과 인증기관이 생성하는 방법이 있다. 가입자가 생성하는 경우에는 계산 능력이 떨어지기 때문에 키 생성을 위하여 많은 시간이 소모된다. 대개의 경우 한 번 생성하고 나서 장기간 사용하는 경우에는 문제되지 않지만 단말기 사용자에 대한 인증서가 빈번하게 변경되는 경우에는 고려되어야 할 문제이다. 또한 인증기관이 키쌍을 생성하는 경우에 서버가 장기간 동안 인증서를 사용하면 문제가 없지만 빈번한 인증서 갱신이 필요한 경우에는 역시 적합하지 않다.

단말기의 경우에서는 인증기관이 생성한 키를 단말기에 설치하는 방법이 별도로 마련되어 있어야 하며 이러한 방법은 충분히 안전한 채널을 통해서 이루어져야 한다. 현재 RSA의 경우에 대해서는 자체연산이 가능한 스마트카드가 나와 있는 상태이며 이것을 단말기에 스마트카드 슬롯을 설치하거나 칩을 부착하여 카드내에서 키생성 및 관련 연산을 수행할 수 있도록 하는 방법이 실용화 단계에 접어들고 있다[26].

b. 알고리즘

기본적으로 무선 인터넷 PKI에서는 단말기의 계산능력이 떨어진다는 제약을 가지고 있으며 이에 따라 많은 사항에 대하여 제한하게 된다. 알고리즘도 역시 이러한 영향을 받게 되는데, 전자서명 등의 기능을 수행할 때 사용되는 알고리즘은 계산량 및 구현가능성 측면을 고려하여 사용되어야 한다.

전자서명 알고리즘은 대부분의 경우 RSA를 사용하고 있고 키분배를 위해 Diffie-Hellman 방식에 ECC의 사용을 제시하고 있는 상황이다. 현재 유선 PKI체계에서는 일반적으로 RSA 와 DSA를 사용하고 있다.

c. 인증서 규격

WTLS 서비스 제공을 위하여 VeriSign과 Entrust.net에서 WAP 서버를 위한 인

증서를 판매하고 있다. 이 인증서들은 인증서 상태검증 서비스를 제공하고 있지 않으며 특히 VeriSign의 경우 CRL확인 대신 CRL갱신 주기 보다 짧은 25시간용 인증서로 대체하고 있다.

ITU-T X.509(1997)표준은 인증서 및 인증서 효력정지 및 폐지목록에 대한 별도의 프로파일을 정의하고 있다. 인증서와 인증서 효력정지 및 폐지목록은 ASN.1 BER/DER 코딩 방식을 사용하므로 대략 800KB정도의 크기를 가진다. 그러나, 무선 인터넷 PKI에서는 무선 인터넷의 특성상 인증서의 크기를 최소화하여야 하므로 인증서 규격, 프로파일, 코딩 방식 등을 기존의 방식과를 달리하여 사용한다. 최종적으로 인증서의 크기를 줄여 대부분 200KB ~ 400KB 정도의 크기를 유지하게 된다[27].

d. 인증서 요청 방식

현재 PKI 체계에서는 사용자가 전자서명용 키 쌍을 생성하여 인증기관에게 인증서를 요청하게 되는데, 이 경우 사용자는 인증 요청서를 생성하여 인증기관에게 온라인 및 오프라인으로 제출하게 된다. 인증서 요청 방식은 사용자 신원 확인 방법 및 가입자 키 생성 방식과 밀접한 관계가 있으며 이러한 절차 및 방법은 가입자의 공개키가 안전하게 전달될 수 있도록 고려하여 개발되어야 한다.

e. 인증서 상태검증 방식

인증서의 유효성을 확인하기 위하여 인증서의 상태를 확인하는 것은 인증서의 신뢰성을 보장하게 되며 이를 위하여 X.509에서는 CRL 및 CRL분배점을 사용하는 방법을 제시하고 있다[28]. 하지만 해당 인증서에 대한 실시간 확인이 어렵다는 점과 CRL의 크기에 따라 전송 시간이 길어질 수 있다는 점이 문제점으로 제시되고 있다.

무선 인터넷 PKI경우에 있어서 이러한 문제점은 무선의 특성상 매우 중요한 부분으로 작용되고 있으며 특히 단말기에서 CRL을 처리하기 위해서는 처리시간 및 계산능력, 사용자 대기시간 등에 대해 불리하게 작용하기 때문에 기피하고 있는 상황이다.

f. 인증서 공고 방식

인증기관은 인증서를 사용하는 시스템 및 신뢰당사자들이 인증 경로 획득 및 인증서 검증을 수행할 수 있도록 발급한 인증서들을 공개하고 관리하여야 하며 이러한 인증서 공고 방식은 사용자가 인증서를 획득하는 방법을 결정하게 된다.

무선 인터넷 PKI에서도 마찬가지로 인증서 공고 방식을 확보하고 있어야 한다. 서버의 경우에는 인증서를 검색하고 획득하는데 어려움이 없지만 단말기의 경우에는 디렉토리에 접근하기 위한 기능이 설치되어야 한다. 인증서 공고 방식을 다른 메커니즘으로 사용하기 위해서는 단말기에서의 인증서 전송, 설치, 관리 방식이 고려되어야 한다.

g. 인증서 유효기간

인증서의 유효기간을 설정하는 것은 인증 서비스를 제공하는 인증기관의 정책적 고려사항이지만 인증서의 유효기간에 따라 인증서 상태확인 방법 및 인증서 공고 방식 등이 달라지므로 이에 대한 고려가 필요하다.

Ⅲ. *Mobile-IP*에서의 기존 인증 방식 고찰

A. Mobile-IP

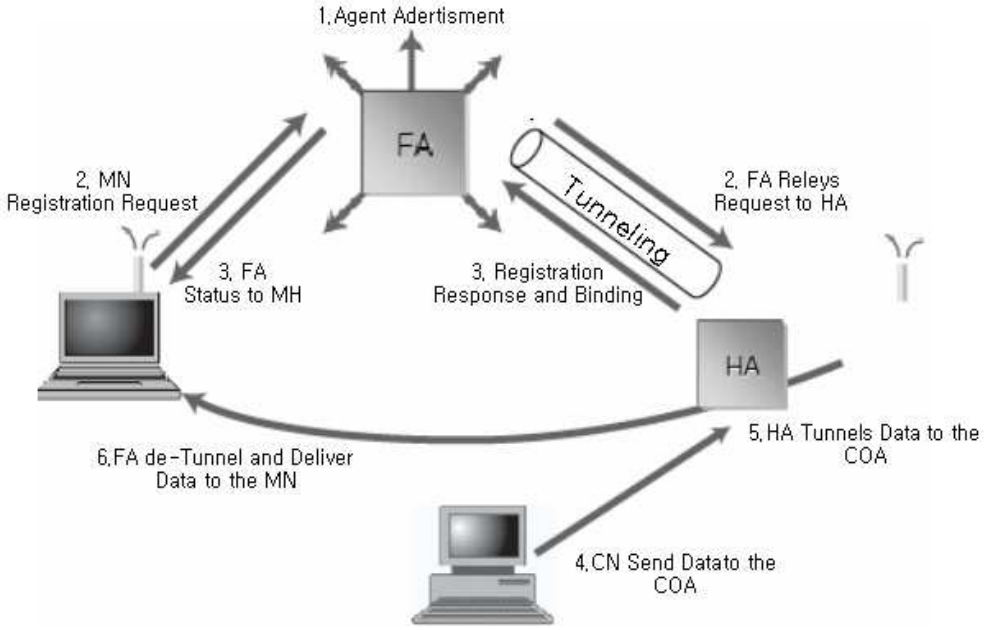
*1. Mobile-Ip*의 정의

초기에는 각 사무실이나 학교에서 사용하고 있는 컴퓨터의 위치가 고정되어 있다는 가정하에 유선을 이용한 인터넷 연결을 하였으나 점점 많은 사용자의 컴퓨터의 위치가 고정되어 있지 않은 상태에서 네트워크 연결을 하게 되었다. 현재에도 이미 노트북에 무선랜 카드를 사용하여 포터블 형태의 이동성을 제공 받고 있으며 그 수요는 점점 늘어나고 있다.

이동 통신 단말의 경우 일정한 기지국에서 다른 기지국으로 이동할 경우 인터넷 접속을 계속 유지, 사용할 수 없게된다. 그 이유는 기존의 인터넷 라우팅 프로토콜은 일종의 PPP (Point to Point Protocol) 이기 때문에 호스트가 다른 네트워크로 바뀔 경우 호스트의 새로운 위치로 데이터를 계속 전달할 수 없기 때문이다. 이와 같은 문제를 해결하기 위한 것이 Mobile-IP의 개념이다. 현재 제공되고 있는 무선 인터넷 서비스는 교환기가 IP를 가지고 있는데 비하여 Mobile-IP의 경우, 기지국과 단말기가 IP를 가지게 된다. 이처럼 Mobile-IP는 네트워크 주소 기반의 IP 경로 설정에서 기인하는 호스트의 서브넷 사이 이동 제한을 극복하기 위하여 고안되었다.

IP에서 이동성을 제공하는 방법으로 IETF에서는 1992년 Mobile-IP 워킹그룹을 결성하여 접속되는 위치가 반드시 고정적으로 지정되어 있던 기존 IP 프로토콜에 단말기의 이동성을 제공하는 Mobile-IP를 제안하였다[29]. Mobile-IP 프로토콜은 IETF의 RFC2002에 기술되어 있으며, 이동 노드가 인터넷에서 연결지점을 바꾸는 동안에도 이동 노드와 통신 노드 사이에 IP 데이터그램을 전달하도록 하는 프로토콜이다[30].

2. Mobile-IP의 관련용어



[그림 8] Mobile-IP의 동작 구조

a. 이동노드(Mobile Node : MN)

Mobile-IP망에서 자신의 IP주소 변경없이 다른 서브 네트워크로 연결점을 변경시키는 이동 호스트나 라우터로 항상 홈 주소를 가지고 있으면서 홈 네트워크를 벗어나면 에이전트 인식을 통해 움직임을 판단하고, 외부 에이전트 임시 주소(COA)를 사용하여 홈 에이전트(HA)에 등록하고, 그 COA 터널을 통하여 HA와 통신한다[31].

b. 홈 네트워크*(Home Network)*

외부 네트워크와 접속되어 있으며 이동 노드는 홈 네트워크에 처음 연결을 시작하며 여기서 고정된 IP 주소를 받는다.

c. 외부 네트워크*(Foreign Network)*

이동 노드가 이동하여 방문한 다른 네트워크나 서브 네트워크로 여기서 임시 IP 주소를 부여 받는다.

d. 고정 *IP* 주소

이동 노드가 처음으로 연결을 시작한 홈 네트워크에서 받은 주소로 이동 노드와 통신하고자 하는 송신자가 목적지 주소로 이용하는 고정된 IP 주소이다.

e. COA(Care-of-Address)

이동 노드가 홈 네트워크를 떠나 외부 에이전트에 등록시 얻는 새로운 주소로 이동 노드에 전송되는 데이터그램에 대한 터널의 종단점 역할을 한다. 이동 노드는 자신의 홈 네트워크에서 부여 받은 고정 IP 주소를 가지고 있으며, 멀리 이동하였을 때에는 새로 연결된 네트워크에서 임시 COA를 얻는다.

f. 홈 에이전트*(Home Agent: HA)*

이동 노드의 홈 네트워크 라우터로 이동 노드에 대한 현재 위치 정보를 유지하면서 이동 노드가 홈 네트워크를 떠날 때 임시 주소(COA)를 홈 에이전트에 등록

함으로써 이동 노드의 현재의 위치 정보를 유지시며 주고, 이동 노느가 다른 서브네트워크에서 자신이 속한 서브넷으로 통신할 수 있도록 이동 노드로 향하는 데이터그램을 전송해 준다.

g. 외부 에이전트*(Foreign Agent: FA)*

이동 노드가 위치 이동을 하여 방문하는 네트워크에 위치하는 라우터로 이동 노드가 멀리 떨어져 있는 동안 홈 에이전트와 접속하여 이동 노드에 데이터그램을 전송 한다.

h. 에이전트 광고*(Agent Advertisement)*

외부 에이전트는 라우터 광고 메시지에 특별한 광고 메시지를 붙인 메시지를 통해 자신의 존재를 알린다.

i. 통신 노드*(Correspondent Node: CN)*

이동 노드가 통신하는 상대로 이동하는 노드이거나 위치가 고정된 노드이다.

j. 이동성 결합*(Mobility binding)*

홈 에이전트에 있는 주소와 COA를 결합시키는 과정을 의미한다.

k. 터널*(Tunnel)*

이동 노드가 홈 네트워크를 떠났을 때 이동 노드로 향하는 데이터그램을 보내기

위해서 홈 에이전트와 외부 에이전트 사이에 생성되는 길로서, 이 때 데이터그램은 인캡슐레이트되어 터널을 따라 전송된 후 외부 에이전트에서 디캡슐레이트되어 최종 이동 노드로 전송 된다.

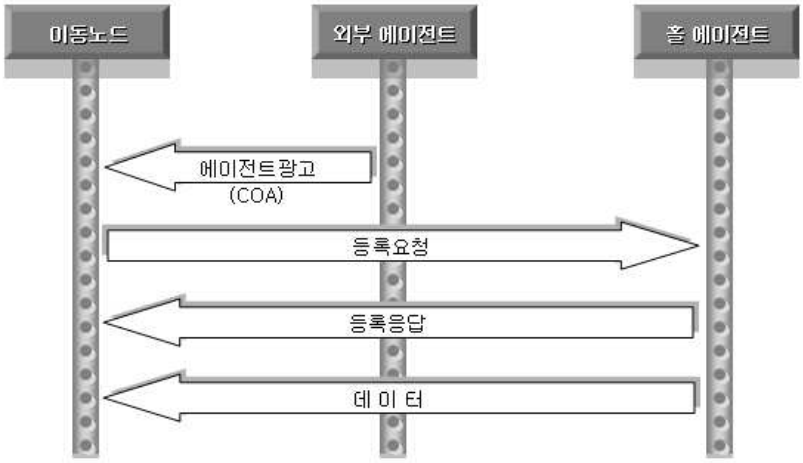
*3. Mobile-IP*의 동작 구조

Mobile-IP는 네트워크 주소 부분이 다를 경우 발생하는 서브넷 간의 이동에 대한 경로 배정 문제를 이동성 바인딩 리스트라는 외부 서브넷 주소를 포함하는 호스트 기반의 경로 배정 엔트리를 유지함으로써 해결하고 있다.

바인딩 리스트의 생성 절차는 호스트가 이동하게 되면 해당 서브넷의 외부 에이전트는 호스트의 홈 네트워크에 있는 홈 에이전트에게 Mobile-IP 등록 요구 메시지를 전송한다. 홈 에이전트는 메시지를 수신하여 현재 이동 호스트의 위치로 패킷 전송이 가능한 IP 주소를 포함하는 이동성 바인딩 리스트를 생성하게 되고, 이와 동시에 Mobile-IP 등록 응답 메시지를 외부 에이전트에게 전송하게 된다. Mobile-IP 등록 응답 메시지를 수신한 외부 에이전트는 호스트에 대한 정보인 방문자 리스트를 생성하게 된다. 이후 이동하는 호스트에게 전송될 패킷은 네트워크 주소 기반의 경로 배정으로 인해 홈 에이전트를 경유한다. 홈 에이전트는 이동성 바인딩 리스트를 검색하여 목적지 호스트가 위치한 외부 에이전트를 찾아내고 본래의 패킷에 외부 에이전트로 경로 배정이 가능한 주소인 의탁 주소를 목적지 주소로 하는 IP 헤더를 추가로 캡슐화하여 전송한다. 캡슐화된 패킷의 목적지인 외부 에이전트는 패킷을 수신하고, 캡슐화된 IP 헤더를 제거함과 동시에 이동성 바인딩 리스트인 방문자 리스트를 검색하여 해당 노드에게 전송한다[31][32].

Mobile-IP에서는 두개의 IP 주소를 이용하는데, 먼저 이동 노드는 처음 연결을 시작한 홈 네트워크에서 고정 IP 주소를 할당 받고 외부 네트워크로 이동함에 따라 외부 네트워크에 위치하는 외부 에이전트로부터 COA라는 임시 IP 주소를 할당

받는다. Mobile-IP는 이 두개의 IP 주소가 결합되어 사용되며, 데이터가 전송되는 과정은 통신 노드가 홈 네트워크에 의해 제공되는 고정 IP 주소로 데이터를 보내면 홈 네트워크에 위치한 라우터가 이 데이터를 외부 네트워크의 임시 IP 주소로 재전송해주는 과정으로 이루어진다[33][34].



[그림 9] Mobile-IP 등록 과정

위의 [그림 9]는 이동 노드의 위치 이동시 이동 노드로부터 홈 에이전트로의 새로운 위치 정보를 등록하는 과정이다. 이 과정은 에이전트 광고, 등록 요청, 등록 대답의 3가지로 구성된다.

첫 번째는 외부 에이전트로부터 에이전트 광고를 통하여 이동 노드로 COA를 보낸다. 이동 노드에서는 COA를 받아 이 메시지에 대하여 어디로부터 온 것인지를 결정한다. 즉, 홈 네트워크에서 온 것인지 외부 네트워크로부터 온 것인지 결정하여, 홈 네트워크에서 온 것이 아니라 외부 네트워크에서 온 것이면 에이전트 광고에 들어있는 COA를 새로운 임시 IP 주소로 부여 받는다. 두 번째는 이동 노드에서는 외부 에이전트로부터 부여 받은 새로운 COA를 홈 에이전트로 등록하기 위하여 홈 에이전트로 등록 요청을 한다. 마지막으로 홈 에이전트에서는 이동 노드의

등록 요청에 대한 결과로 등록 대답을 이동 노드에게로 보낸다. 그 결과 이동 노드는 등록 대답을 받게 된다. 이와 같은 등록 과정을 마치게 되면 이동 노드는 데이터그램을 주고 받을 수 있게 된다.

이동 노드는 처음 연결을 시작하여 홈 네트워크의 홈 에이전트로부터 할당 받은 고정 IP 주소와 COA를 결합시켜 Registration Lifetime이 끝날 때까지 홈 에이전트에 보관하게 된다. 이동 노드와의 데이터 전송을 시도하는 다른 노드는 이동 노드가 홈 네트워크에서 떠나간 것을 모르는 상태이므로 데이터그램을 고정 IP 주소로 보내게 되고 홈 에이전트는 전송된 데이터그램을 가로채 임시 COA로 터널링 한다.

이와 같이 다른 노드로부터 전송되는 모든 데이터가 홈 네트워크로부터 이동 노드가 새로 이동한 외부 네트워크로 재전송되는데 만약 이동 노드가 아닌 다른 사용자가 다른 COA를 가지고 등록 시도를 하여 다른 COA를 홈 네이전트의 라우팅 테이블에 잘못 등록을 하게 되면 보안에 큰 문제가 발생한다. 그러므로 이동 노드의 새로운 위치 정보를 홈 네트워크에 등록하는 과정에서의 인증은 매우 중요한 부분이다. 따라서 홈 에이전트에서는 정상적인 이동 노드로부터 등록 메시지가 왔다는 확인을 하여야 한다. 이동 노드의 인증에 관한 기존의 메커니즘으로는 비밀키를 기반으로 한 인증 메커니즘과 공개키를 기반으로 한 인증 메커니즘이 대표적이며 여기에서는 공개키를 최소로 사용하는 인증 메커니즘까지 살펴 보겠다.

B. 기존 인증메커니즘 고찰

1. 비밀키 기반 인증 메커니즘

a. 기밀성

비밀키를 공유하는 사람들만 공유하는 비밀키로 암호화한 파일을 복호화할 수

있다는 것에 대한 보증이다. 강력한 암호는 컴퓨터 디스크에 저장된 암호화된 파일들의 무결성을 확신하게 해야 한다. 비밀키를 공유한 사람들만이 암호화된 메시지를 복호화해서 그 평문의 내용을 이해할 수 있어야 하기 때문이다. 그러나 기밀성만으로는 통신 보안을 확신하기에는 부족하다. 그런 보안을 확신하기 위해선 다른 컴퓨터로 암호화된 데이터를 보내거나 다른 컴퓨터에서 데이터를 받기 전에 수신자와 의사소통을 하고 있는 상대방이 자신이 주장하는 바로 그 사람이라는 것을 확인하는 인증이 필요하다. 또한 다운로드받은 소프트웨어가 받는 도중에 변경되지 않았다는 것을 확인하는 무결성도 필요하다. 또한 통신에 대한 부인을 할 수 없다는 것을 확신할 수 있는 부인방지를 원한다[35].

b. 인증

상대방의 신원에 대한 보증이다. 인증은 제3자가 자신과 교신하는 상대방이 척하는 것을 막는다. 인증 공격(Authentication Attack) 이란 해커가 신청과 응답을 엿듣고 기록하고 있다면 해커는 통신자로 가장할 수 있다는 것이다. 왜냐하면, 해커는 통신자들 사이의 공유 비밀키가 A를 B로 암호화한 것을 알기 때문이다. 즉 해커는 송신자의 답변 요구가 수신자에게 도착하기 전에 그것을 가로챈다. 해커는 이전에 기록한 응답을 사용하고 정확하게 송신자에게 응답을 한다. 송신자는 수신자의 응답으로 알 것이다. 그러므로 좋은 암호 시스템은 1과 매우 큰 숫자 사이에 있는 답변 요구를 선택한다. 좋은 암호 시스템은 가능한 한 알아내기 어려운 패턴을 가진 난수 생성기를 사용한다.

의사 난수(Pseudo-Random Number)란 일반적으로 매번 사용할 때마다 새로 뽑는 것이 아니라 가장 랜덤하게 수를 뽑아서 테이블에 넣어두고 그 값을 난수를 사용할 때마다 뽑아서 쓰는 방식으로 되어 있다. 이 때문에, 테이블이 어디에서 시작하는지 알 수 있으면 아주 쉽게 다음 난수를 알아낼 수가 있게 되는 것이다. 이로 인해, 프로그램시에는 시간이라는 개념을 투입하여 매번 시간에 따라 다른 난수가 채택될 수 있도록 설정하는 방법을 사용한다.

c. 무결성

메시지 인증은 파일이 전송도중에 변경되지 않았다는 것에 대한 보증이다. 즉, 무결성이라는 개념은 메시지가 노출되지 않고는 어느 누구도 송신자의 메시지를 변경할 수 없다는 것을 보증하는 것이다. 그러므로 인증과 무결성은 매우 관련이 깊다.

송신자와 수신자는 그들의 키를 사용하고 MAC(Message Authentication Code)로 알려진 메시지에 지문(Fingerprint)을 넣음으로써 무결성을 확인한다. 메시지와 메시지 지문은 매우 밀접한 관계가 있다. 어느 누구도 쉽게 메시지 지문(Message Fingerprint)과 똑같은 또 다른 메시지를 찾아낼 수 없다. 비밀키 암호 시스템을 사용하기 때문에, 송신자와 수신자가 공유하는 비밀키가 메시지 지문을 보증하기 때문에 위조 메시지 지문이 아니라는 것을 알 수 있다. 만약 지문을 찾아냈을 지라도 메시지 지문의 장식이 메시지의 한 문자만 바뀌어도 메시지 지문의 약 반정도가 바뀌는 방식이기 때문에 역시 문제가 없다.

메시지에 어떠한 변화가 메시지의 전자 지문을 변화시키게 된다. 예를 들어, 만약 $10.00이 $10.01로 바뀌었다면, 그것은 완전히 다른 메시지 인증 코드(MAC)를 만들어낸다. 이것을 쇄도 효과(Avalanche Effect)라고 하는데, 이것은 암호 해독가가 성공적인 위조 메시지를 만들었을 때, 그 위조 메시지는 전혀 쓸모 없는 메시지가 된다는 것을 의미한다. 비밀키 암호화 방법과 마찬가지로 MAC의 방식도 비밀이 아니고 공개적으로 알려진다.

d. MAC

메시지 무결성을 보증하기 위해 MAC를 사용한다.

송신자가 비밀키와 메시지로 MAC을 만든다. 메시지와 MAC 두가지 모두를 수신자에게 보낸다. 수신자는 그 메시지를 사용하고, 송신자와 공유한 비밀키로 송신

자에게서 받은 MAC가 아닌 또 다른 메시지 지문을 계산한다. 만약, 수신자가 독립적으로 만들어낸 메시지 지문이 송신자에게서 받은 것과 동일하다면, 송신자는 메시지가 전달과정에서 변경되지 않았다는 것을 확신할 수 있다.

MAC를 이용하면 메시지 전송 중에 수신자의 변경 여부를 확인할 수 있으며, 메시지가 순서 번호를 갖고 있다면, 올바른 순서로 도착하는지도 확인이 가능하다. MAC는 인증 교환 메커니즘의 제 3자의 공격으로부터 메시지를 보호할 수는 있으나 통신 당사자들이 거짓메시지를 만들거나 메시지 발신 사실을 부인하는 행위에는 효과적으로 대처할 수 없다. 이러한 통신 당사자들의 부정한 행위를 방어하는 수단으로 전자 서명이 사용된다.

MAC은 전자 서명과는 다르게, 의도한 수신자만이 확인할 수 있도록 같은 키를 가지고 하도록 계산된다. MAC은 절대적으로 안전한 해쉬 함수 기반, 스트림 암호 기반, 블록 암호 기반으로 분류될 수 있다. Simmons와 Stinsom은 원타임 패드를 가지고 암호화하는 기반의 절대적으로 안전한 MAC를 제안하였다. 누구도 원타임 패드에 접근할 수 없듯이, 메시지의 암호문은 이것 자체로 인증되지만 메시지에 몇 가지 잉여물을 가진다. 절대적으로 안전한 MAC는 원타임 비밀키를 사용함으로써 얻을 수 있으며 해쉬 함수 기반 MAC는 메시지에 추가하는 검사합을 만들기 위해서 키나 해쉬 함수와 결합한 키를 사용한다. 예를 들어, 키가 있는 MD5 메시지 인증 방법이 있는데 Lai, Rueppel, Woolven은 스트림 암호 기반 MAC를 제안하였다. 이 알고리즘에서 입증할 수 있는 안전한 스트림 암호는 두 개의 작은 스트림으로 메시지를 나누는데 사용되거나 각 스트림은 LFSR에 넣어준다. 검사합은 두 개의 LFSR의 마지막 상태이다. MACs는 블록 암호로부터 나올 수도 있다. DEC-CBS MAC는 미국과 국제 표준으로 넓게 사용된다. 기본 아이디어는 DEC-CBC를 이용하여 메시지 블록을 암호화하고, 암호문에서 검사합처럼 마지막 블록을 출력한다.

MAC(Message Authentication Code)를 사용하는데 있어서 문제점은 첫째, 소프트웨어 업데이트가 몇 메가 바이트일 수도 있고 또 비밀로 할 필요가 없기 때문이며 그것을 암호화하고 복호화하는데는 시간이 필요하다. 그에 비해 MAC는 대부분 보낼 메시지의 크기와 비교하면 너무 작다.

둘째, 비밀키 기밀성만으로는 메시지의 무결성을 확신할 수 있다는 것은 잘못된 개념이다. 암호화는 해커가 메시지를 변경하는 것을 막지 못하므로 메시지 지문은 기밀성만큼 중요하고 항상 메시지들과 함께 보내져야 한다.

e. 부인방지

메시지를 보내는 사람이 파일을 보내지 않고도 파일을 보냈다고 부인할 수 없다는 것에 대한 보증이다. 부인방지는 비밀키만으로는 할 수 없으며 제 3의 단체나 공개키 암호화 방법을 사용해야 한다.

Mobile-IP에서는 인증과 제어 메시지의 무결성을 보장하기 위하여 MAC를 의무로 한다. 등록 요청을 안전하게 전송하기 위하여 각 메시지에 유일한 데이터를 포함시킴으로써 다른 등록 요청이 같은 해쉬값을 가지지 못하도록 한다. 이동 노드는 홈 에이전트와 미리 나누어 가진 비밀키를 가지고 등록 요청에 대해 MD5(Message Digest 5) 해쉬 함수를 수행하여 다이제스트 메시지를 얻어 요청에 덧붙여 전달하면 홈 에이전트는 같은 비밀키를 이용하여 전달받은 등록 요청에 대해 해쉬 함수를 수행하여 덧붙어온 내용과 일치하는지 확인한다[36][37]. 이와 같은 과정으로 이동 노드는 홈 에이전트에게 인증을 받으며 홈 에이전트에서 이동 노드로 보내는 등록 대답의 경우에도 같은 방법으로 인증 받는다.

또한 재공격(Replay Attack)을 막기 위해서는 이동 노드와 홈 에이전트 사이에 난수를 발생시켜 주고 받거나 타임스탬프(Timestamp)를 이용하여 제한된 시간 내에만 사용할 수 있도록 한다. 이와 같은 방법으로 악의를 가진 사용자가 돌아다니는 유효한 등록 메시지를 가로채 등록정보를 빼낸 후 재등록 하는 것을 방지할 수 있다. [그림 10]은 임의의 수인 난수를 이용한 비밀키 기반 인증 메커니즘을 표기한 것이다.

(From previous HA's reply
HA (MN : N_{HA}
(Registration
MN (FA : M_1, <M1>S_{MN-HA}
where M_1 = Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}
FA (HA : M_1, <M_1>S_{MN-HA}
(verify < M_1>S_{MN-HA} using S_{MN-HA}
HA (FA : M_3, <M_3>S_{MN-HA}
where M_3 = Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N_{HA}, N_{MN}
FA (MN : M_3, <M_3>S_{MN-HA}
(verify < M_2>S_{MN-HA} using S_{MN-HA}

[그림 10] 비밀키 인증 메카니즘

이 방법은 간단하게 등록 메시지의 보안을 제공하는 듯 보이지만 실제로는 이동 노드와 홈 에이전트 사이의 인증만 보장한다. 외부 에이전트는 단지 수동적으로 받은 등록 요청과 등록 대답을 전달해주는 역할 외에는 하지 않는다.

2. 공개키 기반 인증 메커니즘

비밀키 기반 인증 메커니즘은 상대와 통신을 하기 전에 안전한 방법으로 비밀리에 상대방과 비밀키를 분배하여야 한다. 그러나 비밀키는 키 분배 방법에 있어서 유연성이 떨어지고 특히 많은 사용자를 수용하기에는 적당하지 못하다는 한계점이 있다. 또한 전자결재를 위해 필요한 부인방지 서비스가 제공되지 않는다는 점을 극복하기 위하여 공개키를 기반으로 한 인증 메커니즘이 제시되었다.

비밀키 기반 메커니즘이 MAC 값을 사용하는 반면 공개키 기반 메커니즘은 공개키를 이용한 전자서명을 사용한다. 공개키 기반 인증 메커니즘에서는 인증과 관련된 내용을 담은 Certificate Extension을 모든 제어 메시지 뒤에 붙도록 정의하여

인증과 관련된 정보를 주고 받는다[38][39][40].

(Agent Advertisement

FA (MN : M_1, $<<M_1>>K^{-1}_{FA}$, $Cert_{FA}$

MN (validate $Cert_{FA}$ using K_{CA}

(verify $<<M_1>>K^{-1}_{FA}$ using K_{FA}

(Registration

MN (FA : M_2, $<<M_2>>K^{-1}_{MN}$, $Cert_{MN}$

FA (validate $Cert_{MN}$ using K_{CA}

(verify $<<M_2>>K^{-1}_{MN}$ using K_{MN}

FA (HA (delete $Cert_{MN}$

: M_3, $<<M_3>>K^{-1}_{FA}$, $Cert_{FA}$

HA (validate $Cert_{FA}$ using K_{CA}

(verify $<<M_3>>K^{-1}_{FA}$ using K_{FA}

(verify $<<M_2>>K^{-1}_{MN}$ using K_{MN} (from $Cert_{MN}$ already has)

HA (FA : M_4, $<<M_4>K^{-1}_{HA}$, $Cert_{HA}$

FA (validate $Cert_{HA}$

(verify $<<M_4>>K^{-1}_{HA}$ using K_{HA}

FA (MN (delete $Cert_{HA}$

: M_5, $<<M_5>>K^{-1}_{FA}$

MN (verify $<<M_5>>K^{-1}_{FA}$ using K_{FA}(from $Cert_{FA}$ already has)

(verify $<<M_4>>K^{-1}_{HA}$ using K_{HA}(from $Cert_{HA}$ already has)

[그림 11] 공개키 인증 메카니즘

여기서는 이동 노드, 외부 에이전트, 홈 에이전트 간에 서로에 대한 인증을 한다. 메시지를 새로 만들거나 받은 메시지를 전달하는 경우 메시지 뒤에 전자서명을 추가함으로써 메시지가 변하지 않았다는 것을 확인시키고, 또한 자신이 메시지를 만들었음을 증명하는 부인방지 서비스를 제공한다.

3. 최소 공개키 인증 메커니즘

최소 공개키 인증 메커니즘은 공개키 기반 인증이 가진 단점을 줄인 방법으로 공개키 암호화를 최소로 사용한다.

이동 노드는 모든 암호화 동작을 비밀키 기반으로 수행하며, CRL(Certificate Revocation List) 접근과 인증서 증명과 같은 부담스러운 작업을 하지않아도 된다. 이동 노드는 홈 에이전트와의 인증에서 비밀키를 기반으로 인증하며 외부 에이전트와의 확인은 홈 에이전트로부터 등록 대답을 받아 외부 에이전트의 인증서가 유효하다는 것을 간접적으로 확인한다. 인증서를 캐쉬에 저장하여 후에 사용할 때 효율을 높일 수 있지만 만약, 이동 노드가 공개키 기반 암호화를 수행할 수 있을 정도로 자원이 풍부하다면 홈 에이전트가 제공하는 서비스와 무관하게 선택적으로 공개키 기반 인증을 할 수도 있을것이다. 외부 에이전트는 홈 에이전트와의 인증에서 직접적으로 공개키 기반 인증을 수행하며, 이동 노드에 대해 홈 에이전트가 이동 노드에게 돌려준 등록 대답에서 간접적으로 인증을 확인한다. 이동 노드는 홈 에이전트와 비밀키 기반 인증을 하기 때문에 이동 노드와 홈 에이전트 사이에 부인 방지서비스가 제공되지 않는다.

(Agent Advertisement

FA (MN : M_1, $<<M_1>>K^{-1}_{FA}$, $Cert_{FA}$

(Registration

MN (FA : M_2, $<<M_2>>S_{MN-HA}$

where M_2=Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA},

N_{HA}, N_{MN}, [message in agent advertisement]

FA (HA : [message in MN (FA step], N_{FA}

HA (validate $<M2>S_{MN-HA}$ using S_{MN-HA}

(check whether FA_{id} in M1 and FA_{id} in M_2 is identical

(validate $Cert_{FA}$ based on existing PKI at HA

(validate $<<M_1>>K^{-1}_{FA}$ using authenticated K_{FA}

HA (FA : M_3, $<<M_3>K^{-1}_{HA}$, $Cert_{HA}$

where M_3=M_4, N_{FA}

M_4=Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN},

$<M_4>S_{MN-HA}$

FA (validate N_{FA}

(validate $Cert_{HA}$ based on existing PKI at FA

(validate $<<M_3>>K^{-1}_{HA}$ using authenticated K_{HA}

(log this msg as a proof of serving MN

(perhaps used in conjunction with the billing protocol)

FA (MN : M_4

MN (validate $<M_4>S_{MN-HA}$ using S_{MN-HA}

(verify $<<M_4>>K^{-1}_{HA}$ using K_{HA}(from $Cert_{HA}$ already has)

[그림 12] 최소 공개키 인증 메카니즘

C. 기존 인증 메커니즘의 문제점 및 분석

안전하고 효율적인 인증을 위하여 인증 참여자, 인증 서비스, 암호 알고리즘에 대하여 기존 인증 메커니즘을 분석하여 본다.

1. 인증 참여자

비밀키 기반 인증 메커니즘에서의 인증은 기본적으로 이동 노드와 홈 에이전트 둘 사이에서 이루어진다. 이동 노드는 등록 요청시 비밀키와 보호된 필드에 대한 MAC을 첨부시켜 홈 에이전트에게 인증 받고, 홈 에이전트도 등록 대답시 동일한 방법으로 이동 노드에게 인증 받는다. 그러나 인증에 참여하는 외부 에이전트의 역할은 전달 받은 메시지를 전달해주는 소극적인 역할만을 수행하여 보안이 완전하지 못하다.

공개키 기반 인증 메커니즘은 세 참여자 서로에 대한 인증을 메시지를 받고 전달할 때마다 수행한다. 등록과정에 참여하는 세 참여자가 모두 서로에 대한 신뢰있는 인증을 할 수 있기 때문에 보안면에서 이상적이나 반복되는 인증은 성능의 저하를 가져온다.

최소 공개키 기반 인증 메커니즘 역시 세 참여자 모두 인증에 참여하되 간접적인 인증을 통해 인증 횟수를 줄이고 비밀키 인증의 사용하여 인증에 필요한 오버헤드를 줄였다. 외부 에이전트는 이동 노드로부터 등록 요청을 받으면 인증 작업을 수행하지 않고 자신이 보냈던 에이전트 광고의 값이 유효한 것인가만 검사한다. 이동 노드가 외부 에이전트를 직접 인증하지 않고 홈 에이전트가 인증한 결과를 받음으로써 간접적으로 공개키 인증 효과를 가짐으로써 모든 인증 참여자에 대한 인증이 가능하다. 이 방법은 외부 에이전트의 인증까지 유지하는 동시에 외부 에이전트의 공개키 인증 부분은 홈 에이전트에게 넘겨 성능 저하를 감소시켰다.

따라서 안전한 인증을 위하여는 인증 참여자 모두를 인증하여야 하고 동시에 효율을 높이기 위하여 기본적으로 반복되는 공개키 인증의 횟수를 줄이고 이동 노드에게는 계산이 비교적 간단한 비밀키 인증을 시키는 방법으로 이루어져야 한다.

2. 인증 서비스

문서의 전자적인 교환이 일반화되면서 문서의 인위적인 변조나 여러 가지 결함 때문에 문제가 많다. 따라서 일반적인 종이문서에 상호 서명이나 도장을 찍는 것과 같이 전자문서의 송신자와 수신자간에 문서내용에 전자 서명을 하는 방식이 필요하다.

비밀키 기반 암호 메커니즘에서는 난수나 타임스탬프를 사용하여 재사용하지 못하게 하며 원문에 대해 유일하게 생성되는 인증 코드를 덧붙여서 인증 받고 문서 내용이 변경되지 않음을 증명할 수 있다. 그러나 암호화하는 키와 복호화하는 키가 동일하여 비밀키가 누설되었을 경우 누구든지 MAC을 생성해낼 수 있어 MAC에는 부인방지 기능이 없다.

공개키 기반 인증 메커니즘에서 역시 난수나 타임스탬프로 재사용하지 못하게 하며 원문에 대하여 전자서명을 함으로써 인증 받고 내용이 변경되지 않음을 증명한다. 공개키 기반 시스템은 개인키와 공개키의 쌍으로 이루어져 이 중 공개키만 외부에 노출되어 있고 개인키는 어떠한 경우에도 개인키 소유자에게만 알려져 있다. 따라서 개인키 소유자가 개인키를 노출시키지 않는 한 누구도 올바로 암호화할 수 없다. 암호화를 할 수 있는 자가 유일하다는 특성은 자신이 제공한 서비스에 대하여 후에 부인할 수 없게 한다. 이것을 전자서명이 제공하는 부인방지 서비스라고 하며 이동하는 노드가 책임을 가지고 네트워크 자원을 사용하도록 한다.

최소 공개키 기반 인증 메커니즘은 공개키를 사용하여 확장성을 높이면서도 이동 노드가 해야 하는 인증 관련 관리와 이동 노드에게 부여된 공개키 계산을 최소로 줄였다. 그러나 이동 노드와 홈 에이전트 사이에는 비밀키를 이용하여 MAC을

생성하였기 때문에 부인방지 서비스가 결여되어 있다. 외부 에이전트와 홈 에이전트 사이에서는 공개키를 이용한 전자서명을 교환하기 때문에 네트워크에서 제공한 것에 대하여 부인할 수 없다. 다만 홈 에이전트는 외부 에이전트에게 공개키로 전자서명을 보냄으로써 이동 노드에게 제공한 서비스에 대하여 부인할 수 없다. 그러나 전자상거래와 같이 보안이 중요한 환경에서 이동 노드의 위치 등록에 대한 부인방지 서비스가 결여되어 있다.

3. 암호 알고리즘의 분석

현재 IETF RFC2002에서 지정해 놓은 표준 Mobile-IP의 인증 메커니즘은 비밀키 기반으로 RFC 1321에 정의된 해쉬 함수 MD5를 이용한다. 해쉬 함수는 임의의 입력 비트 열에 대하여 일정한 길이의 안전한 비트 열을 출력하는 것이다. 입력 데이터 스트링을 고정된 길이의 출력인 해쉬 코드로 대응시키는 함수로서 주어진 해쉬 코드에 대하여 이 해쉬 코드를 생성하는 데이터 스트링을 찾아내는 것은 계산상 실행 불가능하며, 주어진 데이터 스트링에 대하여 같은 해쉬 코드를 생성하는 또 다른 데이터 스트링을 찾아내는 것은 계산상 실행 불가능하다. MD5는 Ron Rivest가 1990년 개발한 MD4 알고리즘을 개선한 것으로 충돌률이 일어날 가능성이 적은 크기인 128 bits 의 해쉬를 만든다. 적은 계산 비용과 빠른 계산 속도면에 있어서 공개키에 비하여 우수하지만 RFC2002에 따라 동작하는 비밀키가 이동 노드와 홈 에이전트 사이에 미리 분배되어야 한다는 문제로 확장성이 떨어진다.

이에 반하여 공개키 인증 메커니즘에서는 이동 노드가 인증서를 기반으로 한 공개키 암호작동을 하도록 요구한다. 공개키 기반 인증 메커니즘은 IETF의 draft로 제시되어 있으며 마찬가지로 어떤 알고리즘이든 사용할 수 있으나 기본적으로 512 bits 키를 사용한 RSA를 제안한다. 보안상의 강점에도 불구하고 암·복호화의 비용이 높아 인증서를 증명하기 위한 인증서 검증 작업과 함께 이동 노드에게 성능 저하를 가져온다. 특히 공개키 동작이 일반적으로 비밀키 동작에 비하여 100 ~

1,000배 이상 복잡하다는 것을 생각할 때 공개키 방식은 상당히 부담스럽다[45]. 일반적으로 자원이 제약되어 있는 이동 노드에게는 인증서를 발급하는 동작은 상당히 무거운 작업이다. 인증서 발급으로 인하여 공개키 기반 인증 메커니즘의 경우 등록 단계에서만 X.509로 정의된 인증 기관에 4번이나 접근하여 인증서 확인 결과를 기다려야 한다. 그런데 이동 노드가 일반적으로 자원이 한정되어 있어 계산할 수 있는 파워가 부족하다는 점과 홈 네트워크에서 멀어질수록 인증 기관에서 메시지를 주고 받는 시간이 길어진다는 면에서 이러한 동작은 손쉬운 것이 아니다.

최소 공개키 기반 인증 메커니즘에서는 이동 노드가 인증 기관에 접근하여 인증서를 발급 받고 유효한 인증서인지 확인하기 위하여 CRL에 접근해야 하는 복잡한 작업에서 해방되었다. 이동 노드는 홈 에이전트와 비밀키를 이용하여 인증하며 자원이 풍부한 외부 에이전트와 홈 에이전트는 공개키를 사용하여 인증한다.

따라서 자원에 제약되어 있는 이동 노드는 계산이 간단한 해쉬 함수를 사용하는 방법으로 인증하는 것이 효율적이며 자원이 풍부한 외부 에이전트나 홈 에이전트는 공개키 암호 시스템을 사용하여 보안을 강화시키는 것이 좋다.

Ⅳ. 이동망에서 *Mobile-IP* 인증 및 성능평가

본 장에서는 기존 인증 메커니즘의 장단점을 비교하고 사용 암호 알고리즘에 대하여 분석하여 새로운 Mobile-IP 인증 방안을 제시하고자 한다.

A. 인증 메카니즘 제시

본 절에서 기존 인증 메커니즘의 분석에 따라 보다 효율적이고 안전한 인증 메커니즘을 제시하고자 한다. 앞에서 분석한 것과 같이 비밀키 기반 인증 메커니즘에서는 가벼운 비밀키 계산으로 인증의 효율성은 높으나 모든 인증 참여자에 대한 인증이 이루어지지 못하고 생성하는 MAC의 특성상 부인방지 서비스가 부족하다는 단점이 있다. 공개키 기반 인증 메커니즘은 모든 인증 참여자에 대하여 공개키를 기반으로 부인방지 서비스가 제공되는 인증을 수행하나 실제로 적용할 수 없을 만큼 시간이 오래 걸린다. 최소 공개키 기반 인증 메커니즘에서는 이동 노드와 홈 에이전트 사이에는 비밀키를 기반으로 신뢰성 있는 관계를 유지하며, 외부 에이전트와 홈 에이전트는 공개키를 기반으로 인증한다. 보안을 유지시키면서 동시에 성능을 높이는 효과가 있으나 이동 노드와 홈 에이전트 사이에는 전자서명을 사용하지 않아 부인방지 기능이 없다. 전자상거래와 같이 이동 노드 행동의 책임성이 짙을 경우에는 위치 등록에 대한 부인방지 서비스가 있어야 한다. 따라서 인증은 사용자가 네트워크에서 사용한 자원과 행동에 대하여 부인을 못하도록 하며 동시에 사용자의 편의와 원활한 네트워크 이용을 위해 등록 과정이 짧아야 한다.

제안된 방법은 공개키 기반 인증 메커니즘과 최소 공개키 기반 인증 메커니즘의 혼합 형태이다. 이동 노드가 등록 요청에 전자서명을 추가하는 것 외에는 최소 공개키 기반 인증 메커니즘과 동일하게 작동한다.

외부 에이전트가 보낸 에이전트 광고를 이동 노드는 홈 에이전트에게 그대로 전

달시키고 홈 에이전트가 인증한 내용은 결과를 통해 간접적으로 인증한다. 이동 노드는 홈 에이전트에게 전자서명을 보내고 홈 에이전트는 인증기관에 접근하여 공개키의 진실 여부를 확인한 후 전자서명을 증명한다. 이로써 홈 에이전트는 이동 노드와 외부 에이전트 모두를 인증할 수 있다. 여기서 이동 노드의 전자서명은 자신이 등록한 위치정보에 대한 중요한 부인방지 기능을 제공하여 네트워크 자원 사용을 관리제어할 수 있다. 홈 에이전트의 경우에는 외부 에이전트에게 전자서명을 보내 인증 받고 이동 노드에게는 MAC을 생성시킴으로써 직접 인증 받는다. 이로서 새로운 위치 등록과정에 관계하는 모든 참여자에 대한 인증을 할 수 있다.

(Agent Advertisement

FA (MN : M_1, $<<M_1>>K^{-1}_{FA}$, $Cert_{FA}$

(Registration

MN FA : M_2, $<<M_2>>K^{-1}_{MN}$, $Cert_{MN}$

where M_2=Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA},

N_{HA}, N_{MN}, [messge in agent advertisement]

HA *validate $Cert_{MN}$ using K_{CA}*

verify $<<M_2>>K^{-1}_{MN}$ using K_{MN}

check whether FA_{id} in M1 and FA_{id}in M_2 is identical

validate $Cert_{FA}$ based on existing PKI at HA

validate $<<M_1>>K^{-1}_{FA}$ using authenticated K_{FA}

HA (FA : M_3, $<<M_3>K^{-1}_{HA}$, $Cert_{HA}$

where M_3=M_4, N_{FA}

M_4=Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN},

$<M_4>S_{MN-HA}$

FA (validate N_{FA}

(validate $Cert_{HA}$ based on existing PKI at FA

(validate $<<M_3>>K^{-1}_{HA}$ using authenticated K_{HA}

(log this msg as a proof of serving MN

(perhaps used in conjunction with the billing protocol)

FA (MN : M_4

MN (validate $<M_4>S_{MN-HA}$ using S_{MN-HA}

(verify $<<M_4>>K^{-1}_{HA}$ using K_{HA}(from $Cert_{HA}$ already has)

[그림 13] 인증 메카니즘의 제시

- MN, FA, HA : 각각 이동 노드, 외부 에이전트, 홈 에이전트
- CA : 인증 기관(Certificate Authority)
- S_{MN-HA} : MN와 HA 사이 공유하는 비밀키

- K_{MN}, K_{HA}, K_{FA}, K_{CA} : MN, HA, FA, CA 각각의 공개키
- K^{-1}_{HA}, K^{-1}_{FA}, K^{-1}_{CA}: MN, HA, FA, CA 각각의 개인키
- MN_{HM} : MN의 고정 IP 주소
- MN_{COA} : MN의 COA
- HA_{id} : ID로서 HA의 IP 주소
- FA_{id} : ID로서 FA의 IP 주소
- N_{MN}, N_{HA} : MN, HA 각각의 난수(Nonce)
- {M}K : 메시지 M을 키 K로 암호화한 값
- <M>K : 메시지 M에 대하여 키 K로 얻은 MAC(Message Authentication Code)
- <<M>>K^{-1}_{A} : 메시지 M에 대하여 A의 개인키로 서명한 전자서명
- $Cert_{HA}$, $Cert_{FA}$: HA, FA 각각의 인증서

이동 노드는 자신의 개인키를 사용해서 전자서명을 생성하고 그 전자서명을 등록 요청에 포함시킨다. 이동 노드는 원문에 전자서명과 인증서를 포함시키지만 미리 인증서를 발급해 놓기 때문에 서명시마다 인증 기관에 접근할 필요가 없다. 홈 에이전트는 전자서명을 받아 증명하고 이동 노드의 서비스 요청에 대한 증거로 보존한다. 등록 요청은 전자서명을 이용하지만, 등록 대답은 MAC에 의존하기 때문에 이동 노드가 등록 대답을 받았을 때에도 미리 나눠 가진 비밀키로 인증함으로써 인증시 인증 기관에 접근할 필요가 없다. 이런 구조는 특히 이동 노드의 공개키 사용을 최소로 한다.

제안된 방법이 공개키 기반 인증 메커니즘에 비하여 가지는 장점은 첫째, 홈 에이전트가 보내는 등록 대답은 비밀키를 사용한 MAC을 포함시켜 이동 노드의 성능 저하를 줄였다는 것이다. 이동 노드와 같이 계산을 최소로 줄여야 하는 환경에서 해쉬 함수가 주는 이점은 크다.

둘째, 이동 노드는 에이전트 광고를 받은 때 외부 에이전트를 증명할 필요가 없고 등록 과정 중 외부 에이전트와 직접 상호 인증을 할 필요도 없다. 홈 에이전트

가 등록 요청을 받아 외부 에이전트를 인증하고 인증이 성공이라면 등록 대답을 이동 노드에게 보낸다. 이동 노드는 등록 대답을 받음으로써 외부 에이전트에 대한 내용을 간접적으로 인증한다.

셋째, 이동 노드는 한 번의 공개키 동작을 수행하여 전자서명을 생성해낸다. 자신의 개인키로 전자서명을 만들고 보내므로 인증기관의 CRL에 접근할 필요가 없다. 일반적으로 전력을 아껴서 사용해야 하는 이동 노드에게 계산을 줄여준다. 또한 홈 에이전트로부터 등록 대답을 받아도 미리 분배 받은 비밀키로 인증하기 때문에 인증기관에 접근할 필요도 없고 계산 비용이 매우 적다.

이렇게 새로 제시된 전자서명을 이용한 최소 공개키 인증 방안은 이동 노드가 위치를 바꾸었을 때, 이후에 이루어질 데이터 통신 경로를 열기 위한 새 위치 등록 단계에 해당된다. 따라서 새 통신 경로를 만드는데 있어서 인증 과정에 관계하는 모든 참여자를 인증한다는 면에서 악의를 가진 사용자의 공격을 방지할 수 있으며, 동시에 비밀키 공개키에서 사용되는 MD5와 RSA와 같은 인증 알고리즘을 통하여 인증의 무결성을 보장할 수 있다. 특히 RSA는 이동 사용자만이 비밀키를 보유한다는 점에서 새 위치 등록과정 행위를 부인을 할 수 없게 한다. 이 방법은 보안을 중요시하는 네트워크에서 새로운 네트워크 경로 설정할 때 네트워크 자원 사용에 대한 부인방지 기능을 부여하는 것으로, 이것은 어플리케이션에서 전자서명을 이용한 문서, 데이터에 대한 부인방지 기능과는 다르다. 이로써 인증 참여자 모두에게 인증을 수행하면서도 공개키를 최소로 사용하여 성능을 높였으며 부인방지 서비스를 이동 노드에게도 포함시킴으로써 보안이 높은 시스템을 가진 네트워크에서 사용될 수 있는 이동 프로토콜로 제안될 수 있다. 그 외에도 등록되어 있던 이동 노드가 오프라인이 되었다가 다시 같은 외부 에이전트에게 재등록하려고 한다면 최적화하여 구현할 수 있다. 이동 노드가 할 일이 없는 동안 먼저 전자서명을 만들어 놓았다가 재등록 시 즉시 사용함으로써 전체 인증시간의 단축을 더 가져올 수 있다. 기존의 세 가지 인증 메커니즘과 제안된 인증 메커니즘을 비교하면 [표 3]과 같다.

[표 3] 인증 메커니즘의 비교

	SK	*PK*	*MinPK*	*MinPKed*
인증방식	MAC	MAC	MAC, 전자서명	MAC, 전자서명
알고리즘	MD5	RSA	MD5, RSA	MD5, RSA
키 종류와 키 길이	비밀키	공개키 (512 bits)	비밀키, 공개키 (512 bits)	비밀키, 공개키 (512 bits)
인증 코드 길이	16bytes	64 bytes	16 bytes, 64 bytes	16 bytes, 64 bytes
*MAC*사용	MN, HA	·	MN, HA	HA
전자서명사용	·	MN, FA, HA	FA, HA	MN, FA, HA

(SK : 비밀키 기반 인증 메커니즘, PK : 공개키 기반 인증 메커니즘 , MinPK : 최소 공개키 기반 인증 메커니즘, MinPKed : 제안하는 전자서명을 첨부한 공개키 기반 인증 메커니즘)

B. 시뮬레이션 구현

1. 모델링 도구

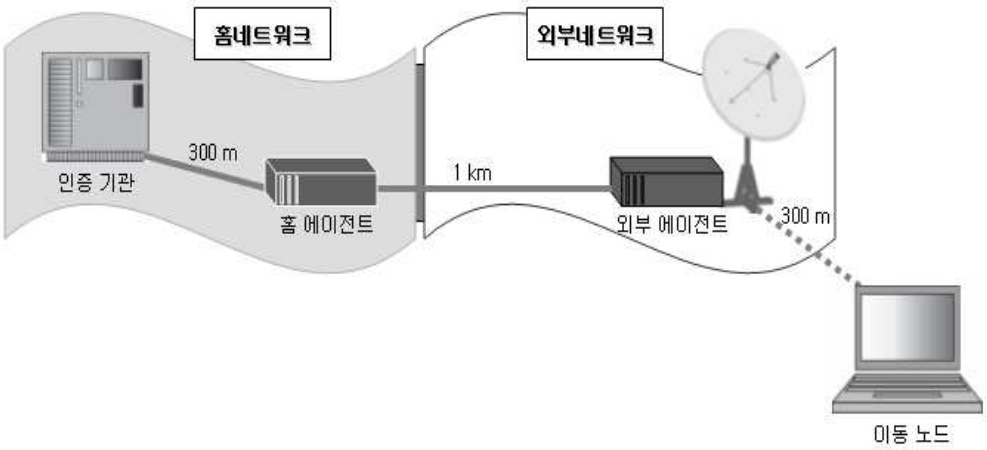
통신 시스템 개발용 명세 언어인 SDL(Specification and Description Language)은 시스템을 명세화하고 기술하는 표준화된 언어이다. 현재 ITU-T로 명칭이 바뀐

CCITT에 의해 개발되었으며 ITU-T Recommendation Z.100으로 표준화되었다. 전기통신 분야에서 분석 및 개발에 많이 쓰이며, 통신 시스템들이 복잡해짐에 따라 시스템의 동작(Behavior)을 명시하는데 사용된다. SDL은 시스템을 계층적으로 표현하기 위해 제안되어 동시 작업과 상호 동작이 중요시되는 사건 중심의 실시간 시스템을 기술하는데 적합하다. 이에 따라 통신 시스템의 동작을 기술해 주는 사용자와 개발자들의 공통언어로 사용되고 실시간 시스템의 구조, 동작 기능 및 데이터를 표시할 수 있는 장점을 보유하며 시스템 분석과 설계에 적용이 가능하다.

2. 시뮬레이션 환경

a. 망 구성

망 구성은 무선랜으로 IEEE 802.11를 따르고 시뮬레이션 구성은 [그림 14]와 같다.



[그림 14] 망 구성

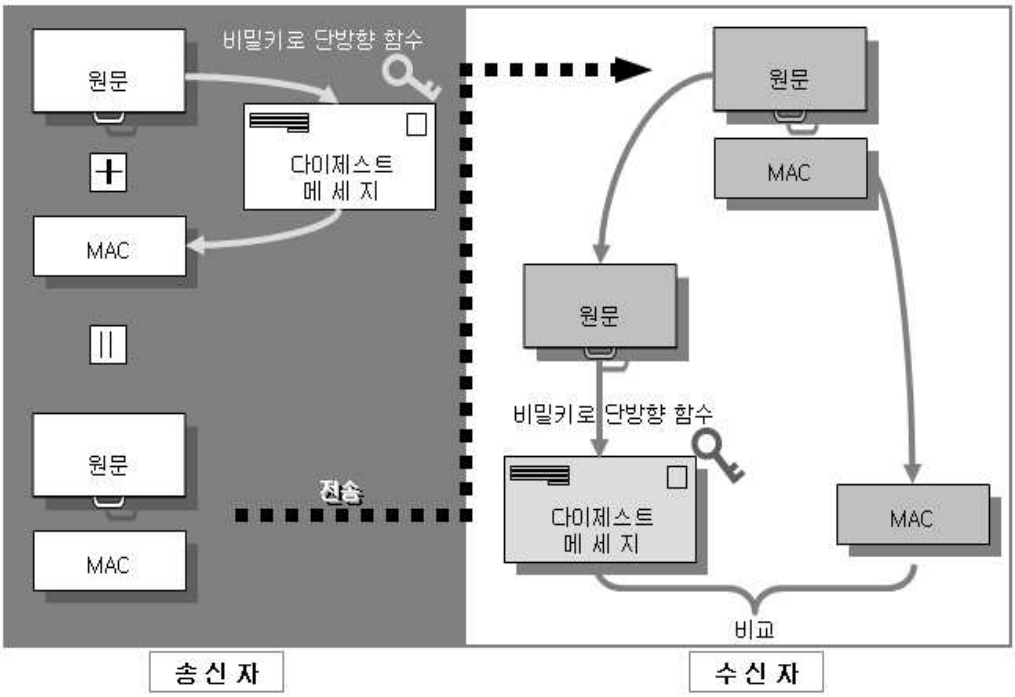
이동 노드는 처음 연결을 시작하여 홈 네트워크의 홈 에이전트로부터 고정 IP를 부여받고 외부 네트워크로 이동하여 외부 에이전트의 에이전트 광고를 통해 새로운 COA를 다시 받아 홈 에이전트로 등록시킨다. 외부 에이전트에서 이동 노드까지의 거리 즉, 서브넷의 반경은 300m로 한다. 이동 노드가 다른 서브넷 즉, 외부 네트워크로 이동함에 따라 홈 에이전트와 외부 에이전트 사이의 거리는 1km에서 30km까지 변화한다. 이동 노드가 위치 이동을 하여 새로운 외부 네트워크로 이동하여 IP가 바뀌게 되면 매 번 홈 에이전트로 위치 정보를 다시 등록하고 홈 에이전트에서는 이에 대한 등록 응답을 보내고 나면 데이터 그램을 터널링 하게 된다. 여기에 사용되는 시뮬레이션 고정 파라미터 값은 [표 4]와 같다.

[표 4] 시뮬레이션 고정 파라미터 값

거 리	홈 에이전트에서 인증기관까지의 거리 (유선 링크)	300 m
	홈 에이전트에서 외부 에이전트까지의 거리 (유선 링크)	1 km
	외부 에이전트에서 인증기관까지의 거리 (유선 링크)	1.3 km
	이동 노드에서 기지국까지의 거리 (무선 링크)	300 m
지연시간	무선 링크의 지연시간	7 ms/km
	유선 링크의 지연시간	5 ms/km
대역폭	무선 링크 대역폭	2 Mbps
	유선 링크 대역폭	10 Mbps

b. 인증 메커니즘의 작동

인증 동작은 먼저 UDP 계층에서 UDP Checksum 필드를 계산한 뒤 재공격을 방지하기 위해 삽입된 식별자(Identification)를 검사한다. 임의의 수인 난수를 삽입하거나 등록 메시지가 사용될 수 있는 Lifetime을 명시한 타임스탬프를 삽입할 수 있는데 여기서는 난수를 포함시키며 상대방의 답변을 받으면 자신이 전 단계에서 삽입시킨 난수가 제대로 들어있는지 검사한다.



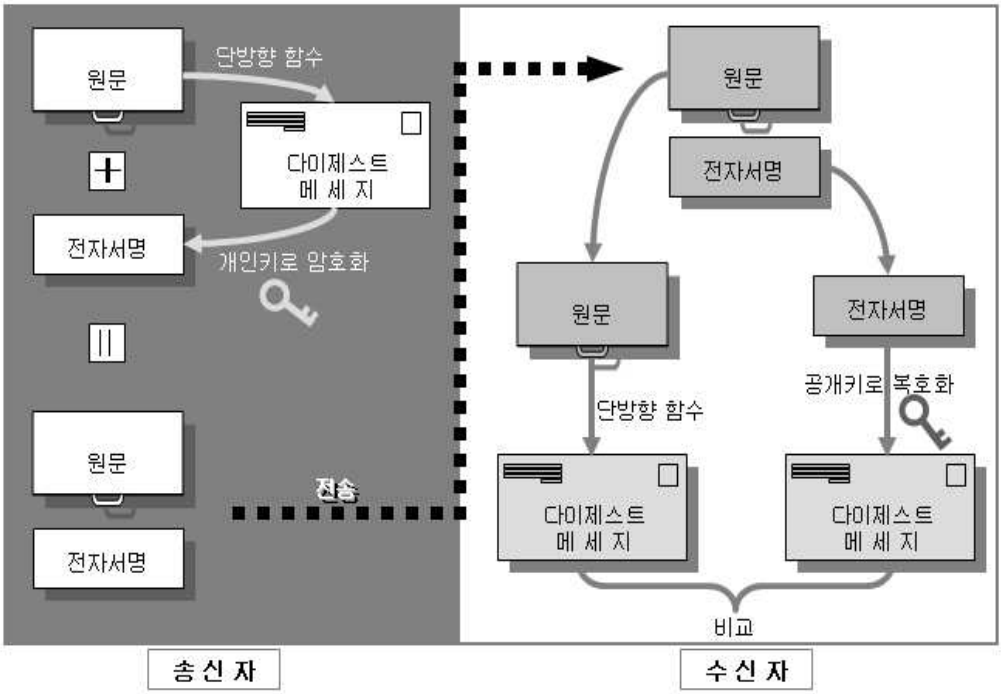
[그림 15] MAC 동작

마지막으로 인증 코드가 삽입된 경우에는 MAC을 증명하고 전자서명이 첨부된 경우에는 인증서를 확인하고 전자서명을 증명한다. [그림 15]은 MAC을 검사하는

동작을 보여준다. 이 때 사용하는 해쉬 함수는 어떤 종류도 사용할 수 있으며, 본 시뮬레이션에서는 RFC 2002에서 기본으로 하는 MD5를 사용한다. 등록 대답에 대하여 Prefix-Suffix 모드로 128 bits의 다이제스트 메시지를 생성한다. 방법은 먼저 공유한 비밀키에 대하여 해쉬 함수를 수행하고 보호하고자 하는 원문 메시지에 대하여 다시 해쉬 함수를 수행하고 다시 한번 비밀키에 대하여 해쉬 함수를 수행한다.

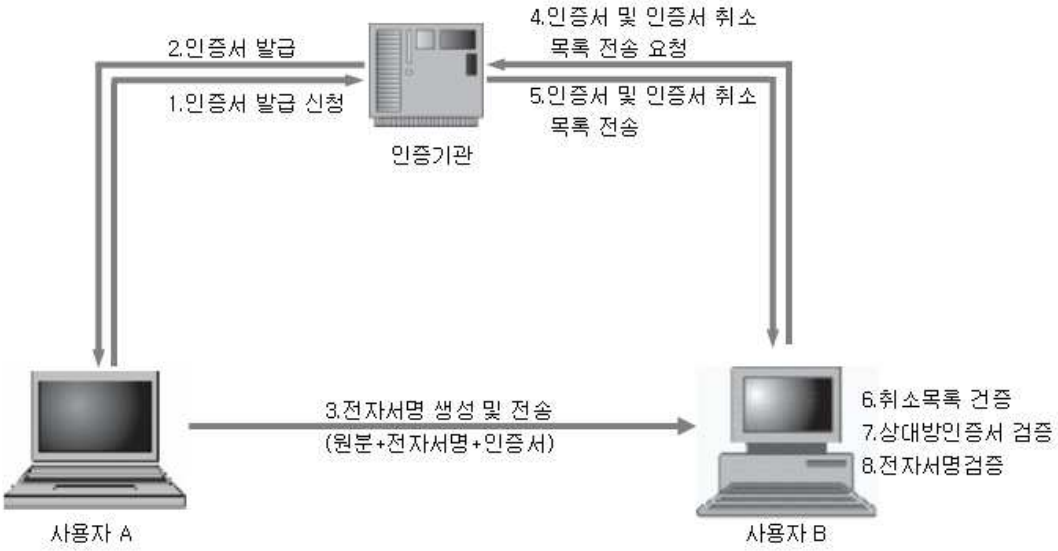
MD5는 RFC1321에 제시된 소스 코드를 따르며, 본 시뮬레이션에서는 앞에서 설명된 해쉬 함수 MD5를 사용한다. 이 때 입력 값은 512 bits이고 결과로 나오는 해쉬 값은 16 bytes이다.

전자서명을 인증하는 경우에는 [그림 16]와 같이 공개키를 사용한 부가형 전자서명(Digital Signature with Appendix)을 이용한다. 보호하는 원문 메시지는 해쉬 함수와 동일하다. 부가형 전자서명은 원문 이외에 서명을 따로 전송해야 하므로 전송량이 조금 늘어나는 반면, 메시지가 아무리 길더라도 단 한번의 서명 생성 과정만이 필요하므로 효율적이다. 임의의 길이의 메시지를 일정한 길이로 압축해 주는 해쉬 알고리즘은 입력 메시지가 조금만 변하더라도 그 해쉬 결과로 전혀 다른 값을 출력하여 서명의 위조나 서명된 메시지의 변조를 막을 수 있다.



[그림 16] 전자서명의 작동

전자서명을 인증하기 위해서는 공개키를 사용해야 하는데, 송신자는 인증 기관으로부터 자신의 공개키가 삽입된 인증서를 먼저 발급받아 원문에 전자서명을 첨부한다. 수신자는 받은 인증서를 확인하여 수신 받은 공개키가 정상적이다고 확인되면 전자서명을 검증하는데 사용한다. 인증 기관을 통한 전자서명의 인증절차 과정은 [그림 17]과 같다.



[그림 17] 인증기관을 통한 전자서명 인증절차

Draft에 따라 여기서 공개키 기반 전자서명은 X.509를 기반으로 하며 표준으로 특정한 알고리즘을 명시하지는 않지만 RSA를 권고한다. 그 외에도 RSA가 가진 단점으로 지적되는 속도를 대폭 향상시킨 타원곡선 암호 알고리즘과 DSA(Digital Signature Algorithm)를 제시하여 키 길이와 전자서명 길이를 명시하고 있다. 타원곡선 암호 시스템은 수학적인 복잡도 때문에 동일한 키 크기의 정수 위에서 구현하는 것보다 훨씬 강도가 세다. 본 시뮬레이션에서는 RSA Laboratory의 RSA 암호 시스템을 시뮬레이션 한다. RSA에서 사용한 키길이는 512 bits이고 결과로 나오는 전자서명은 64 bytes이다.

C. 시뮬레이션의 성능 평가

본 절에서는 시뮬레이션의 성능 평가에 대한 결과를 분석한다. 모델링은 이동 노드가 위치 이동을 하여 다른 외부 네트워크로 이동 하였을 때 외부 에이전트의 에

이전트 광고를 통해 새로운 COA를 받고 새로운 이동 정보를 홈 에이전트에 등록하는 과정이다.

시뮬레이션은 비밀키 기반 인증 메카니즘, 공개키 기반 인증 메카니즘, 최소 공개키 인증 메카니즘과 제안된 인증 메커니즘으로 나누어 수행된다. 본 모델링은 Ultrasparc SUN OS 5.6 버전의 운영체제를 사용하고, CPU가 552 MHz, RAM이 256M인 워크스테이션에서 실행되었다.

1. 암·복호화 횟수 및 인증 평균시간

인증 메커니즘에서는 암호화·복호화가 차지하는 비중이 크기 때문에 암호화・복호화를 수행하는 횟수와 인증을 하는데 드는 평균시간을 통해 인증 메커니즘에서 암호화・복호화가 차지하는 영향을 분석할 수 있다.

다음은 시뮬레이션 결과를 수치로 계산하기 위하여 사용된 수식이다.

T = Operation + Delay + EncrypDecrypTime ----------(수식 1)

Delay = PropDelay + TransDelay ----------(수식 1-1)

EncrypTime = SecretEncryp + PublicEncryp ----------(수식 1-2)

DecrypTime = SecretDecryp + PublicDecryp ----------(수식 1-3)

EncrypDecrypTime = EncrypTime + DecrypTime ----------(수식 1-4)

(수식 1)의 전체 등록 시간(T)은 노드 프로세싱 시간(Operation), 전달지연시간(Delay), 암호화복호화 시간(EncrypDescrypTime)의 합이다.

첫 번째, 노드 프로세싱 시간(Operation)시간(T)은 이동노드의 등록 요청 시간과 홈 에이전트의 등록 대답을 포함하여 홈 에이전트와 외부 에이전트의 테이블 갱신 시간을 포함한다.

두 번째, (수식 1-1)의 전달지연시간(Delay)은 노드와 에이전트 사이에 메시지가 전달되는데 걸리는 지연 시간 즉, 인증 참여 노드사이의 거리와 미디어에 따른 전송 지연 시간(Propagation Delay)과 회송 지연 시간(Transmission Delay)의 합이다.

마지막으로 암호화복호화 시간(EncrypDescrypTime)은 (수식 1-4)에서와 같이 MAC이나 전자서명을 만드는데 필요한 시간으로 각각 암호화 시간(EncrypTime)과 복호화 시간(DecrypTime)의 합이다. 이 때, 암호화 시간(EncrypTime)은 (수식 1-2)에서와 같이 MD5가 비밀키로 사용된 비밀키 기반 암호화 시간(SecretEncryp)과 RSA가 공개키로 사용된 공개키 기반 암호화 시간(PublicEncryp)의 합이다. 또한 복호화 시간(DecrypTime)은 (수식 1-3)에서와 같이 비밀키 기반 복호화 시간(SecretDecryp)과 공개키 기반 복호화 시간(PublicDecryp)의 합이다.

각각의 인증 메커니즘에서 요구되는 암호화·복호화 횟수는 [표 5]와 같다.

[표 5] 암호화·복호화 횟수

		해쉬함수		공개키전자서명	
		암호화	복호화	암호화	복호화
SK	전체	2	2		
	이동노드	1	1		
PK	전체			10	11
	이동노드			1	4
MinPK	전체	2	2	4	4
	이동노드	1	1		
MinPKed	전체	1	1	6	5
	이동노드		1	1	

[표 5]와 같이 전체 노드에서 SK의 경우는 해쉬 함수 계산이 4번이지만 PK의 경우에는 공개키 계산 횟수가 21번으로 증가하였다. 이는 PK의 경우 공개키의 계산이 100 ~ 1,000 배 정도 오래 걸린다는 점을 고려한다면 PK의 경우는 SK의 경우 보다 시간이 많이 걸리며 계산 비용 또한 많이 요구한다는 것을 알 수 있다. 그러나 MinPK의 경우는 공개키의 계산이 8번으로 PK의 경우에 비해 공개키의 계산이 절반 이하로 줄었다. 이처럼 공개키 계산을 최소로 할 경우에는 시간이 많이 걸리며 비용이 많이 드는 공개키 계산이 매우 줄게 된다. 제안된 MinPKed에서는 PK의 경우에 비해 공개키의 계산이 절반 수준이지만 MinPK의 경우에 비하면 공개키의 계산이 3회 증가하였다. 이는 부인방지 서비스를 위해 전자서명을 추가시켰기 때문이다. 그러나 이동 노드에서의 공개키 계산 횟수 증가는 1번으로 최소로 하였다.

[표 6] 인증 코드의 평균 시간 (단위 : ms)

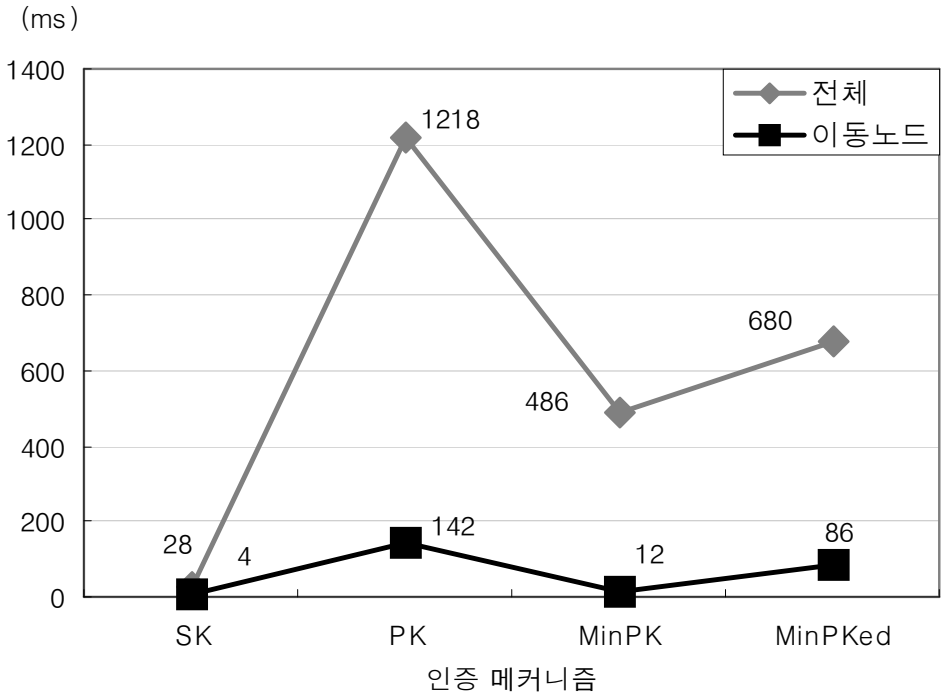
	MAC		전자서명	
	생성	증명	생성	증명
평균 시간	0.23	0.21	82.96	12.38

인증 코드를 생성하고 증명하는데 필요한 평균 시간은 [표 6]과 같다. MAC를 생성하는 평균시간은 0.23 ms이고, 증명하는 평균시간은 0.208 ms 이다. 이는 MAC을 생성하고 증명하는 인증 메커니즘이 같기 때문에 이에 걸리는 평균시간이 거의 비슷하다. 전자서명은 생성하는 평균시간이 82.96 ms이고 증명하는 평균시간이 12.38 ms이므로 생성하는 평균시간이 증명하는 평균시간에 비해 54 ~ 399배나 오래 걸린다. 이는 해쉬 함수에 비하여 공개키 함수 구조가 복잡하여 계산하는데 드는 시간이 더 오래 걸리기 때문이다. 이와 같이 공개키 계산은 계산구조가 복잡하여 시간이 더 많이 걸리고 비용이 많이 들며 많은 자원을 필요로 하므로 전력을

소모가 많다. 또한 암호화·복호화하는 시간이 오래 걸리고 자신의 공개키를 발급받아 키 관리소에 맡기고 상대방의 공개키를 부여 받아 복호화에 사용하는 과정으로 이루어지므로 비밀키 계산에 비하여 계산 비용이 상당히 높다는 것을 알 수 있다. [표 6]의 인증코드의 평균 시간에서 보듯이 보안을 유지하면서 공개키 사용을 최소화 하는 것이 효율적이라는 것을 알 수 있다.

2. 전체 등록시간과 이동 노드에서의 등록시간

전체 등록 시간(T)은 노드 프로세싱 시간(Operation), 전달지연시간(Delay), 암호화복호화 시간(EncrypDescrypTime)으로 구성된다. 즉, 이동 노드가 위치 이동을 하여 다른 외부 네트워크으로 이동 하였을 때 외부 에이전트를 통해 홈 에이전트로 새로운 위치 정보를 등록시키는 네트워크 계층에서 걸리는 시간이다. 이 때, 노드 프로세싱 시간(Operation)은 등록 요청, 등록 대답을 만드는 시간과 각 에이전트가 자신이 가진 테이블을 갱신하는 시간을 포함하며 전달 지연 시간(Delay)은 노드와 에이전트 사이에 메시지가 전달되는데 걸리는 지연 시간이며 암·복호화 시간은 MAC이나 전자서명을 만드는데 걸리는 시간이다.



[그림 18] 전체 등록 시간

[그림 18]는 인증 메커니즘별 전체 등록 시간과 이동 노드에서의 인증시간을 보여준다. SK와 PK의 경우 전체 등록 시간은 각각 28 ms, 1218 ms으로 PK의 경우는 SK일 경우에 비하여 44배나 시간이 더 걸린다. 이 시간은 새로운 등록과정이 네트워크 계층에서 이루어진 후 핸드오프 서비스나 TCP/UDP 계층에서의 서비스가 이어질 경우 상당히 긴 시간이다. 즉, 공개키는 보안을 높여준다는 사실에도 불구하고 사용이 어렵다는 것을 알 수 있다. 그렇다면 보안은 그대로 유지하면서 공개키 사용을 최소로 줄이는 MinPK의 경우에는 PK에 비하여 전체 등록시간이 40%밖에 걸리지 않는다. 이 방안은 공개키 암호화·복호화 과정이 반이하로 줄어들었음은 물론이며 이동 노드가 외부 에이전트를 통해 홈 에이전트가 인증 기관에게서 인증서를 발급 받고 공개키를 구하는 횟수가 많고 노드들 사이에 데이터그램을

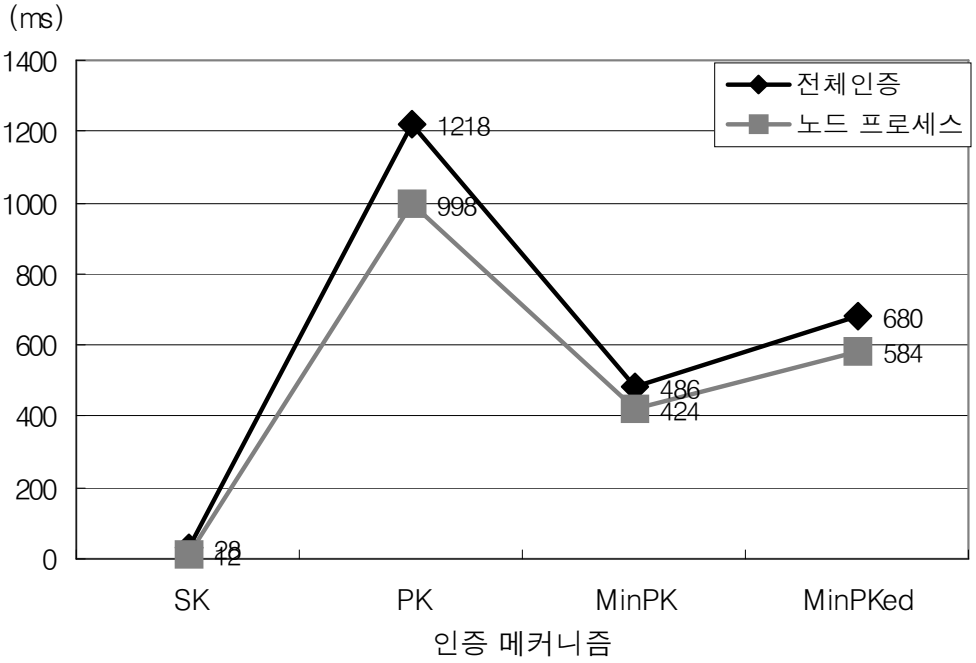
많이 주고 받아 전달 지연시간이 길어졌기 때문이다. 그러나 여기에는 부인방지 서비스가 결여되어 있으므로 제시된 MinPKed의 경우에는 이동 노드가 전자서명을 하도록 하였다. MinPKed는 PK에 비하여 등록시간을 56%로 줄여 성능을 향상시켰고 부인방지 서비스를 위한 전자서명을 추가시키면서 MinPK에 비하여는 140% 증가 폭을 보였다. 필요한 서비스를 제공하면서도 효율성을 최대한 떨어뜨리지 않는 동시에 부인방지 서비스를 제공한다.

이동 노드에서의 등록 시간은 전체 등록시간 중에서 이동 노드에서의 수행시간이다. 이동노드에서 PK의 경우 SK의 경우보다 35.5배나 더 걸린다. 즉, PK의 경우는 4 ms 로 수행 시간이 무척 적은데 비해 PK의 경우는 142 ms가 걸렸다. PK의 경우 공개키 기반 암호화·복호화가 매우 오래 걸린다는 점에서 수행 시간이 길 수 밖에 없다. 이는 SK의 경우 이동 노드와 홈에이전트 사이에서만 있던 상호 인증이 PK의 경우에는 공개키를 사용하기 위하여 인증 기관에 접근하는 시간과 인증서를 발급 받는데에 걸리는 시간이 추가로 걸릴 뿐만아니라 이동 노드, 외부 에이전트, 홈 에이전트 사이에서 인증이 이루어지기 때문에 인증 횟수가 늘어났다. PK의 경우 이동 노드에서 인증 시간이 길며 이동 노드에게 계산 비용을 너무 많이 요구하게 된다는 것을 알 수 있다. 그러나 MinPK의 경우에는 꼭 필요한 부분에서만 공개키를 사용하고 그 외에는 비밀키를 사용하여 계산 비용이 높은 공개키의 사용을 최소화 하였다. 특히 이동 노드에서는 SK의 경우와 시간차가 별로 나지 않은 12 ms이 걸렸는데 이는 암호화・복호화를 수행 하는데 있어서 비밀키를 사용하였기 때문이다. 제안한 MinPKed의 경우는 전자서명을 추가하여 이동노드가 자신의 개인키로 암호화 하게 하고 등록 요청을 보낸 후 홈 에이전트는 이동 노드의 공용키로 복호화 하여 메시지를 확인 할 수 있다. MinPK에 비하여 MinPKed의 경우에는 전자서명을 하기 위하여 이동 노드가 개인키를 이용하여 전자서명에 서명을 하기 때문에 시간이 7.2배 증가하였다. 그러나 PK에 비하여 시간이 61% 줄어든 것은 이동노드가 외부 에이전트로부터 에이전트광고를 받고 수행 할 인증 과정을 홈 에이전트가 대신 수행하기 때문이며 홈 에이전트에 대한 인증에서는 전자서명 대신 비용이 적은 비밀키를 이용한 MAC를 이용하여 때문에 홈 에이전트에 대한 인증기

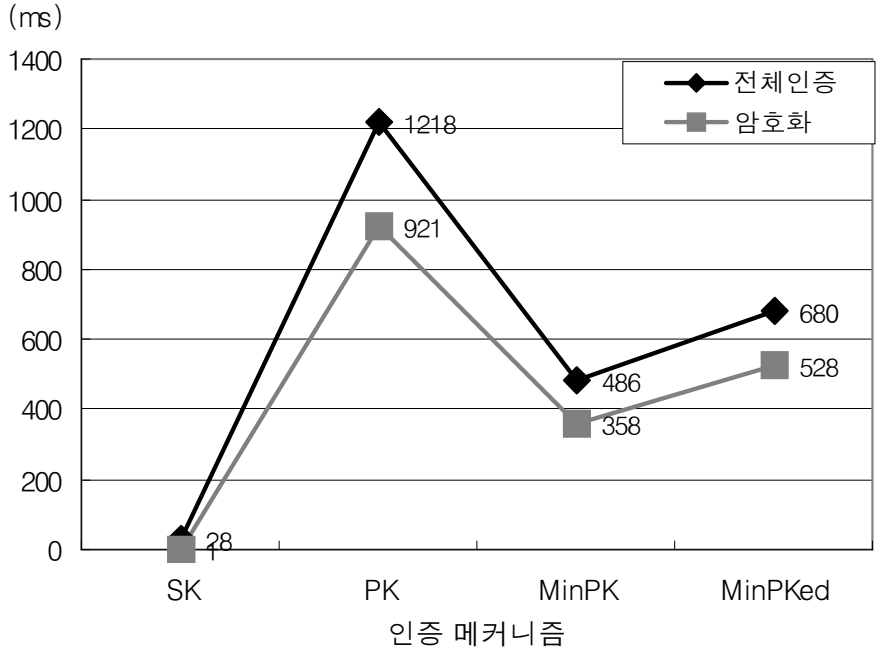
관으로부터 공개키를 받아 인증서를 증명하는 시간이 들지 않기 때문이다. 이와 같이 전자서명을 추가하였음에도 불구하고 MinPKed의 경우에는 이동노드의 등록시간이 86 ms으로 PK에 비하여 61%나 줄었다.

3. 전체 등록시간, 노드 프로세스 시간 그리고 암호화 시간

전체 등록과정에 있어서 이동 노드와 에이전트, 인증기관 사이에 메시지를 주고받는 전달 지연시간을 제외한 시간은 노드 프로세스 시간으로 나타내었다. 노드 프로세스 시간 중 등록 요청, 등록 대답을 생성하는 시간, 이동 노드나 에이전트가 가진 정보테이블을 갱신하는 시간, 난수나 타임스탬프를 검사하는 시간, 아이디를 검사하는 시간을 제외한 시간은 암호화·복호화에 들어가는 주요 계산 시간이다. 계산 비용이 높은 암호화·복호화 과정은 노드의 자원을 대부분 사용하게 되며 이동 노드의 전력 소모를 가속화 시킨다. 키를 사용하여 암호화·복호화 하는 시간은 계산 비용이 높은 작업으로 직접적으로 성능을 좌우하며 많은 작동은 전력 소모를 일으킨다. 인증 메카니즘별 전체 등록 시간과 노드 프로세스 시간은 [그림 19]와 같다. 앞에서 살펴본 바와 같이 순수한 노드 프로세스 시간은 암호화・복호화 시간을 제외한 시간이지만 시뮬레이션 결과를 확인하기 위하여 암호화・복호화 시간을 포함한 시간을 나타내었다. SK에서는 대부분의 등록시간은 노드와 에이전트 사이의 전달 지연시간에 의한 것이다.



[그림 19] 노드 프로세스 시간



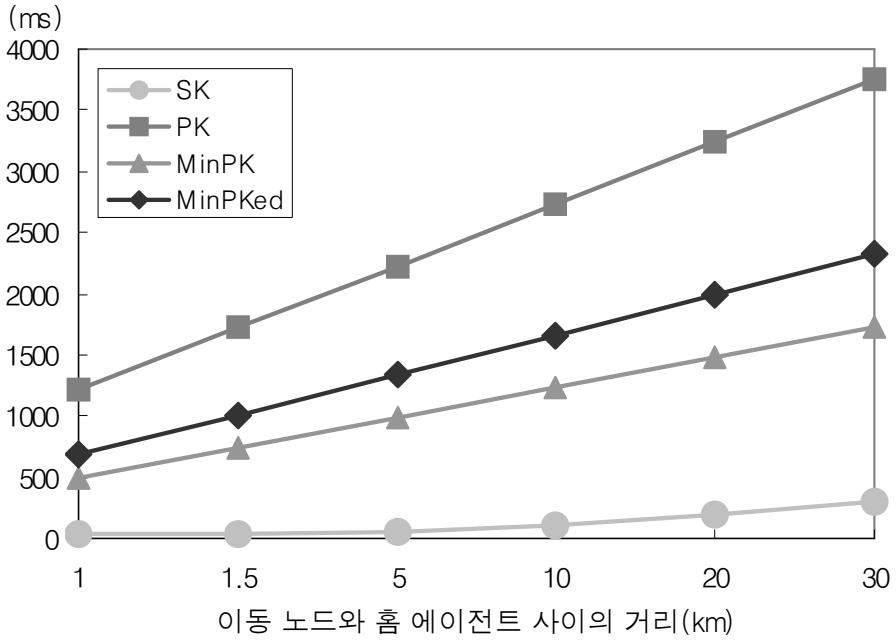
[그림 20] 암호화시간

[그림 20]은 인증 메커니즘별 전체 인증 시간, 암호화 시간을 나타내었다. 비밀키를 이용한 암호화·복호화 시간은 매우 적다. 그러나 PK에서는 공개키를 이용한 암호화·복호화를 하는 시간이 SK에 비하여 1118배나 늘어나서 공개키 과정의 비용이 높다는 것을 다시 한번 확인할 수 있다. 공개키의 과정이 복잡하다는 것 뿐 아니라 PK에서는 암호화·복호화 과정이 여러 번 일어난다. 공개키 이용이 늘어날수록 전체 등록시간에서 차지하는 암호화·복호화 과정이 차지하는 비중이 증가한다. 전체 등록시간에서 암호화·복호화 시간이 차지하는 부분은 공개키 계산 과정이 많은 경우일수록 높다. PK에서 암호화·복호화 시간이 높은 것은 노드와 에이전트사이에 인증과정에서 공개키를 이용하여 인증을 하고, 공개키 사용을 보장하기 위하여 인증기관에서 인증서를 발급할 때 공개키 계산을 하기 때문이다. 결국 전체 등록시간을 증가시키는 중요 요인으로는 공개키 사용으로 인한 계산 비용의 증가

와 공개키 사용에 따른 인증서 발급으로 추가 인증 기관의 공개키 사용이 있으며 전달받는 메시지 수의 증가로 인한 긴 지연시간에 기인한다.

4. 이동 노드의 위치 변화에 따른 전체 등록 시간

다음은 매크로 이동성을 기반으로 한 Mobile-IP를 가정으로 하여 이동 노드의 거리 변화에 의한 인증 시간의 계산이다.



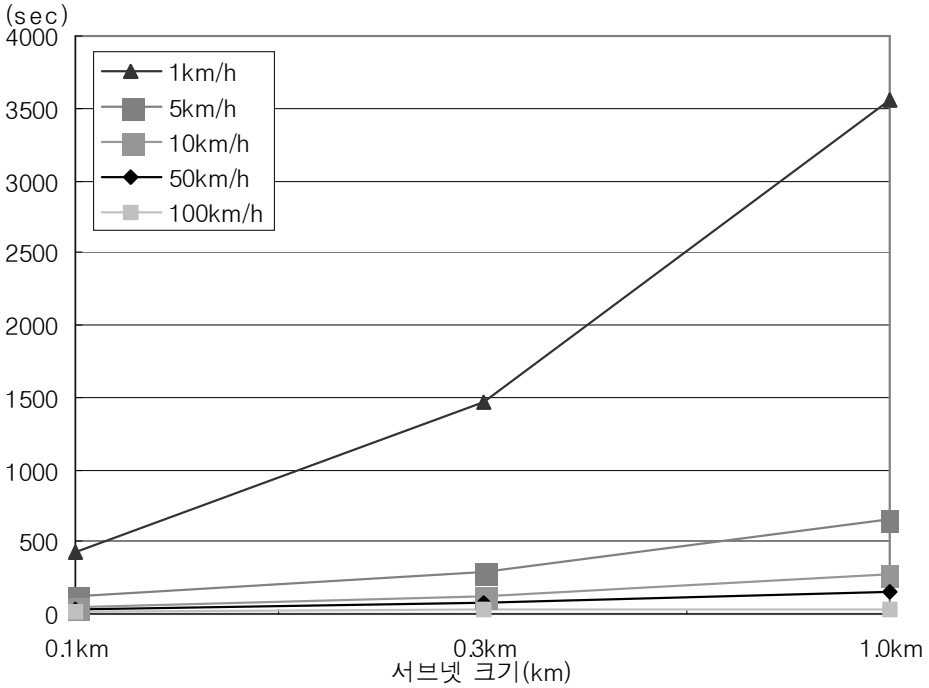
[그림 21] 이동 노드의 위치 변화에 따른 등록 시간

위의 [그림 21]은 이동노드와 홈 네트워크 사이의 거리가 1 km에서 30 km로 변화 할 때 인증에 필요한 시간변화를 보여준다.

먼저 SK의 경우 등록 시간이 11배 증가하였으나 시간은 300 ms으로 매우 짧다. 반면 PK의 경우에는 등록시간이 3.1 배로 증가하였으나 인증시간은 3500ms으로 등록시간의 증가율은 낮지만 시간이 많이 걸린다는 것을 알 수 있다. MinPK의 경우에는 PK의 경우에 비하여 50%이하의 시간이 걸리며 제안한 MinPKed의 경우에도 MinPK보다는 조금 더 걸리지만 PK에 비하면 시간이 훨씬 적게 걸린다. 그러므로 MinPKed의 경우 이동노그가 홈 네트워크에서 멀어질수록 더 효율적임을 알 수 있다.

5. 서브넷 크기와 이동 속도에 따른 실제 적용 가능성

다음은 앞서 살펴본 네 가지의 인증 메커니즘이 서브넷의 크기와 이동 노드가 이동하는 속도에 따라서 실제 어떤 메커니즘을 알맞게 사용할 수 있는가를 살펴보고자 한다.

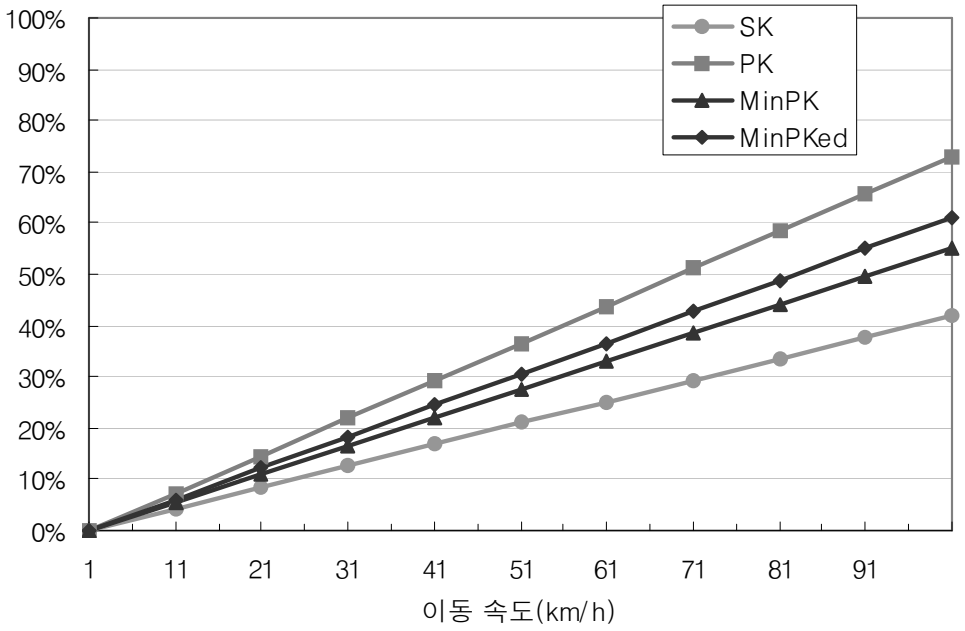


[그림 22] 이동 속도에 따른 서브넷 머무는 시간

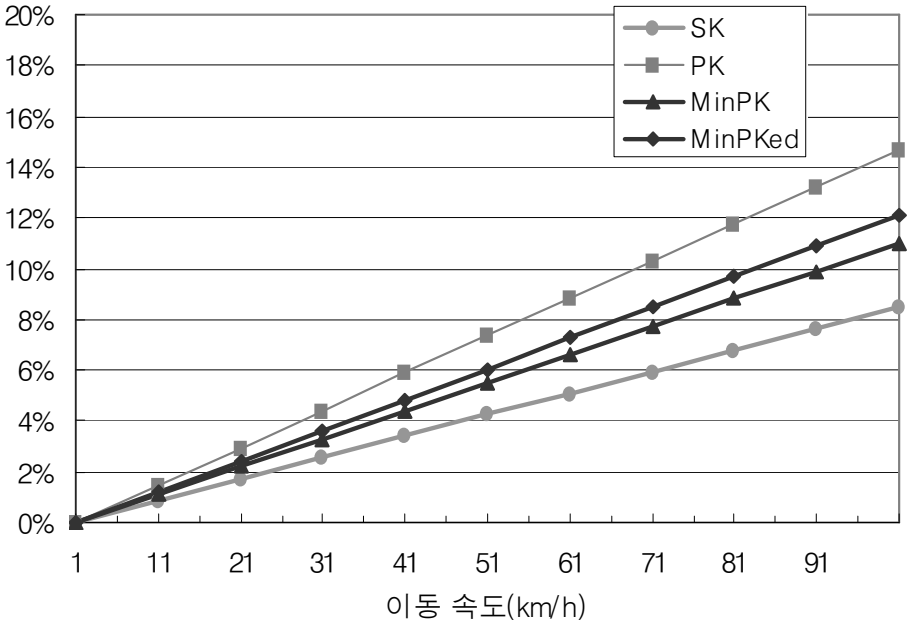
위의 [그림 22]는 이동노드가 이동하는 속도에 따라 해당 서브넷에서 머무는 시간을 비교한 것이다. 서브넷의 크기는 0.1 km 부터 1 km 사이에서 변한다. 이처럼 다양한 시뮬레이션 환경을 기반으로 인증 메카니즘에 따라 전체 서브넷에 머무는 시간 중 등록시간이 차지하는 비율을 살펴 보았다.

[그림 23]에서는 서브넷의 크기가 0.1 km일 때의 인증 차지율이다. 그림에서 보는 바와 같이 전체 서브넷에 머무는 시간에 대한 인증이 차지하는 비율이 크며 이동속도가 빨라짐에 따라 인증이 차지하는 비율은 급격하게 증가 한다. 실제로 Mobile-IP에서 새로운 서브넷에 들어가면 새 위치 정보에 대하여 인증을 받고 데이터그램을 터널링해서 받는데 시간이 오래 걸리므로 인증이 차지하는 비율이 적어야 한다. 그렇지 않을 경우 인증을 받고 터널링 되어 오고 있는 데이터그램을 받기도 전에 또 다른 새로운 서브넷으로 이동하게 되어 인증과 터널링에 드는 오버

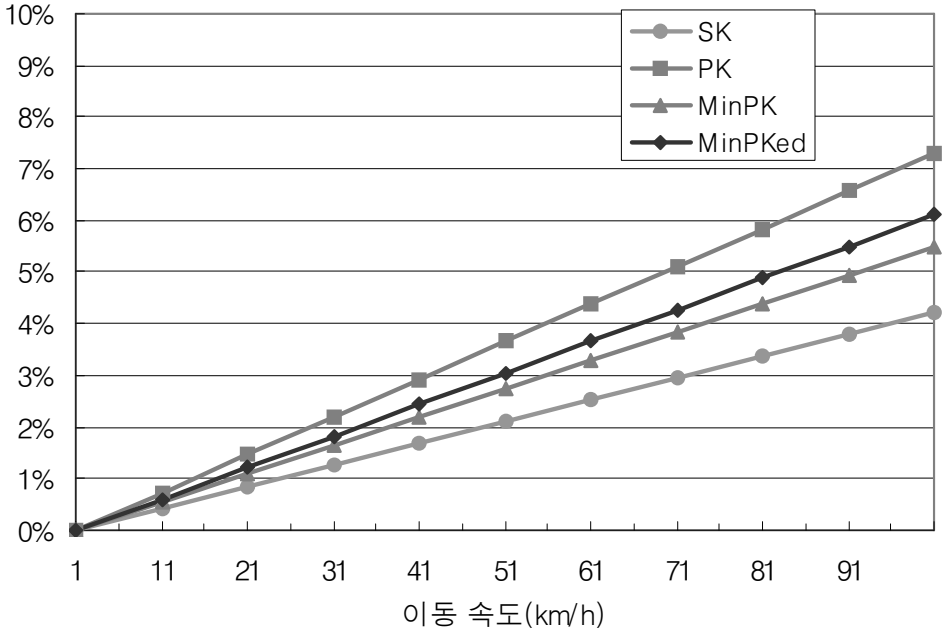
헤드만 지나치게 높아지고 실제로 데이터그램을 전송 받는 시간이 짧아진다. 이 경우에는 인증 시간이 짧은 것이 중요하므로 성능 저하가 가장 적은 SK를 사용하는 것이 바람직하다.



[그림 23] 서브넷 크기 0.1 km일 때 인증 차지율



[그림 24] 서브넷 크기 0.3 km일 때 인증 차지율



[그림 25] 서브넷 크기 1km일 때 인증 차지율

앞의 [그림 24]와 같이 서브넷의 크기가 0.3 km일 경우 20 ~ 30 km/h일 때에는 PK의 경우에도 5% 이내 이므로 사용할 수 있으나 그 이상의 속도로 움직일 경우에는 MinPKed를 사용하여 원하는 서비스를 제공받으면서 성능 저하를 줄이는 방법이 효율적이다. 그러나 [그림 25]와 같이 서브넷의 크기가 1 km일 경우에는 이동 속도가 100 km/h까지 빨라져도 서브넷에 머무는 시간에 대한 인증 차지 비율이 8% 미만으로 유지된다. 실제로 60 km/h로 이동할 때까지는 5% 미만이므로 PK를 사용해도 좋다.

위에서 보는 바와 같이 서브넷의 크가와 이동노드의 이동 속도에 따라 인증메카니즘을 선택적으로 사용할 수도 있다. Mobile-IP에서는 인증에 사용될 메카니즘을 등록시에 선택적으로 사용 할 수 있으므로 이동노드 사이에서 먼저 사용하고자 하는 인증 메카니즘을 적절히 선택하면 된다.

V. 결론 및 향후 과제

M-Commerce는 인터넷의 확장이며 기존의 고정된 PC에 의한 전자상거래의 한계를 넘어 액세스 단말에 있어서 이동성(Mobility)이나 휴대성(Portability)을 부가한 것으로써 무선 인터넷이 가능한 휴대 단말의 증가에 따라 중요성이 부각 되고 있다. M-Commerce는 최종 이용자뿐만 아니라 산업 전반에 지대한 영향을 미칠것으로 전망되며, 이미 소비자들은 광범위한 M-Commerce 서비스를 이용하고 있다. M-Commerce를 구성하고 있는 여러 가지 요소 중에서 보안과 지불은 가장 중요시 되고 있다. 본 논문에서는 이동성을 제공하는 Mobile-IP망의 보안 인증 메카니즘을 제시하였다. Mobile-IP망에서 제공하는 인증 메커니즘 중 기존에 제안되어 있는 방식에 대하여 비교·분석을 하였고, M-Commerce에서 매우 중요한 보안 서비스를 제공하면서 전자서명을 첨가한 최소 공개키 인증 메커니즘을 제시하였다.

시뮬레이션은 네 가지 종류의 메커니즘으로 나누어 구현되었다. 첫번째는 비밀키 기반 인증 메커니즘으로 적은 계산 비용으로 이동 노드에게 적합하고 전체 인증 시간이 짧다는 면에서 효율적이다. 그러나 비밀키의 사용으로 많은 사용자에게 서비스를 제공하기에는 확장성이 떨어지고 외부 에이전트의 보안이 제공되지 않는다는 단점이 있다. 두 번째는 공개키 기반 인증 메커니즘으로 인증 기관을 통한 공개키 사용으로 사용자가 많은 인터넷에서 확장성을 제공하나 이동 사용자가 계산하기에는 부담스러운 공개키 사용으로 현실적으로 구현되기에는 부적합하다. 세 번째는 계산이 복잡한 공개키를 최소로 사용하는 최소 공개키 기반 인증 메커니즘으로 보안을 유지하면서 높은 성능 향상을 보여주었다. 다만 이 방법은 이동 노드가 부인방지 서비스를 제공하지 않기 때문에 보안이 중요한 시스템이 있는 네트워크에 들어가 새로운 위치를 등록시키기에는 그 위치 등록 인증 기능이 부족하다는 단점이 있다.

따라서 본 논문에서는 이동 노드가 전자서명을 함으로써 위치 등록에 대한 부인방지 서비스를 제공하였고 공개키를 최소 사용함으로써 효율성을 유지하기 위하여

외부 에이전트가 보낸 에이전트 광고를 이동 노드가 홈에이전트에게 그대로 전달하여 홈 에이전트가 인증한 내용은 결과를 통해 간접적으로 인증하도록 하였다. 또한, 이동 노드는 홈 에이전트에게 전자서명을 보내고 홈에이전트는 인증기관에 접근하여 공개키의 사실 여부를 확인한 후 전자서명을 증명하도록 하였다. 이동 노드의 전자서명은 자신이 동록한 위치정보에 대한 중요한 부인방지 기능을 제공하여 네트워크 자원 사용을 관리·제어할 수 있도록 하였다. 홈 에이전트의 경우에는 외부 에이전트에게 전자서명을 보내 인증을 받고 이동 노드에게는 MAC를 생성시켜 직접 인증을 받도록 하였다. 그리하여 새로운 위치 등록과정에 대한 모든 참여자에 대한 인증을 하도록 하였다. 시뮬레이션 결과를 통해서 본 논문에서 제안한 인증 메커니즘이 안전하고 효율적으로 작동하는 사실을 확인할 수 있었다. 제안한 인증 메커니증은 보안을 유지하면서도 공개키 사용을 최소로 사용하여 등록 중 필요한 인증 과정을 수행할 수 있었고, 특히 이동 노드에 전자서명을 첨가함으로써 보안이 중요한 시스템에서 위치 등록에 사용될 수 있는 방안으로 기능을 향상시켰다. 또한, 이동 노드에서 수행된 계산 시간을 감소시켜 이동 노드의 전력 소모를 줄였고 이동 노드가 가진 자원 제약의 문제를 해결하였다. 이런 방법으로 제안된 인증 메커니즘은 Mobile-IP가 가진 이동성이란 특성에 적합하도록 구성되었으며 이동 노드에서 위치 등록에 대한 부인방지 서비스를 제공함으로써 보안이 중요한 시스템에서 필요한 서비스를 충분히 제공함을 확인하였다.

향후 연구 과제로는 많은 사용자가 Mobile-IP를 이동하는 환경에서 성능을 향상시키기 위한 다양한 구현 방법이 연구되어야 할 것이다. 많은 사용자가 인증 기관에 동시에 접근하는 경우에 인증 기관의 성능에 따라서 인증서를 발급받고 확인하는 시간이 달라질 것이다. 그 외에도 이동 노드에서 계산을 최소로 줄이기 위해서는 이동 장치에서 많이 사용되고 있는 불균형 공개키 기반 알고리즘을 적용해보아 성능 향상이 가능한지 연구되어져야 할 것이다. 더 나아가 전체 인증 시간, 핸드오버, 데이터그램의 전송시 보안 부분을 연결하여 연구할 경우 전반적인 Mobile-IP의 구현상 최적화 방향을 찾아볼 수 있을 것이다.

참 고 문 헌

[1] M. Jackobsson and M.Yung, "Revokable and versatile electronic money", 3rd ACM Conference on Computer and Communications Security, pp. 76-87, 1996.

[2] Bryant, W., "Designing an Authentication System : A Dialogue in four Scenes," Project Athena Document, February 1988.

[3] Security Architecture for the Internet Protocol(RFC 2401), IETF, ftp://ftp.isi.edu/in-notes/rfc2401.txt

[4] Uyless Black, Advanced Internet Technologies, Prentice Hall, 1999.

[5] 이재규 외 3인, "전자상거래 원론", 범영사, 2000.

[6] 박정서, "성공적인 M-커머스 비즈니스 전략", 이비컴, 2001. 6.

[7] Durlacher, "Mobile Commerce report", 1999. 11.

[8] "M-Commerce 시장과 기술현황", Mobile Business, 2001. 7.

[9] Rhee. Man-Young, "CDMA cellular Mobile Communications and Network Security," Prentice-Hall, N, 1998.

[10] Forester Research, "Mobile Payment's Slow Start" May-2001.

[11] J. Camenisch, M. Piveteau and M. Stadlerr, "An Efficient Fair Payment System", proceedings of 3rd ACM Conference on Computer Communications Security, ACM press, pp.88-94, March 1996.

[12] Rhee. M.Y, "Cryptography and Secure Communications", McGraw-Hill, 1993.

[13] 최길환, 신민화, 배상현, "분산 웹 환경에서 이동 에이전트 보안 모델에 의한 전자서명 메카니즘", 한국정보처리학회 논문지 10-C(6), pp.787-792, 2003. 10.

[14] Denning, d., "Protecting Public Keys and Signature Keys," Communications of the ACM, Aug 1981.

[15] Diffie, W., "Authenticated Key Exchange and Secure Interactive

Communication," Proceedings of SECURICOM' 90, 1990.

[16] Rhee, Man-Young, "Cryptogtaphy and Secure Communications," MCGraw-Hill, New York, 1994.

[17] Kravitz D. and I. Reed, "Extension of RSA Cryptiostructure : A Galois Approach," Electronics Letters, v. 18, Mar 1982, pp.255-256.

[18] 염흥열, 홍기융, "공개키 기반 구조", 통신정보보호학회 학회지, 제8권 3호, pp.5-18, 9, 1998.

[19] Christan F. Tschudin, "Mobile Agent Security," Available form authors, February 1998.

[20] Stallings. W, "Network and Internetwork Security, Prentice Hall, 1995.

[21] Brands, S. "Rethinking Public Key Infrastructures and Digital Certificates," Cambridge, MA: MIT Press, 2000.

[22] Booz-Allen and Hamilton Inc. "Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile", January. 1999.

[23] Housley, R. and P. Hoffman. "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP." Internet Request for Momments 2585, May. 1999.

[24] 이종후, 류재철, "무선인터넷 환경에서 전자상거래를 위한 보안 솔루션", SK Telecommunications Review 제10권, 1호, pp.213-237, 2000. 1.

[25] 박기준, "무선인터넷 보안 표준, WPKI 시스템 구축 실전", 프로그램세계, pp.19-25, 2002. 3.

[26] RSA Laboratory, RSAREF Demonstration Program, http://www.geocities.com/SiliconValley/Network/2811/algo/rsa/rsaref20.zip, 1991.

[27] 이재일, "무선인터넷을 위한 PKI 구축", 제5회 정보보호 심포지엄, 한국정보보호센터.

[28] ITU Rec. X.509, "The Directory : Authentication Framework, Information

Technology - Open Systems Interconnection", http://www.itu.int, Nov. 1993.

[29] C. Perkins, "IP Mobility Support," RFC2002, http://www.ietf.org/rfc/rfc2002.txt, 1996.

[30] Maurizio Dell'Abate, Martino De Marco, Vittorio Trecordi, "Performance Evaluation of Mobile IP Protocols in a Wireless Environment," Proceedings of the 1998 IEEE International Conference on Communications, V. 3, pp.1810-1816, 1998.

[31] Charles E. Perkins, "Mobile IP," IEEE Communication Magazine, pp. 84-99, May. 1997.

[32] J. Williams, Bots and other Internet Beasties, Samsnet., 1996.

[33] S Jacobs, "Mobile IP Public Key Based Authentication, "http:..search.ieth/org/internet-drafts/draft-jacobs-mobileip-pki-auth-0.1.txt, 1999.

[34] Vipul Gupta, Abhijit Dixit, "The Design and Development of a Mobility Supporting Network," ISPAN96, 1996.

[35] Charles P. Pfleeger, Security in Computing Second Edition, Prentice Hall, 1997.

[36] R. Rivest, "The MD5 Message-Digest Algorithm", FRC 1321, April 1992.

[37] Berson, T. "Diferential Cryptanalysis Mod 232 with Applications to MD5," Proc. Eurocrypt '92, May. 1992.

[38] Mihir Bellare, Phillip Rogaway, "The Exact Security of Digital Signature - How to Sign with RSA and Rabin" Proceedings of the Advanceds in Cryptology Eurocrypt 96, pp. 309-416, 1996.

[39] Digital Certificates/Applied Internet Security, Jalal Feghhi, Peter Williams, Addison-Wesley, pp.127-161.

[40] Radia Perlman, "An Overview of PKI Trust Models," IEEE Network, pp. 38-43, Nov./Dec. 1999.

[41] Camenisch. J., U. Maurer, and M. Stadler. "digital Payment Systems with Passive Anonymity-Revoking Trustees." Computer Secutity - ESORICS 96. pp.33-43.

[42] William Stallings, Data and Computer Communications Fifth Edition, Prentice Hall, 1997.

[43] Janathan T. Moore, Mobile code Security Techniques, Available from authors, May 1998.

[44] Colin Boyd, Anish Mathuria, "Key Establishmenet Protocols for Secure Mobile Communications : A Selective Survey,"Information Security and Privacy(ACISP98), Vol.1438, pp 344-355, 1998.

[45] J. E. White, "Telescript Technology : The Foundation for the Electronic Marketplace," General Magic White Paper, from Internet, http://www.genmagic.com/Telescript/WhitePapers/, 1994.