情報保護學會論文誌
第18卷 第1號, 2008. 2

3GPP2 C.S0024-A v.2.0 표준을 적용한 CDMA2000 1x EV-DO 보안 계층 설계 및 구현*

양 종 원[1†], 조 진 만[2], 이 태 훈[3], 서 창 호[1‡]
[1]공주대학교, [2]한국전자통신연구원, [3]광주대학교

Design and Implementation of the CDMA2000 1x EV-DO Security Layer to which applies 3GPP2 C.S0024-A v.2.0 Standard*

Jongwon Yang[1†], Jinman Cho[2], TaeHoon Lee[3], Changho Seo[1‡]
[1]Kongju National University, [2]ETRI, [3]Gwangju National

요 약

CDMA2000 1x EV-DO 에서의 보안 계층은 현재 3GPP2를 통해 표준화 규격(C.S0024-A v2.0)을 완성해 나가고 있는 중이다. 이에 따라 CDMA2000 1x EV-DO 환경의 AT(Access Terminal)와 AN(Access Network) 간 전송되는 데이터에 대한 보안 기능을 적용하기 위하여 표준 문서에 명시된 보안 계층 구현에 필요한 보안 장치가 요구되고 있다. 본 논문은 3GPP2의 C.S0024-A v2.0 표준을 준용한 CDMA2000 1x EV-DO 보안계층 설계 및 구현을 통해 AT와 AN간의 안전하고 빠른 데이터 전송 및 다양한 플랫폼 환경에 적용 가능한 보안계층 시스템을 실제 적용했다.

ABSTRACT

In security layer in the CDMA2000 1x EV-DO, a standard - C.S0024-a v2.0 is being accomplished under the project of 3GPP2(3rd Generation Partnership Project2). Therefore, a security device is needed to implement the security layer which is defined on the standard document for data transfer security between AT(Access Terminal) and AN(Access Network) on CDMA2000 1x EV-DO environment. This paper realizes the security layer system that can make safe and fast transfer of data between AT and AN. It could be applied to various platform environments by designing and implementing the Security Layer in the CDMA2000 1x EV-DO Security Layer to which applies C.S0024-A v2.0 of 3GPP2.

Keywords : 3GPP, EV-DO, C.S0024-A v2.0

I. 서 론

현재 WCDMA 라디오 액세스 기술을 기반으로 하는 3GPP 3세대 이동통신 시스템은 전세계에서 광범위하게 전개되고 있으며, 특히 CDMA2000 이동통신 표준 개발을 맡고 있는 3GPP2에서는 중기 진화 전략으로 CDMA2000 E-PDAI(Enhanced Packet Data Air Interface) 요구규격을 준비하고 있다. Enhanced CDMA2000 Phase2 혹은 1xEv-DO Rev. C로 불리기도 하는 이 기술은 2008년 하반기까지 상용화를 목표로 하고 있으며 고속 데이터 서비스 제공을 위한 무선 규

접수일: 2007년 7월 20일; 채택일: 2007년 11월 1일
* 이 논문은 2007년도 한국과학재단 특정기초사업의 지원에 의하여 연구되었음(R01-2005-000-10200-0)
† 주저자, nobody@kongju.ac.kr
‡ 교신저자, chseo@kongju.ac.kr

격을 정의할 예정이다[1].

특히 CDMA2000 1x EV-DO 에서의 보안 계층은 현재 3GPP2를 통해 표준화 규격(C.S0024-A v2.0)을 완성해 나가고 있는 중이다[2][3]. 이에 따라 CDMA2000 1x EV-DO 환경의 AT와 AN 간 전송되는 데이터에 대한 보안 기능을 적용하기 위하여 표준 문서에 명시된 보안 계층 구현에 필요한 보안 장치가 요구되고 있다[4].

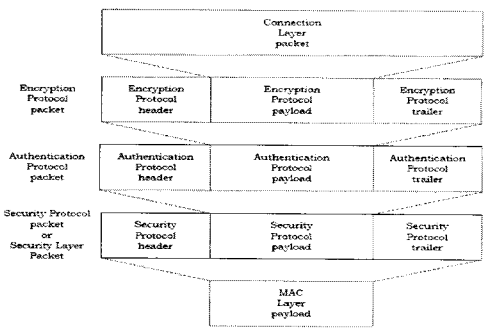
본 논문은 3GPP2의 C.S0024-A v2.0 표준을 준용한 CDMA2000 1x EV-DO 보안계층 설계 및 구현을 통해 AT와 AN간의 안전하고 빠른 데이터 전송 및 다양한 플랫폼 환경에 적용 가능한 보안계층 시스템을 실제 적용했다. 예를 들면 보안 프로토콜 데이터에 대한 로깅 지원 및 AT와 AN의 보안 프로토콜 지원을 위한 CDMA2000 1x Ev-DO용 보안계층 구현 라이드러리 모듈 및 AN과 AT이 시스템으로 운용될 수 있도록 하는 테스트를 위한 시뮬레이터 그리고 마지막으로 USB2.0 인터페이스를 이용한 데이터 전송 처리 지원과 3GPP2의 C.S0024-A v2.0 표준에 명시된 알고리즘을 지원할 수 있는 하드웨어를 구현하였다.

본 논문의 구성은, 2장에서 CDMA2000 1x EV-DO 보안장치 구조에 대해 설명하며, 3장에서는 제안한 CDMA2000 1x EV-DO 보안계층 설계 및 구현을 설명한다. 마지막으로 4장에서 결론을 맺는다.

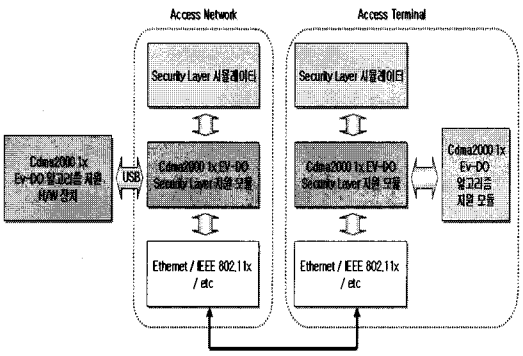
Ⅱ. CDMA2000 1x EV-DO 보안 장치 구조

2.1. 전체적인 시스템 구조

[그림 1]은 본 논문에서 필요로 하는 PC 보안 정책 관리 시스템에 대한 물리적인 구성 및 개발 범위에 따



[그림 1]. CDMA2000 1x EV-DO 보안계층 패킷 구조



[그림 2]. CDMA2000 1x EV-DO 보안계층 구현장치 구조

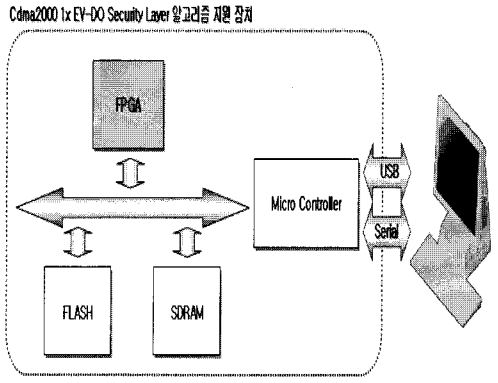
른 시스템의 논리적인 구성 및 모듈 구성을 보인다.

CDMA2000 1x EV-DO의 보안계층에서는 다양한 알고리듬을 사용하고 있는데, AN 장비의 경우 다양한 AT로부터 요청을 처리해야 하므로 알고리듬 처리에 시간을 단축하기 위해 하드웨어 장치를 통해서 알고리듬을 수행토록 하드웨어 장치를 제공하며, 하드웨어 장치를 통해서 보안계층에 필요한 프로토콜을 관리하는 기능을 제공하는 라이브러리 모듈이 존재한다.

전체적인 시스템 구조는 [그림 2]와 같다.

보안계층 알고리듬 지원 하드웨어 장치는 CDMA 2000 1x EV-DO의 보안계층에서 명시하는 다양한 알고리듬을 지원함과 동시에 추가적인 암호화 알고리듬인 SEED 및 ARIA알고리듬을 지원한다[그림 3].

보안계층 지원 라이브러리 모듈은 노드 타입 즉, AN 혹은 AT 타입에 따라 달리 동작하면서 상대방과의 세



[그림 3]. 하드웨어 장치 구조

션을 유지하면서 각 프로토콜을 처리하도록 기능을 제공하고 있으며, 또한 노드 타입이 AN인 경우 알고리듬 처리를 하드웨어에 의존하여 처리되며, AT의 경우에는 자체적으로 지원하는 소프트웨어 알고리듬을 이용하여 처리된다[6].

다음은 보안계층 지원 라이브러리 모듈의 구성을 보인다[그림 4].

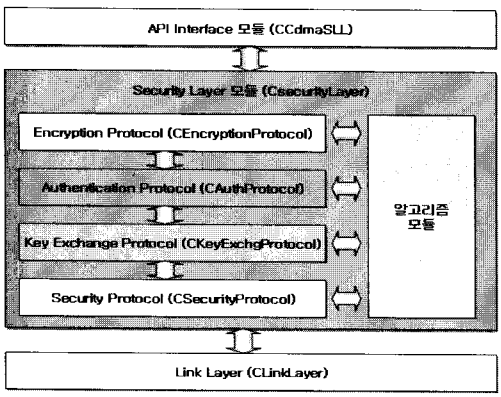
2.2. EV-DO 보안계층 알고리듬 지원 모듈

[그림 5]와 같이 EVDO 암호처리 장치는 호스트 인터페이스를 처리하는 USB 2.0 Controller (CY7C68013A)와 암호 알고리듬을 처리하는 FPGA (XC2V3000 - FF152)로 구성된다.

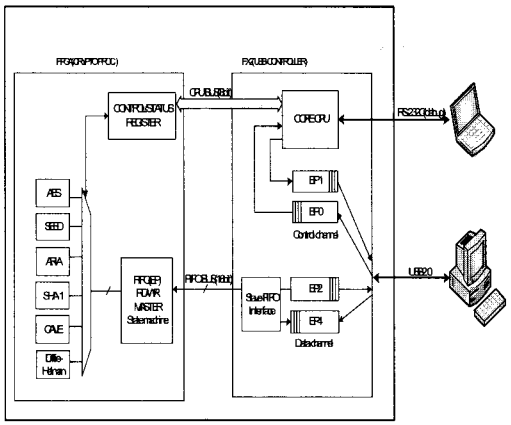
2.2.1. 암호 알고리듬 처리

암호 알고리즘 처리는 FPGA에서 하드웨어로 구현되며 AES, SEED, ARIA, SHA-1, CAVE, Diffie-Helman 방식을 선택적으로 사용할 수 있으며, 암호 알고리즘 처리부는 FIFO 인터페이스부와 제어 레지스터리부 그리고 각 암호 알고리즘으로 구성된다[5].

FIFO 인터페이스부는 USB 컨트롤에 대하여 FIFO 마스터로 동작하며 호스트로 부터의 데이터가 Endpoint4에 도착되어 있는지를 감시하여 도착된 데이터를 해당 알고리즘에 입력시키고 알고리즘의 연산 결과를 Endpoint2로 전송하는 기능을 한다.



〔그림 4〕. 보안계층 지원 라이브러리 모듈 구조



〔그림 5〕. 보안계층 지원 라이브러리 모듈 구조

제어 레지스터리부는 제어 파이프를 통해 하달되는 사용자 명령을 CORE CPU가 FPGA에 전달하거나 FPGA의 상태정보를 CORE CPU를 통해 호스트로 전송할 수 있도록 각종의 레지스터를 8비트 CPU BUS에 실어주며, 알고리즘은 다양한 알고리즘을 호스트의 선택에 따라 서비스 될 수 있도록 FIFO 인터페이스부에 미싱 한다.

2.2.2. 보안계층 라이브러리 모듈

보안계층 라이브러리 모듈은 내부적으로 8개의 모듈로 구성되며 핵심 모듈은 다음과 같다. 그 중 4개의 모듈을 알아보면 다음과 같다.

① AP 인터페이스 모듈

보안계층 API 모듈은 외부 프로그램에서 보안계층 모듈의 기능을 호출하기 위한 인터페이스 역할을 수행하는 기능을 제공한다.

② 보안계층 모듈

보안계층모듈은 보안계층에서 사용되는 모든 프로토콜1을 통제하고, AN과 AT간 연결 세션에 대한 관리 기능을 제공하며, 세션의 정상적인 프로토콜 처리를 도와주며, 또한 API 인터페이스 모듈, 연결계층 모듈과 연계하여 데이터 전송/수신에 관여하여, 안정적인 데이터 전송 및 수신 기능을 지원한다.

③ 알고리즘 모듈

알고리즘 모듈은 보안계층에서 필요로 하는 각종 알고리즘을 제공하며, 해당 알고리즘을 통해서 키 교환, 인증, 암호화 기능을 제공하고, 또한 AN의 경우 소프트웨어적인 알고리즘 처리에는 속도상의 문제가 있으므로 하드웨어적인 처리를 위해 하드웨어 장치와의 연동을 통해서 알고리즘 처리를 수행하기도 한다.

④ 보안 프로토콜 모듈

마지막으로, 보안 프로토콜 모듈은 연결계층에서 전송된 패킷을 상위 프로토콜인 키교환 프로토콜에게 전송하거나 혹은 키교환 프로토콜에서 전송된 패킷을 연결계층으로 전달하는 기능을 제공하며, 이 과정에서 Cryptosync 정보를 헤더에 포함하여 AT와 AN간 전송을 수행하게 된다.

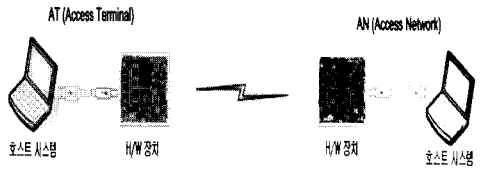
Ⅲ. CDMA2000 1x EV-DO 보안계층 설계 및 구현

본 장에서는 CDMA2000 1x EV-DO 보안계층 구현 목적 및 범위를 기준으로 설계 및 구현을 한다.

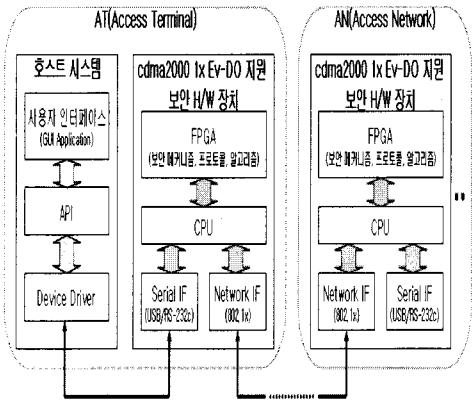
3.1. 개요

3.1.1. 구현 목적

CDMA2000 1x EV-DO에서의 보안 서비스를 제공하기 위해 보안계층을 지원하는 보안 모듈을 설계했으며, 또한 3GPP2의 C.S0024-A v2.0 표준을 준용한 하드웨어 장치와 AT 및 AN간의 통신 및 제어를 위한 효율적인 인터페이스 소프트웨어 구현을 통해 다양한 플랫폼 환경에 적용 가능하도록 하였다[그림 6].



[그림 6]. 전체적인 CDMA2000 1x EV-DO 보안장치 구성



[그림 7]. CDMA2000 1x EV-DO 보안 장치 상세구조

- CDMA2000 1x EV-DO용 보안계층 구현 라이브러리 모듈
  - 3GPP2의 C.S0024-A v2.0 표준을 준용한 CDMA2000 1x EV-DO 보안계층 지원
  - 하드웨어 장치와 연계된 알고리즘 연동 지원
  - AT와 AN간의 보안 프로토콜 지원
  - 보안 프로토콜 데이터에 대한 로깅 지원

- CDMA2000 1x Ev-DO 보안계층 테스트를 위한 시뮬레이터
  - AT 시스템으로 운용되는 시뮬레이팅 기능 지원
  - AN 시스템으로 운용되는 시뮬레이팅 기능 지원
  - 보안 프로토콜을 통해 전송되는 데이터 흐름을 실시간 출력
  - 보안 프로토콜의 보안 파라미터 값을 설정하여 AT와 AN간 통신 확인 지원

- CDMA2000 1x Ev-DO 보안계층을 위한 알고리즘 지원 하드웨어 장치
  - 3GPP2의 C.S0024-A v2.0 표준에 명시된 알고리즘을 지원
  - USB 2.0 인터페이스를 이용한 데이터 전송 처리 지원

3.1.2. 구현 환경

CDMA2001 1x Ev-DO 보안장치를 구동하기 위해서

- 모듈 인스턴스 획득
- 모듈 초기화 기능
- AN 접속 및 해제 기능
- 데이터 전송 및 수신 기능
- 메모리 반환 기능
- 디버깅 정보 수신 기능

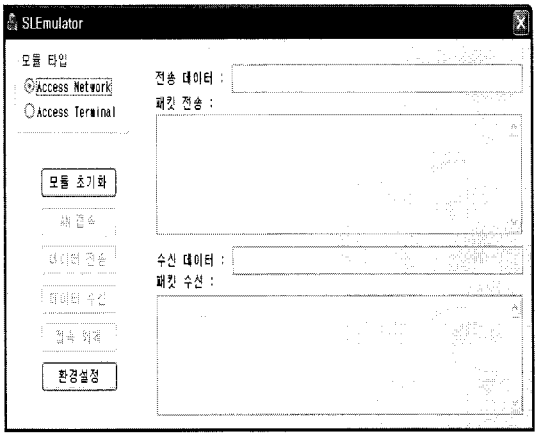
는 다음과 같은 환경이 필요하다. 먼저 서버로 보낼 수 있으므로, 전송 데이터를 안전하게 전달하기 위하여 데이터를 해쉬값(Hashcode)으로 계산하고, 센서의 개인키(KRs)와 함께 디지털 서명을 한 후, 센서와 서버 사이에 전달된 난수정보를 이용한 세션키(key:N3)로 모든 정보를 암호화한다. 센서는 서버로 암호화된 데이터를 전송함으로써 클라이언트가 암호화된 데이터를 수정하거나 읽을 수 없으며, 서버는 데이터를 복호화하고 첨부된 디지털 서명을 검증하며, 사용자를 인증하기 위해 서버에 저장되어 실행한다.

- 실행 환경
  - Pentium 3 500Mhz 이상의 CPU
  - Microsoft Windows XP SP1 이상의 운영체제
  - 128 MByte 이상의 메모리
  - 20 MByte 이상의 하드디스크 여유 공간

- 하드웨어 환경
  - USB 2.0 지원
  - 시리얼 통신 포트
  - IEEE 802.11x 무선랜 혹은 이더넷

3.1.3. 지원 보안 메커니즘 및 알고리즘

사용자 인터페이스를 통해 보안 메커니즘의 운용 상태를 볼 수 있도록 기능을 지원하며, 필요에 따라 알고리즘을 사용자 선택에 의해 처리될 수 있도록 기능을 지원하여야 한다. 먼저 키 교환을 위해 786비트나 1024비트 Diffie-Hellman 알고리즘을 지원하며 패킷 인증은 SHA1, 암호는 AES, SEED, ARIA 그리고 알고리즘의 고성능을 위해 8MGate 이상의 FPGA를 사용한다(현존하는 최대 FPGA는 16MGate임) 마지막으로 암호화 및 복호화 각각의 기능에 대하여 별도의 포트를 사용 하지 않고 동일 포트를 사용한다.



〔그림 8〕. CDMA2000 1x EV-DO 보안장치 실행화면

3.2. CDMA2000 1x EV-DO 운용 및 테스트

3.2.1. 초기 실행 화면 및 모듈 초기화

[그림 8]과 같이 프로그램을 실행하면 위 그림과 같은 초기 화면을 볼 수 있다.

화면의 좌측 상단에는 해당 프로그램이 AN 장치로 동작할 것인지 아니면 AT장치로 동작할 것인지를 선택하는 모듈 타입 그룹이 존재하며, 정상적인 테스트를 수행하기 위해서는 하나의 AN 장치에 대해서 다수의 AT 장치가 존재하는 형태가 될 수 있다.

그리고 화면 좌측에는 프로그램의 기능을 실행하기 위한 기능 버튼들이 존재하고, 화면 우측에는 AN과 AT간에 전송되는 데이터에 대해서 화면으로 출력되도록 기능을 제공한다.

먼저, 환경설정 화면은 CDMA 1x EV-DO의 보안계층에서 지원하는 보안 기능에 대한 알고리즘에 대한 설정을 수행할 수 있도록 기능을 제공한다. 예를 들어 키 교환 프로토콜에 대한 속성을 설정 및 키 교환 알고리즘을 사용하는 경우 체크박스를 선택하여 해당 알고리즘을 선택할 수 있으며, 인증 프로토콜에 대한 속성을 설정하면, 알고리즘을 결정해, 인증을 위한 SectorID 값을 필요에 따라 입력하면 된다.

또한 모듈 초기화는 프로그램의 기능을 초기화하는 것으로 AN과 AT에 따라서 초기화 내용이 약간씩 다를 수 있고, AN의 경우 모듈 초기화를 수행하게 되면 보안장치 하드웨어와의 연결을 수행하게 되므로, 네트워크

소켓을 초기화 하여 AT의 접속을 대기하게 된다.

반대로 AT의 경우에는 모듈 초기화를 수행하는 경우 네트워크 소켓을 초기화 하는 기능을 수행하게 된다.

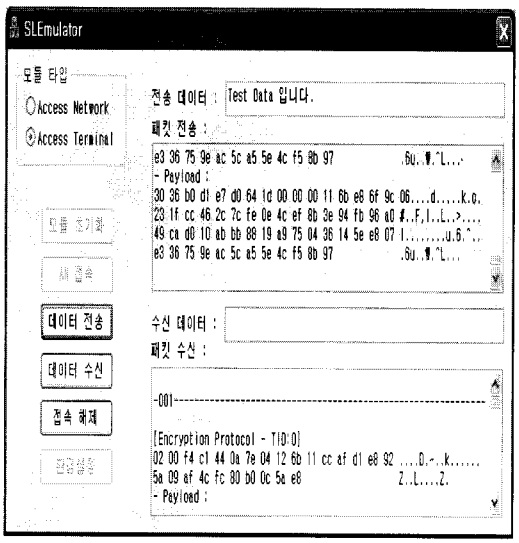
3.2.2. AN과 AT간 데이터 전송 및 수신

AN 접속기능은 AT장치에서만 보이는 기능으로 AT가 AN으로 접속을 하고자 하는 경우 AN 접속을 수행하여 AT와 AN간에 접속을 수행하게 된다.

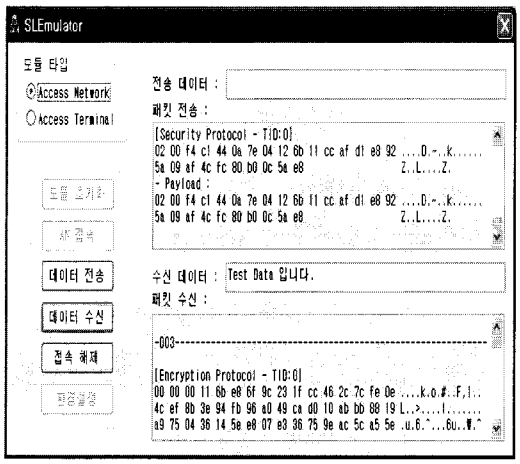
이때 AN의 접속은 환경설정에서의 AN 정보를 이용해서 접속을 하게 되며, 접속이 완료되면, CDMA 1x EV-DO의 표준에 맞게 보안계층의 보안통신을 수행하게 된다. (물론 이것 역시 환경설정에서 각 프로토콜에 대한 속성 설정을 어떻게 하였는가에 따라서 통신을 처리하게 된다).

데이터 전송은 AT와 AN간에 임의의 데이터를 전송하고자 하는 경우 사용하는 기능으로 AT의 화면 우측 상단에 "전송 데이터" 부분에 임의의 데이터를 입력하고, 데이터 전송 버튼을 누르게 되면 해당 정보가 암호화되어 AN으로 전송되는 패킷을 볼 수 있게 된다.

이때 AN에서는 "패킷 수신" 부분에 프로토콜이 수신되는 것을 볼 수 있고, "데이터 수신" 버튼을 누르면 "수신 데이터" 부분에 AT에서 전송한 데이터가 수신된 것을 볼 수 있게 된다[그림 9, 10].



〔그림 9〕. AT에서의 데이터 전송 화면



〔그림 10〕. AN에서의 데이터 수신 화면

Ⅳ. 결 론

3GPP에서는 3G 이동통신 시스템의 진화를 위해 각 WG에서 해당기술을 별도로 연구하고 있으며, 요구에 따라 합동회의를 통해 표준규격을 작성하고 있으며, 그 중 CDMA2000 1x EV-DO에서의 보안 계층은 현재 3GPP2를 통해 표준화 규격(C.S0024-A v2.0)을 완성해 나가고 있는 중이다. 현재 이동통신과 관련된 분야에서 국내의 경우 본 논문과 관련된 연구 및 개발이 활발하게 이루어지고 있지만, 실제 필드에서 적용한 예는 극히 드물게 존재하는 상태이며, 이제 이동통신 시장에서 기지개를 펴고 있는 상황이라 판단된다.

본 논문은 3GPP2의 C.S0024-A v2.0 표준에 준용한 CDMA2000 1x EV-DO 보안계층 설계 및 구현을 통해 AT와 AN간의 안전하고 빠른 데이터 전송했다는데 의의가 있으며, 또한 다양한 플랫폼 환경에 적용 가능한 보안계층 시스템을 실제 적용한 것에 가치가 있다고 볼 수 있다. 또한 실제 필요한 3GPP2의 C.S0024-A v2.0 표준 스펙과 프로세스에 대한 개념을 파악하게 되었고, 내부적으로 구동되는 모듈을 구현함으로써 관련 개발에 발판이 될 것이다

참고문헌

[1] 김윤관(3GPP2 SC의장) cdma2000표준화 동향 한국정보통신기술협회, 2006.09.18

[2] 3GPP2 C.S0029-AVersion 1.0 Test Application Specification (TAS) for High Rate Packet Data Air Interface. September 29, 2005

[3] 3GPP2 C.S0054-AVersion 1.0 cdma2000 High Rate Broadcast-Multicast Packet Data Air Interface Specification. February 14, 2006

[4] 3GPP2 C.S0024-A Version 2.0 cdma2000 High Rate Packet Data Packet Data Air Interface. July 2005

[5] 3GPP2 S.S0053 Version 1.0 Common Cryptographic Algorithms,21 January 2002

[6] IMT-2000 3GPP2-Introduction to cdma2000 spread spectrum systems (Release D) 한국정보통신기술협회,2006.04.19

〈著者紹介〉

양 종 원 (Jongwon Yang) 학생회원

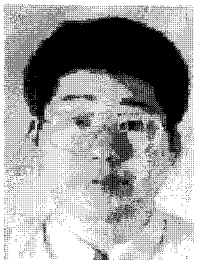
2003년 : 공주대학교 전자계산학과(학사)
2005년 : 공주대학교 일반대학원 컴퓨터공학과 (공학석사)
2005년 : 공주대학교 일반대학원 바이오정보학과(정보보호전공) 박사과정
2006년~현재 : 한국전자통신연구원 위촉연구원
<관심분야> 무선 인터넷 보안, 시스템 보안, 생체인식, 암호 알고리즘,

조 진 만(Jin-Man Cho) 정회원

1989년 : 충남대학교 계산통계학과(이학학사)
1991년 : 충남대학교 일반대학원 전산학과 (이학석사)
1991년~현재 : 한국전자통신연구원 선임연구원, 과제책임자
2005년~현재 : ISO/IEC JTC1 SC17(개인 식별 및 ID 카드) 국내 전문 위원장
<관심분야> 스마트카드 응용 기술 - 공공 분야 IC카드, 바이오카드 등

이 태 훈(TaeHoon Lee)

1982년 : 한국항공대학교 전자공학과 졸업(공학사)
1984년 : 아주대학교 대학원 전자공학과 졸업(공학석사)
1999년 : 아주대학교 대학원 전자공학과 졸업(공학박사)
1984년~1993년 : 한국전자통신연구원
1989년~1990년 : 일본 NTT연구소 객원연구원
1993년~현재 : 광주대학교 정보통신학과 교수
<관심분야> Network Security, 멀티미디어 통신 및 서비스
e-mail: thlee@gwangju.ac.kr



서 창 호 (Changho Seo) 종신회원

1990년 : 고려대학교 수학과(학사)
1992년 : 고려대학교 일반대학원 수학과 (이학석사)
1996년 : 고려대학교 일반대학원 수학과 (이학박사)
1996년~1996년 : 국방과학연구소 선임연구원
1996년~2000년 : 한국전자통신연구원 선임연구원, 팀장
2000년~현재 : 공주대학교 응용수학과(정보보호전공) 부교수
2001년~현재 : 공주대학교 바이오정보학과 부교수
<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보안, 시스템 보안 등