《主 題》

CDMA 이동통신에서의 보호(security)

이 상 곤*, 문 상 재**
(*창신전문대학, **경북대학교)

■ 차 례 ■

Ⅰ. 머리말

기존 전화망은 이동성이 거의 없어 통화장소와 대화자의 호출에 제약이 있다. 이동통신에서는 이러한 제약이 극복될 수 있어 언제, 어디서나, 누구와도 통신이 가능하다. 이러한 제약이 해결되어 통화의 자유를 얻은 반면에 통화도용, 도청 혹은 불법적인 통신사기와 같은 통신범죄가 언제든지, 보이지 않는 곳에서, 누구에게도 가해질 수 있는 가능성이 높아지고 감시도 어려워 진다.

국내에서도 지난 3월부터 보름기간동안에 걸쳐 이동통신에서 국제전화 100여회, 국내통화 200여회에 따른 통화료 400여만원을 타인의 이름으로 도용한 통신범죄가 발생하였다. 이러한 통신범죄는 유료 데이타 통신망에서도 빈번히 발생되고 있는 실정이다. 불법적인 통신활동의 방지는 정보사회의 안전과 특히 무선 이동통신의 신뢰와 발전을 위해서 필히 해결되야 할 과제이다. 몇년전부터 국내에서도 통신정보보호를 위한 학회활동이 시작된 바 있으며[1], 통신범죄에 대한 방지기술 및 감시체계에 대한 발전이 절실히 실정이다.

디지틀 통신방식인 CDMA(code division multiple access) 이동통신은 기존의 아나로그 이동통신 혹은 디지틀 TDMA(time division multiple access) 방식보다 가입자수를 경제적으로 확장할 수 있을 뿐 아니라, 통신범죄 방지성능이 우수하다. 현재까지 표준으로 채택된 디지틀 이동통신 방식으로는 유럽의 TDMA 방식인 GSM(grobal system for mobile communications), 미국의 TDMA 방식인 DAMPS(digital AMPS), 그리고 일본의 TDMA 방식인 JDC(Japan digital cellular) 방식으로 대부분이 TDMA방식이다. 미국의 경우 TDMA방식이 규격으로 채택되었으나 1993년 7월 16일 미국 업계단체 TIA(미국 전기통신 공업협회)는 Qualcomm사가 제안한 CDMA 방식을 디지틀 이동전화 표준으로 채택하였다[2]. 우리나라에서는 차세대 digital cellular 이동통신시스템을 개발하기위해 한국전자통신 연구소가 주축이 되어 89초부터 연구개발에 착수하였다. Qualcomm사의 CDMA가 우리나가 차세대 시스템으로 적합하다고 판단하여 Qualcomm사와 공동 개발 중이다[3].

본고에서는 EIA/TIA/IS-95안을 근거로 하여 CDMA 이동통신에서의 보호를 채널의 대역확산보호와 인증방법을 중심으로 살펴본다. 먼저 대역확산을 위한 의사잡음(PN, pseudo noise) 시퀀스(sequence)의 발생과 보호에 관련된 신호의 형식을 알아보고, 다음으로 기지국이 이동국을 인증하는 방법과 호처리과정을 서술한다.

Ⅱ. 채널의 대역확산보호 및 보호신호 형식

2.1 채널의 대역확산보호

2.1.1 역방향 채널

이동국에서 기지국으로의 CDMA 통신채널을 역방향 CDMA 채널이라 하며 엑세스 채널과 역방향 트래픽 채널로 구성되어 있다. 이들 채널은 직접 시퀀스(direct-sequence) CDMA를 이용하여 동일한 주파수 대를 공유한다. 각 채널의 정보는 20ms 길이의 프레임(frame) 단위로 전송되는데 엑세스(access) 채널은 데이타 전송율이 4800bps이므로 프레임 당 96비트이며, 역방향 트래픽(traffic) 채널은 데이타 전송율이 9600, 4800, 2400 그리고 1200bps로 가변적이며 각기 프레임당 192, 96, 48, 그리고 24비트이다. 데이타 전송율은 프레임 단위로 가변된다.

전송 전에 채널은 그림1과 같은 long code 발생기에서 나오는 PN(pseudo noise) 시퀀스(sequence)에 의해 직접 시퀀스 확산된다. 그림1의 선형궤환이동레지스터(linear feedback shift register)의 다항식은 $p(x) = x^{42}+x^{35}+x^{33}+x^{31}+x^{27}+x^{26}+x^{25}+x^{22}+x^{21}+x^{19}+x^{18}+x^{17}+x^{16}+x^{10}+x^{7}+x^{6}+x^{5}+x^{3}+x^{2}+x^{1}+1$이고, 그 주기는 $2^{42}-1$ 칩이다. 그림2에서 사용되는 long code mask의 내용이 채널형성 시마다 고유하게 만들어지므로 일종의 대역확산보호가 된다.

엑세스 채널은 이동국이 기지국과 접속을 시도하거나 수신한 페이징 채널 메시지에 응답할 때 사용된다. 엑세스 채널 설정시 구해지는 이동국의 42비트 long code mask의 내용은 그림2와 같으며 PN 발생기에 사용되며 다른 이동국과 구별하는데 사용된다. 그림2(a)는 엑세스 채널의 long code mask 구조를 나타낸다. 엑세스 채널 번호, 페이징(paging) 채널 번호, 기지국(base station) 신분번호, 그리고 순방향 CDMA 채널의 PN 시퀀스 오프셋(offset) 등으로 구성되어 있다.

역방향 트래픽 채널은 사용자 및 신호 정보를 기지국에 보내는데 사용된다. 이동국은 역방향 트래픽 채널 전송중 이동국 고유의 두가지 long code mask 즉, public long code mask 와 private long code mask 중 한 개를 선택하여 PN 시퀀스를 발생시킨다. 그림2(b)는 역방향 트래픽 채널에 사용되는 public long code mask의 구조를 나타낸다. public long code mask는 생산 공장에서 부여한 이동 수신기의 고유번호인 32비트 ESN(electronic serial number)을 이용한다. 만약 영구 기억소자에 저장된 ESN을 고의로 변경할려고 시도하면 회로적으로 이동 수신기가 훼손되어 작동되지 않도록 장치되어야 한다. 이렇게 함으로써 다른 수신기를 사용한 도용 통화를 방지할 수 있다. private long code mask는 34비트 MIN(mobile identification number)을 사용하여 생성되며, NIN은 10자리 가입자 전화번호가 생성 절차에 이용되어 생성된다. 트래픽 채널의 long code mask는 정보 데이타의 프라이버시를 보호한다.

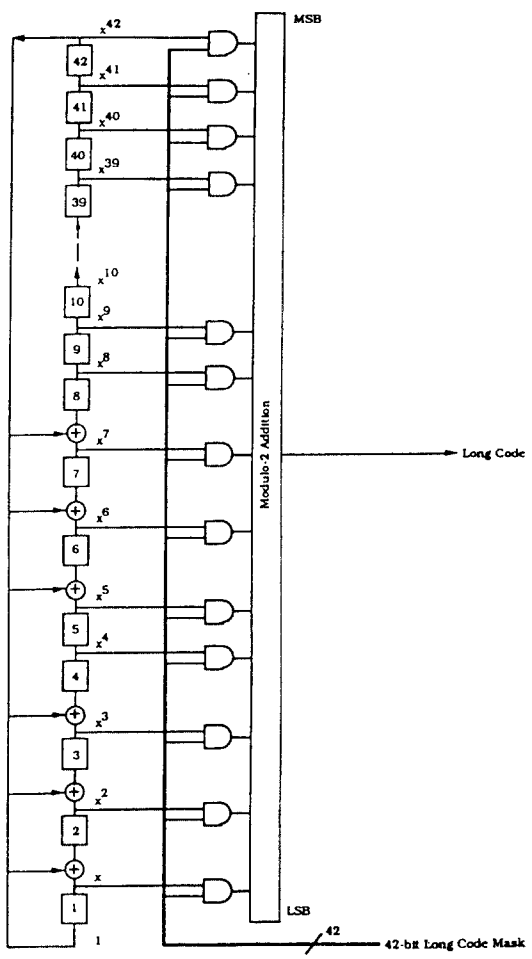


Fig 1. Long code generator

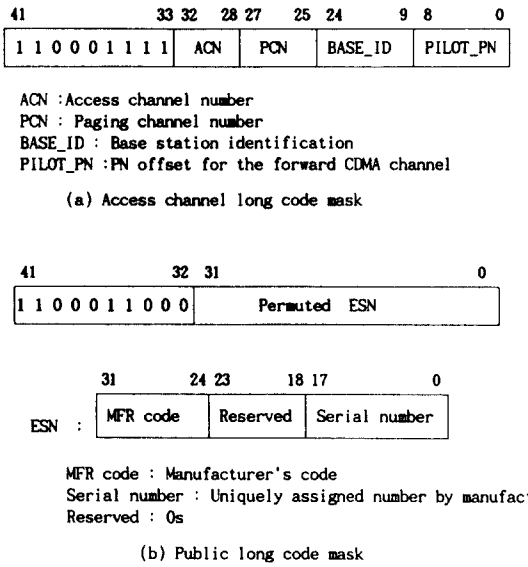


Fig 2. Long code mask format for the access and traffic channel

2.1.2 순방향 채널

기지국에서 이동국으로의 CDMA 통신 채널을 순방향 CDMA 채널이라 하며 서로 직교하는 Walsh 함수들에 의해 확산되는 64개의 부호채널이 있다. 순방향 CDMA 채널은 기능별로 구분하여 파일롯(pilot) 채널, 싱크(sync)채널, 페이징 채널, 그리고 트래픽 채널로 나누어진다. 파이롯 채널은 1개이며 항상 동작한다. 싱크 채널은 1개, 페이징 채널은 최대 7개까지 동작하거나 없을 수도 있으며, 나머지는 트래픽 채널이다.

파일롯 채널은 기지국 관할 영역에서 작동하는 이동국이 동기를 얻는데 사용되며 항상 전송된다. 각 기지국은 순방향 CDMA 채널을 구별하기 위해 파이롯 PN 시퀀스의 서로 다른 시간 오프셋을 사용한다.

싱크 채널은 이동국이 채널 시작 시간 동기를 얻는데 사용되며, 데이타 전송율은 1200pbs이고 해당 기지국의 파이롯 채널과 동일한 파이롯 PN 시퀀스의 오프셋을 사용한다. 페이징 채널은 이동국이 기지국과 함께 동작하기 위해 필요한 시스템 오버헤드(overhead) 정보와 이동국에 관한 메시지를 전송하는데 사용된다. 정보 비트 전송율은 9600bps와 4800bps로 고정이다. 페이징 채널 역시 해당 기지국의 파이롯 채널과 동일한 파이롯 의사 잡음 시퀀스의 오프셋을 사용한다. 페이징 채널의 데이타 프레임은 20ms이며 이를 페이징 슬롯(slot)이라 한다. 페이징 채널의 데이타 스크램블링(scrambling)을 위한 long code mask는 그림3과 같은 형식을 갖는다.

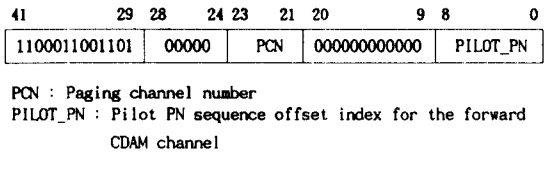


Fig 3. Paging channel long mask

순방향 트래픽 채널은 호(call)가 설정된 동안 사용자 및 신호 정보를 특정 이동국에 전송하는데 이용되며 최대 트래픽 채널의 수는 63에서 동일 순방향 CDMA 채널에서 작동 중인 페이징 채널과 싱크 채널의 수를 뺀 것이다. 데이타 전송율은 9066, 4800, 2400, 그리고 1200bps로 가변적이다. 프래임의 길이는 20ms이며 데이타 전송율은 프레임 단위로 가변 된다. 데이타 스크램블링에 사용되는 long code mask는 역방향 트래픽 채널의 것과 동일한다.

2.2 보호신호 형식

2.2.1 엑세스 채널의 신호

엑세스 채널에서 사용되는 메시지의 종류는 Registration, Order, Data Burst, Origination, Page Response,

Table 1. Common layer 2 and identification fields

Field	Length(bits)
MSG_TYPE(message type)	8
ACK_SEQ(acknowledgement sequence number)	3
MSG_SEQ(message sequence number)	3
ACK_REQ(acknow edgement required indicator)	1
VALID_ACK(valid acknowledgement indicator) 1 : acknowledge a paging channel number 0 : no	1
ACK_TYPE(acknowledgement address type) = ADDR_TYPE of received paging chanel message	3
MSID_TYPE(mobile station identifier field type)	3
MSID_LEN(moblie station identifier field length)	4
MSID(Mobile station identifier) if MSID_TYPE = '0000', MSID = (MIN, ESN)	8xMSID_LEN

Authentication Challenge Response 메시지 등이다. 모든 메시지들은 2계층 및 이동국 신분 증명 공통 필드를 가지며 메시지 종류에 따라 신분인증 공통 필드를 가지는 메시지도 있다. 두 공통 필드의 형식을 표1과 표2에 나타내었다. 신분인증 공통 필드를 갖는 메시지는 Registration, Origination, Page Response, Authentication Challenge Response 메시지 등이다.

Table 2. Common authentication field

Field	Length(bits)
AUTH_MODE(Authentication mode) 00→not required 01→required	2
AUTHR(Authentication data) if '01', set the data	0 or 18
RANDC(Random challenge value) if '01', set the data	0 or 18
COUNT(call history parameter) if '01', set te data	0 or 16

2.2.2 역방향 트래픽 채널의 신호

역방향 트래픽 채널에서 사용되는 메시지 종류는 표3과 같으며 모든 메시지는 MSG_TYPE(8 bits), ACK_SEQ(3 bits), MSG_SEQ(3 bits), 그리고 ACK_REQ (1 bit)로 구성된 공통 acknowledgement 필드를 갖는다. 그리고 모든 필드는 메시지 암호 표시자 Encryption (2 bits) 필드를 공통으로 갖고 있으며 기지국에서 보내온 Channel assignment message, Handoff direction message, 그리고 Message encyption mode order의 ENCRYPTION_MODE로 값을 설정한다.

Table 3. Reverse traffic channel messages

Message Name
Order message
Authentication challenge response message
Flash with information message
Data burst message
Pilot strength measurement message
Power measurement report message
Send burst MTMF message
Status message
Origination continuation message
Handoff completion message
Parameter response message

트래픽 채널의 메시지는 Encryption 필드에 값에 따라 암호화가 설정된다. 그리고 인증에 관계되는 메시지는 Authentication Challenge Response Message 이며 그 형식은 아래 표4와 같다.

Table 4. Authentication challenge response message format

Field	Length(bits)
MSG_TYPE	8
ACK_SEQ	3
MSG_SEQ	3
ACK_REQ	1
ENCRYPTION	2
AUTHU	18
RESEVED	5

2.2.3 명령

명령 메시지는 엑세스 채널이나 역방향 트래픽 채널상의 이동국에 의해 보내지며 6비트의 명령 코드와 0 또는 그 이상의 명령 특유의 필드를 갖는다. 여러 가지 명령이 있으나 인증에 관계되는 명령은 Base station challenge order, SSD update order, SSD update rejection order이며, 음성 프라이버시에 관계되는 명령은 Long code transition requst order, Long code transition response order이다.

2.2.4 보호 상태(Security Status)

아래의 항목들은 이동국의 인증, 메시지 암호화 그리고, 음성 프라이버시 유형(mode)을 기지국으로 되돌리기 위해 역방향 트래픽 채널의 Status Message에 포함될 수 있다.

- AUTH_MODE(Authentication mode, 2 bits) : 만약 표준 인증 정보가 제공된다면 '01', 그렇지 않다면 00으로 둔다.
- ENCRYPT_MODE(Message encryption mode, 2 bits) : 이 부분은 기지국에서 보내 온 Channel as-

signment message, Handoff direction message, 그리고 Message encryption mode order의 ENCRYPTION_MODE 값이며 프레픽 채널 메시지의 메시지 암호 표시자 값이 된다. '00'는 메시지를 암호화하지 않음을 의미하며, '01'은 모든 제어 메시지(control message)를 암호화 함을 의미한다.

- PRIVATE_LCM(private long code mask indicator, 1 bits) : 트래픽 채널에서 private long code mask를 사용하면 '1', 그렇지 않으면 '0'으로 표시한다.

2.3 순방향 채널의 신호

2.3.1 페이징 채널의 신호

트래픽 채널을 할당 받지 않은 이동국에게 제어정보를 보내기위해 사용되며 메시지의 종류는 표5와 같다. 많은 메시지들은 아래와 공통 필드를 갖는데 이들은 메시지가 전달될 이동국의 주소를 정의한다.

- ADDR_TYPE(3 bits) : 주소 필드의 형을 표시하는데 주소가 MIN(MIN1과 MIN2)이면 '000', ESN이면 '001'이다.
- ADDR_LEN : 주소 필드의 길이를 octet로 표시하면 주소형이 MIN이면 5, ESN이면 4이다.
- ADDRESS : 만약 ADDR_TYPE = '000'이면 주소 필드는 MIN(24 bits)과 MIN2(10 bits)로 구성되고, ADDR_TYPE = '001'이면 주소 필드는 ESN(32 bits)로 구성된다.

Table 5. Paging channel messages

System parameter message
Access parameter message
Neighbor list message
CDMA channle list message
Slotted page message
Page message
Order message
Channel assignment message
Data Burst Message
Autentication challenge message
SSD Update message
Feature notification message
Null message

인증과 암호화에 관계되는 메시지는 Access parameters message(AUTH, 2 bits, RAND, 0 또는 32 bits), Channel assignment message(ENCRYPT_MODE, 2 bits), Authenticaton challenge message(RANDU, 24 bits), 그리고 SSD update message(RANDSSD, 56 bits)이다.

2.3.2 순방향 트래픽 채널의 신호

순방향 트래픽 채널을 통하여 전달되는 메시지의 종류는 표6과 같다. 모든 순방향 트래픽 메시지들은 표7의 acknowledgement 공통 필드를 갖는다. 또한 모든 순방향 트래픽 메시지 들은 메시지 표시자 Encryption (2 bits) 필드를 갖는데 이것은 이동국에 보낸 마지막 Channel assignment message,, Handoff direction message 또는 Message encryption mode order의 ENCRYPT_MO-

Table 6. Forward traffic messages

Message name
Order message
Authentication Challenge message
Alert with information message
Data burst message
Handoff direction message
Analog handoff direction message
In-traffic system parameters message
Neighbor List update message
Send burst DTMF message
Power control parameters message
Retrieve parameters message
Set parameters message
SSD update message
Flash with information message
Mobile station registred message

Table 7. Common acknowledgement field of forward traffic channel message

Field	Length(bits)
MSG_TYPE	8
ACK_SEQ	3
MSG_SEQ	3
ACK_REQ	1

DE 값으로 둔다. 표6의 메시지중 인증에 관계되는 것은 Authentication challenge message(RANDU, 24 bits), Handoff direction message(ENCRYPT_MODE, 2 bits) 그리고 SSD update message(RANDSSD, 56 bits)이다.

2.3.3 명령

명령 메시지는 페이징 채널이나 순방향 트래픽 채널 상의 기지국에 의해 보내지며 6비트의 명령 코드와 0 또는 그 이상의 명령 특유의 필드를 갖는다. 여러가지 명령이 있으나 인증에 관계되는 명령은 Base station challenge confirmation order, Parameter update order, 신호 메시지 암호화에 관계되는 명령은 Message encryption mode order, 그리고 음성 프라이버시에 관계되는 명령은 Long code transition request order이다.

Ⅲ. 인증, 암호화 방법 및 호처리

3.1 인증 및 암호화 방법

3.1.1 인증방법

인증은 이동국의 신분 확인을 위한 기지국과 이동국 사이의 정보 교환 절차이며, 기지국과 이동국이 동일한 공유 비밀 데이타를 가질때 성공한다. 인증 데이타(AUTH_SIGNATURE)의 계산과정은 양국이 동일하며 그림4와 같다. 입력 파라메타의 필드는 RAND_CHALLENGE(32 bits), ESN(32 bits), AUTH_DATA (24 bits), 그리고 SSD_AUTH(64 bits)로 구성되어 있다. 입력 파라메타에 따라 인증 알고리듬[4]에 의하여 18 비트 AUTH_SIGNATURE가 출력된다. 표8에 인증을 요하는 호처럼 절차들과 해당 절차에서 입력되는 파라메타들을 나타내었다.

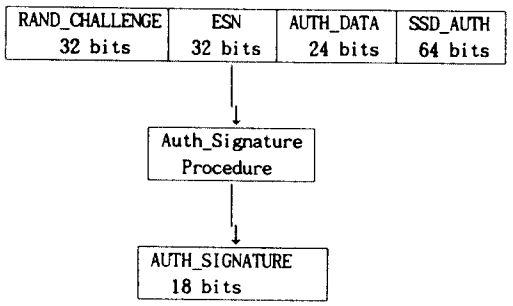


Fig 4. Computation of AUTHR_SIGNATURE of authentication

다음에서는 인증절차에 사용되는 주요 파라메타와 인증기능이 있는 호처리 절차의 인증과정을 간단히 설명하기로 한다.

SSD(shared secret data)는 SSD_A(64 비트)와 SSD_B (64 비트)로 구성되어 있으며 이동국의 준영구 기억소자에 저장된다. SSD_A는 인증과정에 사용되며, SSD_B는 CDMA 음성 프라이버시와 CDMA 및 아날로그 시스템 메시지 비밀성을 위해 사용된다. 생성절차는 뒤에 나오는 SSD 갱신절차에서 설명된다. RAND(Random challenge Memory)는 페이징 채널상에서 수신된 마지막 Access parameters message의 RAND 값인데 originations, terminations, registrations의 인증에 사용된다. COUNTs-p는 modulo-64 카운터로써 순방향 트래픽 채널을 통하여 Parameter updata message를 송신하면 갱신된다.

이동국의 Registrations 인증절차는 다음과 같이 수행된다.

수행조건 : 기지국의 페이징 채널로부터 수신한 Access

Table 8. Auth_Signature Input Parameters

Procedure	RAND_CHALLENGE	ESN	AUTH_DATA	SSD_AUTH	SAVE_REGISTERS
Registration	RANDs	ESNp	MIN1	SSD_A	FALSE
Unique Challenge	256xRANDU + (8 LSBs OF MIN2)	ESNp	MIN1	SSD_A	FALSE
Origination	RANDs	ESNp	Digits	SSD_A	TRUE
Termination	RANDs	ESNp	NIN1	SSD_A	TRUS
Base Station Challenge	RANDBS	ESNp	MIN1	SSD_A_NEW	FALSE

parameters message의 AUTH = "01"이고 이동국이 등록을 시도할때 아래의 인증과정이 수행된다.

〈이동국 절차〉

1) 인증 데이타 계산을 위한 파라메타를 표8과 같이 설정한다.
2) SAVE_GEGISTERS = FALSE로 둔다.
3) Auth_Signature 과정을 수행한다.
4) Registration message의 AUTHR = AUTH_SIGNATURE로 둔다.
5) AUTHR + RANDC(8 MSB of RAND) + COUNTs-p를 Rregistration message에 담아 엑세스 채널을 통하여 보낸다.

〈기지국 절차〉

1) 수신된 RANDC를 내부에 저장된 RAND의 MSB 8bit와 비교한다.
2) 수신된 COUNT를 MIN/ESN과 관련하여 내부적으로 저장된 것과 비교한다.
3) 내부에 저장된 SSD_A를 사용하여 Auth_Signature 과정을 수행한다.
4) 수신된 AUTHR과 내부적으로 계산된 AUTHR을 비교한다.
5) 만약 비교결과 실패하면 등록을 실패로 간주하고 Unique challenge-response 절차를 시작하거나 SSD update 절차를 수행한다.

Unique challenge-response의 인증 절차는 다음과 같이 수행된다.

기지국에서 시작되며 페이징 채널과 엑세스 채널 또는 순, 역방향 트래픽 채널에서도 실행된다.

〈기지국〉

1) 24비트 랜덤 데이타 RANDU를 생성시켜 순방향이나 역방향 트래픽 채널의 Authentication challenge message를 통하여 이동국에 전송한다.
2) 인증 데이타 계산을 위한 파라메타를 표8과 같이 설정한다. 이때 내부에 저장된 SSD_A를 사용한다.
3) Auth_Signature 절차를 실행한다.
4) 이동국에서 보내온 AUTHU를 내부에서 생성된 것과 비교한다.
5) 만약 틀리면 더 이상 이동국의 접근시도를 받아들이지 않고 수행중인 호를 취소시키거나 SSD update 과정을 시작한다.

〈이동국〉

1) 기지국으로부터 Authentication challenge message를 받는 즉시 표8과 같이 입력 파라메타를 설정한다.
2) SVAE_REGISTERS = FALSE로 둔다.
4) Auth_Signature 절차를 실행한다.
5) AUTH_SIGNATURE = AUTHU로 두어 Authentication challenge response message를 이동국에 보낸다.

이동국의 Originations 인증절차는 다음과 같이 수행된다.

수행조건 : 기지국의 페이징 채널로 부터 수신한 Access parmeters pessage의 AUTH 필드 = "01"이고 엑세스 채널을 통해 Origination message을 보냄으로써 호을 시도할때 다음의 인증과정이 수행된다.

〈이동국〉

1) 인증 데이타 계산을 위한 파라메타를 표8과 같이 설정한다.

AUTH_DATA 필드는 Origination message의 CHARi 필드의 마지막 6자리 수로서 설정 한다. 첫번째 자리 숫자가 첫 4 비트 MSB를 차지한다. 만약 6개 미만의 자리수가 있다면 MIN1의 MSB들이 나머지 자리를 채운다.

2) SAVE_RIGISTERS = TRUE로 둔다.
3) Auth_Signature 절차를 실행한다.
4) Origination message의 AUTHR_SIGNATURE로 둔다.
5) RANDC(RAND의 MSB 8 비트)와 COUNT를 이동국의 현재값으로 설정한 Origination message를 전송한다.

〈기지국〉

1) 수신된 RANDC와 저장된 RAND의 MSB 8 비트를 비교한다.
2) 수신된 COUNT를 해당 이동국 관련 데이타 MIN/ESN의 COUNT와 비교한다.
3) 이동국과 같은 방법으로 AUTHR를 생성한다. 단 내부에 저장된 SSDD_A를 사용한다.
4) 계산된 AUTHR를 수신된 그것과 비교한다. 일치하면 채널할당 절차를 수행한다. 채널할당후에 기지국은 순방향 트래픽 채널을 통해 Parameter update order를 이동국에 보내 COUNTs-p값 갱신토록 지시한다.
5) 실패하면 기지국은 서비스를 거부하고 Unique challenge-response 절차나 SSD update 절차를 수행한다.

이동국의 Terminations 인증절차는 다음과 같이 수행된다.

수행조건 : 기지국의 페이징 채널로 부터 수신된 Access parameter message의 AUTH = '01'이고 엑세스 채널을 통해 page response message를 보내어 페이지에 응답할 때 다음 과정이 수행된다.

〈이동국〉

1) 인증 데이타 계산을 위한 파라메타를 표8과 같이 설정한다.
2) SAVE_REGISTERS = TRUE로 둔다.
3) Auth_Signature 절차를 수행한다.
4) Page response message의 AUTHR = AUTH_SIGNATURE로 둔다.
5) RANDC(RAND의 MSB 8 비트)와 COUNT를 이동국의 현재값으로 설정한 Page response message를 전송한다.

〈기지국〉

1) 수신된 RANDC와 저장된 RAND의 MSB 8 비트를 비교한다.
2) 수신된 COUNT를 해당 이동국 관련 MIN/ESN의 COUNT와 비교한다.
3) 이동국과 같은 방법으로 AUTHR를 생성한다. 단 내부에 저장된 SSD_A를 사용한다.
4) 계산된 AUTHR을 수신된 그것과 비교한다. 일치하면 채널할당 절차를 수행한다. 채널할당 후에 기지국은 순방향 트래픽 채널을 통해 Parameter update order를 이동국에 보내 COUNTs-p 값을 갱신토록 지시한다.
5) 실패하면 기지국은 서비스를 거부하고 Unique challenge-response 절차나 SSD update 절차를 수행한다.

SSD 갱신 절차는 다음과 같이 수행된다.

SSD 이동국 특유의 정보(ESN), 랜덤 데이터, 이동국의 A-Key로써 초기화된 SSD Generation pocedure를 수행하여 생신된다. A-Key는 64비트이며 각 이동국 고유의 것을 보호화 관련된 영구 기억 장소에 저장되어 있다. A-Key는 이동국과 관련된 Home Location Register/Authentication Center(HLR/AC)에만 알려져있다[5].

SSD 갱신절차는 그림5와 같으며 아래와 그 절차를 설명한다.

1) 기지국이 페이징 채널이나 순방향 트래픽 채널을 통해 HLR/ACR에서 SSD 계산에 사용된 것과 동일한 RNDSSD를 가진 SSD update message를 송신한다.
2) 이동국은 SSD Update Message 수신 즉시 그림6과 같이 SSD_generation 과정을 수행하여 SSD_A_NEW와 SSD_B_NEW를 출력한다.
3) 이동국은 32비트 랜덤 RANDBS를 선택하여 Base station challenge order에 포함시켜 페이징 채널이나 역방향 트래픽 채널을 통해기 지국에 보낸다.
4) 기지국과 이동국 둘다 인증 데이타 계산을 위해 파라메타를 표8과 같이 설정한다.
5) Auth_Signature procedure를 수행한다. 기지국과 이동국 둘다 SAVE_REGISTERS = FALSE로 둔다.
6) 이동국과 기지국은 AUTHBS = AUTH_SUGNATURE로 둔다.
7) 기지국은 Base station challenge confirmation order에 계산된 AUTHBS를 포함시켜 페이징 채널이나 순방향 트래픽 채널을 통해 이동국으로 송신한다.
8) 이동국은 Base station challenge confirmation order을 수신한 즉시 자신의 내부값과 비교한다. 만약 이동국이 이전에 SSD update message를 수신하

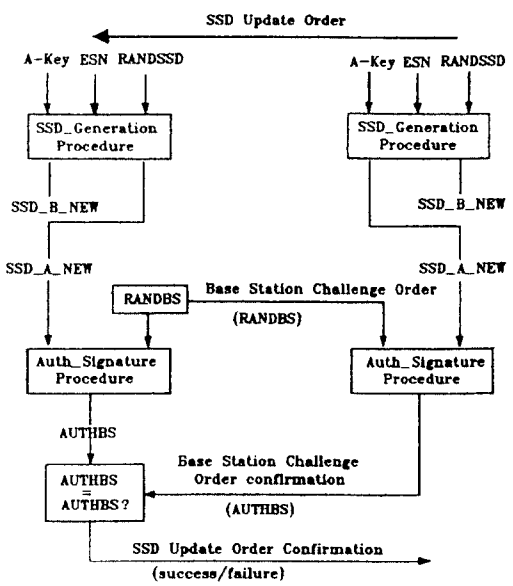


Fig 5. SSD update message Flow

지 않았다면 SSD Update rejection order을 응답한다.

9) 만약 비교가 성공적이면 이동국은 SSD_update 절차를 수행하여 SSD_A와 SSD_B를 각각 SSD_A_NEW와 SSD_B_NEW로 갱신한다. 그리고는 SSD update confirmation order를 기지국에 송신하여 성공을 알린다.

10) 만약 성공이 아니면 SSD_A_NEW와 SSD_B_NEW를 버리고 SSD rejection order를 보낸다.

11) 기지국은 SSD update confirmation order를 받는 즉시 SSD_A와 SSD_B를 HLR/AC로부터 수신된 값으로 설정한다.

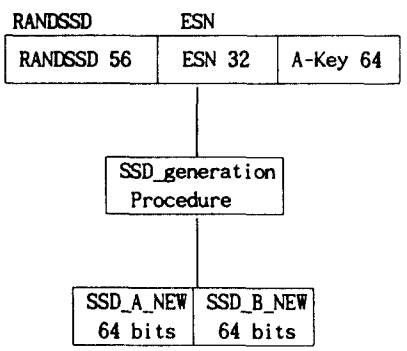


Fig 6. Computation of SSD

3.1.2 신호 메시지 암호화

인증과정을 향상시키고 민감한 가입자 정보(가령 PIN,)를 보호하기 위하여 트래픽 채널 신호 메시지의 선택된 부분들을 암호화할 방법 필요하다. 우선 암호화할 메시지를 결정하여야 하여 암호화 알고리듬을 일반적으로 알려진 알고리듬을 사용할 수 있다.

Access parameters message의 AUTH = '00'이면 메시지는 암호화되지 않으며 신호 메시지 암호화는 각 개별 호에 따라 제어된다. 초기 암호화 모드는 Channel assignment message의 ENCRYPT_MODE의 값에 따라 설정된다. 만약 채널할당 후에 암호화를 개시 할려면 기지국에 다음 중 하나의 순방향 채널 메시지를 보내야 한다.

1) Handoff Direction Message with ENCRYPT_MODE = '01'

2) Analog Handoff Direction Message with MEN = '1'

3) Message Encryption Mode Orde with ENCRYPT _MODE = '01'

만약 신호 메시지 암호화를 종료할려면 기지국은 다음의 순방향 채널 메시지 가운데 한개를 이동국에 보내야 한다.

1) Handoff Direction Message with ENCRYPT_MODE = '00'

2) Analog Hanrodd Direction Message with MEN = '0'

3) Message Encryption Mode Orde with ENCRYPT _MODE = '00'

3.1.3 음성 프라이버시

음성 프라이버시는 PN확산을 위해 사용되는 private long mask에 의해 CDMA에서 제공된다. 음성 프라이버시는 트래픽 채널에서만 제공된다. 모든 호들은 PN 확산을 위한 public long code mask를 사용하여 시작된다. 이동국은 호 설정시 Origination message나 Page reponse message를 사용하거나 트래픽 채널 동작시 Long code transition request order를 사용하여 음성 프라이버시를 요구할 수 있다. 만약 인증이 수행되지 않았다면 private long code mask로의 전환은 수행되지 않는다.

3.2 호처리 과정

3.2.1 역방향 채널의 호처리

이동국의 호처리 과정은 아래와 같이 4단계로 구성되어 있다.

1) 이동국 초기화 상태 - 이 상태에서는 이동국이 CDMA를 사용할 것인지 아니면 아날로그 시스템을 사용할 것인지 선택한다. CDMA를 선택하였다면 기지국의 CDMA 채널을 획득하고 동기를 맞추는 단계로서 시스템 결정 부상태(substate), 파이롯 채널 획득 부상태, 싱크 채널 획득 부상태, 그리고 타이밍 변경 부상태로 나누어 진다.

2) 이동국 아이들(Idle) 상태 - 이동국은 페이징 채널을 감시하여 메시지나 이동국으로 들어오는 호를 받을 수 있고, 발호, 등록 및 메시지 전송을 시작할 수 있다.

3) 시스템 액세스 상태 액세스 채널을 통하여 기지국에 메시지를 보내고 기지국의 페이징 채널로부터 수신된 메시지를 처리하게 된다. 오버헤드 정보 갱신 부상태, 이동국 origination 시도부상태, 페이징 응

Mobile station power up or from any other system o Supervise pilot channel	Pilot channel ←	o Pilot channel transmission
o Sync channel acquisition	Sync channel ←	o Sync channel transmission
o Updates system overhead information	Paging channel ←	o System overhead message transmission . System parameters message . Access parameters message . Neighbor list message . CDMA channel list message
o Sends Registration messages (Idle state) . Power up gegistration . Parameter-change registration . Timer based registration . Distance based registration . Zone based registration	Access channel → Authentication <-->	. Process received Registration messages
Detects user-initiated call o Sends Origination Message	Access channel → Authentication <-->	o Process received Origination messages o Sets up traffic channel o Begins sending null traffic channel data
o Sets up Traffic channel o Receives N_{5m} consecutive valid frames	Paging channel ←	o Sends Channel assignment message
o Begins sending the traffic channel preamble	Reverse traffic channel →	o Acquires the reverse traffic channel
o Begins transmitting null traffic channel data	Forward traffic channel ←	0 Sends Base station acknowledgement order
o Send Long code transition response order	Forward traffic channel ← Reverse traffic channel →	o Sends Long code transition requset order
o Begins processing primary traffic in accordance with Service option 1	Forward traffic channel ←	o Sends service option reponse order
Optional o Sends Origination continuation message	Reverse traffic Channel →	Optional
Optional o Applies ring back in audio path	Forward traffic channel ←	Optional o Sends Alert with information message (Ring back tone)
Optional o Removes ring back form audio path	Forward traffic channel ←	Optional o Sends Alert with informaiton message (tones off)
(User conversation)		(User conversation)

Fig 7. Simple call flow, Mobile station origination example

Mobile station power up or from any other system o Supervise pilot channel	Pilot channel ←	o Pilot channel transmission
o Sync channel acquisition	Sync channel ←	o Sync channel transmission
o Updates system overhead information	Paging channel ←	o System overhead message transmission . System parameters message . Access parameters message . Neighbor list message . CDMA channel list message
o Sends Registration messages (Idle registration) . Power up gegistration . Parameter-change registration . Timer based registration . Distance based registration . Zone based registration	Access channel → Authentication ←--→	. Process received Registration messages
	Paging channel ←	o Sends page message or Slotted page massage
o Sends Page response message	Access channel →	o Set up traffic channel o Begins sending null traffic channel data
o Sets up Traffic channel o Receives N_{5m} consecutive valid frames	Paging channel ←	o Sends Channel assignment message
o Begins sending the traffic channel preamble	Reverse traffic channel →	o Acquires the reverse traffic channel
o Begins transmitting null traffic channel data	Forward traffic channel ←	0 Sends Base station acknowledgement order
o Send Long code transition response order	Forward traffic channel ← Reverse traffic channel →	o Sends Long code transition requset order
o Begins processing primary traffic in accordance with Service option 1	Forward traffic channel ←	o Sends service option reponse order
o Starts ringing	Forward traffic Channel ←	o Sends Alert with information massage (ring)
o User answers call o stop ringong o Applies ring back in audio path o Sends Connect order	Reverse traffic channel →	
o Begins sending primary traffic packets from the service option 1 application (User conversation)		(User conversation)

Fig 8. Simple call flow, Mobile station termination example

답 부상태, 명령/메시지 응답 부상태, 엑세스 부상태, 그리고 이동국 메시지 전송 부상태로 구성되어 있다.

4) 트래픽 채널상의 이동국 제어 상태 - 기지국과 순방향 및 역방향 트래픽 채널을 통하여 상호 통신하며 트래픽 채널 초기화 부상태, 명령 대기 부상태, 이동국 대답 대기 부상태, 대화 부상태, 그리고 해재(release) 부상태로 구성되어 있다.

3.2.2 순방향 CDMA 채널의 호처리

기지국의 호처리 과정은 다음의 4단계로 구성되어 있다.

1) 파이롯과 싱크 채널 처리 - 이 과정 동안 기지국은 이동국이 이동국 초기화 상태에 있는 동안 CDMA 채널을 획득하고 동기를 맞출 수 있도록 파이롯 채널과 싱크 채널을 전송한다.

2) 페이징 채널 처리 - 이동국이 아이들 상태와 시스템 엑세스 상태에 있는 동안 메시지를 수신하기 위해 감시하는 페이징 채널을 전송한다.

3) 엑세스 채널 처리 - 이동국이 시스템 엑세스 상태에 있는 동안 보내오는 메시지를 수신하기 위하여 엑세스 채널을 감시한다.

4) 트래픽 채널 처리 - 이동국이 트래픽 채널 제어 상태에 있는 동안 이동국과 통신하기 위해 순 역방향 트래픽 채널을 사용한다.

3.2.3 호 처리의 간단한 예

그림7에서는 이동국에서 시작되는 호, 그림8에서는 기지국에서 시작되는 호의 간단한 예를 보았다. 이 예에서는 모든 메시지가 오류없이 수신 되었고, acknowledgements를 나타내지 않았다.

V. 맺는말

EIA/IS-95안을 근거로 하여 CDMA 이동통신에서의 보호방법에 대해서 알아 보았다. 직접 대역확산을 위한 PN 시퀀스 발생에 사용될 long code mask는 채널마다 고유하게 생성되어 확산대역을 보호하고 이동국을 식별한다. 이동국의 인증은 고유한 정보를 사용하여 계산한 인증 데이타를 기지국이 확인하는 인증 절차에 의해서 이루워진다. 민감한 정보는 정해진 암호화 알고리듬에 의해서 보호될 수 있고, 음성 프라이버시는 private long code mask에 의해서 대역확산 되어 보호된다. 이러나 CDMA 이동통신은 아나로그 이동통신에 비해 보호체계가 강화되었다고 볼 수 있다. 그러나 여러 형태의 통신범죄를 근원적으로 방지하고, 기존의 통신망과 호환되어 사용될 음성, 화상 및 데이타 통합 이동 통신망에서의 보호 서비스가 제공되기 위해서는 통합적인 보호체계가 구축되어져야 할 것이다.

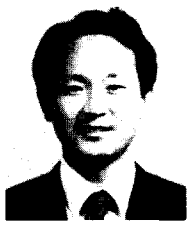
참 고 문 헌

1. 이만영, "암호의 역사적 고찰," 통신정보보호학회지, 창간호, pp. 11-23, 1991년 4월.
2. "미국, 디지틀 셀룰러 전화 표준으로 CDMA 방식 결정," 1993년 9월 6일 단신, 주간기술동향, 한국전자통신연구소.
3. 이석규, "각국의 디지틀 이동통신 개발동향(II)," 1993년 8월 9일 주간기술동향, 한국전자통신연구소.
4. EIA/TIA Standards, *Common Cryptographic Algorithm*
5. TSB 50, *User Interface for Authentication Key Entry*

李 相 坤

- 1960년 12월 1일생
- 1986년 2월 : 경북대학교 전자공학과(공학사)
- 1988년 2월 : 경북대학교 대학원 전자공학과(공학석사)
- 1993년 2월 : 경북대학교 대학원 전자공학과(공학박사)
- 1988년 9월~1991년 2월 : 2월 경북대학교 전자공학과 조교
- 1991년 3월~현재 : 현재 창신전문대학교 전자통신과 조교수

※주관심분야 : 부호기술, 이동통신, 위성통신 암호화 등.



文 相 在

- 1948년생
- 1972년 2월 : 서울대학교 공과대학 공업교육과 전자전공(공학사)
- 1974년 2월 : 서울대학교 대학원 전자공학과(공학석사)
- 1985년 6월 : 미국 U.C.L.A. 통신공학전공(공학박사)
- 1985년 7월~1986년 7월 : 미국 U.C.L.A. 포스탁터
- 1985년 7월~1986년 7월 : 미국 OMNET 회사 컨설턴트
- 1990년 12월~현재 : 경북대학교 공과대학 전자공학과 교수

※ 관심분야 : 디지틀통신시스템, 부호기술, 정보보호, 음성통신 등