차세대 이동 통신을 위한 PKI 기반의 이동 보안 구조 연구†

중앙대학교 구자범 · 김관연
한국정보보호진흥원 이재일 · 박세현

1. 서 론

최근 몇 년간 IMT-2000에 관한 활발한 연구와 개발로 이제 상용화를 앞두고 있고, 현재 3G와 4G 망 구조의 윤곽이 어느 정도 드러나고 있어 통신의 역사에 있어 매우 중요한 시점으로 예측되고 있다[1~2]. 차세대 이동통신인 3G와 4G 망에 대한 연구는 무엇보다도 "양질의 멀티미디어 서비스"에 초점을 맞추고 있어 통신시스템의 하드웨어적 기술뿐만 아니라 서비스가 제공하는 내용(contents)의 중요성이 부각되고 있다[3]. 차세대 이동 통신 시스템에서 요구되는 다양한 서비스를 제공하기 위한 연구 중의 하나가 All-IP 구조에 의해 기존의 다양한 소프트웨어를 수용하는 방법이다[4~5]. All-IP 구조는, 특히, 현재 다양하게 존재하는 이동 통신 인터페이스를 하나로 통합하기 위한 핵심 구조로 그 중요성이 부각되고 있다[6]. 본 논문에서는 이러한 All-IP 기반의 *Open Mobile Communication Environment* (개방적 이동 통신 환경)에서 보안 구조상의 취약점을 논의하고, PKI(Public Key Infrastructure)를 기반으로 한 새로운 보안 구조를 제안하여 문제점들을 해결하고자 한다. 표 1은 3G 시스템, 802.1x를 보안구조로 한 무선랜, 그리고 본 논문에서 제안한 이동 보안 구조의 보안적 요소들을 비교한 것이다.

차세대 이동 통신의 향상된 시스템 · 네트워크 자원을 바탕으로 현재 유선망에서 제공되고 있는 수많은 애플리케이션들이 차세대 이동 통신 기반에서 이루어질 것으로 예측되며, 특히 인터넷 뱅킹, 증권거래, 전자 지불 · 결제 등은 무엇보다도 중요한 응용분야가 될 것으로 기대된다. 이러한 전자결제 관련 서비스는 이용자 확인과 인증 등의 보안 기능이 매우 중요하며, 이를 위하여 현재 많은 연구와 개발이 진행 중인 PKI가 중추적인 역할을 수행할 것으로 기대된다. 따라서 본 논문에서는 차세대 이동 통신에서 PKI를 이용한 보안 구조가 갖는 장점과 함께 여러 시나리오별로 성능 분석을 통한 기능적 실용 가능성을 제시하고자 한다.

지금까지 제안된 차세대 이동 통신의 특징적인 요소를 다음과 같이 요약할 수 있다[7~8](2장 참고).

① 다수의 네트워크 관리자 및 서비스 제공자
② 국가간, 지역간 광대역 로밍(Global roaming)
③ 다중 인터페이스
④ All-IP 구조
⑤ 향상된 시스템 성능과 네트워크 자원

표 1 이동 무선 네트워크 구조들의 보안 요소 비교

	3G 시스템	무선랜 (802.1x)	제안된 이동 보안 구조
구성환경	폐쇄적 환경	폐쇄적 환경	개방적 환경
Secure Association	가정	가정	지원
상호 인증	AP↔MT 사이만 지원	지원안함	단대단 보안 인증 지원
인증 프로토콜	PPP, RADIUS	EAP	Roaming PKI
이동성 지원	지원(Mobile IP 사용)	지원안함	지원(Token 사용)

상기 요소들을 본 논문에서는 통합 지칭하여 *Open Mobile Communication Requirements* (OMCRs) 이라고 정의한다. 즉, MT(Mobile Terminal)가 보다 다양한 네트워크 환경에서 서비스를 받

† 본 연구는 한국과학재단 목적기초(R01-2001-00303), 중앙대학교학술연구(2001년도) 및 한국정보보호진흥원의 지원에 의한 결과임.

게 되고, 따라서 '서비스 질의 향상과 서비스 종류의 다양화'가 기대된다. 그러나 다양성으로 인한 복잡성의 증대와 All-IP 구조의 채택은 기존의 'cell' 기반의 이동 통신망에서 '폐쇄적 환경(closed environment)'에 의해 어느 정도 보완되던 요소(entity)들이 '개방적 환경' 하에서 외부로 노출되어 유선망에서 존재하던 각종 취약점과 공격방법들, 예를 들면 *Piggy-backing, Snooping, Crosstalk, Rogue Bridge*등이 그대로 이동 통신 시스템에 적용된다는 의미가 된다. 따라서 *Always Best Connected (ABC)*와 *Any Where, Any Time, Any Service*라는 표현으로 대표되는 차세대 이동 통신을 고려할 때, 다음과 같은 요소들을 고려한 새로운 보안 요구사항이 OMCRs에 추가될 필요성이 있다.

- *상호 인증 (Mutual Authentication)을 지원하는 Secure Association*: MT가 매우 다양한 SD(Serving Domain)과 지속적인 상호 인증이 가능해야 신뢰성을 갖고 서비스를 제공받을 수 있다.
- *네트워크 도메인간의 보안*: IP 기반의 네트워크를 통해 SD과 HD(Home Domain)간의 통신 접속 정보가 전송되므로 암호화에 의해 기밀성을 유지할 수 있어야 한다.
- *확장 가능한 과금체계*: 광대역 로밍 측면에서 어느 곳에서든지 서비스를 받을 수 있기 위해 유동적인 과금서비스(신원확인, 부인방지 등)가 가능해야 한다.

기존의 이동 통신 시스템 및 무선랜 등의 폐쇄적 환경에서는 상기 요소들을 대칭키 방식의 보안 구조를 통해서 부분적으로 제공하였다[9~10]. 이러한 이유는 속도 면에서 대칭키 방식이 주는 장점과 함께 기존의 시스템이 폐쇄적 환경이라는 점이 대칭키 방식의 단점, 즉 키 관리의 취약점을 보완해 주는 역할을 하여, 최적의 성능을 내면서도 보안성을 유지하는 것이 가능했기 때문이다. 또한, 3G나 4G 시스템에서는 *Secure Association*을 가정하고 상호 인증을 수행한다. 이러한 *Secure Association*의 과정은 그림 1과 같은 예에서 보듯이 다음의 순서로 진행된다.

Step① : 새로운 사용자 등록정보가 DC(Domain controller)로 전송

Step② : HE로부터 사용자 인증서 획득

Step③ : 사용자 인증서 검증 및 사용자 권한 부여

Step④ : 새로운 *Token* 생성 및 전송

Step⑤ : *Secure Association* 종료 후 DC에서 테이블 갱신

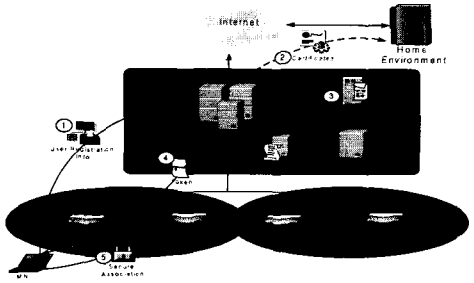


그림 1 Secure Association 과정의 예

3G나 4G 시스템에서는 이러한 *Secure Association*을 위해 *Association Local Agent*를 사용한다. 그러나 *Local Agent*는 국가간, 지역간 핸드오버(handover) 시 시간적 공간적 제약요소가 될 수 있다. 따라서 *Logical Agent*가 필요하며 로밍이나 핸드오버 등을 고려하여 시스템 및 네트워크 자원의 적절한 조화를 위해 *Secure Association & Authentication*을 On-line에서 동시에 수행하는 구조가 필요하다. 무선랜은 802.1x를 적용하더라도 여전히 *Secure Association*을 가정하고 인증 절차를 수행하게 되나, 로밍에 대한 데이터 링크상의 키관리 체계와 같은 보안 서비스를 위한 구조적 결함으로 단대단 상호 인증(Peer-to-Peer Mutual Authentication)은 지원되지 않는다.

또한 3G나 4G 시스템과 무선랜이 연동하게 되면, 더욱 개방적 환경이 형성되어, 단대단 상호 인증이 가능하지 않고 단순히 상위 계층에 의존함으로써 데이터 링크 계층간의 보안 취약점이나 지연을 도출시키며, OS에 독립적인 보안구조가 가능하지 않을 수 있다. 더우기 개방된 환경 하에서 MT는 수많은 네트워크 도메인의 경계를 이동해 가면서 서비스를 받아야 하고, 때로는 다른 국가에서 서비스를 받는 경우도 있을 수 있다. 이 때 도메인 간 보안 연속성을 위해 임의의 노드들 간의 인증이 필요하게 되므로, HD과 SD간에 긴밀한 상호신뢰 관계를 지속적으로 보장하는 것이 필요하다. 따라서 본 논문에서는 Beyond IMT-2000과 같은 차세대 이동통신의 광대역 로밍 환경에서 키관리 문제를 해결하고 다양한 보안 서비스를 제공하기 위해 PKI 기반의 새로운 보안 구조를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 이동 통신의 환경적인 특징과 보안 요구사항을 바탕으로 하여 이동 통신 시스템 모델을 설정하였다. 3장에서는 PKI 모델에 대한 간략한 설명과 함께 본 논문에서 사용될 *Trust*와 *Token*의 개념을 설명하였다. 4장에서는 본 논문에서 제시하는 보안구조의 세부 사항 및 인증과 핸드오버 과정을 상세히 설명하였으며, 제시된 보안 구조의 성능평가를 5장에서 제공하고, 6장에서 결론을 맺었다.

2. 배 경

2.1 차세대 이동 통신 시스템

그림 2는 차세대 이동 통신 시스템 구조를 보여준다. 이 구조의 개방된 환경을 이루는 다수의 서비스 제공자, 다중 인터페이스, 그리고 All-IP 구조와 함께 이러한 환경이 갖는 보안상 문제점 및 특징에 대한 설명은 다음과 같다.

2.1.1 다수의 서비스 제공자 및 광대역 로밍

하나의 도메인은 하나의 서비스 제공자에 의해 서비스되는 지역과 그 지역에 포함된 서비스 노드들이 포함된다. 도메인의 범위는 매우 다양해서 작게는 사무실 단위나 밀집 지역이 될 수도 있고, 학교나 기업이 될 수 있으며 크게는 국가 단위가 될 수 있다. MT는 이러한 다양한 도메인 사이를 이동하면서 서비스를 받아야 하므로, 임의의 개체와 상호 인증이 가능해야 하고, 따라서 기존의 대칭키 방식을 사용할 경우 키 분배 및 관리 문제가 심각해진다. 특히 이질적인 서비스 제공자에 의해 운영되어 각각의 도메인은 매우 다양한 보안 정책을 갖게 되므로, MT와 도메인 사이에서 뿐 만 아니라 도메인과 도메인 사이에서도 매우 복잡한 시스템 및 보안 연동구조가 필요하다.

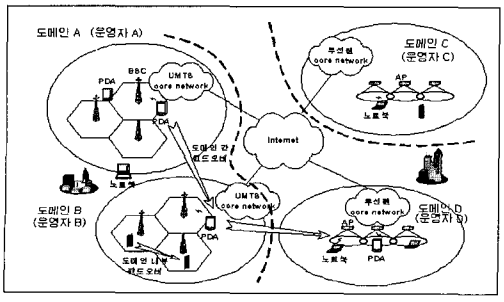


그림 2 개방적 이동 통신 환경

2.1.2 다중 인터페이스

그림 2의 개방적 환경은 하나의 표준 인터페이스를 기반으로 하는 것이 아니라 매우 다양한 인터페이스(Bluetooth, 무선랜, UMTS등)를 혼용하는 구조이다. 이렇게 표준들 간에 다양한 보안 구조(특히 *Access Network*에 대한 보안 구조의 경우)를 제시하고 있어 상호간의 연동을 할 경우에 공개적 환경에서 계층간 보안이 보장되지 않아서 결국 상위 응용계층에 의존하게 되고 보안의 일관성과 확장성(scalability)이 부족해져서 링크 간 *encapsulation*등이나 보안성이 취약한 공유키 쌍을 사용하게 되어 *snooping*등이 가능한 문제를 야기 할 수 있다. 따라서 실질적인 단대단 보안이 불가능하게 된다.

2.1.3 All-IP 구조

All-IP의 수용으로 인해 모든 기기들이 IP를 가지게 되어 기기간의 인증이 필요해져 다양한 기기들 간 보안연동성과 같은 네트워크 관리 측면이 계속 복잡해질 것으로 예상된다. 기존의 보안 구조는 HD과 SD이 하나의 망 운영자에 의해서 운영되는 형태이기 때문에 별다른 인증 시스템 없이 기능적 *Trust* 관계를 최소한 유지할 수 있었다. 그러나 차세대 이동 통신에서 All-IP 네트워크를 수용함에 따라 이러한 중요 정보들이 더욱 다양한 네트워크 기점들을 통해서 전달 될 수 있으며, 더욱이 유선망에서 존재하던 각종 취약점과 공격방법들, 예를 들면 *Piggybacking, Snooping, Crosstalk, Rogue Bridge*등이 그대로 이동 통신 시스템에 적용되므로 그에 따른 대비방안이 필요하다.

2.2 이동 통신 시스템의 보안 요구 사항

이동 통신에서의 보안 요구사항은 유선망에서 제공될 수 있는 것과 동일한 수준의 보안 서비스를 제공하는 것에 있다고 할 수 있다. 그러나 공개된 환경에서 물리적 보안의 취약점 때문에 이동 통신 시스템에서는 보안적으로 적절하고 시스템적으로도 효율적인 인증, 기밀성, 권한 부여, 과금, 접근 제어 등의 보안 서비스가 제공되어야 한다. ITU-R에서는 이러한 보안 서비스를 몇 가지 분류로 재편성하여 설명하고 있다. 다음은 그에 대한 요약이다.

- 서비스 관련 요구사항: 간단한 조작에 의해서 보안 서비스의 사용이 가능해야 하고, 이로 인해 추가로 생기는 콜 셋업(call set-up) 시간을

최소화해야 한다. 그리고 로밍 시에도 보안을 유지할 수 있어야 한다. 또한 다중 도메인에서 사용가능 해야 하고, 자원의 사용을 최소화할 수 있어야 한다.

- 접근 관련 요구사항: 시스템을 악용하기 위한 목적으로 사용자나 서비스 제공자의 명의를 도용할 수 있는 가능성을 최소화해야 한다.
- 이동단말 관련 요구사항: 단말을 분실한 경우에 대한 대비책이 있어야 하고, 복제한 단말을 사용할 수 없도록 해야 한다.
- *Association* 관련 요구사항: HD 관리자가 과금 등의 목적으로 올바른 사용자임을 확인하는 것이 필요하다.

차세대 이동 통신 시스템은 이러한 기본적인 요구사항 이외에 앞에서 서술한 네트워크 노드들 간의 상호 인증, 심층 네트워크 데이터 전송의 기밀성, 그리고 확장 가능한 과금체계 등이 추가로 요구된다. 이러한 다양한 요구 사항들을 수용하기 위해서 본 논문에서는 PKI 기반의 보안 프레임워크인 *Mobile PKI*를 제안한다.

2.3 Mobile PKI 시스템

그림 3은 앞에서 설명된 보안 요구사항들을 바탕으로 간략화한 이동 통신 시스템 구조와 이러한 구조에서 각 개체들 사이에 필요한 보안 서비스를 나타낸 것이다. 이 모델은 그림 2의 차세대 이동 통신 시스템 구조를 도메인 구조로 일반화한 형태이다. 도메인은 MT에 직접적인 서비스를 제공해주는 SD과 MT의 인증 정보와 과금 등에 대한 관리를 하는 HD으로 나누어진다. SD은 다수의 노드로 구성되는데, 간략화를 위하여 무선 인터페이스를 제공하는 AP를 제외하고 나머지의 SD 핵심 노드들을 통합하여 DC라고 칭한다. 따라서 DC는 MT에 대한 위치 관리, 과금, 인증을 위한 기능을 포함하고 있어 GSM/UMTS의 GGSN (또는 SGSN)[8, 9] 그리고, *Mobile IP*에서의 FA(Foreign Agent)와 유사한 기능을 수행한다. MT의 정보는 HD에서 관리하기 때문에 과금, 위치 관리를 위한 노드 등이 HD에 포함되어 있다. SD의 DC와 구분하기 위해서 본 논문에서는 HD의 핵심 노드들인 DC와 AAA(Authentication, Authorization, Accounting)을 통합하여 HE(Home Environment)로 명칭 한다. 각각의 도메인은 인증 경로 상에서 HE, MT 또는 DC의 상위 노드인 서비스 제공자에 의해 운영된다. 하나의 서비스 운영자는 여러 개의 도메인을 제공할 수 있다. 핵심망(Core network)은 All-IP 구조로 되어 있고, 과금 정보나 위치 정보 등 MT를 관리하기 위해서 SD과 HD 사이의 제어 정보는 모두 IP 네트워크를 통해서 전달이 된다. MT는 서로 다른 서비스 제공자에 의해서 운영될 수 있으며 매우 다양한 보안 정책을 갖고 있는 SD 사이를 핸드오버하면서 서비스를 받게 된다.

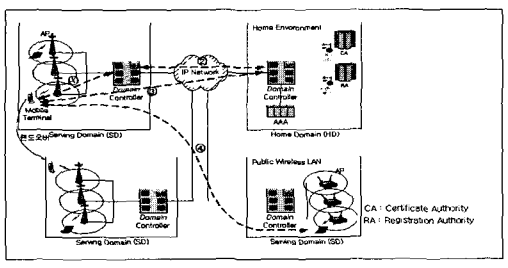


그림 3 Mobile PKI 시스템 모델

이동 단말이 단대단 통신을 하기 위해서는 그림 3에서 다음과 같은 여러 경로에 대한 신뢰성 확립이 필요하다.

- MT↔SD 간의 상호 인증 ①
- HE↔SD 간의 상호 인증 ②
- HE↔MT 간의 상호 인증 및 과금 ③
- 사용자 노드간의 상호 인증 ④

핸드오버가 이루어질 경우 이러한 과정을 반복한 이후에 상대방과 통신을 재개할 수 있으므로 인증과 암호화·복호화의 반복에 의해 자원이 낭비된다. 따라서 본 논문은 MT가 도메인 내에서나 도메인 사이를 이동할 때 *Mobile PKI* 기반으로 상호 인증 및 신뢰성을 향상함과 동시에 효율적으로 시스템 및 네트워크 자원을 관리하는 방안으로 *Trust*와 *Token*을 제안한다.

3. Mobile PKI 기반 Trust와 Token

3.1 X.509 model

최근 인터넷 보안의 가장 중요한 이슈가 되고 있는 것 중 하나가 PKI이다. PKI는 전자상거래에 필수적인 전자서명을 비롯하여 공개키를 사용하는 모든 보안 문제에 대한 신뢰성 있는 해답을 제시하기 위한 보안 서비스의 전반적 인프라 개념이라고 할 수 있다[12].

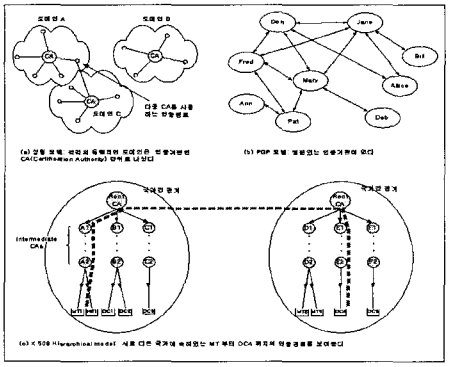


그림 4 PKI 모델

X.509에서 제안된 구조는 인증기관들이 계층적 구조를 갖는 형태이다(그림 4(c) 참고). 그 외에 일반적인 PKI 모델은 그림 4와 같다.

그림 4(a)는 현재 유선망에서 인터넷 보안을 위해 주로 사용되고 있는 성형 구조의 독립된 도메인 형태를 갖는 모델이다. 성형 구조는 여러 개의 인증기관이 존재하고, 각각이 발행하는 인증서가 웹 브라우저에 저장되어 있거나 새로이 추가할 수 있는 형태로 되어 있다. 이 구조의 가장 큰 특징은 인증기관들이 서로 완전히 독립되어 있기 때문에 단대단 통신의 보안을 위한 신뢰성 확립(상호 인증)을 위해서는 두 개체 모두 동일한 인증기관으로부터 인증서를 발급 받아야 한다는 것이다. 그림 4(b)는 PGP(Pretty Good Privacy)에서 사용된 모델이다. PGP의 인증 모델은 PGP의 성공과 더불어 많은 사용자를 확보하고 있기는 하지만, 체계적인 관리 부족으로 인하여 확장성에 문제가 발생하기 때문에 소규모의 그룹에만 적당하다. 그림 4(c)는 X.509 표준에서 제시하고 있는 PKI 모델이다. X.509 표준에서 제안한 모델은 계층적 구조를 갖고 있어 최상위의 인증기관부터 최하위의 사용자까지 인증 경로와 상·하위 개체간의 관계가 명확하다. 그리고 인증기관이 인증 도메인(보안 도메인)을 구성하는 주체이므로 X.509의 계층 구조를 이용하여 다양한 인증 정책을 펼 수 있는 장점이 있다. 이러한 계층 구조는 또한 차세대 이동통신망과 같은 개방 환경의 다중 도메인 구조에서도 적합한 구조이나, 그림 4(c)에서 보듯이 MT와 HE는 동일한 CA의 하위 노드이고, DC까지의 인증 경로는 매우 다양하게 존재할 수 있다. 따라서 본 논문에서는 로밍과 개방 환경에 적합한 X.509기반의 새로운 보안구조로 *Trust*와 *Token* 방식을 제안하며 구조적 복잡성에 의한 성능 저하를 최소화 하였다.

3.2 Trust와 Token

본 절에서는 본 논문에서 제안하는 *Mobile PKI*의 핵심 요소인 *Trust* 와 *Token*에 대해 설명한다. *Trust*와 *Token*은 X.509의 계층적 PKI 모델을 기반으로 하여, 차세대 이동통신에서 빈번히 발생할 광대역 로밍 문제와 이에 따른 AAA 실현 시 자원의 효율적 활용성을 위한 새로운 보안구조의 구성요소이다.

3.2.1 Trust

공개키 방식의 보안 구조에서는 인증과 권한부여가 가장 큰 목적이며, 특히 공개키-개인키 쌍에 대해서 상대방이 해당 개인키를 소유하고 있는지에 대한 확신이 중요하다. 이러한 것을 해결하기 위해 PKI 인증서와 인증 경로가 이용된다. 상대에 대한 *Trust*가 생성되었다는 것은 상대방에 대해 신분을 확인(identification)하고 인증 경로를 따라서 인증서를 검증하여 올바른 요소임을 확신하고, AAA 조건을 만족할 수 있는 상황이 되었다는 의미이다.

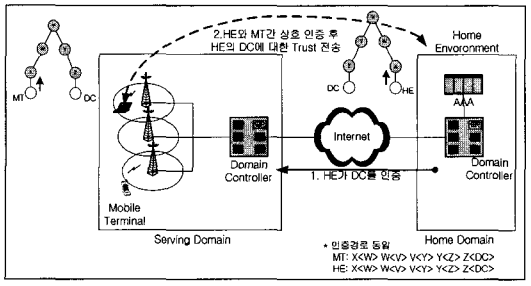


그림 5 간접적인 Trust 생성 과정

그림 5는 본 논문에서 사용하는 모델과 PKI 계층 구조와의 관계 및 *Trust* 생성과 전달에 대한 설명을 위해서 MT와 HE가 DC에 대해 인증하는 과정을 보여준다. 여기서 MT, HE, DC간의 인증 경로는 MT가 어떠한 DC에 위치해 있는가에 따라서 유동적으로 변화되며 MT와 HE가 DC를 인증하기 위해서는 DC까지의 인증 경로를 따라 인증해야 한다. 본 논문에서는 MT의 로밍과 자원을 고려하여 MT가 직접 DC에 대한 *Trust*를 생성하지 않고, HE를 통해서 간접적으로 생성하는 방식을 이용한다. MT와 HE는 동일한 CA로부터 인증서를 발급 받았으므로 이들 간의 상호 인증은 비교적 쉽게 이루어지며 HE와

MT가 DC에 대한 *Trust*를 생성하기 위한 과정이 동일하다는 점을 이용하여 이동 보안구조를 최적화한다. HE는 DC에 대한 *Trust*를 생성하고 이것을 암호화하여 MT로 전달한다. HE의 DC 역시 MT와 HE에 대한 *Trust*를 생성하는데, 이것은 특히 MT가 이동하여 인접한 도메인으로 넘어가는 경우 새로운 도메인의 DC가 MT와 HE에 대해 새로운 *Trust*를 생성하지 않고 이전의 DC에서 생성된 *Trust*를 전달받아서 사용하는 방식으로 구현된다.

3.2.2 Token

본 논문에서 제시한 이동 보안구조를 보면 DC가 MT에 대해 *Trust*를 생성한 이후에 도메인 내에서의 확인과 도메인간의 핸드오버 지원을 위해서 MT에게 *Token*을 부여하게 되고 도메인 내에서 MT는 AP 사이를 이동하면서 서비스 받는데, 이때 DC가 MT의 위치 정보를 수정하고 서비스하기 위한 목적으로 *Token*을 사용한다. 제시된 이동 보안구조의 *Secure Association* 과정에서 PKI를 이용하여 인증하는 과정을 그대로 적용할 경우, 보안성 측면에서 IEEE 802.1x나 3GPP(3rd Generation Partnership Project) [10]와 같은 표준안에서는 해결하지 못한 종합적 보안문제를 해결한 AAA를 지원할 수 있는 좋은 방안이 될 수 있다. 그러나 MT의 이동성을 고려할 경우 MT가 도메인 내에서 이동 할 때 또는 새로운 도메인으로 이동 할 때마다 PKI 인증에 의한 *Secure Association* 과정을 진행하는 것은 많은 시스템·네트워크 자원을 필요로 하게 된다. 따라서 본 논문에서는 도메인 내에서의 핸드오버가 있을 때는 MT와 DC간의 *Token* 교환으로 PKI 인증을 대신하는 방식을 제안한다. 도메인간의 이동이 있는 경우에는 이전의 DC가 생성한 *Trust*와 MT가 갖고 있는 *Token*을 이용하여 DC에서 인증하는 방식을 제시한다. *Token*은 MT와 DC간에 임시적인 확인 목적으로 사용되므로 *Nonce*를 이용한다.

Token 생성과 활용에 관한 절차는 4장에서 설명하며, 표 2는 *Trust*와 *Token*에 관련된 기호의 정의이다.

4. Token과 Trust를 이용한 이동 보안 절차

이 장에서는 3장에서 제안된 계층적 *Mobile PKI* 모델과 *Trust* 및 *Token* 방식을 이용한 이동 보안 구조의 구체적인 보안 과정을 설명한다.

표 2 Trust와 Token 기호 정의

$TR_{<X>}$: X에 대해 직접 생성한 *Trust*
$TR_{<X,Y>}$: X와 Y에 대해 직접 생성한 *Trust*
$TR'_{<Y>}$: Y에 대해 간접적으로 전달받은 *Trust*
$TO_{<Z>}$: Z에게 부여된 *Token*
DCnew: 핸드오버 시 새로운 연결의 DC
DCold: 핸드오버 시 이전 연결의 DC

MT, DC, HE의 세 가지 통신 요소는 AAA 목적을 달성하기 위해서 지속적 상호 *Trust*를 생성할 필요가 있다. 본 절에서는 단대단 통신에서 일반적으로 사용되는 *Naive Mutual Authentication* 방식을 세 가지 요소 간 *Trust* 생성에 적용할 때의 문제점을 알아보고, 이러한 문제점들을 해소하기 위해 새로운 인증 방안을 제안한다. 본 절에서 소개되는 인증 방안은 핸드오버 시에*Token*을 이용하는 SA(Simple Authentication) 방안과 구별하여 *Secure Association & Authentication*이 동시에 이루어지는 과정을 FA(Full Authentication) 이라고 명한다.

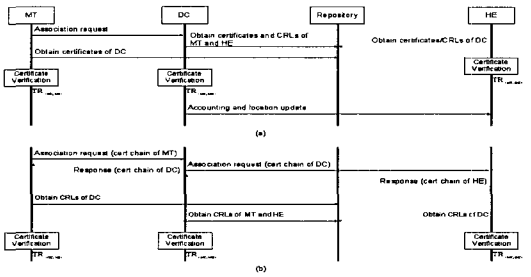


그림 6 일반적인 Naive Mutual Aauthentication 절차

4.1 Secure Association & Authentication

그림 6은 *Naive Mutual Authentication*에 의한 일반적인 인증 방법을 MT, HE, DC간의 인증에 사용한 경우이다. 이 세 요소는 각각 <MT↔DC>, <MT↔HE>, 그리고 <DC↔HE> 세 개의 쌍을 구성하여 서로 인증한다. 이러한 경우에 가장 문제가 되는 것은 MT의 성능이다. 본 논문에서는 비교적 향상된 성능을 가정하였지만, MT와 DC간의 인증 경로는 길이가 매우 커질 수도 있기 때문에 MT의 성능을 고

려할 때 심각한 자원부족을 가져올 수 있다. 또 다른 문제는 그림 6의 (a),(b)에서 볼 수 있듯이 MT가 DC를 인증하기 위해서 DC의 인증 경로와 CRL (Certificate Revocation List)들을 저장소(repository)로부터 무선망을 통해 전달받아야 한다는 것이다. 이때 전달되는 데이터의 양은 인증 경로가 증가함에 따라 많은 인증서가 전달되어야 하므로, 부족한 무선네트워크 자원을 비효율적으로 사용하는 결과를 가져온다. 그림 6(a)는 인증 경로와 CRL들을 저장소로부터 가져오는 경우이고, 그림 6(b)는 각 요소가 인증 경로를 저장하고 있다가 상대방에게 전달해 주는 방식이다. 그림 6(a)에서는 저장소를 통해서 인증 경로를 가져오기 때문에 인증 경로 획득에 필요한 시간이 그림 6(b) 보다 더 소요된다. 그러나 그림 6(a),(b) 모두 CRL을 획득하는 과정이 추가로 필요하다.

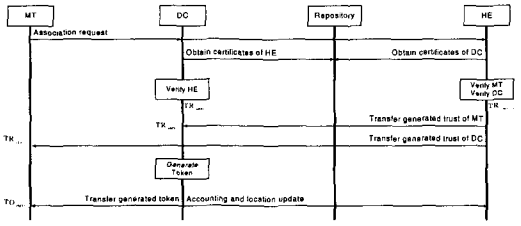


그림 7 제안된 FA(Full Authentication) 절차

그림 7은 본 논문에서 제안하는 FA 방안이다. 본 논문에서는 그림 6에서 *Naive Mutual Authentication* 방식이 DC에 대한 *Trust*를 MT와 HE가 각각 생성하기 때문에 MT의 자원이 소비됨은 물론이고, 무선망을 통한 인증서와 CRL의 전달로 인해 네트워크 자원이 낭비되는 문제점을 보안하기 위해서, 3장에서 설명된 *Trust*의 간접 생성 및 전달을 이용하였다. 제안된 방안은 3장에서 설명된 *Trust* 전달 방식에 의해 상호간의 *Trust*를 형성할 때 효율성을 높인 것이다. 즉, DC에 대한 *Trust*를 HE가 단독으로 생성하여 MT에게 전달하는 방법을 이용한다(그림 5). 또한 DC가 생성하고자 하는 MT에 대한 *Trust* 역시 HE가 생성해서 DC에게 전달해 주어서 간접적으로 생성한다. DC는 MT의 요청을 받아서 HE로 전달하고, 자신은 HE에 대한 인증 경로와 CRL 들을 획득하여 HE에 대해 검증하고 $TR_{<HE>}$를 생성한다. HE는 MT에 대해 검증하고, DC의 인증서와 CRL을 획득하여 검증하고 그 결과로 $TR_{<MT, DC>}$를 생성한다. HE는 생성한 MT에 대한 *Trust*인 $TR_{<MT>}$와 DC에 대한 *Trust*인 $TR_{<DC>}$를 각각 DC와 MT로 보낸다. 이 결과 DC는 MT에 대한 *Trust*를 추가로 갖게 되고, MT는 DC에 대한 *Trust*를 갖게 된다. DC는 MT가 핸드오버 할 때 효율성을 위해서 사용하게 되는 *Token*을 생성하여 MT로 보내준다. MT↔HE 간의 상호 인증은 그림 4(c)에서 보인 것처럼 동일한 CA의 하위 노드인 것을 가정하였으므로 최소의 인증 경로를 유지할 수 있다.

4.2 핸드오버 절차

도메인 내에서의 핸드오버 뿐만 아니라 도메인간의 핸드오버가 있을 때에도 인증, 과금, 그리고 위치 갱신 등의 목적으로 MT에 대해 지속적으로 인증할 필요가 있다. 본 논문에서 제시하는 차세대 이동 통신망에서 핸드오버시의 인증은 다음 세 가지 방식 중, 이동 환경에 따라서 적응적으로 선택 가능하다.

- FA (Full Authentication)
- 도메인 내에서 핸드오버 시 *Token*을 사용하는 SA(Simple Authentication)
- 도메인 간 핸드오버 시 *Token*을 사용하는 SA

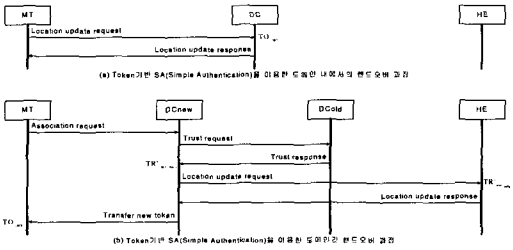


그림 8 핸드오버 과정

그림 8(a)는 도메인 내에서 이동할 경우에 *Token*만을 확인하고, DC의 위치정보를 갱신하는 과정이다. 핸드오버시의 인증은 최대한 신속하게 이루어져야 할 필요가 있는데 이동이 있을 때마다 FA에 의해서 인증을 하는 것은 연속된 서비스를 보장하기 어렵고, 많은 MT들의 이동을 하는 상황이 된다면 MT 뿐만 아니라 DC나 HE도 자원이 부족하게 된다. 따라서 핸드오버시의 주된 인증 방법으로 본 논문에서 제안한 *Token*에 의한 SA을 사용한다. 그림 8(b)는 도메인간의 이동에서 인증 절차를 줄이기 위해 SA을 사용한 경우로, 암호화된 핸드오버 요청을 받은

DC_{new}는 DC_{old}로부터 *Trust*를 전달받는다. 이때 DC_{old}가 갖고 있던 DC_{new}에 대한 *Trust*($TR_{<DCnew>}$)를 HE로 전달해 줄 수 있어 HE의 부담도 줄인다. DC_{new}는 새로운 *Token*을 MT에게 부여한다.

그러나 *Token*을 사용할 수 없는 초기 인증 과정이나 *Token*을 오래 사용한 상황에서는 FA 방식을 제한적으로 사용한다. DC_{new}는 MT의 핸드오버 요청을 받고 FA을 이용할 것인지 SA을 이용할 것인지 결정한다.

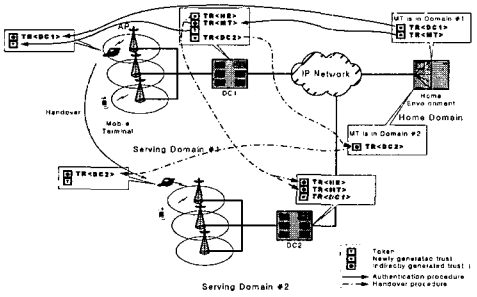


그림 9 인증과 핸드오버 과정

MT -> DCnew:	$req\,[E_{MK}(token), E_{PK}(ID_{MT}), ID_{DC_{new}}]$
DCnew -> DCold:	$req\_trust[E_{MK}(token)]$
DCold -> DCnew:	$res\_trust[E_{MK}(trust1), E_{HK}(trust2)]$ $(trust1 = TR_{<MT:\ DC_{old}>}, trust2 = TR_{<MT:\ HE>})$
DCnew -> HE:	$AAA\_request[E_{HK}(ID_{MT}), E_{HK}(trust2)]$
HE -> DCnew:	AAA_confirm
DCnew -> MT:	$E_{MK}(token)$

그림 10 핸드오버 과정에서 필요한 메시지 포맷

그림 9는 본 논문에서 제안한 FA와 SA절차에 기반한 도메인 내부 핸드오버에서 *Trust*와 *Token*을 생성하고 전달하는 과정을 보여준다. DC1은 자신이 MT를 서비스하기 위해 필요한 HE와 MT에 대한 *Trust*를 생성하는데, HE에 대한 *Trust*는 직접 생성하지만, MT에 대한 *Trust*는 HE로부터 전달받는다. DC1은 *Trust* 생성 후에 MT에게 *Token*을 부여한다. MT가 DC2로 이동하는 경우에 DC2는 DC1이 갖고 있던 MT와 HE에 대한 *Trust*를 그대로 전달받아 사용하므로 핸드오버 시에 새로 생성하는 *Trust* 수를 줄일 수 있으므로 효율성을 높일 수 있다. DC2는 간접적인 *Trust* 생성 이후에 MT에게 새로운 *Token*을 부여한다.

그림 10은 핸드오버 과정의 각 세부 메시지 형태를 보여준다. 이러한 메시지는 각 요소에서 핸드오버 시의 계산 량을 규정하는데 사용되며, 5장에서는 이것을 토대로 본 논문에서 제시한 *Mobile PKI* 기반의 FA와 SA 성능을 분석하였다.

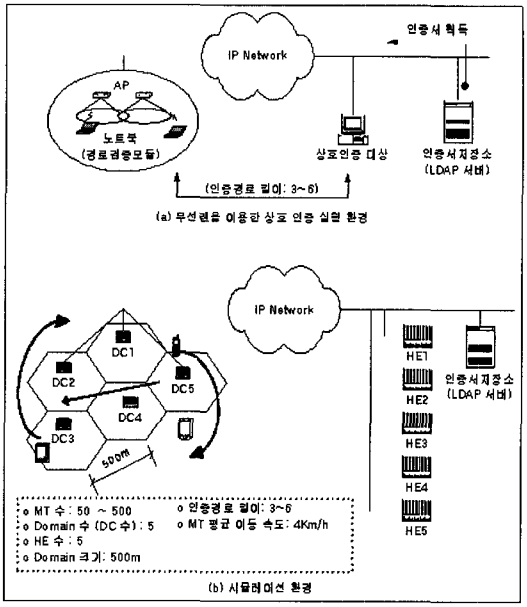


그림 11 무선랜 실험 환경과 시뮬레이션 모델

5. 성능평가

5.1 실험 환경과 시뮬레이션

본 논문에서 제안하는 이동 보안 구조의 성능평가를 위해서 실험 환경을 통해 구한 실험치에 기반 하여 시뮬레이션을 수행하였다. 그림 11(a)는 무선랜을 이용한 실험 환경을 보여준다. 실험 환경에 사용된 각 노드들은 3장에서 설명된 X.509의 계층구조 상에서 여러 경로에 위치하는 노드들을 이용하였고, 이들 노드들 간에 인증 경로를 따라서 인증서 저장소로부터 인증서를 획득하고 검증하는 과정에 대한 실험치를 구하였다. 인증서 저장소는 외부 네트워크에 위치한 LDAP (Lightweight Directory Access Protocol) 서버를 이용하였다. 표 3은 무선랜 환경에서 CPU와 메모리 사양이 각각 PentiumIII-450MHz와 256MB인 시스템을 이용하여 측정한 값을 보여준다. 이러한 실험치는 최근 개발되고 있는 이동 전화, PDA, 노트북 등에 활용 가능할 것으로 기대된다. (PDA의 경우 현재 200MHz이상의 고성능 CPU와 64MB이상의 메모리를 탑재한 기종이 출시되고 있고, 이동 전화의

경우에도 PDA와 성능 면에서 거의 동등할 정도로 성능이 향상되고 있는 추세이므로, 본 논문에서 실행한 시스템 사양을 적용하여 추후 성능 예측이 가능할 것으로 사려 된다.) 실험 환경의 인증 경로 검증은 OpenSSL[11]의 기본 라이브러리를 경로검증이 가능하도록 수정하여 사용하였다. 실험 환경에서 구한 실험치를 다음과 같은 시뮬레이션의 변수와 함께 사용하여 MT가 갖게 될 다양한 조건과 환경 적인 요소들을 시뮬레이션을 통해 분석하였다.

- *MT의 수*
- *MT의 Association과 핸드오버 빈도*
- *인증서 경로 길이에 따른 인증서 획득 및 검증 소요 시간 변화*

표 3 실험 환경에서 구한 시뮬레이션 파라미터

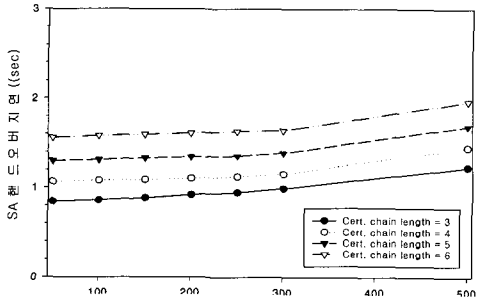
시뮬레이션 파라미터	내 용	값
해쉬	MD5	100.7MB/sec
RSA 서명	512bits	4.92ms
RSA 서명검증	512bits	0.43ms
MT 평균 속도		4Km/h
인증 경로 길이에 따른 검증 소요 시간	길이 = 2 길이 = 3 길이 = 4 길이 = 5	30ms 43ms 60ms 76ms
인증서 획득 시간 (LDAP)	인증서와 CRL	170ms

그림 11(b)는 이러한 조건들과 실험치를 이용하여 구성한 시뮬레이션의 환경 구성을 보여준다. 전체 네트워크는 총 5개의 도메인으로 구성되어 있고, 하나의 도메인 크기를 500m로 하였으며, 도메인 내에 약 10~20개의 AP를 설정하였다. MT의 수는 전체 네트워크에서 평균적으로 50~500개까지 변화하여 측정하였다. MT의 이동 속도는 1~7 Km (평균 4Km)로 다양하게 설정하였다. 총 10시간동안 시뮬레이션 시간 동안 평균 30회 정도의 *Secure Association*을 수행하고, 지속적인 핸드오버를 수행하도록 설정하였다.

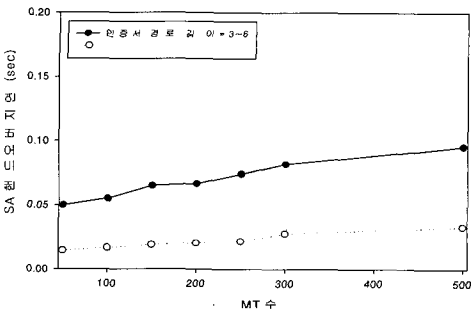
5.2 시뮬레이션 결과

5.2.1 SA에 의한 핸드오버

본 논문에서 제안한 *Token*과 *Trust*를 이용한 *SA*에 의한 핸드오버 방안의 효율성을 다음과 같은 실험결과를 통해 검증할 수 있었다. 그림 12 (a)는 도메인 간의 핸드오버에서 MT 수가 증가함에 따라 DC에서 발생하는 핸드오버 지연에 대해 *SA*를 이용하지 않고 *FA* 방식에 의해 핸드오버를 수행한 경우를 나타내고, 그림 12 (b)는 본 논문에서 제안한 *SA*에 의한 방식을 이용하는 경우와, 암호화 기능 및 *Token*과 *Trust* 방식이 포함되지 않고 단순히 핸드오버 요청/응답 프로토콜에 의해서만 핸드오버를 수행하는 경우에 대한 시뮬레이션 결과를 비교하여 나타내었다. *SA*를 사용하지 않는 경우에는 인증서 경로 검증에 소요되는 시간이 추가되므로 DC의 성능 저하의 요인이 되고, 인증 경로가 증가에 따라서 핸드오버 지연도 함께 증가하는 것을 볼 수 있다. *Token*과 *Trust*에 의한 *SA*를 이용하는 경우에는 평균적인 핸드오버 지연이 MT 수 변경에 따라서 50~90ms의 분포를 보이고, 인증서 경로 길이의 변화에 대해서는 일정하게 유지되는 것을 볼 수 있다. 보안 기능 (SA, 암호화



(a) Token과 Trust 방식을 사용하지 않는 경우



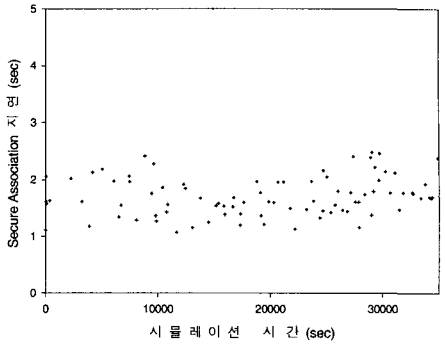
(b) Token과 Trust 방식을 사용한 경우와 Mobile PKI를 사용하지 않은 경우의 비교

그림 12 DC에서 Trust와 Token의 사용 여부에 따른 핸드오버 지연

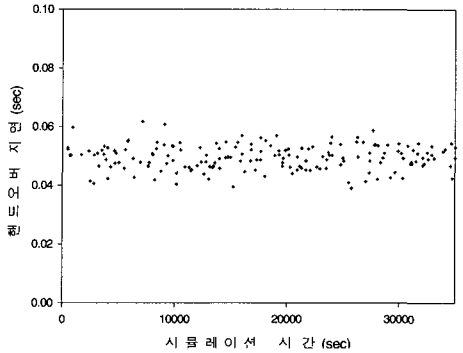
/복호화)을 제외한 시뮬레이션 결과는 네트워크와 시스템 지연에 의해 15ms 정도의 지연을 보이고 있어, SA가 추가됨으로써 약 30~40ms (MT수가 100인 경우) 정도의 오버헤드가 추가로 발생한 것을 알 수 있다. SA 기능을 현재의 11MHz 무선랜 상에서 VoIP나 비디오 스트림 서비스에 이용하는 경우에는, 음성 프레임 간의 평균 간격이 100ms 이상이 되므로 SA 핸드오버 지연에 의한 패킷 손실이 거의 없을 것으로 기대된다. 300Kbps 비디오 스트림의 경우에는 스트림 패킷간의 평균 간격이 30ms 정도로 제한되어야 하므로 어느 정도 패킷 손실이 일어날 수 있다. 이러한 손실은 MT 수가 증가 될 경우 네트워크와 DC에 오버헤드가 증가로 인해 더 늘어날 수 있다. 그러나 본 논문에서 제안한 SA 방식이 *Token*과 *Trust*에 의해 도메인간의 핸드오버 시에 30~40ms 정도의 추가 지연만으로 상호 인증을 지원하고 있다는 점은 보안 서비스 측면에서 매우 중요하며, 단순히 핸드오버 요청/응답 프로토콜인 경우에도 300Kbps의 비디오 스트림을 지속적으로 서비스 하는 것이 가능하지 않으므로, 안정된 이동 보안 구조로 기대된다. 따라서, *Token*과 *Trust*를 사용해서 *FA*와 *SA*를 병행할 경우 본 논문에서 제시한 *Mobile PKI*는 도메인간 로밍시 발생하는 보안적 취약점을 해결함과 동시에 지연시간의 최소화로 다양한 멀티미디어 서비스 제공이 가능할 것으로 예상된다.

5.2.2 Secure Association과 핸드오버 시의 평균 지연

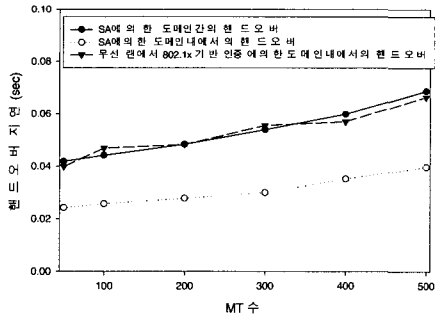
그림 13(a),(b)는 시뮬레이션이 진행되는 동안 (10시간) MT가 *Secure Association*과 핸드오버를 수행하는 과정에서 발생하는 지연을 보여주고, 그림 13(c)는 도메인 내에서의 핸드오버와 도메인간의 핸드오버시의 지연을 비교하여 나타낸 것이고, 이것을 무선랜에서 802.1x 기반의 인증 프로토콜과 비교한 것이다. 그림 13(a),(b)에서 각 MT가 갖는 인증서 경로 길이는 2~6으로 다양하게 설정하였고, MT 수는 50으로 설정하였다. 그림 13(a)에서 *FA*를 이용한 *Secure Association*의 지연 시간은 1.5초 정도를 보이고 있으며, *Secure Association*이 완료된 이후에는 도메인 내에서 이동이나 도메인 간을 이동할 때 *Token*과 *Trust*를 사용하여 핸드오버를 수행하므로 그림 13(b)에 보인 것처럼 핸드오버 지연을 40~50ms 정도로 유지할 수 있다. 그림 13(c)의 802.1x를



(a) Sesure Association의 지연



(b) Token과 Trust를 이용한 핸드 오버의 지연



(c) SA를 이용한 도메인 내에서 핸드오버와 도메인 간의 핸드오버 지연 비교

그림 13 Secure Association과 핸드오버 지연

사용한 인증 구조에 의한 핸드오버는 무선랜에서 실험환경과 802.1x 프로토콜 (EAP : Extensible Authentication Protocol)을 *Mobile PKI*와 유사하게 설정하여 측정하였다. 무선랜의 경우에 이동성을 보장하지 않기 때문에 AP간의 핸드오버에 대해 MT가 새로운 AP 쪽으로 다시 *Secure Association* 한 후에 인증 서버와 EAP기반의 802.1x를 통해 인증하는 구조이다. 이러한 구조를 적용하여 시뮬레이션 한 결과

*Token*과 *Trust*를 사용하여 도메인간의 핸드오버를 할 때 지연과 유사한 것으로 나타났고, 도메인 내에서의 핸드오버는 본 논문에서 제시한 방안이 50% 정도의 성능 향상을 보이고 있다. 따라서, 본 논문에서 제시한 *Token*과 *Trust*에 의한 SA 방식은 상호 인증에 의한 신뢰성을 제공하는 측면에서 *Secure Association*과 핸드오버 시에 MT의 계산 량과 지연을 최소화하는데 효과적인 방안이 효과적임을 보여준다. 또한, 도메인 내에서는 DC와 MT간에 *Token*만 확인하므로 도메인간의 핸드오버와 비교할 때 약 50% 정도로 지연이 적게 나타난다.

표 4 HE(DC)와 MT에서 인증서 경로 길이에 따라 Secure Association 시에 소요되는 처리시간

HE (DC)에서 Association 처리 시간					
인증 경로 길이	2	3	4	5	6
처리 시간	0.640	0.747	1.063	1.253	1.462
MT에서 Association r요청 처리 시간					
처리 시간	0.014	0.016	0.015	0.016	0.014

5.2.3 FA에서 Trust를 이용한 검증 대행의 효율성

표 4는 HE (DC)와 MT에서 인증서 경로 길이에 따라 *Secure Association* 시에 소요되는 처리시간을 보여준다. HE와 DC의 경우에는 *Secure Association*을 처리하기 위해 인증서 경로를 검증해야 하므로 인증서 경로 길이 증가에 따른 처리시간 증가를 보이는 반면 MT는 HE로부터 전달받은 정보를 이용하여 간접적인 인증을 수행하므로 인증서 경로 길이가 증가하더라도 추가적인 부담이 생기지는 않는 것을 볼 수 있다. 따라서, *Mobile PKI*를 최근 상용화되고 있는 PDA 등 시스템 자원이 적은 MT의 경우에도 효율적으로 적용할 수 있을 것으로 기대된다.

6. 결 론

본 논문에서는 차세대 이동 통신의 다양하고 복합적인 환경 특성에서 발생할 수 있는 보안 취약점들을 분석하였으며, 이를 기반으로 차세대 이동 통신 시스템이 필요로 하는 보안 요소들을 OMCRs(*Open Mobile Communications Requirements*)로 정의하였고, 이들 요소들을 해결하기 위한 방안으로 PKI 기반의 새로운 보안 구조인 *Mobile PKI*를 제안하였다. 또한, *Mobile PKI* 성능을 평가하기 위해서 무선랜을 이용하여 실험 환경을 구성하여 PKI 관련 함수들(인증서 획득 및 검증과 OpenSSL 라이브러리의 암호화 함수)이 무선랜 상에서 실행되는 경우에 대한 성능을 측정하였다. 이를 바탕으로 시뮬레이션을 수행하여 MT, DC 그리고 HE가 FA에 의한 SA 에 의한 핸드오버 과정에 상호 연계되어 동작하는 시뮬레이션 환경을 구성한 후에 802.1x의 인증체계와 비교하여 성능을 평가하였다. 이러한 성능평가를 통해서 본 논문에서 제안한 보안 구조의 실용성을 확인하였고, 특히 *Token*과 *Trust*에 의해 *Secure Association* 시에 상호 인증에서 MT의 부담을 줄이고, 핸드오버 시의 지연을 효과적으로 최소화할 수 있음을 확인하였다. 따라서, 본 논문에서 제시한 Mobile PKI 보안 구조를 차세대 이동 통신에 적용 시, 다양한 멀티미디어 서비스가 가능하고, AAA 지원을 위해 효과적으로 사용될 수 있을 것으로 기대된다.

참고문헌

[1] Magnus Frodigh, Stefan Parkvall, Christiaan Roobol, Per Johansson, Peter Larsson, "Future-Generation Wireless Networks", IEEE Personal Communications, Vol. 8 No. 5, Oct. 2001,

[2] Toru OTSU, Ichiro OKAJIMA, Narumi UMEDA, and Yasushi YAMAO, "Network Architecture for Mobile Communications Systems Beyond IMT-2000", IEEE Personal Communications, Vol.8 No. 5, Oct. 2001,

[3] K. W. Richardson "UMTS overview", ELECTRONICS & COMMUNICATION ENGINEERING JOURNAL, JUNE 2000.

[4] Girish Patel and Steven Dennett , "The 3GPP and 3GPP2 Movements Toward an All-IP Mobile Network", IEEE Personal Communications Interactive, Aug. 2000.

[5] Tomas Robles, Arndt Kadelka, "QoS Support for an All-IP System Beyond 3G", IEEE Communications Interactive , Vol. 39, No. 8, Aug. 2001.

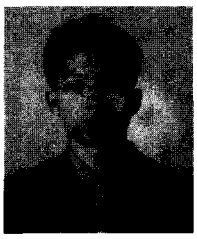
[6] Tao Zhang and Prathima Agrawal, Telcordia Technologies, Inc. Jyh-Cheng Chen, National Tsing Hua University, "IP-Based Base Stations and Soft Handoff in All-IP Wireless Networks", IEEE Personal Communications

Interactive, Vol. 8 No. 5, Oct. 2001.
[7] ITU-R Recommendations M.1078(09/94), "Security Principles for International Mobile Telecommunications-2000 (IMT-2000)."
[8] UMTS 33.21, "Universal Telecommunications System (UMTS); Security Requirements."
[9] GSM 03.20, "Digital Cellular Telecommunications System; Security Related Network Functions".
[10] 3GPP TS 33.102, "3GPP Technical Specification Group Service and System Aspects; Security Architecture".
[11] OpenSSL. OpenSSL Project. http://www.openssl.org
[12] ITU-T Recommendation X.509: Information Technology-Open Systems Interconnection-The Directory: Authentication Framework.

구 자 범

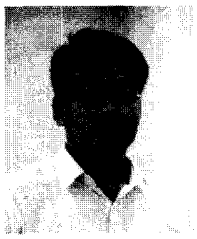
2000 2 학사, 중앙대학교, 전자전기공학부
2002 2 석사, 중앙대학교, 전자전기공학부
2002 3~현재 박사과정, 중앙대학교, 전자전기공학부
관심분야:무선인터넷보안, 무선 PKI, 무선 가상 사설망
E-mail:jabeom@ms.cau.ac.kr

김 관 연



2001 2 학사, 중앙대학교, 전자전기공학부
2001 3~현재 석사과정, 중앙대학교, 전자전기공학부
관심분야 무선인터넷보안, 무선 PKI, 무선 LAN
E-mail:cityhero@wm.cau.ac.kr

이 재 일



1986 학사, 서울대학교, 계산통계학과
1988 석사, 서울대학교, 계산통계학과
1996 한국 IBM 소프트웨어연구소
1996~현재 한국정보보호진흥원, 전자서명인증관리센터장
관심분야:유·무선 PKI, 전자상거래 보안
E-mail:jilee@kisa.or.kr

박 세 현

1986 2 학사, 중앙대학교, 전자공학과
1988 2 석사, 중앙대학교, 전자공학과
1998 컴퓨터 공학 박사, University of Massachusetts at Amherst, ECE Dept.
1988 2~99 2 한국전자통신연구원, 선임연구원
1999 3~현재 중앙대학교 전자전기공학부, 조교수
관심분야:무선인터넷보안, 유·무선 PKI, New Trust Model
E-mail:shpark@cau.ac.kr