CDMA에서 단문 메시지 서비스(SMS)의 보안 적용 알고리즘

Adaptation of Secure Algorithm of Short Messaging Services(SMS) on CDMA Network

김 윤
한국재활복지대학 컴퓨터정보보안과

Yoon Kim(ykim@hanrw.ac.kr)

요약

현재 CDMA 규격으로 정의되어 있는 TIA/EIA/IS-637-A의 단문메시지 전송 규격에는 보안을 위한 별도의 대책이 포함되어 있지 않다. 따라서 필요할 경우 이러한 단문메시지에 별도의 보안대책을 강구하는 것이 바람직할 것으로 보인다. 이 논문에서는 기존의 단문메시지 서비스에 높은 수준의 기밀성과 무결성의 보안을 제공하고 아울러 적정한수준의 인증 기능을 제공함으로써 단문메시지를 통한 개인 정보의 유출을 방지하여 예상치 못한 사고에 대비하고 사생활을 보호할 수 있는 단문 메시지 서비스를 위한 보안 알고리즘을 제안한다.

■ 중심어 : | CDMA | SMS(Short Messaging Services) | SEED 알고리즘| Handshake 프로토콜 |

Abstract

At the present, Short Messaging Transfer Protocol Standard described under TIA/EIA/IS-637-A does not cover the measures for security at all. Sequentially, in case of necessity, it seems to be a better idea that security functions are made up for current short messaging transfer protocol. This paper proposes security mechanisms including algorithms and protocols for Short Messaging Services(SMS) which present not only high levels of confidentiality and integrity but also appropriate level of authentication.

■ keyword : | CDMA | SMS(Short Messaging Services) | SEED Algorithm | Handshake Protocol |

I. 서 론

현재 CDMA 네트워크 환경에서 휴대폰의 사용이 보편화 되었다. 휴대폰을 이용한 서비스는 크게 음성통화, 무선인터넷 그리고 단문메시지 전송의 세 가지로 분류할 수 있다. 이 중에서 단문메시지 전송의 경우 메시지를 주고받을 수 있는 단문메일서비스, 주식정보나 은행계좌를 통한 결제내역의 조회 등이 있는데 이렇듯 단문메시지 전송 서비스는 현재 다양한 생활정보로부터 보안이 요구되는 중요한 정보의 송수신 수단으로 폭넓게 이용되고 있다. 이러한 서비스를 통해 전송되는 메시지의 내용 중에는 소액결제시스템, 은행 및 증권정보서비스 등 경우에 따라 적절한 보안이 요구되는 경우가 있을 수 있다. 또한 개인 간 메시지를 주고받는 경우에도 악

접수번호 : #060703-001
접수일자 : 2006년 07월 03일
심사완료일 : 2006년 08월 24일
교신저자 : 김 윤, e-mail : ykim@hanrw.ac.kr

의를 가지고 있는 제 3자에 의해 사생활이 노출될 수도 있다. 하지만 현재의 CDMA 규격으로 정의되어 있는 TIA/EIA/IS-637-A의 단문메시지 전송 규격에는 보안을 위한 별도의 대책이 포함되어 있지 않다. 따라서 필요할 경우 이러한 단문메시지에 별도의 보안대책을 강구하는 것이 바람직할 것으로 보인다.

이 논문에서는 기존의 단문메시지 서비스에 높은 수준의 기밀성과 무결성의 보안을 제공하고 아울러 적정한수준의 인증 기능을 제공함으로써 단문메시지를 통한 개인 정보의 유출을 방지하여 예상치 못한 사고에 대비하고 사생활을 보호할 수 있는 방안을 마련하고자 한다.

II. 제안 배경

1. 현 단문 메시지 전송 규약

본 논문은 CDMA 네트워크 상에서 동작하는 단문 메시지 전송 규약을 기반으로 하고 있다. CDMA 네트워크에서 단문메시지 서비스의 전송은 TIA/EIA/IS-637-A 규격에 정의되어 있다. 전체적인 시스템의 구성은 [그림 1]과 같다.

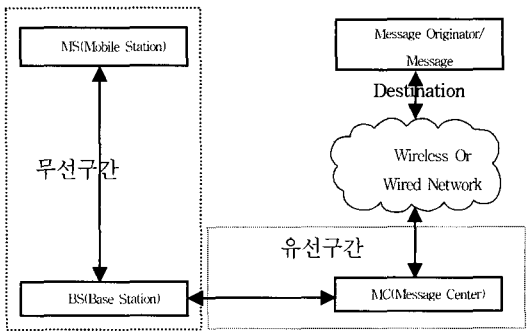


그림 1. 단문 메시지 전송 시스템

TIA/EIA/IS-637-A에 정의된 단문 메시지 서비스에서는 Paging, Messaging, 그리고 음성 메일 알림(Voice Mail Notification) 등을 위한 텍스트 또는 숫자로 구성된 단문 메시지 전송에 관한 기술적 표준을 제시하고 있다. TIA/EIA/IS-637-A에서는 SMS Relay Layer, SMS Transport Layer, SMS Teleservice Layer를 정의하여 단문 메시지의 전송에 관한 규약을 정의하고 있다[1][2]. 단문 메시지 전송 프로토콜의 계층적 구조는 [그림 2]에 나타나 있다. 각각의 계층에서 수행하는 기능들에 대해서는 다음 절에서 상세히 언급한다.

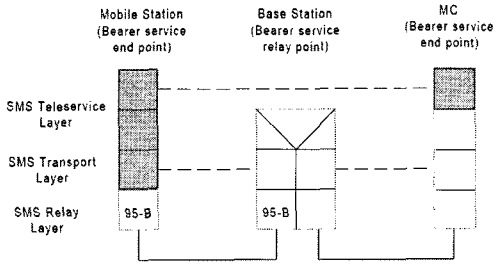


그림 2. 단문 메시지 전송 프로토콜의 계층구조

2. 현 단문 메시지 전송 방식

TIA/EIA/IS-637-A에서 정의하고 있는 단문 메시지 전송 규격은 물리계층과 링크계층을 제외하고 크게 세 개의 계층으로 이루어진 계층적 구조를 가지고 있다[3]. 링크계층과 통신하는 계층은 SMS Relay Layer로서 다음과 같은 기능을 한다.

① SMS Transport Layer로부터 메시지를 수신하여 해당 종단점(end point) 혹은 지정된 중계점(relay point)으로 전달한다.

② 메시지가 해당 종단점(end point) 혹은 지정된 중계점(relay point)으로 전달이 안 되는 경우 SMS Transport Layer로 오류발생을 알린다.

③ Link Layer로부터 메시지를 수신하여 SMS Transport Layer로 메시지를 전달한다.

④ 메시지를 중계에 필요한 Link Layer와 접속하고 제어한다.

⑤ Link Layer 혹은 Peer SMS Layer에 따라 SMS 표준 혹은 기타 메시지 표준 형식으로 메시지를 정형화(Formatting)한다.

SMS Transport Layer는 두 가지 기능을 한다. 하나는 Bearer Service End Point로서의 기능이고 다른 하나는 Bearer Service Relay Point로서의 기능이다. 다음

은 종단점(End Point)으로서의 기능을 서술하고 있다.

① SMS Teleservice Layer로부터 메시지를 받아 SMS Transport Layer메시지를 formatting하고 해당 SMS Relay Layer Service Primitive를 통해 SMS Relay Layer로 전달한다.

② 전송된 메시지에 대해 Acknowledge를 모두 수신하면 SMS Relay Layer에게 알린다.

③ SMS Relay Layer로부터 오류가 전달되면 이를 SMS Teleservice Layer에게 알린다.

④ SMS Relay Layer로부터 메시지를 받아 SMS Teleservice Layer에게 전달한다.

⑤ TIA/EIA/IS-95-B에서 정의된 대로 무선 단말기에서 인증인자(Authentication Parameter)들을 계산한다[4].

다음은 중계점(Relay Point)으로서의 기능을 서술한다.

① SMS Relay Layer로부터 메시지를 전달받아 필요한 경우 Reformatting한 후 해당되는 SMS Relay Layer Service Primitive를 이용하여 다른 Relay Layer전달한다.

② SMS Relay Layer간에 오류 보고 혹은 메시지 확인이 필요한 경우 이를 전달한다.

③ TIA/EIA/IS-95-B 기지국에서는 인증 인자들을 계산하거나 혹은 인증 인자들을 계산하는 다른 장치와 접속한다.

SMS Teleservice Layer는 Bearer Service End Point에서 단문메시지의 전달에 관한 규약으로 기본적인 단문메시지의 전송 뿐 아니라 다양한 형태의 메시지의 전송을 지원하기 위한 각각의 SMS Teleservice들을 정의해 놓았다. TIA/EIA/IS-637-A에서는 SMS Transport Layer에서의 Service Primitive들을 이용한 SMS Teleservice를 정의하고 있으며 이 밖에도 별도의 자체적인 SMS Teleservice Layer Protocol을 사용할 수 있다.

단문메시지 보안규격은 정보제공자와 무선단말기를 통한 정보이용자 간에 SMS Telservice Layer보다 상위 계층에서 단대단(End to End) 보안을 제공하는데 기밀성은 별도의 키 생성 함수와 128비트 블록 암호화 알고리즘을 사용하여 제공하며 무결성은 해시 함수를 이용한 메시지 인증코드(MAC) 방식을 사용하여 제공한다[5]. 이 규격은 크게 두 가지 형태로 나눌 수 있는데 첫째는 Handshake Protocol이고 다른 하나는 Record Layer Protocol이다. Handshake Protocol의 기능은 다음과 같다.

① 암호화된 세션을 만들고 유지한다.

② 사용자와 서버의 양방향 인증을 수행한다.

③ 암호화에 필요한 일회용 암호화 세션키를 생성한다.

Record Layer Protocol은 세션이 설정된 다음, 메시지의 전송을 담당하는 기능을 한다. 세부 기능은 다음과 같다.

① 메시지의 암호화와 복호화를 담당한다.

② 각 메시지 별 메시지 인증 코드의 생성 및 확인을 담당한다.

③ 각각의 세션에 있어 오류가 발생할 경우 handshake protocol을 통해 새로운 세션을 생성 혹은 세션 재시작 요구 등을 하여 세션을 유지한다.

3. 현 단문 메시지 전송방식의 보안성 검토

TIA/EIA/IS-637-A 규격에 의거 제공되는 단문 메시지 서비스는 별도의 보안이 수립되어 있지 않다. TIA/EIA/IS-637-A의 규격에 따르면 단문 메시지는 SMS Relay Layer에서 TIA/EIA/IS-95-B가 규정하는 Link Layer로 메시지 전송을 요구하도록 하고 있으며 이 때 사용할 수 있는 채널은 Paging Channel 및 Traffic Channel이다.

① CDMA Paging Channel을 이용하는 경우

해당 기지국(BS)이 커버하는 지역 내에서 Broadcasting을 함으로써 해당 기지국을 이용하는 모든 단말기 중Paging Channel Access가 가능한 단말기들은 전송되는 단문 메시지를 모두 볼 수 있다. Paging Channel을 통해 특정 단말기로 메시지를 전송할 경우 SMS Transport Layer에서 주소를 해당 필드에 세팅하도록 되어 있으나 Link Layer에서 감지된 메시지는 상

위 계층의 헤더를 모두 포함하고 있으므로 TIA/EIA/IS-637-A의 규격에 의거 Decapsulation 과정을 통해 모든 정보를 알 수 있다.

② CDMA Traffic Channel을 이용하는 경우

평문 데이터를 인코딩해서 트래픽 채널에 실어 보내기 위해서는 해당 단말기의 MIN(Mobile Identification Number)과 ESN(Electronic Serial Number)을 이용한 Private Masking Code를 생성하여 XOR을 통한 Masking을 하게 된다. 그러나 ESN, 및 MIN은 쉽게 노출될 수 있는 정보이므로 공격자(Attacker)가 위에서 언급한 Private Masking Code를 생성함으로써 정보의 내용을 확인할 수가 있으며 메시지 조작도 가능하므로 기밀성 및 무결성이 결여되어 있다고 볼 수 있다.

III. 암호화된 단문 메시지 전송 프로토콜

이 논문에서 제안하고자 하는 SSMS(Secure Short Messaging Service)는 보안 모듈이 장착된 무선 단말기와 SMSC(Short Message Service Center)에 설치되는 보안 서버로 구성된다. 보안이 되는 구간은 에어구간으로 무선 단말기로부터 SMSC까지 설정되며 이후의 구간은 유선망을 통해서 전송되므로 신뢰영역(Trusted Domain)으로 가정한다. 우선, 보안기능을 구현하기 위해 단말기와 SSMS 서버는 Long Term Key와 Short Term Key를 공유해야 한다. 이러한 Long Term Key와 Short Term Key를 통하여 각 메시지마다 키 생성과 초기화 벡터(Initialization Vector, IV)를 생성하게 된다. 단말기가 공장에서 생산되어 처음으로 에어 구간에 접

```
MS                                                                    SVR
------------------------REQ||E_K(LT_KEY[1]||LT_KEY[2])||MAC---------------------->
<-------------------------h(LT_KEY[1]||h(LT_KEY[2])----------------------------
```

MS에서 SVR

REQ = 초기화 요청 : 1 바이트

Most Significant 4 bits = 0101

Least Significant 4 bits = Random

$K = f_1(MIN_{MS}, ESN_{MS}, (REQ\&0x0F|((REQ\&0X0E)\hat{}0X0D)<<4))$

$IV = f_2(MIN_{MS}, ESN_{MS}, (REQ\&0x0F|((REQ\&0X0E)\hat{}0X0D)<<4))$

LT_KEY[1] = A_KEY(16)||B_KEY(10) : 26바이트

LT_KEY[2] = C_KEY(16)||D_KEY(10) : 26바이트

MAC = MD5(REQ|| LT_KEY[1]|| LT_KEY[2]) : 16바이트

전체 메시지 길이 : 69바이트

SVR에서 MS

h(M) = MD5(M) : 16바이트

전체 메시지 길이 : 32바이트

● 보안 관련 함수 정의

f_1 : 초기화 프로토콜 암호화 키 생성 함수, f_2 : 초기화 프로토콜 초기화 벡터 생성 함수

함수 인자

MIN : 무선 단말기의 Mobile Identification Number, 12바이트

ESN : 무선 단말기의 Electronic Serial Number, 4바이트

SEED : 랜덤 Seed = (REQ&0x0F|((REQ&0X0E)^0X0D)<<4), 1바이트

그림 3. 초기화 프로토콜

속했을 때 서버는 등록된 Long Term Key가 해당 단말기의 기록에 존재하지 않을 때 초기화 프로세스를 통해서 Long Term Key를 공유하게 된다.

1. 초기화 프로토콜

[그림 3]에 제시된 초기화 프로토콜은 일반 단문메시지 서비스를 이용한 것이다. 이는 현재 메시지의 최대 길이를 70바이트(7비트 인코딩 가정)로 하여 설정한 것으로 바이너리 전송으로 최대 80바이트나 그 이상 전송이 가능할 경우 B_KEY와 D_KEY는 늘어날 수 있다. f_1과 f_2는 랜덤한 비트 패턴을 생성하는 함수로서 해시함수를 반복적으로 적용하여 생성되는 값을 사용하게 된다.

2. 암호화된 메시지 전송 프로토콜

일단 초기화가 이루어지면 무선 단말기와 보안서버 사이에 암호화된 메시지를 전송할 준비가 완료된다. 암호화된 메시지를 단문 메시지 서비스를 통해 전송하기 위해서는 하나의 메시지마다 다른 키를 적용하여 암호화하여야 한다[6]. 이는 세션을 구성할 수가 없기 때문으

SMSC에서MS로메시지전송

MS ---------- SVR

----------SEED||E_K(M)||$HMAC_K$(M||SEED)----------

SEED = Random Seed	: 8바이트
M = Plaintext Message	: 최대 46 바이트
HMACK(M) = Keyed Hash Function under K	: 16바이트
K = f_3(MIN_{MS}, ESN_{MS}, SEED, A_KEY, D_KEY)	: 16바이트
IV = f_4(MIN_{MS}, ESN_{MS}, SEED, IV_{OLD}, M_{OLD} , B_KEY, C_KEY)	: 16바이트
IV_{OLD} = 이전 IV, 초기값은 0xA796EC1239BFD2A0BFD2A0B685DB01:28ADECF9	
M_{OLD} = 이전 메시지, 초기값은 0xCDS2BA4DFE8ACEEDD0829CFE9D8A38B69	
전체 메시지 길이	: 70바이트

MS에서SMSC로메시지전송

MS ---------- SVR

---------- SEED||E_K(M)||$HMAC_K$(M||SEED)----------

● 보안 관련 함수 정의

f_3 : 메시지 암호화 키 생성 함수

함수 인자

MIN : 무선 단말기의 Mobile Identification Number, 12바이트
ESN : 무선 단말기의 Electronic Serial Number, 4바이트
SEED : 랜덤 Seed, 8바이트
A_KEY : :Long Term Shared Secret Key A, 16바이트
D_KEY : :Long Term Shared Secret Key A, 10바이트

f_4 : 메시지 암호화 초기화 벡터 생성 함수

MIN : 무선 단말기의 Mobile Identification Number, 12바이트
ESN : 무선 단말기의 Electronic Serial Number, 4바이트
SEED : 랜덤 Seed, 8바이트
IV_{OLD} : 이전 초기화 벡터, 16바이트
M_{OLD} : 이전 메시지를 해시한 값, 16바이트
B_KEY : :Long Term Shared Secret Key B, 10바이트
C_KEY : :Long Term Shared Secret Key C, 16바이트

그림 4. 암호화 메시지 전송 프로토콜

MS SVR

---------- SYNC_FAIL ----------

----------$E_K(IV_{NEW})||HMAC(IV_{NEW})$----------

MS SVR

---------- SYNC_FAIL || $E_K(IV_{NEW})||HMAC_K(IV_{NEW})$----------

SYNC_FAIL=0x0000|| $E_K(IV_{OLD2})||HMAC_K(IV_{OLD2})$: : 34바이트

전체 메시지 길이 : 34~66바이트

$K = f_5(IV_{OLD2}, MIN, ESN, A_KEY, C_KEY)$

● 보안 관련 함수 정의

f_5 : 초기화 벡터 동기화에 사용될 암호화 키 생성 함수

IV_{OLD2} : 두 번째로 최근에 사용된 초기화 벡터, 16바이트

그림 5. 초기화 벡터 동기화 프로토콜

MS SVR

----------LT_KEY Update Request----------

----------LT_KEY Update Response----------

---------- $E_K(LT_KEY_{NEW})||MAC$----------

----------LT_KEY Update Confirm----------

LT_KEY Update Request

LT_KEY Update Response

LT_KEY Update Confirm

$K = f_6(MIN, ESN, LT_KEY[1]_{OLD}, LT_KEY[2]_{OLD})$

$MAC = MD5(LT_KEY[1]_{NEW}, LT_KEY[2]_{NEW})$

● 보안 관련 함수 정의

f_6 : 초기화 벡터 동기화에 사용될 암호화 키 생성 함수

그림 6. Long Term Key Update

로 결국, 세션을 구성하여 세션 지속기간 동안 같은 키를 사용하는 방식이 아닌 각 메시지 별 다른 암호화 키를 생성하게 되는 것이다. 본 논문에서는 각 메시지에 8바이트 길이의 난수를 SEED로서 전송하고 있는데 이 SEED는 키 및 초기화 벡터를 생성하는 데 사용된다[7][8]. [그림 3]에서는 실제 암호화된 메시지의 전송 프로토콜을 제시하고 있다[9][10].

현재 암호화 알고리즘은 국가 표준인 SEED 알고리즘을 사용하는데 SEED 알고리즘은 128비트 키와 128비트 블록 단위를 사용하므로 사용되는 키와 초기화 벡터 역시 128비트 길이가 되어야 한다. 또한 한 블록을 넘어가는 경우 데이터 Padding과 블록 암호화 알고리즘의 동작 모드를 결정해야 하는데, 여기서는 데이터 Padding의 경우 CTS(Cipher-Text Stealing) 기법을, 동작 모드는 CBC(Cipher Block Chaining) 모드를 사용한다[11][12]. 암호화한 이후에는 초기화 벡터를 전송하

지 않는다. 이것은 메시지의 크기가 아주 제한적인 단문 메시지 서비스에서 오버헤드를 줄이기 위함이다.초기화 벡터 역시 체이닝 기법을 사용하여 랜덤하게 생성한다. HMAC은 Keyed Hash Function으로서 암호화 키를 사용한 해시 함수이다[13]. f_3와 f_4는 랜덤 시퀀스 생성 함수로서 각각 128비트씩의 랜덤 시퀀스를 생성한다. I_{VOLD}와 M_{OLD}는 각각 이전의 초기화 벡터와 메시지로서 M_{OLD}는 실제 메시지가 아닌 해시한 값을 사용하도록 하고 무선 단말기와 서버에서는 각각 가장 최근의 값을 캐시하고 있어야 한다. [그림 4]에 실제 암호화 프로토콜을 제시하였다.

3. 초기화 벡터 동기화

초기화 벡터는 이전의 메시지와 초기화 벡터, 그리고 공유 정보들을 이용하여 생성한다. 따라서 서버와 단말기 사이에 반드시 이전의 메시지와 초기화 벡터가 같은 내용을 유지하고 있어야 하는데 만약 이 같은 내용이 일치하지 않을 때에는 초기화 벡터를 동기화 하여야 한다. 이러한 동기화 프로세스는 [그림 5]에 제시하였다.

여기서, IV_{OLD2}는 현재 저장되어 있는 IV의 두 번째 앞서 사용된 IV를 뜻한다. 즉, 캐시는 각각 두개씩의 엔트리를 저장하고 있어야 한다. 만약, 초기화 벡터 동기화 후에도 계속해서 동기 실패 에러가 발생하는 경우에는 모든 과정을 초기화하고 최초의 Long-term Key부터 새로 생성하여 시작하여야 한다.

4. Long Term Key Update

[그림 6]에 제시한 프로토콜은 심각한 사유로 무선 단말기 내부의 공유정보가 지워지거나 오류가 발생했을 경우 모든 과정을 초기화하고 Long-term Key를 새롭게 생성하는 과정이다. 이러한 과정은 Agent에서 수행될 수도 있고 Over-the-air로 수행될 수도 있다.

Long-term Key의 갱신을 위해서는 반드시 서버에 저장되어 있는 공유정보를 모두 알고 있어야 하며, 만일 특별한 사유로 인해 단말기의 모든 메모리 내용이 삭제되어 Long-term Key의 갱신이 안 될 경우 Agent와 같은 안전한 채널을 통한 초기화 과정이 필요하게 된다. 이는 서버에는 공유정보가 있으나 단말기에 공유정보가 없는 경우에 해당한다. 서버에 등록되어 있지 않은 단말기는 다른 Teleservice ID를 통해서 전송되므로 여기서는 다루지 않는다.

서버는 상기한 관리용 프로토콜이 수행 중일 때는 모든 메시지의 전송을 잠시 중단하고 관리용 프로토콜의 수행을 정상적으로 완결한 후에 메시지 큐에 쌓여 있는 메시지들을 전송한다.

Ⅳ. 결 론

본 논문에서는 현재 실제로 이동통신업체로부터 휴대폰 가입자들에게 제공되고 있는 서비스들 중 단문 메시지 서비스에 대해 높은 수준의 기밀성과 무결성의 보안을 제공하고 아울러 적정한 수준의 인증 기능을 제공하는 프로토콜 및 알고리즘을 제안하였다. 추후 과제로 이 알고리즘을 검증하기 위한 적절한 테스트베드를 구성하고 그 결과를 분석함으로써 보다 나은 성능의 알고리즘을 제안하는 작업을 진행하고자 한다.

참 고 문 헌

[1] ANSI J-STD-008, *Personal Station-Base Station Compatibility Requirements for 1.8 to 2.0 GHz Code Division Multiple Access(CDMA) Personal Communications Systems*, 1996.

[2] TSB74(Including TIA/EIA/IS-95-A), *Support for 14.4kbps Data Rate and PCS Interaction for Wideband Spread Spectrum Cellular Systems.*

[3] TIA/EIA-637-A, *Short Message Service for Spread Spectrum Systems.*

[4] TIA/EIA-95-B, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum System.*

[5] B. Schenier, *Applied Cryptography*, 2nd Edition, John Wiley and Sons, New York, 1996.

[6] ANSI X9.17, *American National Standard X9.17 : Financial Institution Key Management*

(Wholesale), American Standard Institute, 1985.

[7] D. Eastlake, S. Crocker, and J. Shciller, *Randomness Recommendations for Security*, RFC1750, IETF, pp.278-281, Dec., 1994.

[8] 한국정보통신기술협회, *128비트 블록 암호알고리즘 표준(SEED)*, 한국정보통신기술협회, Apr., 1999.

[9] R. Reviest, *The MD5 Message-Digest Algorithm*, RFC1321, Apr., 1992.

[10] G. Tsudik, "Message authentication with one-way hash functions," Proceedings of Infocom'92, May, 1992.

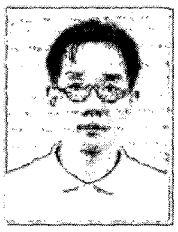
[11] FIPS PUB 81, *Federal Information Processing Standards Publication 1980 DES Modes of Operation*, National Institute of Standards and Technology(NIST), Dec., 1980.

[12] ISO/IEC 9798-1, *Information Technology-Security Techniques-Entity authentication mechanisms-part 1 : General model*, International Organization for Standardization, Geneva, Switzerland, pp.197-213, 1991.

[13] H. Krawczyk, M. Bellare, and R. Cannetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC2104, IETF, Feb., 1997.

저 자 소 개

김 윤 (Yoon Kim) 정회원



- 1982년 2월 : 한양대학교 공과대학 기계공학과(공학사)
- 1989년 5월 : Stevens Instute of Technology(이학석사)
- 2002년 3월~현재 : 한국재활복지대학 컴퓨터정보보안과 교수

<관심분야> : CDMA이동통신, 분산시스템