CDMA 셀룰라 이동통신을 위한 인증시스템의 개발

°이 국희*, 박 영호*, 이 상곤**, 문 상재*

* 경북대학교 전자공학과

** 창신전문대학

The development of authentication system for CDMA cellular mobile communication

°Kook-Heui Lee*, Young-Ho Park*, Sang-Gon Lee**, Sang-Jae Moon*

* Dept. of Electronics, Kyungpook National University

** Changsin Junior College

요 약 문

이동통신은 통화의 편리성을 제공하는 반면 통화도용의 가능성이 높아 이를 예방하기 위한 사용자 인증서비스가 필요하다. 본 논문에서는 국내 CDMA 이동통신 표준방식인 TIA/EIA/IS-95에서의 사용자 인증시스템을 분석한다. 그리고 실제 인증시스템에 적용 가능한 고속의 해쉬함수를 개발하고 이를 이용하여 인증시스템을 구현한다.

1. 서 론

이동통신은 언제, 어디서나, 누구와도 통신이 가능한 반면에 통화도용, 도청 혹은 불법적인 통신 사기와 같은 통신범죄가 언제든지, 보이지 않는 곳에서, 누구에게도 가해질 수 있다. 특히 통화도용 문제는 요금징수와 직결되어 통신사업자에게는 큰 피해를 주고, 사용자에게는 요금체계와 통화서비스에 대한 불신감을 주어 이동통신 서비스에 매우 큰 장애요인이 된다. 그러므로 이러한 통화도용을 막기 위한 신분인증(authentication) 보호서비스가 중요하다.

국내 CDMA 이동통신 방식인 TIA/EIA/IS-95[1] 인증시스템에서는 이동국의 인증을 위하여 인증서명 절차(Auth_Signature procedure)를 거쳐 생성된 18비트의 인증값이 사용된다. 그러나 인증값을 생성하는 구체적인 인증서명 절차 알고리듬은 공개되지 않았다.

본 논문에서는 TIA/EIA/IS-95 인증시스템을 분석하고, 인증서명 절차 알고리듬으로 사용할 해쉬함수를 개발한다. 인증서명 절차가 18비트의 인증값의 생성뿐만아니라 128비트의 공유비밀 데이타의 생성에도 사용될 수 있는 점과 알고리듬 수행속도가 빨라야 한다는 점을 고려하여 MD5를 근간으로 하여 실제 인증시스템에 적용가능한 고속의 해쉬함수를 개발한다. 그리고 개발된 해쉬함수를 사용하여 인증시스템을 구현한다.

2. CDMA 이동통신 인증시스템

인증은 이동국의 신분확인을 위해 기지국과 이동국 사이에 정보를 교환하는 절차이며, 동일한 공유비밀 데이타(shared secret data, SSD)를 가질때 성공한다. 인증값의 계산과정은 양국이 동일하며 그림1과 같다.

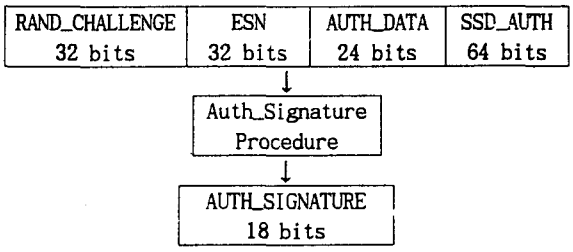


Fig.1. Computation of AUTH_SIGNATURE

인증서명 절차에 사용되는 알고리듬은 CAVE(cellular authentication and voice encryption) 알고리듬으로 32비트의 RAND_CHALLENGE과 ESN(electronic serial number), 24비트의 AUTH_DATA, 그리고 64비트의 SSD_AUTH를 입력으로 가지며 18비트의 AUTH_SIGNATURE를 출력으로 가진다. 표1에 인증을 요하는 호처리 절차와 해당 절차에서의 입력 데이타를 나타내었다.

Table 1. Input parameters of CAVE algorithm

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	MIN1	SSD_A	TRUE
Base Station Challenge	RANDBS	ESNp	MIN1	SSD_A_NEW	FALSE

공유비밀 데이타는 64비트의 SSD_A와 SSD_B로 구성되며 이동국의 반영구(semi-permanent) 기억소자에 저장된다. SSD_A는 CAVE 알고리듬의 입력으로 사용되며, SSD_B는 CDMA 음성 비화(voice privacy)와 메세지의 비밀성을 위해 사용된다. RANDs는 페이징 채널상에서 수신된 마지막 Access Parameters message의 RAND영역의 값이며 이동국의 발호(origination), 착호(termination), 등록(registration)확인 절차에 사용된다. $COUNT_{s-p}$는 모듈라-64 카운터이다.

1) 이동국 등록확인 절차(authentication of M.S. registration)

Access Parameters message의 AUTH영역의 값이 '01'이고 이동국이 등록을 하고자 할 때 이루어지는 절차이다. 기지국과 이동국간의 메세지 흐름은 그림2와 같으며, CAVE 알고리듬의 입력데이타는 표1과 같다.

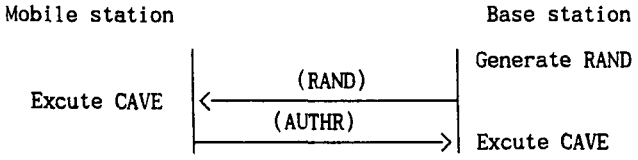


Fig.2. Authentication of M.S.

2) 이동국 발호확인 절차(authentication of M.S. origination)

Access Parameters message의 AUTH영역의 값이 '01'이고 이동국이 호를 시작하고자 할 때 이루어지는 절차이다. 기지국과 이동국간의 메세지 흐름은 그림2와 같으며, CAVE 알고리듬의 입

력데이타는 표1과 같다.

3) 이동국 착호확인 절차(authentication of M.S. termination)

Access Parameters message의 AUTH영역의 값이 '01'이고 이동국이 기지국의 호출에 응하고자 할 때 이루어지는 절차이다. 기지국과 이동국간의 메세지 흐름은 그림2와 같으며, CAVE 알고리듬의 입력데이타는 표1과 같다.

4) 고유시도 응답 절차(unique challenge-response procedure)

이동국 등록확인 절차나 이동국 발호확인 절차가 실패할 경우 기지국에의해 시작되고 기지국과 이동국간의 메세지 흐름은 그림2와 같다. CAVE 알고리듬의 입력데이타는 표1과 같다.

5) 공유비밀 데이타의 갱신(updating the shared secret data)

이동국의 고유시도 응답 절차가 실패할 경우 수행되며 기지국과 이동국간의 메세지 흐름은 그림3과 같다. CAVE 알고리듬의 입력데이타는 표1과 같다.

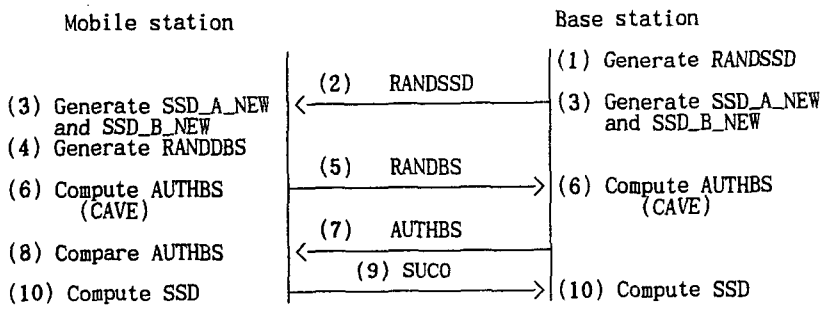


Fig.3. SSD updating procedure

3. CAVE 알고리듬의 개발

CAVE 알고리듬은 152비트의 입력 데이타로 18비트의 인증값 혹은 128비트의 공유비밀 데이타를 생성하는 것으로 실제적인 인증시스템의 안전도를 결정한다고 할 수 있다. 그러나 미국과의 수출규제로 인해 구체적인 알고리듬은 알려지지 않았다. 이에 본 논문에서는 CAVE 알고리듬에 상응하는 알고리듬을 개발한다.

3.1 해쉬함수

일방성 해쉬함수(one-way hash function)는 임의 길이의 입력을 이용하여 일정한 길이의 출력을 만들어 내는 함수로서, 컴퓨터 시스템에서 사용자 및 데이타의 인증과 데이타 무결성을 보장하기 위한 암호학적 도구로 사용되고 있다. 해쉬함수는 다음과 같은 성질을 만족하여야 한다[2]. 여기서 y는 출력값, x는 입력값, 그리고 F는 해쉬함수를 나타낸다.

1. F는 임의의 길이를 갖는 입력에 대해서 적용할 수 있다.
2. F는 고정된 길이의 출력을 생성한다.
3. 어떤 주어진 x에 대해서 F(x)는 비교적 쉽게 계산될 수 있어야 한다.
4. 주어진 y에 대하여 F(x)=y 되는 x를 찾는 것은 계산상 불가능하다.
5. 어떤 정해진 x에 대하여 F(x)=F(x') 되는 x'≠x을 찾는 것은 계산상 불가능하다.

위의 사항 중 (4)는 해쉬함수가 일방성이어야 함을 의미하고, (5)는 충돌이 없어야 함(collisionl-ss)을 의미한다.

해쉬함수는 기초가 되는 함수에 따라 블럭암호(block cipher)에 기초한 해쉬함수, 모듈라연산

(modular arithmatic)에 기초한 해쉬함수, 부울함수(boolean function)에 기초한 해쉬함수로 나눌 수 있다[3].

본 장에서는 블럭암호에 기초한 해쉬함수와 부울함수에 기초한 해쉬함수를 중심으로 CAVE 알고리듬으로서의 타당성을 검토해 본다. 모듈라 연산에 기초한 해쉬함수는 이동국의 계산능력을 고려해 볼때 CAVE 알고리듬으로서의 타당성이 희박하다고 할 수 있다.

3.2. 해쉬함수의 선택

블럭암호에 기초한 해쉬함수 중 그 사용도와 구현의 용이성을 고려하여 DES(data encryption standard)를 기초함수로 가지는 해쉬함수를 후보 알고리듬으로 검토한다. 그리고 부울함수에 기초한 해쉬함수중에서 SSD와 동일한 길이의 출력을 가지는 MD5를 후보 알고리듬으로 검토한다.

DES의 운용모드에는 ECB(electronic code book) 모드, CBC(cipher block chaining) 모드, OFB(output feedback) 모드, 그리고 CFB(cipher feedback) 모드가 있다. DES를 CAVE 알고리듬으로 사용할 경우의 문제점은 다음과 같다.

1) ECB 모드 : 18비트의 인증값 생성에는 DES가 한번만 수행되면 되지만 152비트의 입력데이타를 64비트로 축약하는 알고리듬이 필요하게된다. 128비트의 SSD 생성에는 64비트의 출력을 갖는 DES가 2번 수행되어야 한다. 그리고 152비트의 입력데이타를 128비트로 축약하는 알고리듬이 필요하다.

2) CBC 모드 : CAVE 알고리듬의 입력데이타가 152비트이므로 DES가 3번 수행되어야 한다. 그리고 192비트의 출력을 18비트 혹은 128비트로 축약하는 알고리듬이 필요한다.

3) OFB 모드 : 152비트의 입력데이타중 인증값 생성시에는 18비트만이 영향을 미치고, SSD 생성시에는 128비트만이 영향을 미친다. 이를 방지하기 위해 152비트의 입력데이타를 18비트 혹은 128비트로 축약한다면 인증시스템에 필요한 데이타를 생성한 후 암호화하는 것에 지나지 않는다.

4) CFB 모드 : OFB 모드와 동일한 문제점을 가진다.

DES를 이용하여 CAVE 알고리듬을 구현할 경우 DES를 여러번 수행해야하고, 입·출력 데이타를 축약하는 또 다른 알고리듬이 필요하다. 그리고 DES가 공격되었을 경우 암호화 키이가 노출되는 문제가 발생한다. 키이의 노출문제는 암호화 키이가 A_KEY일 경우 심각한 문제점을 발생시킨다.

위와같은 관점에서 본 논문에서는 부울함수에 기초한 해쉬함수 가운데 디지탈 서명등을 위한 표준으로 채택 가능성이 높으며 공개된 알고리듬인 MD5의 안전성을 분석하여 개선하고, 이를 CDMA 이동통신 프로토콜에 적합하도록 변형한다.

3.3. 알고리듬의 개발

부울함수에 기초한 해쉬함수가 안전하기 위해서는 부울함수가 다음의 성질을 만족하여야 한다[4,5].

- P1 : 0-1 balanced 이어야 한다.
- P2 : 높은 비선형도(nonlinearity)를 가져야 한다.
- P3 : SAC를 만족하여야 한다.
- P4 : 입력 좌표들을 선형변환하여 집합 내의 다른 함수로 변환되지 않아야 한다.
- P5 : 상호 output-uncorrelated 여야 한다.

P1은 부울함수의 출력이 0 혹은 1일 확률이 0.5로 동일하게 만든다. P2는 선형함수의 집합을 사용하여 암호시스템을 공격하기 어렵게한다[6]. P3는 암호화 알고리듬에 애벌런치(avalanche) 효과를 야기한다. P4는 암호 알고리듬에 활용된 함수들이 구조적인 면에서 서로 닮지 않도록 한다. P5는 함수들의 시퀀스가 상호 상관관계를 갖지 않도록 한다.

표 2에 MD5의 부울함수에 대하여 P1, P2 그리고, P3의 성질을 조사하여 나타내었다. 4개의 함수는 0-1 balanced는 만족하지만, 1차 SAC[7](SAC of order 1)는 만족하지 못한다. 그리고 H는 선형함수이므로 비선형도가 0이고 나머지 함수들은 비선형도가 2인데 이것은 V_3 상에서 얻을 수

Table 2. Security analysis of Boolean function of MD5

함수	f(x, y, z)	0-1 blanced	nonlinearity	SAC	1차 SAC
F	xy V not(x)z (53H)	O	2	O	×
G	xz V Ynot(z) (27H)	O	2	O	×
H	x xor y xor z (69H)	O	0	×	×
I	y xor (x V not(z)) (9CH)	O	2	×	×

* 1. ( ) : sequence of function(hexadecimal)
2. V : bitwise OR
not : bitwise complement
xor : bitwise XOR
xy : bitwise AND of x and y

있는 최대의 비선형도이다. V_3는 GF(2)의 원소로 구성된 n개의 튜플로 이루어진 벡터공간을 나타낸다[4,5]. G함수는 좌표축을 x→y, y→z, z→x 로 변환하고, I 함수는 좌표축을 x→y xor z, y→x xor z xor 1, z→x로 변환하면 F함수와 동일한 함수가 되므로 P4를 만족하지 못한다. 그리고, 표3에 MD5 함수집합의 상호 *output-uncorrelated*를 표시하였다. 표3에서 보듯이 P5를 만족하지 못한다.

Table 3. Output-correlation of Boolean function of MD5
* O : mutually output-uncorrelated
× : mutually not output-uncorrelated

27H	O		
69H	O	O	
9CH	×	×	×
	53H	27H	69H

V_3 상에서 가능한 모든 함수의 시퀀스 갯수는 2^8개이다. 이 가운데 표2의 조건들을 모두 만

Table 4. Functions on V_3 satisfying 0-1 balancedness, maximum nonlinearity, SAC and 1st order SAC

sequence of function	descriptions
E8H	not(x)not(y) V not(x)not(z) V not(y)not(z)
D4H	not(x)not(y) V not(x)z V not(y)z
B2H	not(x)not(z) V not(x)y V not(z)y
8EH	not(z)x V not(y)x V not(y)not(z)
71H	not(x)y V not(x)z V yz
4DH	not(y)x V xz V not(y)z
2BH	not(z)y V not(z)x V xy
17H	xy V zy V xz

족하는 함수를 찾아 본 결과 8개가 발견되었다. 그 결과를 표4에 나타내었다. 이 중에서 B2H는 좌표축을 x→x, y→z, z→y 로 변환하면 D4H가 되고, 8EH는 좌표축을 x→y, y→x, z→z로 변환하

면 B2H와 동일 함수가 되므로 D4H, B2H 그리고 8EH는 구조적으로 선형적 등가이다. 그리고, 4DH는 좌표축을 x→x, y→z, z→y로, 71H는 x→z, y→y, z→x로 각각 변환하면 2BH와 같은 함수가 되므로 4DH, 71H 그리고 2BH는 구조적으로 선형적 등가이다. 구조적으로 등가인 함수를 같이 묶어서 표5에 다시 정리하였다.

Table 5. Classification of functions in Table 4
according to linearily equivalence in structure

class	sequences of function
1	E8H
2	D4H, B2H, 8EH
3	4DH, 71, 2BH
4	17H

표6에는 표4의 함수들 사이의 상호 output-uncorrelated 관계를 나타내었다.

Table 6. Output-correlation of Boolean function in Table 4
○ : mutually output-uncorrelated
× : mutually not output-unclrrelated

D4H	○						
B2H	○	○					
8EH	○	○	○				
71H	○	○	○	×			
4DH	○	○	×	○	○		
2BH	○	×	○	○	○	○	
17H	×	○	○	○	○	○	○
	E8H	D4H	B2H	8EH	71H	4DH	2BH

표5와 6에서 가급적 구조적으로 등가가 아니면서 output-uncorrelated인 함수 집합으로 {17H, 2BH, 71H, B2H }를 선택하여 기초 부울함수로 사용한다.

MD5 알고리듬을 근간으로 하고 앞에서 선택한 부울함수를 이용하여 160비트가 입력되어 18비트의 인증 데이타 혹은 128비트의 공유 비밀 데이타를 생성하는 해쉬함수를 개발한다. 알고리듬은 아래와 같이 4단계로 나누어 진행된다.

1단계 : 패딩(padding) 비트 추가

입력 데이타는 인증 데이타 생성의 경우 RAND(32비트), ESN(32비트), MIN1(24비트) 그리고 SSD_A(64비트) 순으로 구성되고, 공유 비밀 데이타 생성시에는 RANDSSD(56비트), ESN(32비트) 그리고 A_KEY(64비트) 순으로 구성된다. 입력 데이타 시퀀스 152비트 다음에 padding 비트로 8비트의 0를 추가하여 5개의 32비트 워드(word)를 만든다.

2단계 : 버퍼의 초기화

4개의 워드버퍼(word buffer : 32 비트길이)를 다음과 같이 초기화한다.

word A : 01 23 45 67

word B : 89 ab cd ef

word C : fe dc ba 98

word D : 76 54 32 10

3단계 : 5개의 워드로된 메시지블럭 처리

메시지 처리의 기본 단위는 32비트이므로 입력 데이타는 5개의 워드 x[1], x[2],...,x[5]로 나뉘어지며, 이 데이타는 4라운드의 반복연산을 거치게 되는데 각 라운드에서 식(1)로 표시되는 5단계

의 반복연산으로 처리된다.

$$a = b + ((a + f(b,c,d) + x[k] + t) << S) \quad (1)$$

여기서 (a, b, c, d)는 각 라운드의 단계마다 정해진 버퍼 A, B, C, D의 순열이다. 그리고 f는 각 라운드 마다 정해진 부울함수로 MD5를 일방향 해쉬함수로 만드는 중요한 기본함수인데 표7에 나타내었다. x[k]는 메시지 블럭을 5개의 워드로 나눈 것 중에서 k번째 워드를 의미하는데 각 라운드의 단계마다 랜덤한 순서로 입력 되어진다. x<<S는 32비트 워드를 왼쪽으로 S비트 만큼 순환 쉬프트(Circular shift)한 값을 의미한다. 그리고 t는 상수값이며, S, k, t는 각 단계마다 고유한 값을 갖는다. +는 32비트 모듈라 덧셈을 표시한다.

Table 7. Basic boolean function for hash

Round No.	function	expression
1	F(x,y,z)	not(x)not(z) V not(x)y V not(z)y
2	G(x,y,z)	not(x)y V not(x)z v yz
3	H(x,y,z)	not(z)y V not(z)x V xy
4	I(x,y,z)	xy V zy V xz

각 라운드별 반복연산의 5단계는 MD5의 처음 5단계를 취하였다. 구체적 실행 과정은 다음과 같다.

라운드 1:

FF(a, b, c, d, x[k], s, t)는 a = b + ((a + F(b, c, d) + x[k] + t)<< S) 의 연산과정을 나타낸다고 정의하면 라운드 1에서는 다음의 과정이 순차적으로 진행된다. i 번째 단계의 상수 t는 4094967296 x abs(sin(i))의 정수부분의 값이다. 여기서 i는 라디안(radians)이다.

FF(a, b, c, d, x[0], 7, 3614090360)
FF(d, a, b, c, x[1], 12, 3905402710)
FF(c, d, a, b, x[2], 17, 606105819)
FF(b, c, d, a, x[3], 22, 3250441966)
FF(a, b, c, d, x[4], 7, 4118548399)

라운드 2:

GG(a, b, c, d, x[k], s, t)는 a = b + ((a + G(b, c, d) + x[k] + t)<< S) 의 연산과정을 나타낸다고 정의하면 라운드 2에서는 다음의 과정이 순차적으로 진행된다.

GG(d, a, b, c, x[1], 5, 4129170786)
GG(c, d, a, b, x[3], 9, 3225465664)
GG(b, c, d, a, x[2], 14, 643717713)
GG(a, b, c, d, x[0], 20, 3921069994)
GG(d, a, b, c, x[4], 5, 3593408605)

라운드 3:

HH(a, b, c, d, x[k], s, t)는 a = b + ((a + H(b, c, d) + x[k] + t)<< S)의 연산과정을 나타낸다고 정의하면 라운드 3에서는 다음의 과정이 순차적으로 진행된다.

HH(c, d, a, b, x[2], 4, 4294588738)
HH(b, c, d, a, x[0], 11, 2272392833)
HH(a, b, c, d, x[3], 16, 1839030562)
HH(d, a, b, c, x[4], 23, 4259657740)
HH(c, d, a, b, x[1], 4, 2763975236)

라운드 4:

II(a, b, c, d, x[k], s, t)는 a = b + ((a + I(b, c, d) + x[k] + t)<< S)의 연산과정을 나타낸다고 정의하면 라운드 4에서는 다음의 과정이 순차적으로 진행된다.

II(b, c, d, a, x[3], 6, 4096336452)
II(a, b, c, d, x[1], 10, 1126891415)
II(d, a, b, c, x[0], 15, 2878612391)
II(c, d, a, b, x[4], 21, 4237533241)
II(b, c, d, a, x[2], 6, 1700485571)

4라운드 연산후에 나온 A, B, C, D 값에 초기 입력 데이타의 상위 128비트 값을 더한다.

4단계 : 최종으로 출력된 버퍼 A, B, C, D를 128비트 압축 데이타로 삼는다. 만약 해쉬의 기능이 인증 데이타 18비트의 생성이면 이중 18비트를 출력으로 택하고, 해쉬의 기능이 비밀키 SSD의 생성이면 버퍼 A와 B의 64비트를 SSD_A 그리고 버퍼 C와 D의 64비트를 SSD_B로 출력시킨다.

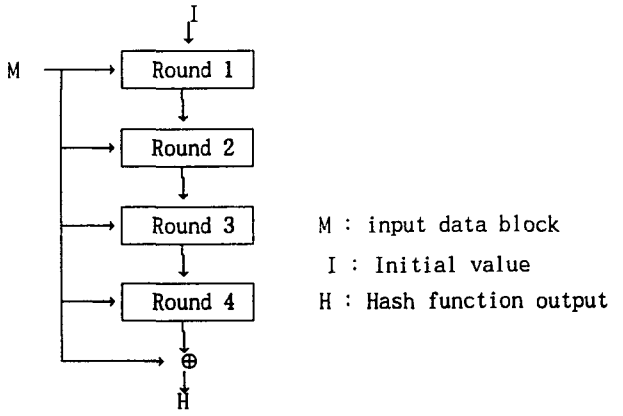


Fig.4. Flowchart of new hash function

그림 4는 새로 개발된 해쉬함수의 데이타 처리 과정을 나타낸다.

4. 인증시스템의 시뮬레이션

4.1. 인증시스템의 구현

본 논문에서는 CDMA 이동통신 인증시스템의 구현을 위해 TIA/EIA/IS-95의 인증 프로토콜을 사용하였다. 그리고, 인증값을 생성하는 CAVE 알고리듬은 본 논문에서 개발한 해쉬함수를 사용하였다. 두대의 PC로 이동국과 기지국을 구성하고 이들의 연결에는 MAYONET(monetarily abating yet operating network)라는 LAN을 이용하였다. 그리고 시뮬레이션 프로그램은 C로 작성되었다.

4.2. 실험 및 고찰

시뮬레이션에 사용한 MIN, ESN, A_KEY와 SSD_A 값은 다음과 같다.

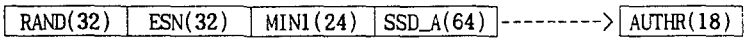
MIN : 0000110101 1110110110 0110011111 1001
ESN : 0000001100 0000000000 0000101010 11

A_KEY : 1001101101 1011011010 1110010100 0101010000 1101011000
1011101100 0010

SSD_A : 0010011101 1101110100 0100000101 1000110110 0100100011
0000101100 0111

1) 이동국의 등록확인 절차

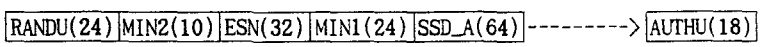
RAND : 1001110110 0111011000 0111000010 01



AUTHR : 1001110100 01110111

2) 고유시도 응답 과정

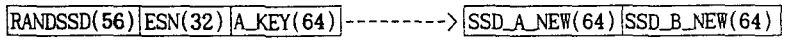
RANDU : 1100101100 0111100111 1100



AUTHU : 1101110111 01011101

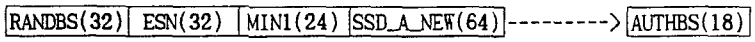
3) 공유비밀 데이타 갱신

RANDSSD : 0110100100 0111000100 1011010110 0110010000
1011110010 111101



SSD : 1011010111 0110001010 0100000111 0110101101 1011001100
0100110000 1101000001 0010101001 0001110100 1100111011
1110010100 0001111000 10101010

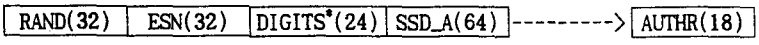
RANDBS : 0100000010 1101111100 0100000011 01



AUTHBS : 0111000100 10110001

4) 이동국 발호 인증

RAND : 0001011110 1111111001 0010010010 11



DIGITS*(24) : 착신처의 전화번호중 하위 24비트

DIGITS : 0101101001 0101010001 0111

AUTHR : 1010110000 01111000

이동국 착호인증 절차는 이동국 등록확인 절차와 동일한 과정을 가지므로 실험결과에는 제외시켰다. 위의 실험결과 이동국이 기지국과 동일한 인증관련 데이타를 가지고 있을 경우 인증에 성공함을 알 수 있었고 인증에 필요한 152비트의 데이타 중 1비트만 차이가 나도 인증에 실패함을 보았다. 그리고, 이동국이 기지국과 동일한 A_KEY를 가지고 있을 경우에만 공유비밀 데이타 갱신과정을 성공적으로 수행할 수 있었다.

5. 결 론

이동통신에서의 통화도용 문제는 요금징수와 직결되어 통신사업자에게는 큰 피해를 주고, 사용자에게는 요금체계와 통화서비스에 대한 불신감을 주어 이동통신 서비스에 매우 큰 장애요인이 된다. 통화도용을 예방하기 위해서는 신분인증 보호서비스가 제공되어야 한다.

본 논문에서는 이러한 통화도용을 방지하기 위한 사용자 인증시스템을 국내 CDMA 이동통신 방식인 TIA/EIA/IS-95를 대상으로 분석하였다. 그리고 실제 인증시스템에 적용 가능한 고속의

CAVE 알고리듬을 개발하였다. CAVE 알고리듬의 개발을 위하여 MD5의 안전성을 부울함수의 안전성이란 관점에서 분석, 개선하였고 이를 TIA/EIA/IS-95 인증시스템에 적용 가능하도록 변형하였다. 그리고, 개발한 CAVE 알고리듬을 사용하여 인증시스템을 구현하고 이의 동작을 실험하였다.

참 고 문 헌

1. TIA/EIA/IS-95, *Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System,* July 1993
2. R.C. Merkle, "One way hash functions and DES," *Proc. of Crypto'89,* Aug. 1989, pp.407-419
3. C.J.Mitchell, F.piper and P.Wild, "Digital signatures," in *Contemporary Cryptology: The Science of Information Integrity,* G.J.Simmons, editor, IEEE Press, 1991, pp.325-378
4. Y.Zheng, J.Pieprzyk, and J.Seberry, " HAVAL - A One-Way Hashing Algorithm with Variable Length of Output," *AusCrypt'92* abstract, 1992
5. Jennifer Seberry and Xian-Mo Zhang, " Highly nonlinear 0-1 balanced boolean functions satisfying strict avalanche criterion," *AusCrypt'92,* Gold Coast, pp.4.1-4.6, 1992
6. A.F.Webster and S.E.Tavares, " On the design of S-boxes," *Proc. of Crypto'85,* 1986, pp.523-534
7. R.Forre, " The strict avalanche criterion: Spectral properties of boolean functions and an extended definition," *Proc. of Crypto'88,* 1989, pp.450-468