Journal of Korea Multimedia Society Vol. 10, No. 3, March 2007(pp. 373-380)

# PAN에서 인증 및 인증서 상태 관리를 위한 효율적인 프로토콜

장화식[†], 이경현[††]


## 요 약

본 논문에서는 Personal Area Network (PAN)을 구성하는 모바일 디바이스에서의 전자서명 생성 및 검증을 위한 계산상 오버헤드를 감소시키는 효율적인 인증 프로토콜을 제안한다. 특히, 제안 프로토콜은 일회용 전자서명 기법을 사용함으로써 전통적인 공개키 전자서명 연산을 제거하였으며, 제한된 컴퓨팅 능력을 가진 모바일 디바이스를 위해 기 제안된 인증 프로토콜과 달리 서명 서버의 지원없이 전자서명 생성 및 검증을 수행할 수 있다. 또한, 제안 프로토콜은 PAN에서 모바일 디바이스들의 인증서 상태 관리를 위한 통신 및 계산상 오버헤드를 경감시키기 위해 해쉬체인에 기반한 간략화된 인증서 상태 검증 절차를 제공한다.


# Efficient Protocol for Authentication and Certificate Status Management in PAN

Hwa-Sik Jang[†], Kyung-Hyune Rhee[††]


## ABSTRACT

In this paper we propose a new efficient authentication protocol that reduces overheads of computation for digital signature generation/verification on mobile devices in the Personal Area Network (PAN). In particular, we focus on eliminating the traditional public key operations on mobile devices without any assistance of a signature server. Moreover, the proposed protocol provides a simplified procedure for certificate status management to alleviate communication and computational costs on mobile devices in the PAN.


**Key words:** PAN(Personal Area Network)(개인영역 네트워크), Authentication(인증), Certificate Status Management(인증서 상태 관리)

## 1. 서 론

최근 PDA와 랩탑과 같이 네트워킹 능력을 가진 모바일 디바이스들은 이미 널리 사용되어지고 있으며, 모바일 디바이스들의 기능과 성능은 나날이 발전하고 있다. 이러한 기술들의 급속한 발전으로 인하여 미래의 모바일 통신에서 네트워크에 대한 접근방법과 네트워크 접근에 사용되어지는 터미널 유형은 현재 사용되고 있는 방식과 다를 것으로 예상되어지며, 물리적으로 사용자에 근접한 범위 내에서 분산 다기능 모바일 터미널은 로컬 무선 통신을 통하여 연결되는 몇몇의 컴포넌트들을 구성할 것으로 예상되어진다. 특히, 개인적인 범위 내에서 구성되어지는 고정된 수의 모바일 컴포넌트들 간의 상호 연결된 무선

※ 교신저자(Corresponding Author) : 이경현, 주소 : 부산시 남구 대연 3동 599-1(608-737), 전화 : 051)620-6395, FAX : 051)626-4887, E-mail : khrhee@pknu.ac.kr
접수일 : 2006년 12월 4일, 완료일 : 2007년 2월 14일
[†] 정회원, 대덕대학 정보보안 · 해킹과 (E-mail : hsjang@ddc.ac.kr)
[††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부
※ 이 논문은 2006년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. R01-2006-00-10260-0)

네트워크를 Personal Area Network (PAN)라 부르며, 전형적으로 Bluetooth 등을 이용하여 10미터이내의 범위에서 구성되어진다. PAN에서의 통신은 기밀정보나 개인 데이터가 주를 이루므로 각 컴포넌트는 안전하고 인증된 채널을 통하여 통신해야 하며, 안전하고 인증된 통신은 PAN 컴포넌트들 간의 적절한 보안 프로토콜과 보안 연계(Security Association)를 통하여 이루어질 수 있다.

PAN에서의 안전하고 인증된 통신 서비스를 제공하기 위한 기반구조로써 C. Gehrmann 등은 PAN내의 모든 컴포넌트들에게 공개키 인증서를 발급하는 Personal CA (Certificate Authority)를 소개하였다[1]. Personal CA는 집이나 작은 사무실내에서 일반 사용자에 의해서 관리되며 시스템 초기화 단계에서 [2]의 임프린팅(Imprinting)을 확장한 매뉴얼 인증 프로토콜 (Manual Authentication Protocol)을 사용하여 모든 모바일 디바이스들은 공개키 인증서를 가지고 부트스트랩 (Bootstrap)된다. 시스템 초기화 단계 이후, PAN내의 모든 모바일 디바이스들은 전통적인 공개키 전자서명 기법과 인증서 상태 관리 기법에 의하여 안전하고 인증된 통신 서비스를 수행한다.

그러나, Personal CA 개념을 PAN 환경에 적용시킬 때 다음과 같은 두 가지 문제점이 존재한다.

1. PAN을 구성하는 대다수의 모바일 디바이스들은 일반적으로 제한된 컴퓨팅 능력을 가지므로, 기존의 RSA나 DSA와 같이 계산상 많은 오버헤드를 요구하는 전통적인 공개키 전자서명 기법들은 컴퓨팅 능력이 제한된 모바일 디바이스들에게 적합하지 않다.

2. PAN을 구성하는 모바일 디바이스들의 인증서 상태 정보를 관리하기 위하여 CRL[3]등의 계산 및 통신상 많은 오버헤드를 요구하는 기존의 인증서 상태 관리 기법들이 그대로 적용되고 있으며, 이를 최적화하기 위한 기법이 고안되지 않았다.

따라서, 위의 두 문제를 해결하는 효율적인 인증 및 인증서 상태 관리 프로토콜을 설계하는 것이 PAN 환경에서의 신뢰성 있고 인증된 통신 서비스를 제공하기 위한 중요한 연구 이슈라 할 수 있다.

본 논문에서는 PAN을 구성하는 모바일 디바이스상에서 전자서명의 생성과 검증을 위한 계산상 오버헤드를 감소시키는 새로운 인증 프로토콜을 제안한다. 특히, 제안 프로토콜은 일회용 전자서명 기법을 통하여 전통적인 공개키 전자서명 연산을 제거하였을 뿐만 아니라 서명 서버의 지원에 의존하여 모바일 디바이스상의 계산상 오버헤드를 감소시키는 기존의 서버지원 전자서명 (Server-Assisted Signature) 기법들과 차별화된다. 따라서, 제안 프로토콜은 서버 지원 전자서명 기법에서 야기되는 분쟁상황 및 서명 서버에서 요구되는 높은 계산·저장공간상 오버헤드들을 해결하였다. 또한, 제안 프로토콜은 해쉬 체인 기법에 기반하여 모바일 디바이스들의 인증서 상태 정보를 검증함으로써, 인증서 상태 관리를 위한 통신 및 계산상 오버헤드를 경감시키는 간략화된 인증서 상태 검증 절차를 제공한다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 제안 방안 설계를 위한 암호학적 기반 기술들을 소개하고, 3장에서는 본 논문에서 제안하는 시스템 모델을 설명한다. 4장에서는 PAN에서 모바일 디바이스들을 위한 효율적인 인증 및 인증서 상태 관리 프로토콜이 제안되고, 제안 방안의 보안성 및 성능 평가는 5장에서 이루어진다. 마지막으로, 6장에서 결론을 맺는다.

## 2. 시스템 설계를 위한 암호학적 기반 기술

### 2.1 일회용 전자 서명 및 프렉탈 Merkle 트리

일회용 전자서명 (One-Time Signature : OTS) [4] 기법은 단일 메시지를 전자서명하기 위한 메커니즘으로, 전통적인 공개키 전자서명 기법과 달리 트랩도어 함수에 기반하는 것이 아니라, 일방향 해쉬 함수에 기반함으로써 전자서명 생성 및 검증이 매우 효율적이다. 하지만, 일회용 전자서명 기법은 다음의 두 가지 이유로 인하여 실용적이지 못한 것으로 간주되어져 왔다.

1. 전통적인 공개키 전자서명 기법에 비하여 전자서명문의 길이가 상대적으로 길다.

2. 일회용이라는 특성으로 인하여 전자서명 생성 시 마다 키 생성이 새롭게 이루어져야 한다. 이로 인하여 각각의 전자서명에 사용되어지는 공개키에 대한 인증된 분배 문제를 야기시킨다.

따라서, 빠르고 효율적인 일방향 함수의 유용성으로 인한 이득은 명백히 손실된다. 그러나, 일회용 전자서명문의 길이를 줄이기 위하여 암호학적 해쉬 함수를 이용한 메시지 다이제스트를 사용할 수 있다.

만약, 160 비트 출력을 가지는 SHA-1 함수를 사용할 경우 메시지 다이제스트를 서명하기 위해서는 단지 168개의 비밀값만이 필요하다[4].

Merkle은 많은 수의 일회용 전자서명을 인증하기 위하여 해쉬 함수를 사용하는 인증 경로(Authentication Path)라는 개념을 소개하였다. 인증 경로란 주어진 잎(leaf)과 근(root) 사이의 경로에 있는 모든 노드들의 형제노드들 값들이다. 또한, Jakobsson 등은 잎들(leaves)이 차례로 사용되어질 때, 각 잎(leaf)의 유효성 검증을 위한 인증 경로로 사용되어지는 Merkle 해쉬 트리(Merkle Hash Tree)의 순차 이동(Sequential Travel)을 제공하는 프렉탈 Merkle 트리(Fractal Merkle Tree)를 제안하였다[5]. 프렉탈 Merkle 트리에서 요구되는 전체 저장 공간은 $1.5\log^2 N/\log\log N$ 해쉬 값들로 제한되며, 최악의 경우의 계산상 비용은 각 출력마다 $2\log N/\log\log N$ 해쉬 연산이 요구된다. 최근, Naor 등은 Merkle의 일회용 전자서명과 Jakobsson 등의 알고리즘을 결합한 기법이 적은 전자서명 길이와 저장 공간으로 효율적인 전자서명을 생성할 수 있음을 실험을 통하여 보였다[6].

### 2.2 개선된 효율적인 공개키 프레임워크

Zhou 등은 인증서의 최대 유효 기간을 짧은 기간들로 나누고, 인증서 소유자(혹은 조직적인 환경에서 관리자)의 통제아래 각 기간의 끝 지점에서 그 인증서가 취소될 수 있는 새로운 공개키 프레임워크를 제안하였다[7]. Zhou 등의 프레임워크는 인증서의 유효성을 검증할 때 CA의 관여를 제거하기 위하여 제안되었으나, 식별되지 않은 사용자로부터 제시되는 정보를 인증하는 비합리적인 방법이 사용되고 있다. 또한, 악의적인 사용자도 아무런 제약없이 항상 유효한 전자서명문을 생성할 수 있는 단점을 가지고 있다.

위와 같은 취약점을 해결하기 위하여, [7]에서는 보안 서버 (Security Server)라는 새로운 형태의 신뢰되는 제 3자를 소개하고 있으나, 이는 단지 앞서 언급된 취약점을 극복하기 위해 추가된 부가적 신뢰 기관일 뿐만 아니라 실질적 시스템 구현시에 보안 서버를 안전하게 유지하기 위한 추가적인 비용이 요구된다는 단점이 있다. 따라서, 본 논문에서는 Zhou의 공개키 프레임워크를 실질적 구현에 적합하도록 만들기 위하여 제어 윈도우 (Control Window) 메커니즘을 제안한다.

**Definition 1.** 제어 윈도우(Control Window)*란 인증서 검증자가 오직 인증서 송신자의 해쉬 체인 검증을 통해서만 송신자의 인증서 취소 유무 상태를 신뢰할 수 있도록 하는 허용된 시간 구간을 의미한다.*

제어 윈도우 메커니즘에서는 CA가 어느 특정한 사용자를 위한 인증서를 발행할 시점에 그 사용자의 제어 윈도우의 크기를 설정한다. 사용자는 제어 윈도우 동안은 단지 해쉬값을 계산하는 것으로 자신의 인증서 상태를 제어할 수 있음을 의미하며, 인증서 검증자는 제어 윈도우 동안 사용자의 인증서 상태에 대한 해쉬값을 신뢰함으로써 CA로부터의 사용자의 인증서 상태 정보에 대한 질의를 수행할 필요가 없다. 그리고, 제어 윈도우의 종점 (End point)에서 검증자는 CA에게 사용자의 인증서에 대한 상태 정보를 질의할 수 있다.

## 3. 시스템 모델

### 3.1 설계 원칙

본 절에서는 PAN 환경을 구성하는 모바일 디바이스들간의 효율적인 인증과 인증서 상태 검증을 제공하기 위한 제안 프로토콜의 설계 원칙을 제시한다. 제안 프로토콜의 설계를 위한 주요 원칙은 아래와 같다.

- **모바일 디바이스에서 전통적인 공개키 연산들의 제거** : 전통적인 공개키 전자서명 기법들은 전자서명 생성 및 검증을 위하여 계산상 복잡한 연산들을 요구하기 때문에, PAN을 구성하는 자원 제한적인 모바일 디바이스들 (8 비트나 16 비트의 매우 저속의 CPU 속도에서 동작하는 마이크로 컨트롤러들을 소유하는 장치들)을 위해서는 적합하지 않다. 그러므로, 어떠한 공개키 연산도 수행할 필요가 없는 인증 프로토콜의 설계는 PAN 환경에서 매우 중요한 과제이다.

- **서명 서버의 제거** : 서명 서버(Signature Server)를 이용하여 공개키 전자서명 생성과 같이 계산량이 많은 연산을 수행하는 암호학적 프로토콜들이 제안되었다[8,9]. 하지만, 이와 같은 프로토

콜들은 분쟁 해결을 위하여 서명 서버 또는 서명 서버와 모바일 디바이스들에게 높은 저장 공간을 필요로 한다. 또한, 모든 전자서명이 서명 서버로부터 수행됨으로써 발생되는 라운드 트립으로 인한 지연 (Delay)이 불가피하다. 따라서, 서명 서버의 지원이 불필요한 인증 프로토콜을 설계하는 것이 바람직하다.

- **인증서 상태 검증를 위한 적은 계산 및 통신 비용** : OCSP[10]와 같은 온라인 인증서 상태 검증 메커니즘은 CRL[3]과 비교했을 때, 자원의 소모가 적어서 이동 장치에게 적절하지만, Personal CA는 높은 통신비용 및 많은 수의 전자서명 생성으로 인하여 높은 계산 비용을 부담해야만 한다. 따라서, Personal CA의 작업 부담을 완화시키기 위하여, Personal CA의 전자서명 생성 횟수와 전체 통신 횟수를 줄일 필요가 있다.

### 3.2 구 조

제안 시스템은 다음과 같은 환경을 가정한다.

- PAN은 무선 인터페이스를 통하여 서로 통신이 가능하며 휴대 가능한 컴포넌트들로 구성된다.
- PAN이 구성될 시점에, PAN의 루틴 연산들을 안전하게 만들기 위해서 필요한 모든 보안 연계(Security Association)가 설정된다. 즉, PAN내의 모든 모바일 디바이스들은 초기 단계 동안 보안 값들(Security Quantities)과 인증서들을 가지고 부트스트랩된다.

제안 시스템은 Personal CA, 모바일 디바이스들로 구성되어지며 각각의 구성요소는 다음과 같은 역할을 수행한다.

- **Personal CA** : Personal CA는 PAN에서 유일하게 신뢰되는 컴포넌트이며, 명령어를 입력하기 위한 간단한 입력 장치와 디스플레이 장치를 소유하고 있다. 또한, Personal CA는 다른 모든 PAN 컴포넌트들에게 인증서와 인증서 상태 정보를 제공하기 위하여 온라인 상태를 유지한다.
- **모바일 디바이스** : PAN에 장비되는 컴포넌트들로써 네트워킹이 가능하며, 일반적으로 제한된 컴퓨팅 능력을 가진다.

### 3.3 용 어

본 논문에서 제안되는 프로토콜의 기술을 위하여 사용되어지는 용어들은 아래와 같다.

- $PCA, M$ : Personal CA 및 모바일 디바이스의 식별자
- $h()$ : 암호학적 안전한 일방향 해쉬 함수
- $SK_X$ : 모바일 디바이스 $X$의 비밀값
- $sk_X^{i,j}$ : 모바일 디바이스 $X$의 일회용 전자서명 비밀키

$$sk_X^{i,j} = h(SK_X|i|j)$$

  $i$는 전자서명문 번호, $j$는 비밀값의 색인, 그리고 $\|$ 는 메시지의 연접이다.
- $pk_X^{i,j} := h(sk_X^{i,j})$ : 각 $sk_X^{i,j}$를 위한 커미트먼트(Commitment)
- $PLC_X^i := h(pk_X^{i,1}\|\cdots\|pk_X^{i,t})$ : $i$ 번째 공개 잎 커미트먼트(public leaf commitment)로서단일 일회용 전자서명의 모든 커미트먼트들의 해쉬값
- $PK_X$ : 모바일 디바이스 $X$의 공개키로서 프렉탈 Merkle 해쉬 트리의 루트
- $AuthPath_X^i$ : 모바일 디바이스 $X$의 $i$ 번째 공개 잎 커미트먼트의 인증 경로
- $VK_X^{n-i}$ : 모바일 디바이스 $X$의 $i$ 번째 검증 키(Validation key)로서 $h()$의 범위 내에서 랜덤하게 선택된 보안 정보 $VK_X$를 기반하여, 모바일 디바이스 $X$는 해쉬 체인 $VK_X^0, VK_X^1, \cdots, VK_X^n$을 계산한다. 여기서, $VK_X^0 = VK_X$, $VK_X^i = h_X^i(VK_X) = h_X(VK_X^{i-1})$이며 $VK_X^n$를 $X$의 루트 검증 키(Root Validation Key)라고 하고, $VK_X^{n-i}$를 $X$의 현재 검증 키(Current Validation Key)라고 한다.
- $Sig_X^i$ : 모바일 디바이스 $X$의 $i$ 번째 일회용 전자서명
- $Cert_X$ : 모바일 디바이스 $X$의 인증서

## 4. 제안 프로토콜

### 4.1 초기화 프로토콜

제안 시스템에서 모든 모바일 디바이스들은 초기

화 프로토콜을 통하여 PAN에 장비된다. 제안 시스템의 초기화 프로토콜은 [1]에서 소개된 매뉴얼 인증 프로토콜 (Manual Authentication Protocol)을 변경하여 일회용 전자서명 기법의 문제점인 공개키의 인증된 분배 문제를 해결하였다. 제안된 초기화 프로토콜의 구체적인 절차는 아래와 같다.

**[단계 1]** Personal CA는 자신의 식별자 $PCA$와 공개키 $PK_{PCA}$를 모바일 디바이스에게 전송한다.

**[단계 2]** 모바일 디바이스는 랜덤하게 두 개의 보안 값인 $SK_M$과 $VK_M$을 생성하고 다음과 같은 연산을 수행한 후 $M, PK_M, n, VK_M^n$을 Personal CA에게 전송한다.

- 전체 전자서명문의 수 $n$ 만큼의 일회용 비밀값/커미트먼트 쌍들 및 대응되는 공개 잎 커미트먼트들을 생성한다. (PAN 환경을 고려할 때, 전체 전자서명문의 수가 $2^{16}$보다 적을 것으로 가정한다.)
- 높이가 $\log n$인 프렉탈 Merkle 해쉬 트리를 초기화하고 공개 잎 커미트먼트 값들 $PLC_M^i$을 사용하여 공개키 $PK_M$을 계산한다. (여기서 $i=1,\cdots,n$.)
- 루트 검증 키 $VK_M^n = h^n(VK_M)$을 계산한다.
- 전자서명 번호 $i$를 0으로 설정한다.

**[단계 3]** Personal CA와 모바일 디바이스는 다음과 같은 매뉴얼 인증 절차를 수행한다.

- Personal CA는 랜덤 키 $k$를 생성한 후, 랜덤 키 $k$를 사용하여 $PCA, PK_{PCA}, M, PK_M, n, VK_M^n$에 대한 MAC 값을 계산한다. 이후, MAC 값과 키 $k$는 Personal CA에 디스플레이된다.
- 사용자는 Personal CA에 디스플레이된 MAC 값과 키 $k$를 모바일 디바이스에 입력하여 위의 파라메터에 대한 MAC 값을 재계산한다. 만약 두 개의 MAC 값이 동일하면, 모바일 디바이스는 사용자에게 성공 신호를 표시하며 그렇지 않으면, 실패 신호를 표시한다.

**[단계 4]** 만약 모바일 디바이스가 성공 신호를 표시하면, 사용자는 Personal CA가 인증서를 생성하도록 명령한다. Personal CA는 인증서를 생성하기 위하여, 시스템 보안 정책에 따라서 제어 윈도우 $CW$를 설정하고, 모바일 디바이스를 위한 아래와 같은 인증서 및 인증서의 인증 경로 $AuthPath_{PCA}^i$를 발행한다.

$$Cert_M = \{Ser\#, M, PK_M, n, VK_M^n, CW, Sig_{PCA}^i\}$$

여기서, $Ser\#$은 시리얼 넘버이다.

**[단계 5]** 인증서를 전송받은 모바일 디바이스는 발행된 인증서의 유효성을 검증하기 위하여 다음과 같은 두 가지 검증을 수행한다.

- $PK_{PCA}$와 $AuthPath_{PCA}^i$를 사용하여, 발행된 인증서에 대한 Personal CA의 일회용 전자서명을 검증한다.
- 인증서내의 모든 데이터 필드들이 올바른 값인지를 검증한다. 만약 모든 검증이 성공적이면, 프로토콜이 완료된다.

## 4.2 효율적인 인증 및 인증서 상태 검증 프로토콜

본 절에서는 서명 서버의 지원없이 빠른 전자서명 생성 및 검증이 가능한 효율적인 인증 프로토콜을 제안한다. 또한, 제안 프로토콜은 제어 윈도우 메커니즘을 사용하여 간략화된 인증서 상태 검증을 제공한다. 제안 프로토콜의 자세한 설명은 아래와 같다.

**[전자서명 생성]** 메시지 $m$에 대한 전자서명을 수행하기를 원하는 모바일 디바이스 $M_s$는 다음을 수행한다.

- Merkle의 일회용 전자서명 기법[4]을 아래와 같이 수행한다.
  - 전자 서명 번호 $i$를 증가시킨다.
  - 메시지 $m$에 대한 메시지 다이제스트 $md = h(m)$를 계산하고, $md$내의 '0'-비트에 대한 체크섬 $C$를 설정한 후, $msg = md \| C$로 설정한다.
  - $\{sk_{M_s}^{i,j}\}_{j=1}^{t}$와 대응되는 $\{pk_{M_s}^{i,j}\}_{j=1}^{t}$를 생성한다. (여기서 $t = |msg|$)
  - 아래와 같은 일회용 전자서명을 생성한다.
    $Sig_{M_s}^i = \{sk_{M_s}^{i,j} \forall j \in \{j | msg_j = 1\}, pk_{M_s}^{i,j} \forall j \in \{j | msg_j = 0\}\}$
- 현재 인증 경로 $AuthPath_{M_s}^i$를 계산하고, 프렉탈 Merkle 트리 알고리즘[5]을 이용하여 인증 경로를 갱신한다.
- 현재 검증 키 $VK_{M_s}^{n-i}$를 계산한다.
- 모바일 디바이스 $M_s$는 $m$, $Sig_{M_s}^i$, $AuthPath_{M_s}^i$, 전자 서명 카운터 $i$ 및 현재 검증 키 $VK_{M_s}^{n-i}$를 모바일 디바이스 $M_v$에게 전송한다.

**[전자서명 검증]** 모바일 디바이스 $M_v$는 모바일 디바이스 $M_s$의 상태를 검증하기 위하여 다음을 수행

한다.

- Personal CA에게 $Cert_{M_s}$의 상태가 유효한지 아닌지를 질의한다.
- $Cert_{M_s}$가 유효한 경우, 인증서내의 루트 검증키를 바탕으로 현재 검증키를 다음과 같이 검증한다.

$$h^i(VK_{M_s}^{n-i})? = VK_{M_s}^n$$

- 만약 모든 검증이 올바르면, 모바일 디바이스 $M_v$는 $Cert_{M_s}$를 캐쉬하고 현재 로컬 시간을 신뢰 시간의 시작점으로 설정한 후, $Cert_{M_s}$내의 제어 윈도우를 바탕으로 신뢰 시간의 종료점을 설정한다.

이후, 모바일 디바이스 $M_v$는 수신된 전자서명을 검증하기 위하여 다음을 수행한다.

- 메시지 $m$에 대한 메시지 다이제스트 $md' = h(m)$를 계산하고, $C'$를 $md'$에서의 '0'-비트 수로 설정한 후, $msg' = md' \| C'$로 설정한다.
- $Sig_{M_s}' = Sig_{M_s}$로 설정한다(여기서, $t = |msg'|$일 때, $Sig_{M_s}' = \{sig_j'\}_{j=1}^{t}$). 그리고, $\forall j \in \{j | msg_j' = 1\}$에 대하여 $sig_j' \leftarrow h(sig_j')$를 갱신하고, $PLC_{M_s}^i = \{sig_1' \| \cdots \| sig_t'\}$를 계산한다.
- 현재 인증 경로 $AuthPath_{M_s}^i$를 사용하여 $PLC_{M_s}^i$를 반복적으로 해쉬하고, $Cert_{M_s}$내의 $PK_{M_s}$과 그 결과를 비교한다.

기존에 제안되었던 서버지원 전자서명 기법들[8,9]와 비교하여, 제안 프로토콜은 서명 서버의 지원 없이 공개키 연산을 수행하지 않으므로, 제한된 컴퓨팅 능력을 가진 모바일 디바이스들의 계산상 오버헤드를 감소시킬 수 있다. 또한, 검증자는 신뢰 시점의 종단점까지 서명자의 인증서를 해쉬 체인에 기반하여 신뢰함으로써, 서명자의 인증서 상태 정보를 Personal CA에게 질의할 필요가 없다. 따라서, 제안 프로토콜은 OCSP[10]나 CRLs[3] 등과 같은 인증서 상태를 검증하기 위한 기법에 비해 보다 낮은 계산 및 통신상 비용을 요구하게 된다.

## 5. 평 가

본 절에서는 제안 프로토콜을 보안성 및 성능 관점에서 평가한다.

### 5.1 보안성 평가

시스템상의 안전한 연산을 제공하기 위하여, 제안 프로토콜에서 사용되는 일회용 전자서명과 제어 윈도우 메커니즘의 보안성이 증명되어야 한다. 먼저, 비밀값 생성 및 Merkle의 일회용 전자서명에서 해쉬 연산을 위하여 사용되는 일방향 해쉬 함수 $h()$가 충돌 회피성을 가진다는 것은 어떤 메시지 $m' \neq m$를 위한 전자서명을 위조 불가능하다는 것을 의미한다. 또한, 제어 윈도우 메커니즘에서 모바일 디바이스의 $i$ 번째 일회용 전자서명에 대응되는 현재 검증 키를 위조하기 위해서는 공격자가 모바일 디바이스의 인증서 내에 있는 루트 검증 키 $VK^n$의 $(n-i)$ 번째 해쉬 함수 $h()$의 역원(Inverse)를 계산해야 하지만 이는 계산상으로 실행 불가능하다.

### 5.2 성능 평가

표 1은 현재 가장 효율적인 서버지원 전자서명 기법[8]과 제안 프로토콜을 계산 및 저장 공간 요구사항의 관점에서 비교한 결과이다. 표 1에 사용되는 용어는 아래와 같다.

- $H$ : 해쉬 연산
- $S$ : 전통적인 전자 서명 생성
- $V$ : 전통적인 전자 서명 검증
- $p$ : OTS 검증을 위한 해쉬 연산의 수
- $m$ : OTS내의 공개 커미트먼트의 수
- $K$ : 보안 정보의 크기
- $C$ : 전자 서명 카운터의 크기
- $A$ : 인증 경로를 위한 해쉬 트리의 크기
- $T_c$ : 인증 경로의 계산
- $T_v$ : 인증 경로의 검증

표 1. 계산 및 저장 공간 요구사항의 비교

| | 컴포넌트 | [8] | 제안 프로토콜 |
|---|---|---|---|
| 계산 요구사항 (전자 서명에 대한) | 서명자 | $(m+1)H$ | $(m+1)H+1T_c$ |
| | 서버 | $(p+2)H+1S$ | - |
| | 검증자 | $1H+1V$ | $(p+1)H+1T_v$ |
| 저장 공간 요구사항 | 서명자 | $mH$ | $2K+1C+1A$ |
| | 서버 | $(m+p+1)H$ | - |
| | 검증자 | $1Cert$ | $1Cert$ |

제안 프로토콜에서 서명자의 계산상 오버헤드는 [8]에서 제안된 기법의 계산상 오버헤드와 유사하나, 제안 프로토콜에서의 전자서명 검증은 전통적인 전자서명 검증을 수행할 필요가 없으므로 [8]에서 제안된 기법보다 효율적이다. 또한, [8]에서는 분쟁상황을 해결하기 위하여, 서명 서버에서 모든 전자서명을 저장해야 하는 문제점을 가지고 있었으나, 제안 프로토콜은 서명 서버를 제거함으로써 서버에서의 높은 저장 공간을 필요로 하는 [8]의 문제점을 해결하였다. 또한, 서명자에서의 저장 공간 요구사항을 고려하면, 제안 프로토콜은 대략 1.9 KB만을 필요로 한다(두 개의 20 바이트 보안 정보, 1920 바이트의 해쉬 트리 및 4 바이트 전자 서명 카운터). 반면에, [8]은 3.3 KB를 필요로 한다(168×20 바이트 = 대략 3.3 KB).

제어 윈도우 메커니즘의 효율성을 고려하면, 검증자가 제어 윈도우 기간 동안 Personal CA에게 인증서 상태 정보를 질의하지 않기 때문에, 제안 프로토콜이 Personal CA에서의 전자서명 생성과 Personal CA와의 통신 패스의 수를 명백히 감소시키는 것을 알 수 있다. 통신비용에 대한 구체적이고 일반적인 측도를 위하여, [11]에서 소개된 파라메터들을 사용하여 OCSP 및 CRLs과의 통신 비용을 비교한다.

- $n$ : 발행된 인증서들의 전체 추정 수 ($n$= 300,000)
- $p$ : 만기일 이전에 취소될 인증서들의 추정 비율 ($p$= 0.1)
- $q$ : 하루에 발생되는 인증서 상태 검증 질의의 추정 수 ($q$= 300,000)
- $T$ : CRL이 하루에 갱신되는 횟수. $T$= 2이면, 12시간마다 주기적인 갱신이 발생
- $C$ : 제안된 공개키 프레임워크에서의 제어 윈도우의 크기. $C$= 2이면, 제어 윈도우의 크기는 2일
- $l_{sn}$ : 인증서의 시리얼 번호(serial number)를 위해 요구되는 비트 수 ($l_{sn}$ = 20)
- $l_{sig}$ : 전자 서명문의 비트 수 ($l_{sig}$ = 1024)
- $l_{hash}$ : 일방향 해쉬함수를 통해 계산된 해쉬값의 비트 수 ($l_{hash}$ = 160)

표 2는 추정되는 일간 통신 비용을 CRLs, OCSP와 제안 프로토콜의 세 가지 인증서 상태 관리 기법에 관하여 아래의 측정 기준으로 비교하였다.

표 2. 일간 통신비용

| | 통신 비용 (비트) |
|---|---|
| CRLs | $1.803\times10^{11}$ |
| OCSP | $3.132\times10^{8}$ |
| 제안 방안 | $2.046\times10^{8}$ |

- CRLs의 일간 통신 비용 : $T\cdot(p\cdot n\cdot l_{sn}+l_{sig})+q\cdot(p\cdot n\cdot l_{sn}+l_{sig})$
- OCSP의 일간 통신 비용 : $q\cdot l_{sn}+q\cdot l_{sig}$
- 제안 방안의 일간 통신 비용 : $\frac{q\cdot l_{sn}}{C}+\frac{q\cdot l_{sig}}{C}+q\cdot l_{hash}$

만약, OCSP를 대신하여 제안되는 제어 윈도우 메커니즘을 사용하면, 인증서 상태 관리를 위한 통신 비용은 대략 65%를 줄일 수 있게 된다.

## 6. 결 론

본 논문에서는 PAN을 구성하는 모바일 디바이스 상에서의 전자서명 생성과 검증시에 요구되는 계산상 오버헤드를 감소시키는 새로운 프로토콜을 제안하였으며, PAN내에서의 인증서 상태 관리를 위한 절차를 단순화하였다. 서버지원 전자서명 기법에 비하여, 제안 프로토콜은 서명 서버의 지원없이 공개키 연산을 수행할 필요가 없으며, 해쉬 체인을 기반한 제어 윈도우 메커니즘을 제안함으로써 인증서 상태 정보를 질의하고 검증하기 위한 통신 및 계산 비용을 경감하였다. 결과적으로, 제안 프로토콜은 제한된 컴퓨팅 능력을 가진 컴포넌트들로 이루어진 PAN 환경의 보안을 위한 적절한 암호학적 도구로 활용될 수 있다.

## 참 고 문 헌

[1] C. Gehrmann, K. Nyberg, and C. Mitchell, "The personal CA - PKI for a Personal Area Network," *Proceedings - IST Mobile & Wireless Communications Summit 2002*, June 2002.

[2] F. Stajano and R. Anderson, "The resurrecting

duckling: security issues for adhoc wireless networks," *The 7th International Workshop on Security Protocols*, pp. 172-194, 1999.

[3] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 public key infrastructure certificate and CRL profile," *RFC 2459*, January 1999.

[4] R. C. Merkle, "A digital signatures based on a conventional encryption function," *Advances in Cryptology - CRYPTO'87*, pp. 369-378, 1987.

[5] M. Jakobsson, F. Leighton, S. Micali, and M. Szydlo, "Fractal Merkel tree representation and traversal," *Topics in Cryptology - CT-RSA 2003*, pp. 314-326, 2003.

[6] D. Naor, A. Shenhav, and A. Wool, "One-Time Signature Revisited: Have They Become Practical?," *Cryptology ePrint Archive*, Report 2005/442, 2005.

[7] J. Zhou, F. Fao, and R. Deng, "An Efficient Public-Key Framework," *The 5th International Conference on Information and Communications Security*, pp. 88-99, October 2003.

[8] K. Bicakci and N. Baykal, "Server assisted signature revisited," *Topics in Cryptology - CT-RSA 2003*, pp. 143-156 March 2003.

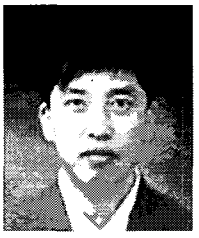
[9] X. Ding, D. Mazzocchi, and G. Tsudik, "Experimenting with Server-Aided Signatures," *2002 Network and Distributed Systems Security Symposium (NDSS'02)*, February 2002.

[10] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet public key infrastructure on-line certificate status protocol (OCSP)," *RFC 2560*, June 1999.

[11] M. Naor and K. Nissim, "Certificate revocation and certificate update," *The 7th USENIX Security Symposium*, January 1998.

**장 화 식**

1993년 계명대학교 통계학과 학사
1995년 부경대학교 전자계산학과 석사
1996년~1999년 제주관광대학 전임강사
2000년 부경대학교 전자계산학과 박사수료
2001년~현재 대덕대학 정보보안해킹과 조교수
※ 관심분야 : 정보보호, 암호학, 공개키 기반구조



**이 경 현**

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 석사
1992년 한국과학기술원 수학과 박사
1993년~현재 부경대학교 전자컴퓨터 정보통신공학부 교수
※ 관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론