초경량 이동 컴퓨팅 환경에서의 보안 컴포넌트 설계 및 구현

준회원 박 래 영*, 유 용 덕**, 종신회원 이 영 석*

Design and Implementation of the Security Components in Ultra-Lightweight Mobile Computing Environment

Rae-young Park*, Yong-duck You** *Associate Members,* Young-seok Lee* *Lifelong Member*

요 약

차세대 컴퓨터는 초경량 이동 컴퓨터로서 작은 크기에 휴대하기 편리하고 사용자가 이동 중이라도 주변의 휴대 장치들과 통신하여 동적으로 사용자 상황에 맞는 서비스를 제공한다. 사용자 상황에 맞는 서비스를 제공하기 위해서는 사용자나 컴퓨터의 정보를 보호할 수 있도록 보안의 문제점이 해결되어야 하며, 전원 제약적이고, 시스템 제한적인 초경량 이동 컴퓨팅 환경에 맞는 보안 기술이 필요하다. 본 논문에서는 초경량 이동 컴퓨팅 환경에서 효율적으로 운영 가능한 컴포넌트 기반 미들웨어를 소개하고 미들웨어에서 동적으로 적재 및 실행되는 보안 컴포넌트를 설계하고 구현한다. 구현된 보안 컴포넌트는 RC5 알고리즘을 이용한 암호화 기술과 SHA-1 알고리즘을 이용한 인증 기술을 포함한다.

Key Words : Security, Ultra-Lightweight, Mobile Computer, Component Based, RC5, SHA1

ABSTRACT

The next-generation computer is the ultra-lightweight mobile computer that communicates with peripheral handheld devices and provides dynamically the services appropriate to user. To provide the dynamic services on the ultra-lightweight mobile computer, security problem for user or computer system information should be solved and security mechanism is necessary for the ultra-lightweight mobile computing environment that has battery limit and low performance. In this paper, the security mechanism on the component based middleware for the ultra-lightweight mobile computer was implemented using RC-5 cipher algorithm and SHA-1 authentication algorithm. The security components are dynamically loaded and executed into the component based middleware on the ultra-lightweight mobile computer.

Ⅰ. 서 론

반도체 기술의 발달과 언제 어디서나 인터넷 서비스를 받고자하는 사용자들의 요구는 PDA (Personal Digital Assistant)나 스마트 폰(Smart Phone)과 같은 모바일 기기와 무선 인터넷 환경을 발전시켰다. 웨어러블 컴퓨터(Wearable Computer)와 같은 차세대 컴퓨터는 초경량의 이동 컴퓨터로서 작은 크기에 휴대하기 편리하고, 사용자가 이동 중에도 컴퓨터는 주변의 장비들과 통신하여 동적으로 사용자 상황에 맞는 정보 및 서비스를 제공한다.

이러한 초경량 이동 컴퓨터들이 실제로 이용되기

※ 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.
* 군산대학교 전자정보공학부 (0403134, leeys@kunsan.ac.kr), ** 충남대학교 컴퓨터공학과 (yyd7724@cnu.ac.kr)
논문번호 : KICS2007-01-039, 접수일자 : 2007년 1월 30일, 최종논문접수일자 : 2007년 3월 22일

위해서는 배터리(battery)나 메모리(memory), CPU (Central Processing Unit)와 같은 제한적인 시스템 자원을 효율적으로 사용하는 방법과 더불어 보안의 문제점이 해결되어야 한다. 초경량 이동 컴퓨터에서 사용자의 상황에 맞는 동적인 서비스를 이용하기 위해서 컴퓨터는 주변의 컴퓨터들과 사용자나 컴퓨터의 정보를 송수신하는 경우가 많으며, 상대적으로 유선보다 보안에 취약한 무선을 이용하여 통신하기 때문에 사용자의 정보를 보호하는 방법이나 신뢰성 있는 채널을 이용하는 방법 등이 요구된다.

현재 PC에서는 위의 보안을 목적으로 PKI Protected Access)등의 기술들이 사용되고 있지만, 초경량 이동 컴퓨터의 경우시스템 자원이 매우 제한적이기 때문에 PC에 적용되는 기술들을 그대로 초경량 이동 컴퓨터에 적용할 수는 없다.

따라서 본 논문에서는 초경량 이동 컴퓨팅 환경에 적용될 수 있는 보안 기술을 구현한다. 구현된 보안 기술은 초경량 이동 컴퓨팅 환경에서 운영될 수 있도록 컴포넌트(Component)화 되어 설계되었으며, 사용자의 정보를 보호하기 위한 암호화 기술과 신뢰성 있는 채널에서 데이터를 확인하기 위한 인증 기술을 포함하고 있다.

논문에서 사용되는 보안 기술은 초경량 이동 컴퓨터를 위한 미들웨어에서 컴포넌트화 되어 사용된다. 초경량 이동 컴퓨터를 위한 미들웨어는 여러 개의 컴포넌트로 구성되며, 컴포넌트 매니저(manager)에 의해 동적으로 관리된다.

이어지는 2장에서는 초경량 이동 컴퓨터와 컴퓨팅 환경 및 초경량 이동 컴퓨터를 위한 미들웨어에 대해 소개하고, 3장에서는 초경량 이동 컴퓨팅 환경에 비슷한 PC 모바일 환경에서의 보안 문제점과 보안 기술에 대해 알아보고, 초경량 이동 컴퓨팅 환경에서 사용될 수 있도록 컴포넌트화 된 보안 기술에 대해 설명한다. 4장에서는 구현된 보안 기술에 대한 성능분석을 기술하고, 5장 결론에서는 이야기한 사항을 요약하고, 향후 연구 과제에 대해 논의한다.

Ⅱ. 초경량 이동 컴퓨팅 환경

2.1. 초경량 이동 컴퓨터와 컴퓨팅 환경

초경량 이동 컴퓨터는 웨어러블 컴퓨터와 같이 작은 크기로 휴대하기 편리하며, 주변의 다른 디바이스들과 통신하여 사용자 상황에 맞는 서비스를 제공한다. 휴대를 위해 배터리를 전원으로 사용하고, 제한적인 메모리와 CPU를 가질 뿐 아니라 컴퓨터의 시스템 소프트웨어나 응용 프로그램 또한 제한적인 자원을 효율적으로 사용할 수 있도록 가벼워야 한다.

초경량 이동 컴퓨터는 사용자가 휴대하고 있는 다양한 종류의 센서, 휴대용 정보 장치, 휴대용 디스 플레이 장치, 착용형 정보 장치 등의 소형 디바이스들 간에 사용자 근거리 네트워크(PAN : Personal Area Network)를 구성하고 단거리의 유선 또는 무선 인터페이스를 통해 각 휴대 장치와 통신한다.

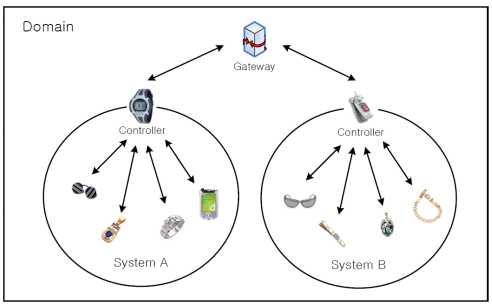


그림 1. 사용자 근거리 네트워크

그림 1에서 컨트롤러(Controller)는 초경량 이동 컴퓨터를 나타내며, 시스템(System)은 초경량 이동 컴퓨터가 디바이스들을 제어할 수 있는 범위, 즉 PAN을 나타낸다. 더불어, 도메인(Domain)은 초경량 이동 컴퓨터가 통신할 수 있는 논리적인 범위를 나타낸다.

초경량 이동 컴퓨터가 주위의 네트워크를 이용하여 여러 가지 응용 서비스들을 이용할 경우, 가장 가까이에 있는 게이트웨이(Gateway)를 이용하여 통신하게 되는데, 전체적인 네트워크는 그림 2와 같이 초경량 이동 컴퓨터와 홈 네트워크(Home Network), 방문 네트워크(Visitor Network), 서비스 제공을 위한 요소로 나눌 수 있다.

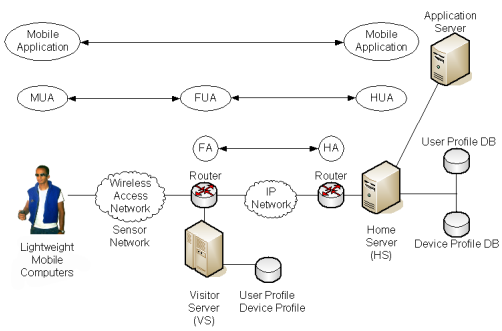


그림 2. 응용 서비스를 위한 네트워크 구성도

사용자 정보 및 디바이스 정보는 사용자의 홈 네트워크의 프로파일에 기록되어 있고, 사용자 이동에 따른 정보는 홈 네트워크와 방문 네트워크의 이동성 지원 기능에 따라 사용자의 이동에 상관없이 지속적인 서비스가 가능하다. 홈 네트워크의 프로파일 정보를 통해 적절한 서비스가 제공되며 사용자의 이동 시, 방문 네트워크는 홈 네트워크와의 프로파일 동기화를 통해 지속적으로 서비스를 제공할 수 있다. 또한 사용자가 새로운 디바이스를 추가할 때도 프로파일을 이용하여 홈 네트워크와 방문 네트워크 어느 곳에서도 투명하게 서비스를 이용할 수 있다.

2.2 초경량 이동 컴퓨터를 위한 미들웨어

초경량 이동 컴퓨터는 다양한 휴대용 디바이스들 간의 근거리 네트워크를 구성한다. 이러한 다양한 디바이스들을 제어하고 시스템에 관계없이 동일한 서비스를 제공할 수 있도록 미들웨어(Middleware)가 필요하다. 미들웨어는 운영체제 위에서 동작하며, 시스템 플랫폼에 대한 고려 없이 응용 프로그램을 개발 및 동작할 수 있도록 시스템 API 제공한다.

이러한 분산 미들웨어로서 CORBA[1]와 Jini[2]가 있다. CORBA(Common Object Request Broker Architecture)는 원격지에 존재하는 객체를 접근하거나 서비스를 이용하기 위하여 가장 일반적으로 사용되며, JINI(Java Intelligent Network Infrastructure)는 IP 기반 네트워크와 플러그 앤 플레이(Plug and Play)를 지원한다. 하지만, 이들 분산 미들웨어는 컴퓨터 디바이스들이 고정되어 있고 네트워크를 통해 연결된 분산 컴퓨팅 환경에 적합한 미들웨어로서, 자원 제한적이고 장비 및 사용자 이동성 특징을 갖는 이동 컴퓨팅 환경에서는 적합하지 않다.

현재 초경량 이동 컴퓨터를 위한 미들웨어에 관한 연구가 여러 곳에서 진행 중에 있다. Puppeteer[3]이나 PARM[4]은 전력을 관리하는 기능을, Aura[5]는 시스템의 상태에 따라 동적으로 자원을 할당하는 기능을, Maté[6]은 초경량 응용 프로그램 개발을 지원하는 기능을 가지고 있으나 이들 미들웨어는 분산 컴퓨팅 환경에서 요구되는 일부 기능을 대상으로 연구되고 있어, 초경량 이동 컴퓨팅 환경에 요구되는 기능에 만족하지는 못한다.

이에 컴포넌트 기반 초경량 이동 컴퓨터 미들웨어를 이용한다. 컴포넌트 기반 초경량 이동 컴퓨터 미들웨어는 여러 개의 컴포넌트로 구성되며, 각각은 컴포넌트 관리자(Component Manager)에 의해 관리된다.

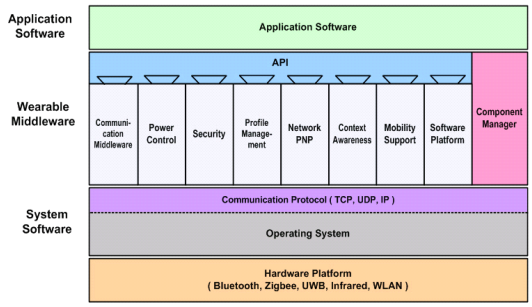


그림 3. 미들웨어 프레임워크 구조

미들웨어의 구조를 보면 그림 3과 같다. 사용된 미들웨어는 컴포넌트 관리자와 각 컴포넌트, 그리고 APIs로 구성된다. 각 컴포넌트는 분산 통신, 전력 제어, 프로파일 관리, 네트워크 PnP, 상황 인지, 이동성 지원, 소프트웨어와 보안 컴포넌트로 구성된다. 각각의 컴포넌트는 사용자의 요청 또는 사용자의 상황에 맞게 동적으로 설정, 설치, 삭제된다. APIs는 컴포넌트 API 집합으로 컴포넌트가 설치, 삭제될 때 동적으로 확장되거나 축소된다.

미들웨어에 대한 자세한 내용은 경량 미들웨어를 위한 소프트웨어 구조[7]에서 찾아볼 수 있으며, 본 논문은 초경량 이동 컴퓨터를 위한 미들웨어에서 보안에 관한 컴포넌트를 설계 구현하였다.

Ⅲ. 초경량 이동 컴퓨팅 환경에서의 보안기술

3.1 PC 모바일 환경의 보안 기술

초경량 이동 컴퓨팅 환경과 비슷한 환경으로 현재 PC 모바일 환경이 있으며, 이 또한 이동으로 인한 사용자 정보 노출 문제와 무선 인터페이스로 사용함으로 인한 신뢰성 있는 채널 확보 등, 현재 초경량 이동 컴퓨팅 환경이 가지고 있는 보안 문제점과 비슷한 문제점과 기술을 가지고 있다. 따라서 현재 PC 모바일 환경의 보안 기술[8]에 대해 정리한다.

3.1.1 WPA(Wi-Fi Protected Access)

PC 모바일 환경은 전파를 이용하여 통신하기 때문에 보안 장치가 없을 경우, 전파의 유효 반경 내에 위치하는 누구든지 통신 내용을 도청할 수 있다. WPA는 Wi-Fi 무선 랜 사용자를 위해 개발된 무선 랜 보안 표준 중 하나로서 이전에 사용되던 WEP

(Wired Equivalent Privacy)의 고정 암호키 방식으로 인한 사용자 인증 문제를 해결하기 위해 개발되었다. WPA는 128비트의 키 길이를 가지며, 데이터 암호화를 위해 RC4 암호화 방식을 사용한다. 또한, 사용자, 네트워크 세션 또는 전송되는 프레임 별로 키를 달리하는 TKIP(Temporal Key Integrity Protocol) 방식을 채택하여 외부 공격자가 네트워크 도청을 통하여 키를 추출하는 공격에 대해 저항성을 갖게 하였다.

3.1.2 RSN(Robust Security Network)

RSN은 상호 인증을 통한 접근제어, 동적인 키 갱신과 강력한 암호 알고리즘을 사용한 새로운 형태의 보안 구조로서, RSN 네트워크를 구축하며 사용자 인증, 접근제어, 권한 검증, 데이터 기밀성, 데이터 무결성 등을 만족한다. CCMP 알고리즘을 사용하고 암호 알고리즘 처리 모듈을 하드웨어로 구현하기 때문에 알고리즘 처리 속도는 빠르다.

3.1.3 PKI(Personal Key Infrastructure)

PC 모바일 환경뿐만 아니라 일반적인 PC 환경에서도 사용자의 정보를 보호하기 위해 PKI를 사용한다. PKI는 인터넷과 같이 보안이 보장되지 않은 사용자가 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 비밀키를 사용하여 암호화/복호화 함으로써 데이터 암호화와 사용자 인증의 문제를 해결한다.

3.2 초경량 이동 컴퓨팅 환경의 보안 기술

3.1에서 PC 모바일 환경의 보안 기술에 대해 알아보았다. 그러나 초경량 이동 컴퓨팅 환경에서는 이동 및 휴대를 쉽게 하기 위해 전원을 배터리로 사용하고, 제한적인 메모리와 CPU를 사용한다. 비슷한 환경에서 보안을 위해 안정적인 전원과 여유로운 시스템 자원을 사용하여 복잡한 계산을 하는 PC 모바일 환경 달리 초경량 이동 컴퓨터의 자원이 제약적이기 때문에 보안에 대해 위의 PC 모바일 환경의 보안 기술을 그대로 초경량 이동 컴퓨팅 환경에 적용하기에는 무리가 있다.

본 장에서는 PC 모바일 환경에서 사용된 보안 기술을 토대로 초경량 이동 컴퓨팅 환경을 위한 보안 기술에 대해 제안한다. 제안하는 기술은 2장에서 소개된 초경량 이동 컴퓨팅 미들웨어에서 사용될 수 있도록 컴포넌트화 되어 설계되었으며, 사용자의 정보를 보호하기 위한 암호화 기술과 신뢰성 있는 채널을 확인하기 위한 인증 기술을 포함하고 있다.

3.2.1 보안 컴포넌트의 구조

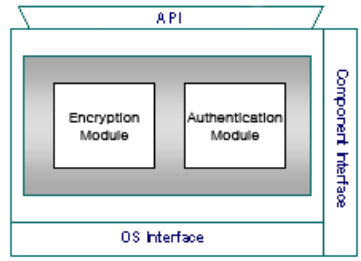


그림 4. 보안 컴포넌트의 구조

보안 컴포넌트는 그림 4와 같이 핵심 모듈과 API, 컴포넌트 인터페이스, 운영체제 인터페이스로 구성되어 있다. 핵심 모듈은 컴포넌트가 수행하는 서비스 기능을 구현한 것이며, API는 핵심 모듈에서 유도된 API로서, 컴포넌트가 응용에게 서비스를 제공하고자 할 때 응용 프로그램에 의해 호출된다. 컴포넌트 인터페이스는 컴포넌트 관리자나 다른 컴포넌트와의 인터페이스를 위해 정의되었다. 운영체제 인터페이스는 컴포넌트가 동작하기 위해 필요한 시스템 콜(system call)로 이루어져 있다.

3.2.2 보안 컴포넌트의 기능 및 설계

PC 모바일 환경에서 보는 바와 같이 보안의 기술은 크게 기밀성을 위한 암호화 기술과 무결성 및 정확성을 위한 인증 기술, 그리고 암호화와 인증을 위한 키를 관리하고 분배하는 키 관리 기술로 나뉜다.

본 논문에서 제안하는 기술은 암호화 기술과 인증 기술로서, 키 관리는 키 사전 분배 방식으로 한정한다.

(1) 암호화 기술

암호화 기술은 초경량 이동 컴퓨팅 환경과 가장 비슷한 WSN(Wireless Sensor Network)에서 고안된 RC5 블록 암호화 알고리즘[9]를 사용하였다. RC5 알고리즘은 마이크로프로세서에서 일반적으로 사용하는 XOR, Shift, 모듈러 연산 등의 기본적인 연산을 사용할 뿐만 아니라 메모리 요구량이 낮고, 간단한 알고리즘을 사용하여 속도가 빠르다.

표 1과 표 2는 WSN 환경에서 6가지 블록 암호화 알고리즘에 대해 성능을 비교 분석한 결과[10] 중에서 메모리 요구에 관한 내용으로 다른 블록 암호화 알고리즘 보다 낮은 메모리를 요청함을 알 수 있다.

표 1. 데이터 메모리 요청

	skey	CBC	CFB	OFB	CTR
RC5	92	64	42	42	44
RC6	62	100	62	62	64
Rijndael	16,32	92	54	54	56
MISTY1	4	62	40	40	42
KASUMI	58	62	40	40	42
Camellia	170	148	110	110	112

표 2. 코드 메모리 요청

	CBC	CFB	OFB	CTR
RC5	1746	908	836	986
RC6	2576	1324	1252	1402
Rijndael	14716	12688	112616	12766
MISTY1	7132	4222	4150	4300
KASUMI	9702	5446	5374	5524
Camellia	19708	12382	12310	12460

RC5 알고리즘의 암호화 과정은 크게 키 확장 과정과 암호화 과정으로 나뉜다.

키 확장은 암호화 각 과정에 사용될 수 있도록 키를 비트 수와 라운드 수에 맞게 확장하는 과정이다. 키 확장을 위해서는 첫째로 각 라운드 별로 2개의 서브키와 별도의 연산에 적용하기 위해 다음 (1)과 같이 w비트 단위의 t개의 서브키가 필요하다.

$$t=2(r+1) \quad (1)$$

서브키를 이용하여 서브 키 배열 S를 만들고, 배열을 초기화(initialize) 한다(2).

```
S[0], S[1], …; S[t-1]          /* 서브키 배열 S */
S[0]=Pw=Odd((e-2)*2**W)        /* 초기화 */
for (i = 1 ; i < t ; i++)
    S[i]=S[i-1]+Qw(Qw=Odd((phi-1)*2**W))   (2)
```

byte키 배열 K를 초기화된 배열 S의 값과 혼합(mix)하기 위해 word 배열 L로 변환(convert)하고, L과 S의 혼합(mix)연산을 실행하여 워드 단위의 서브 키 배열 S를 생성한다.

암호화 과정에서 평문 2word를 w비트 레지스터 A와 B에 각각 저장하여 암호화한다. 각 라운드에서 좌우 양쪽 단어의 치환, 순열, 키 의존치환 처리 과정을 거치며, 양쪽 단어는 각 반복시마다 갱신된다. 암호화 과정은 (3)과 같은 과정을 통해 진행된다.

```
A=A+S[0];
B=B+S[1];
for (i=1 ; i<=R ; i++) {
A=A^B;
A=ROTL(A,B,W)+S[2*i];
B=B^A;
B=ROTL(B,A,W)+S[(2*i)+1];}   (3)
```

(2) 인증 기술

인증은 데이터가 안전하지 않는 채널을 통하여 수확인한다.

해시(hash) 함수는 임의의 길이의 메시지를 일정 길이의 출력으로 변환해주는 함수로, 주어진 출력에 대해서 입력 값을 구하는 것이 불가능(일방향성)하고, 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것 또한 불가능(충돌 회피성)한 특성을 가지고 있기 때문에 인증에 많이 사용된다.

보안 컴포넌트의 인증 기술은 해시 함수 중 SHA-1 알고리즘[11]을 이용하여 구현하였다. SHA-1 알고리즘은 임의의 길이를 가지는 입력 메시지를 512bit 블록 단위로 처리하여 40bit (5byte)의 출력을 낸다. 알고리즘의 과정은 임의의 길이의 메시지 M이 입력으로 들어오면 이 M을 패딩(padding)과정을 통해 512bit의 배수로 만든 후, 512bit 블록 $M_i(1 \le i \le n)$로 나눈다. 각 블록 M_i를 단계 연산 과정을 통해 압축한다. 512bit 단위 블록을 처리하는 압축 함수는 모두 4라운드, 80단계로 구성된다.

단계 연산에서 아래의 논리 함수를 이용하여 연산한다. 각각의 $f_i(0 \le t \le 79)$는 3개의 32bit 워드를 입력으로 받아 32bit 워드를 출력한다.

```
f(t;B,C,D)=(B AND C) OR ((NOT B) AND D)
                                  (0<=t<=19)
f(t;B,C,D)=B XOR C XOR D          (20<=t<=39)
f(t;B,C,D)=(B AND C) OR (B AND D)
        OR (C AND D)              (40<=t<=59)
  f(t;B,C,D)=B XOR C XOR D        (60<=t<=79)
                                   (4)
```

메시지 다이제스트를 계산하기 위해서는 먼저 다섯 개의 초기 연쇄변수를 초기화하고, M_i를 16개의 32bit 워드 W_0, W_2, …; W_{15}로 분할한 후, $16 \le t < 79$에 대해서 다음과 같이 연산한다(5).

$$Wt=S_1(W_{t-3} \ XOR \ W_{t-8} \ XOR \ W_{t-14} \ XOR \ W_{t-16}) \quad (5)$$

다음으로 $A=H_0$, $B=H_1$, $C=H_2$, $D=H_3$, $E=H_4$로 갱신하고, $0 \le t < 79$에 대해 (6)를 수행한 후 $H_0=H_0+A$, $H_1=H_1+B$, $H_2=H_2+C$, $H_3=H_3+D$, $H_4=H_4+E$로

갱신한다.

$$TEMP=S_5(A)+f_t(B,C,D)+E+W_t+K_t \ ;$$
$$E=D;\ D=C;\ C=S_{30}(B);\ B=A;\ A=TEMP \quad (6)$$

M_1부터 M_n까지 모두 처리한 후, 연쇄변수 H_0, H_1, H_2, H_3, H_4를 연결시킨 것이 40bit MAC이 된다.

본 논문에서 구현한 인증 기술의 메시지 형식은 메시지 상태를 표현하기 위한 헤더(header) 4바이트와 가변길이의 데이터, 5바이트의 MAC으로 구분된다.

Ⅳ. 보안 기술 구현 평가

본 장에서는 구현한 보안 컴포넌트의 성능을 비교 분석한다. 첫째로, 초경량 이동 컴퓨팅 환경에서의 성능 및 기능을 테스트하기 위하여 센서 네트워크 운영체제인 TinyOS의 보안 프로토콜 TinySec과 비교한다. 표 3에서 보는 바와 같이 보안 컴포넌트는 자원 제약적인 센서 네트워크를 위한 보안 프로토콜과 비슷한 성능과 기능을 가지고 있다.

표 3. 보안 컴포넌트와 TinySec 비교

	보안 컴포넌트	TinySec
언어	C	NesC
크기	40.5K	7.1K
암호화	RC5	RC5, Skipjack
인증	SHA-1 MAC	CBC MAC

두 번째는 보안 컴포넌트를 초경량 이동 컴퓨터에서 운영함에 있어 암호화 기능과 인증 기능이 이상 없이 동작하는지 확인한다. 테스트를 위한 컴퓨터는 표 4와 같은 성능을 가지며, 토크(talk) 프로그램을 사용하여 전송된 데이터에 암호화와 인증을 테스트 한다.

표 4. 테스트 컴퓨터 사양

CPU	ARM 9 Core Freescale i.MX21(350MHz)
Memory	128MB
OS	Embedded ARM Linux 2.4.20
Network	DWL-G122 Wireless Lan Card

암호화는 테스트 컴퓨터와 데스크톱 컴퓨터를 이용하여 테스트 컴퓨터에서 평문을 입력받아 암호문으로 변환하여 데스크톱 컴퓨터에 전송하는지 확인하고, 데스크톱 컴퓨터에서 전송한 암호문을 수신하여 평문으로 복호화 하는지 테스트 한다. 인증은 데스크톱 컴퓨터에서 테스트 컴퓨터로 메시지와 MAC을 전송하고 받은 MAC와 테스트 컴퓨터에서 생성한 MAC을 비교하여 일치 여부를 검사한다.

마지막으로, 컴포넌트 동적 재구성 성능을 테스트하기 위해 다른 컴포넌트를 비롯하여 설치 및 삭제에 따른 소요 시간을 분석한다. 컴포넌트의 동적 재구성 기능은 미들웨어의 확장성과 유연성을 제공하지만 재구성을 위한 시간을 예측할 수 없거나 지연이 큰 경우에 성능이 저하되며, 사용자에게 불편을 주기 때문에 적절한 재구성 시간을 가져야 한다.

미들웨어 내에서 동적 재구성을 위한 소요 시간만을 측정하기 위하여 컴포넌트를 컴포넌트 서버에서 테스트 컴퓨터에 다운로드 한 상태에서 실험하였다. 측정하는 컴포넌트 및 컴포넌트의 크기, API 수는 표 5와 같으며, 측정된 소요 시간은 해당 컴포넌트 메모리 로드에 따른 시간과 컴포넌트에서 제공하는 API에 대한 참조 정보를 APIRT(API Reference Table)로 구성하는 시간을 포함한다. 측정은 컴포넌트 당 90회씩 반복 시험하였다.

표 5. 컴포넌트 정보

컴포넌트	크 기	API 수
보 안	15Kbyte	7
분산 통신	11Kbyte	27
프로파일 관리	59Kbyte	11
이동성 지원	271Kbyte	11

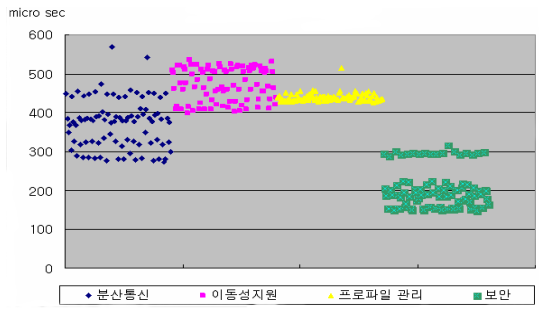


그림 5. 컴포넌트 설치 소요 시간 분포

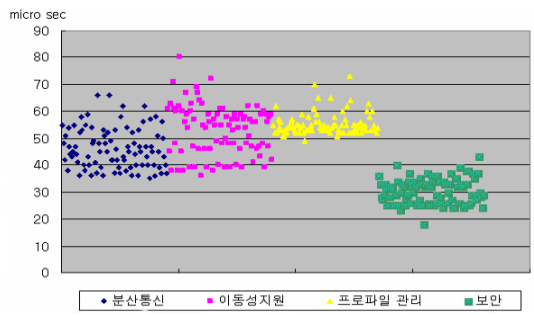


그림 6. 컴포넌트 삭제 소요 시간 분포

테스트 결과는 컴포넌트 설치 시간과 삭제 시간은 그림 5와 그림 6과 같이 측정되었으며, 각 컴포넌트에 대한 자세한 소요 시간은 표 6과 같다.

표 6. 컴포넌트 별 설치 소요/삭제 시간 (단위:μs)

컴포넌트	최소시간	최대시간	중앙값	평균값
보안	148/18	316/43	192/29	204.1/30
분산통신	273/35	552/66	381/45	372.5/48.24
프로파일 관리	425/49	516/73	437/54	439.5/55.3
이동성 지원	399/36	537/80	472/55	473.1/58.5

테스트 결과, 표 6에서 보는 바와 같이 보안 컴포넌트의 설치 및 삭제 소요 시간의 중앙값과 평균값이 192μs, 204.1μs와 29μs, 30μs인 비슷한 범위로 컴포넌트 설치와 삭제가 일정 시간 범위 안에서 일어나고, 미들웨어를 재구성함에 있어 사용자에게 컴포넌트의 설치 및 삭제에 불편함을 느끼지 않을 정도의 시간적 성능을 보인다.

Ⅴ. 결론 및 향후 연구 계획

초경량 이동 컴퓨팅 환경에서의 컴퓨터는 작은 사이즈에 휴대하기 편리하면서도 주변의 휴대 장치들과 통신하여 사용자 환경에 맞는 서비스를 동적으로 제공한다. 이러한 서비스를 사용하기 위해서는 배터리, 메모리, CPU와 같은 제한적인 시스템 자원을 효율적으로 사용하는 방법과 함께 빈번한 사용자 및 컴퓨터의 정보를 안전하게 송수신하기 위한 초경량 이동 컴퓨팅 환경에 맞는 보안 기법이 필요하다. 본 논문에서는 초경량 이동 컴퓨팅 환경에 맞는 컴포넌트 기반 미들웨어와 미들웨어에서 사용할 수 있는 경량화 된 보안 컴포넌트를 제안하였다. 보안 컴포넌트는 사용자 요구에 따라 미들웨어 내의 컴포넌트 관리자에 의해 동적으로 설정, 설치, 삭제될 수 있다. 또한, RC5 알고리즘을 이용하여 사용자의 정보를 보호할 수 있는 암호화 기술과 SHA-1 알고리즘을 이용하여 신뢰되지 않은 채널에서 전송된 데이터의 신뢰성을 확인하기 위한 인증 기술을 초경량 이동 컴퓨팅 환경에서도 운영될 수 있도록 구현하였다. 향후 초경량 이동 컴퓨팅 환경에 맞는 키 관리 기술과 ECC(Elliptic Curve Cryptography)와 같이 공개키 기반 구조에서 보안 메커니즘을 적용하는 방안에도 연구가 필요하다.

참 고 문 헌

〔1〕 S. Vinoski, "CORBA: integrating diverse applications within distributed heterogeneous environments", *IEEE Communications Magazine*, pp. 46-55, Volume 35, Issue: 2 , Feb. 1997

〔2〕 J. Waldo, "Alive and well: Jini technology today", *Computer*, Vol.33, No. 6, pp.107 - 109, June 2000

〔3〕 J. Flinn, E. D. Lara, M. Satyanarayanan, D. S. Wallach, and W. Zwaenepoel, "Reducing the energy usage of office applications," *IFIP/ACM*, 2001

〔4〕 S. Mohapatra and N. Venkatasubramanian, "PARM : Power aware reconfigurable middleware," Proc. of Int'l Conf. on Dist. *Computing Systems*, pp.1-8, 2003

〔5〕 D. Garlan and et al., "Project Aura: Toward Distraction-Free Pervasive Computing," *IEEE Pervasive Comp.*, Apr. June 2002

〔6〕 P. Levis and D. Culler, "Maté : A Tiny virtual machine for sensor networks," *Proc. of Int'l Conf. Architectural Support for Prog. Languages and Op. Sys.* 2002

〔7〕 유용덕, 최훈, 김형신, 권영미, Takeshi Nanri "경량 미들웨어를 위한 소프트웨어 구조", *한국차세대PC학회 논문지*, Vol.1 No.2, pp.34-42. December 2005.

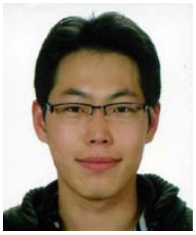
〔8〕 최경호 김정식, 임을규, "모바일 환경에서의 보안 기법 연구", *한국정보보호학회 하계정보보호학술대회 논문집*, Vol 16, No.1, pp 314-315, June 2006.

〔9〕 R. Baldwin, R. Rivest "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", *RFC 2040*, October 1996

〔10〕 Y. W. Law and J. M. Doumen and P. H. Hartel, "Benchmarking Block Ciphers for Wireless Sensor Networks(Extended Abstract)", *1st IEEE Int. Conf. on Mobile Ad-Hoc and Sensor Systems (MASS 2004)*, Fort Lauderdale, Florida, October 2004

〔11〕 D. Eastlake, P. Jones, "US Secure Hash Algorithm 1(SHA1)", *RFC 3174*, Sep. 2001.

박 래 영 (Rae-young Park) 준회원



2006년 2월 : 군산대학교 전자정보공학부 졸업
2007년 3월~현재 : 군산대학교 전자정보공학부 석사과정
<관심분야> 이동컴퓨팅, 시스템/네트워크 보안

유 용 덕 (Yong-duck You) 준회원

1999년 2월 : 충남대학교 컴퓨터공학과 졸업
2002년 2월 : 충남대학교 컴퓨터공학과 석사
2007년 2월 : 충남대학교 컴퓨터공학과 박사
2007년 3월~현재 : 충남대학교 박사 후 연수과정
<관심분야> 이동컴퓨팅, 임베디드 시스템, 미들웨어, 자가 치유 기법

이 영 석 (Young-seok Lee) 종신회원

1992년 2월 : 충남대학교 컴퓨터공학과 졸업
1994년 2월 : 충남대학교 컴퓨터공학과 석사
2002년 2월 : 충남대학교 컴퓨터공학과 박사
1994~1997년 : LG전자 정보통신 연구소 연구원
2002~2004년 : 한국전자통신연구원 선임연구원
2004년~현재 : 군산대학교 전자정보공학부 교수
<관심분야> 시스템/네트워크 보안, 이동컴퓨팅, 분산시스템