A Security Weakness of the CDMA(Code Division Multiple Access) Cellular Service

Dae Hyun Ryu,† and Seung Ju Jang††,

+Hansei Univ. Dept. of Info. Comm. Engineering, Korea
++Dongeui Univ. Dept. of Computer Engineering, Korea

Summary
We consider the problem of security in the CDMA. CDMA system has wireless channels to transmit voice or data. By this reason, CDMA communication has a possibility of being eavesdropped by someone. It is known that eavesdropping in CDMA system is impossible because the voice data spreads with the PN. However, we can eavesdrop the CDMA data using FCM protocol in case that we know the ESN and the MIN. In CDMA system, ESN and MIN are exposed to the wireless channel. In this paper, we analyze the flow of the voice and signal in the CDMA system and monitor the forward traffic channel by the FCM protocol. The FCM protocol is proposed to monitor the forward channel in CDMA system. We can show the possibility of monitoring in one-way channel of CDMA system by the FCM protocol. The test instrument based on the FCM protocol is proposed to monitor the CDMA forward channel. We will show the system architecture of the test instrument to monitor the forward channel in CDMA.
Key words: *CDMA, Security Weakness, FCM(Forward Channel Monitoring) protocol, ESN(Electronic Serial Number)*

Introduction

As the cellular telephony industry has boomed, the need for security has increased: both for privacy and fraud prevention. All cellular communications are sent over a radio link and anyone with the appropriate receiver can passively eavesdrop all cell phone transmissions in the area without fear of detection. In 1992, the wireless industry adopted an encryption system that was deliberately less secure than what knowledgeable experts had recommended at that time. As a result, the potential of eavesdropping has always existed and some say that it has been waiting for criminals with advanced techniques to exploit [1,7,9,19].

The cellular telephony industry workers are especially concerned with fraud prevention. Cell phone cloning is probably the foremost form of fraud prevention problem. As today's most cell phones identify themselves over public radio links by sending their identity information in the clear, eavesdroppers can get easily others' identity information to make fraudulent phone calls. The latest digital cell phones currently offer some protection against casual eavesdroppers. In addition, digital technology is so new that inexpensive digital scanners have not yet been available widely.

The scope of analysis deals with numerous techniques for computation of 18-bit hash codes from the 152-bit message block for *CDMA*(Code Division Multiple Access) cellular systems. The *MS*(Mobile Station) operates in conjunction with the *BS*(Base Station) to authenticate the identity for the *MS*. Authentication is the process by which information is exchanged between the *MS* and the *BS* for the purpose of confirming the identity of the *MS*. A successful outcome of the authentication process occurs only when it can be demonstrated that the *MS* and the *BS* process identical sets of Shared Secret Data (SSD) [2,3,10,12,15]. The majority of proposed techniques are based on cryptography where encryption of the information with a random key is employed [4,21,22].

We consider the problem of security in the *CDMA* mobile communication. Mobile communication has an attribute of wireless. By this reason, mobile communication has a possibility of being eavesdropped by someone. The Distributed Sample Acquisition (DSA) technique [1], recently presented for fast acquisition of long-period Pseudo Noise (PN) sequences, substantially outperforms the existing Serial Search Acquisition (SSA) technique [2] in acquisition time performance. However, in case of knowing the ESN(Electronic Serial Number) and MIN(Mobile station Identification Number), we can eavesdrop the *CDMA* data by the *FCM(Forward Channel Monitoring)* protocol. In *CDMA* system, the ESN and MIN are exposed to the wireless channel [5]. We can easily know the ESN and MIN value by using HP8924C instrument.

Manuscript received May 25, 2006.
Manuscript revised May 30 , 2006.

The forward channel spreads the data by the Walsh Code, but the reverse *CDMA* channel spreads the data by the Long Code [2, 4]. While sending data to the *BS* on the access channel, the *MS*(Mobile Station) constructs the mask with the *BS*(Base Station) identity, the paging channel number, and the access channel number. While sending traffic to the *BS*, the *MS* uses the constructed mask from its ESN(Electronic Serial Number) [1, 3]. We consider the problem of security in the *CDMA*. It is known that eavesdropping in *CDMA* system is impossible because they spread the voice data wrapping with the Pseudo Noise (PN).

In this paper, we propose the *FCM* protocol that analyzes the flow of the voice and signal in the *CDMA* system and monitors the forward traffic channel by the *FCM* protocol. This paper was structured and outlined in the following order: Section 2 – Signal Flow of Forward Channel, Section 3 - Security Architecture and Security Issues of *CDMA* System, Section 4 - Monitoring of Forward Traffic Channel and Experiments, Section 5 – Conclusion.

2. Signal Flow of Forward Channel

The long code is a period 2^{42}-1 LFSR(Linear Feedback Shift Registers) sequence that is used for spreading the reverse link. There is only one long code *sequence*. Different stations are distinguished not by the sequence itself but by its *relative phase*. The fact that the long code is added to each of the two (I and Q) short code sequences to ensure cross correlation between signals from distinct stations [29,31]. The long code LFSR tap polynomial is as follows:

$$G(X) = x^{42} + X^{35} + X^{33} + X^{31} + X^{27} + X^{26} + X^{25} + X^{22} + X^{21} + X^{19} + X^{18} + X^{17} + X^{16} + X^{10} + X^{7} + X^{6} + X^{5} + X^{3} + X^{2} + X^{1} + 1 \quad (1)$$

When transmitting to an access channel, the *MS* constructs the mask from the *BS* identity, the paging channel number, and the access channel number. When transmitting traffic, the *MS* uses a mask constructed from its ESN(Electronic Serial Number) [11,27]. Hadamard-Walsh functions(H_M in eq. (2)) are binary orthogonal sequences, with power-of-two lengths. They can be generated by the recursion [6,11,14].

$$H_M = \begin{bmatrix} H_{M/2} & H_{M/2} \\ H_{M/2} & -H_{M/2} \end{bmatrix} \quad (2)$$

where

$$H_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

and M is a power of two. The rows of any instance form a mutually orthogonal set over the inner product.

The Walsh functions of order 64 are used as orthogonal cover on the forward link channels. They are also used as orthogonal modulation symbols in the reverse link. Although the functions are the same, they are used for entirely different purposes in the forward and reverse links.

There are three types of overhead channel in the forward link: pilot, sync, and paging. The pilot is required in every station. The paging channel is the vehicle for communicating with mobile stations when they are not assigned to a traffic channel. As the name implies, its primary purpose is to convey pages, that is, notifications of incoming calls, to the mobile stations. It carries the responses to the *MS* accesses, both page responses and unsolicited originations. Successful accesses are normally followed by an assignment to a dedicated traffic channel.

The code channels are mathematically orthogonal. The orthogonality is established by covering the FEC(Forward Error Correction) code symbols with one of sets of 64 so-called Walsh functions. As only whole periods of the Walsh functions occur in each code symbol, the effect of the Walsh cover is to make the channels completely separable in the receiver, at least in the absence of multipath. The orthogonality means not only that there is no co-mingling of channels, but that there is no interference between users in the same cell, again in the absence of multipath. This has a substantially beneficial effect on the forward link capacity. All the channels are added together and sent to the modulator. When the *BS* supports multiple forward *CDMA* channels, frequency division multiplex is used.

The PN code of period 242-1 chips is used in IS-95 systems at a chipping rate of 1.2288 Mchips/sec. This PN code is called the long code because its period is much longer than that of the pilot or short PN codes which are 215 or 32,768 chips. At the chipping rate of 1.2288 Mchips/sec, the time period of the pilot code is only 262/3 msec or exactly 75 periods every 2 seconds. Figure 1 is a forward traffic channel structure.

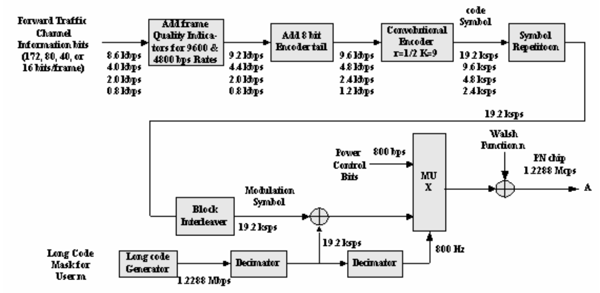

Figure 1. Forward Traffic Channel Structure

Each mobile unit is identified as the following sets of numbers. The first number is the Mobile Identification Number (MIN). This 34 bits binary number is derived from the unit's telephone number, MIN1 is the last seven digits of the telephone number and MIN2 is the area code. The MIN is your telephone number. MINs are keypad programmable. You or a dealer can assign any number what you want. A MIN is ten digits long. A MIN is not your directory number since it is not long enough to include a country code. Figure 2 shows the data flow between the *MS* and the *BS*.

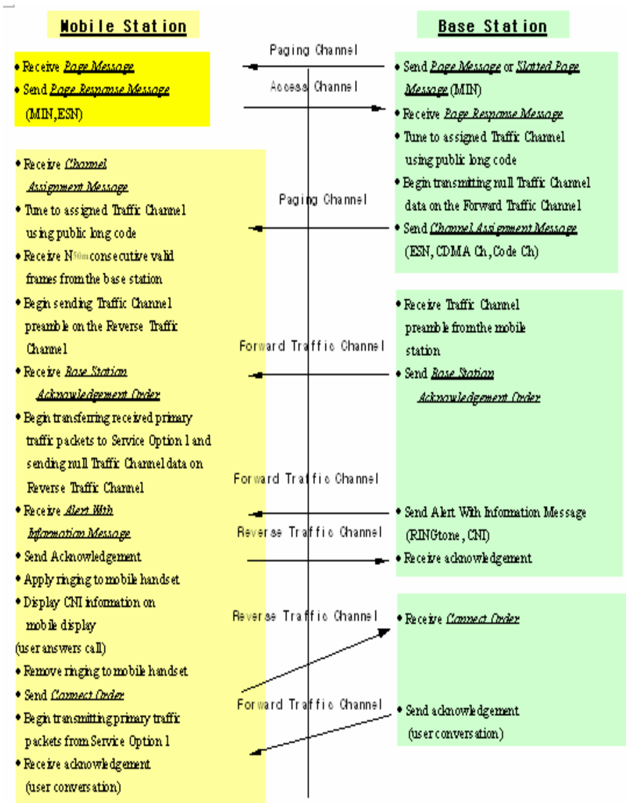

Figure 2. Data Flow between the *MS* and the *BS*

3. Security Architecture of the *CDMA* System

3.1 CDMA Data Channel

The authentication system with TIA/EIA/IS-95 standard in cellular phone provides authentication, signaling message encryption, and voice privacy. To provide these services, The CAVE(Cellular Authentication and Voice Encryption Algorithm), CMEA(Cellular Message Encryption Algorithm), and PN sequence(private long code mask) were used. In an effort to enhance the authentication process and to protect sensitive subscriber information(such as PINS), a method is needed to encrypt certain fields of selected traffic channel signaling messages. The CAVE algorithm is used as authenticated signature algorithm, the CMEA is used as signal encryption algorithm, and PN sequence is used as voice privacy. The range of security in *CDMA* is constrained between the authentication and encryption for the *MS* and the *BS*.

3.1.1 The Authentication System

The *CDMA* system confirms the *MS* by communicating the shared secret data i.e., the SSD between the *BS* and the *MS*. The calculation procedure of authenticated value is the same in both stations. The CAVE algorithm is used for the authenticated procedure. The SSD is composed of the SSD_A and SSD_B. The SSD is stored into semi-permanent semiconductor of the *MS*. The *CDMA* uses the SSA_A for authentication function and SSD_B for voice privacy and signaling message encryption.

3.1.1.1 Forward Link

There are three types of overhead channel in the forward link: pilot, sync, and paging. The whole number of the forward link is 64 channels that are one pilot channel, one sync channel, maximum seven paging channels, and 55 traffic channels. The QPSK(Quadrature Phase Shift Keying) was to be used to demodulate the channel.

1) Pilot Channel

The pilot channel is required in every station. The phase reference is used to demodulate the receiving data from other channel in the *MS*. The W0 Walsh Function is assigned with the pilot channel that also uses the PN sequence for the QPSK demodulation. The pilot PN sequence that is derived from the fifteen shift registers is used in the I-Channel and Q-Channel. The primitive polynomial for generation of PN sequence is as follows eq. (3), (4).:

$$PN(x) = x^{15} + x^{13}+x^{9}+x^{8}+x^{7}+x^{5}+1 \quad (3)$$

$$PNQ(x) = X^{15} + x^{12}+x^{11}+x^{10}+x^{6}+x^{5}+x^{4}+x^{3}+1 \quad (4)$$

2) Sync Channel

The sync channel is available for determination of the initialization variable in power on system of the mobile system. The data of sync channel includes the identification number of the *BS*, pilot power amplifier, and phase offset for the PN sequence.

3) Paging Channel

The paging channel operates at a data rate of 4800 or 9600 bps and transmits overhead information, pages, and orders to a *MS*. The paging channel message is similar to the form of the sync channel message. The message length includes the header, body, and CRC, but not the padding. Paging Channel messages can use synchronized capsules that end on a half-frame boundary or unsynchronized capsules that end anywhere within a half-frame. The paging channel has W1 ~ W7 Walsh function. The hash function is available for assigning the paging channel into the *MS*. The hash function is as follows eq. (5).:

$$R = \lfloor N\times((40503\times(L\oplus H\oplus DECORR)) \bmod 2^{16})/ 2^{16} \rfloor \quad (5)$$

(Where R is paging slot number(hashed value), *N* is channel number(seven), *L* is lower sixteen bits of hash key, *H* is upper sixteen bits of hash key, *DECOOR* is decorrelate hash value;N : total slot number = 2048; DECOOR =6XHASH_KEY[0,1,2,…11]; HASY_KEY=MIN1+2^24XMIN2)

4) Traffic Channel

The traffic channel includes the real voice, which is transformed into the digital signal by QCEP(QualComm Code Excited Linear Predictive Coding). The voice signal is transformed into electronic control data by MUX of 800bps electronic data before assigning the Walsh function. Figure 1 shows the structure of the forward link.

3.1.1.2 Reverse Link

The channel number of a reverse link is 64 bits. Maximum 32 access channels and 64 traffic channels was used. The QPSK was used to demodulate the channel.

1) access channel

The reply, command, and registration of page are included into the access channel. The transfer rate of data in the access channel is 4.8 Kbps. The data passes Convolution Encoder, Repetition, and Block Interleaving. Walsh function creates new data with 6 bits group data and amplified by Long Code PN sequence.

2) traffic channel

The traffic channel has a voice data and signal data like the forward link channel.

3) *CDMA* system communication

The MSC(Mobile Switching Center) in the *CDMA* communication manages the wireless frequency, channel, the track of the *MS*, and handoff mechanism. The HLR(Home Location Register) manages the home position of user. The HLR also manages the user identification and data during communication. VLR(Visitor Location Register) manages the temporary data that is not enrolled as a normal user. The AC(Authentication Center) handles the user key for an user authentication.

3.2 Security Mechanism and Issues for the Long Code Mask and the CMEA Algorithm

The security is achieved both in the paging channel and the traffic channel for the forward link and in the access channel and the traffic channel for the reverse link. The following polynomial (6) is long code sequence in Figure 3.:

$$f(x) = x^{42}+x^{41}+x^{40}+x^{39}+x^{37}+x^{36}+x^{35}+x^{32}+x^{26}+x^{25}+x^{24}+x^{23}+x^{21}+x^{20}+x^{17}+x^{16}+x^{15}+x^{11}+x^{9}+x^{7}+x^{1} \quad (6)$$

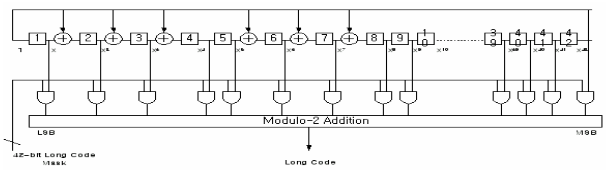

Figure 3. Long Code Sequence

3.2.1 Security Mechanism for Long Code Mask in the Paging Channel

The Long Code Mask in the paging channel is Figure 4. The PCN(Paging Channel Number) is the channel number which has a seven paging channels. Therefore, The '000' through '110' were used. The paging channel number are decrypted easily, because the hash function uses the channel number as known value. The PILOT_PN is given 0 to 512 as a random combination.

We can get easily the PILOT_PN when we are monitoring the pilot channel.

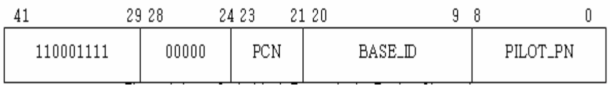

Figure 4. Long Code Mask Format in the Paging Channel

3.2.2 Security Mechanism for Long Code Mask in the Traffic Channel

The long code provides voice privacy in CDMA system. The long code is a PN sequence with $2^{42} - 1$ that is used for scrambling on the forward CDMA channel and spreading the reverse CDMA channel. The long code is characterized by the long code mask that is used to form either the public long code or the private long code.

Figure 5 shows the Long Code Mask in the traffic channel. The Public Long Code Mask and the Private Long Mask were used by managing the Encrypt-Mode in the message field on Forward Traffic Channel. In case of Encrypt-Mode is 00, it is disabled encryption mode and created Long Code using Public Long Code Mask.

The Public Long Code Mask is only composed of the combination ESN. Whenever the Encrypt-Mode is set as 01, the encryption mode is used. In this case, the forty bits of the Private Long Code Mask was used. The Private Long Code Mask is created with 34 bits MIN and SSD_B field. The same phone number is always created as the same Long Code Mask. The Private Long Code Mask is simple structure that uses linear recursive register. For the viewpoint of cryptography theory, it has almost unsecured feature.

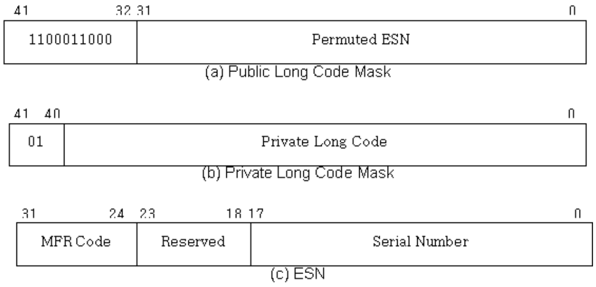

Figure 5. Long Code Mask Format in the Traffic Channel
(MFR : ManuFactuRe)

3.3 Authentication

The authentication mechanism is the procedure that identifies an user of the *MS*. Whenever both the *BS* and the *MS* are the same secret key, the authentication procedure will be done. A-key, COUNT, and SSD parameters are stored into the nonvolatile memory.

4. The *FCM* Protocol and Experiments

It is easy to monitor the forward channel of *CDMA*. We propose the *FCM* protocol to monitor the forward channel. The monitoring equipment that includes the *FCM* protocol is developed by modifying the terminal S/W partially and the *CDMA* terminal. The monitor equipment that is a hardware part of the *FCM* protocol is divided into two parts that are logic circuit part and RF circuit part. The logic circuits are MSM(Mobile Station Modem), Audio PCM Codec, speaker, memory, PC(Personal Computer), and UART. RF circuit, which transforms *CDMA* signal into BASE BAND signal, has BBA(Base Band Analog Processor), PLL(Phase Locked Loop), AMP, and filter. Figure 6 shows the block diagram of the logic circuit for the *FCM* protocol.

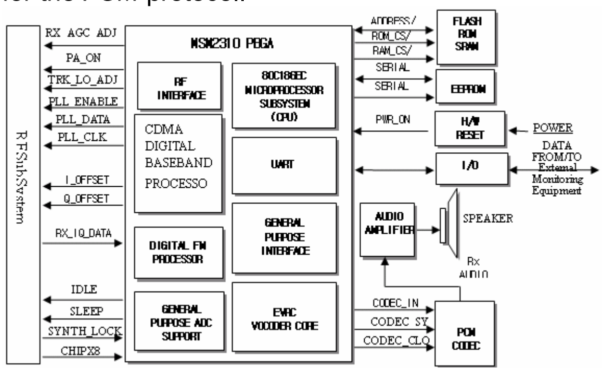

Figure 6. The Block Diagram of the Logic Circuit for the *FCM* protocol

The monitoring software architecture for forward traffic channel is shown in Figure 8. The system software architecture is composed of the REX(Real Time Executable) Operating System which includes multitasking structure. The REX Operating System is developed by Qualcom. Corp., which is executed on the Intel processor 80x86. REX O.S is based on priority preemption scheduling that provides task change. Also it provides system call interface that is task creation, timing related service, suspense and resume of task. REX O.S uses the data structure of TCB(Task Control Block) to manage the task efficiently. When we power on the device, the real time Operating System is running with Main Control(MC) task. The Main Control task initializes the hardware of DECODER, ENCODER, and VOCODER and creates the whole tasks.

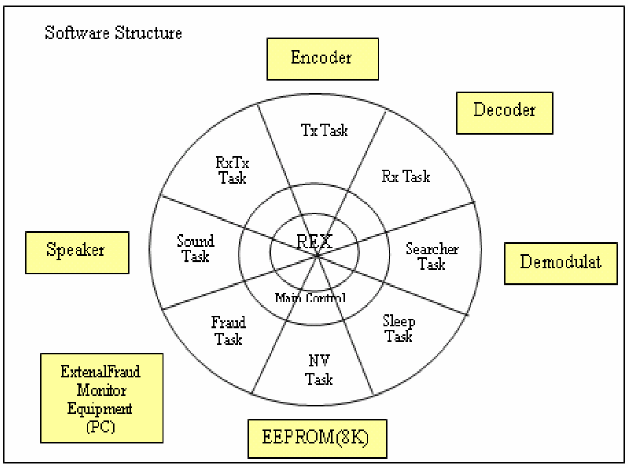

Figure 7. Software Structure for the Monitoring System

Someone can monitor the communication channel in IS95-A protocol in case of not using authentication algorithm or encryptor. We can easily know the ESN and MIN value by using HP8924C instrument. Moreover, The CSM(Cell Site Modem) is available to monitor the ESN and MIN value.

This paper suggests monitoring methodology of call processing procedure for forward channel in IS95-A protocol. There are two kinds of monitors in forward channel: Mobile origination call and mobile terminated call. There are six kinds of cases in service options that are provided by the *BS*, and the *MS*.

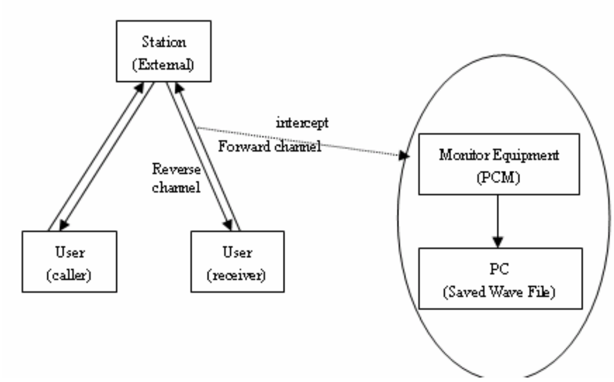

Figure 8. Experiment System Environment

4.1 Call Processing to Monitor the Mobile Origination Call

consider three types(below case A, B, and C) of call origination processing procedure for the sake of service options, which are provided by the *BS* and the *MS*.

The test instrument cannot know the fact that the *MS* sends call by the service option 1 or service option 3. However, the test instrument can use the same option as the *MS* option by monitoring the forward messages, which are negotiated the *MS* with the *BS*.

A. The *MS* : Service Option 1, The BS : Service Option 1

[Algorithm 1] is an algorithm at *MS* for receiving message from *BS*. The *MS* receives Channel Assignment Message(MSG_{cam}) from *BS*((3) statement in [Algorithm 1]). The *BS* sends Base Station Acknowledgement Order(MSG_{bsao}) to the *MS*((4) statement in [Algorithm 1]). Next, The *MS* receives Alert with Information Message(MSG_{aim}) ((5) statement in [Algorithm 1]). After establishing the status of communication between *BS* and *MS*, data is communicated with each station.

```
Input : Receive Page Message from BS
Output : Conversion between MS and BS
Algorithm
begin
(1) Rcv(MSG_page, BS, MIN);
(2) Send(MSG_page, BS, MIN, ESN);
(3) Rcv(MSG_cam, BS, ESN, CDMA_CH,
      CODE_CH);
(4) Rcv(MSG_bsao, BS);
(5) Rcv(MSG_alm, BS);
(6) Send(MSG_ack, BS);
(7) Ans(MS);
(8) Send(MSG_co, BS);
(9) Rcv(MSG_ack, BS);
(10 WHILE(!DISCON) begin
(11)      Comm(MS, BS);
(12) end
end.
```

[Algorithm 1] Algorithm for Receiving Message from *BS* at *MS*

```
Input : Receive Message from MS
Output : Grabbing Pa's Data
Algorithm
begin
(1) Initialize HP89294C;
(2) GET(ESN, MIN, P_a, HP89294C);
(3) S_o = {S_1,S_2,S_3,S_4,S_5,S_6}
(4) St(MS) = (S_1 || S_3) | S_o;
(5) St(BS) = {S_1 | S_o}
(6) St(ME) = St(MS)
(7) SEND(MSG_org, MS, BS, S_1);
(8) MSG_ack = ASSIGN(MSG_ch, MS);
(9) if(MSG_ack != NULL) begin
(10)        WAIT(Srv, MS);
(11)        SEND(MSG_soro, BS, MS, S_1);
(12)        WAIT(Srv, BS);
(13)        DISCON(Srv, MS);
(14)        WHILE (Channel is connected)
(15)        begin
(16)              SEND(MSG_data, BS, MS, S_1);
(17)              WRITE(MSG_data, PC);
(18)              SEND(MSG_data, MS, BS, S_1);
(19)              WRITE(MSG_data, PC);
(20)        end
(21) end
end.
```

[Algorithm 2] Algorithm for *FCM* Protocol

We can easily know the ESN and MIN value by using HP8924C instrument. Moreover, The CSM(Cell Site Modem) is available to monitor the ESN and MIN value. This paper suggests *FCM* protocol for call processing procedure in IS95-A protocol. There are two kinds of monitoring methods in forward channel: Mobile origination call and mobile terminated call. There are six kinds((3) statements in [Algorithm 2]) of cases in service options that are provided by the *BS* and the *MS*

We should consider three types of call origination processing procedure for the sake of service options, which are provided by the *BS* and the *MS*. The service options that are used currently are service option 1 and service option 3 for voice communication. The service option 1 is the voice communication based on 8Kbyte Q-CELP codec. The service option 3 is the voice communication based on 8K-EVRC codec. We just show the *FCM* protocol in the service option 1((4) statement in [Algorithm 2]) (8-K EVRC), because other cases are similar to service option 1.

Figure 9 and [Algorithm 2] show the monitoring procedure of call processing that the *MS* supports the service option 1 and the *BS* supports service option 1, respectively. When the *MS* sends the origination message to the *BS* by service option 1, the *BS* assigns the communication channel to the *MS* whether it is enrolled or not ((7) statement in [Algorithm 2]). When the *MS* gets the assigned message of channel ((8) statement in [Algorithm 1]), it waits for the service negotiation ((10) statement in [Algorithm 1]) through the forward communication channel and backward communication channel. Also the test instrument acknowledges the fact that the *MS* sends the call. And then the test instrument starts monitoring data from the assigned communication channel ((14) to (21) statement in [Algorithm 2]). The *BS* serves the service option 1 from the call of the *MS* and sends the assigned message for channel through call channel. After this, the *BS* sends the Service Option Response Order message to forward communication channel and waits for the service negotiation. The *MS* disconnects the service negotiation and communicates with the *BS* when it receives Service Option Response Order message ((13) statement in [Algorithm 2]). The test instrument detects the service option, stores the whole voice packets from forward channel, and sends the monitored voice packets to the PC((14) to (21) statements in [Algorithm 2]). When finishing the call, the *BS* sends release order to the forward channel. The *MS* and the test instrument end the call, when it receives the Release Order message. The theorem for the *FCM* protocol shows that the *BS* and the *MS* are equal to the same data in communicating each other.

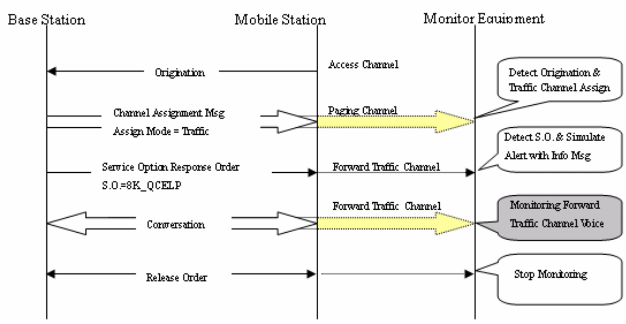

Figure 9. Data Flow of Call Processing to Monitor the Mobile Origination Call
(In Case of the Mobile Station Sends Service Option1)

B. The *MS* : Service Option 3, The *BS* : Service Option 1

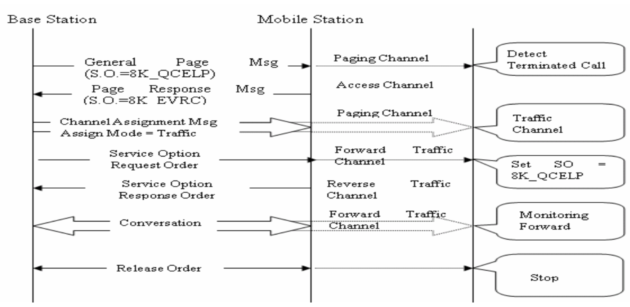

Figure 10. In Case of The Mobile Station Sends Service Option 3 and The Base Station Supports Service Option 1

Figure 10 shows the monitoring procedure of call processing that the *MS* supports the service option 3 and the *BS* supports service option 1, respectively. When the *MS* sends the origination message to the *BS* by service option 3, the *BS* assigns the communication channel to the *MS* whether it is decided to enroll or not. When the *MS* gets the assigned message of channel, it is waiting for the service negotiation through the forward communication channel and backward communication channel. Also the test instrument acknowledges the fact that the *MS* sends the call and start monitor from the assigned communication channel. The dotted arrow line is monitoring a data from the *MS* using the *FCM* protocol.

C. The *MS* and the *BS* : the Service Option 3

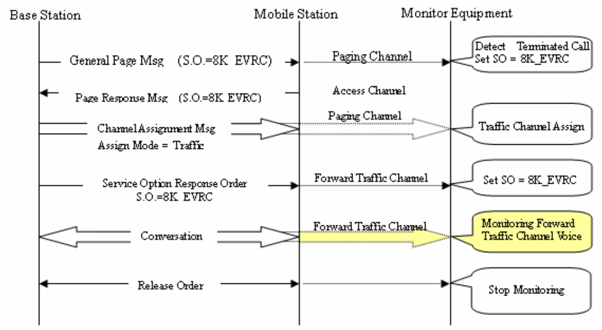

Figure 11. In Case of The Mobile Station Sends Service Option 3 and The Base Station Also Supports Service Option 3

Figure 11 shows the monitoring procedure of call processing that both the *MS* and the *BS* support call service option 3, respectively. When the *MS* sends the origination message to the *BS* by service option 3, the *BS* assigns the communication channel to the *MS* whether it is decided to enroll or not. When the *MS* gets the assigned message of channel, it is waiting for the service negotiation through the forward communication channel and backward communication channel. Also the test instrument acknowledges the fact that the *MS* sends the call and start monitor from the assigned communication channel. The dotted arrow line is monitoring a data from the *MS* using the *FCM* protocol.

6. Conclusions

The *CDMA* technology is generally known as powerful security during communication. However, the communication data might be eavesdropped and forged, because the mobile communication sends data through wireless communication channel. So it is essentially necessary to setup the entire system securely. This paper analyzes the security hole and proves a weak point of *CDMA* system. Based on the results, we emphasize the necessity of security in *CDMA* system. For the sake of this, we analyze the IS-95 protocol and propose the monitor mechanism of forward channel in call processing procedure. The IS-95 and GSM only define the security features between the mobile station and the base station.

The monitor equipment is divided into two parts that are a logic circuit part and RF circuit part. The logic circuits are MSM(Mobile Station Modem), Audio PCM Codec, speaker, memory, PC(Personal Computer), and UART. RF circuit, which transforms *CDMA* signal into BASE BAND signal, are BBA, PLL, AMP, and filter. We propose only the methodology of the forward channel monitoring by modifying the terminal S/W partially in *CDMA* terminal. We propose S/W and H/W architecture for the call process of the forward channel monitor and analyze the call process procedure. The REX Operating System in equipment terminal was used to monitor the *CDMA* system. If we know the ESN and the MIN, we can eavesdrop the *CDMA* data. We can easily know the ESN and MIN value by HP8924C instrument.

We suggest the *FCM* protocol to monitor *CDMA* system. This paper proves a weakness of *CDMA* system using the *FCM* protocol. We also prove that the BS and the MS are the same data in communicating each other. We implement the test instruments including the *FCM* protocol. In the experiment of monitoring system based on the *FCM* protocol, we can monitor an user communication message by the monitoring environments. In the future, based on the result, we will suggest a new system architecture for the secure *CDMA* system

References

[1] N. Asokan. "Anonymity in a Mobile Computing Environment". *Proceedings of Workshop in Mobile Computing Systems and Applications*, December 1994.

[2] M. Bellare, S. Goldwasser. "New Paradigms for digital Signatures and Message Authentication

Based on Non-Interactive Zero Knowledge Proofs". *Proceedings of Crypto 89*. 1989.

[3] D. Chaum. "Security Without Identification: Security Systems to Make Big Brother Obsolete". *Comm. of the ACM*. October 1985.

[4] D. Chaum. "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability". *Journal of Cryptology* (1988) 1.

[5] J. Dunlop, D. G. Smith. "Telecommunications Engineering, 3rd Ed". Chapman & Hall, 1994.

[6] A.K. Elhakeem, Haiying Zhu, Saud A. Al-Semari, "Virtual Matched Filtering: A new Hybrid CDMA code acqusition Technique under Doppler and higher CDMA loads, IEEE, 2000.

[7] J. Elliott. "Hide yourself in Cyberspace". *Internet*. May 1995.

[8] T. A. Freeburg. "Enabling Technologies for Wireless In-Building Network Communications - Four Technical Challenges, Four Solutions". *IEEE Communications Magazine*. April 1991.

[9] G. H. Forman, J. Zahorjan. "The Challenges of Mobile Computing". *IEEE Computer*. April 1994.

[10] C. Harrison, D. M. Chess, A. Kershenbaum. "Mobile Agents: Are they a good idea?" *IBM Research Report*. March 28, 1995.

[11] A. Herzberg, H. Krawczyk, G. Tsudik. "On Travelling *Incognito*". *Proceedings of the 1994 Workshop on Mobile Computing*, 1994.

[12] J. Ioannidis. "Protocols for Mobile Internetworking". *PhD Thesis, University of Columbia*. ftp://ftp.cs.columbia.edu/pub/ji/thesis.ps.gz

[13] D. B. Johnson. "Routing in Ad-Hoc Networks of Mobile Hosts". *Computer Science Department, Carnegie Mellon University*.

[14] Youngkook Kim, Saewoong Bahk, "Multiaccess scheme to ensure security in CDMA-based wireless LANs", Electronics Letters 27th May 1999, Vol. 35, No. 11.

[15] Byoung-Hoon Kim and Byeong Gi Lee, "PDSA: Parallel Distributed Sample Acquisition for M -ary DS/CDMA Systems", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 49, NO. 4, pp. 589-593, APRIL 2001.

[16] B. Marsh, F. Douglis, R. Cáceres. "Systems Issues in Mobile Computing". *MITL Technical Report MITL-TR-50-93*. February 1993.

[17] A. Mukherjee, D. P. Siewiorek. "Mobility: A Medium for computation, Communication, and Control". *School of Computer Science, Carnegie Mellon University*.

[18] R. Needham. "Denial of Service: An Example". *Communications of the ACM*, November 1994.

[19] Paul Newson, Mark R. Heath, "The Capacity of a Spread Spectrum CDMA System for Cellular Mobile Radio with Consideration of System Imperfections', IEEE journal of selected areas in communications, vol. 12, No. 4, May, 1994.

[20] C. Park, K. Kurosawa, T. Okamoto, S. Tsujii. "On Key Distribution and Authentication in Mobile Radio Networks". *Proceedings of EUROCRYPT'93,*Springer-Verlag.

[21] D. Samfat, R. Molva. "A Method Providing Identity Privacy to Mobile Users during Authentication".

[22] F. Stoll. "The Need for Decentralization and Privacy in Mobile Communications Networks". In *Network Security Observations*, January 1995.

[23] J. Scourias. "Overview of the Global System for Mobile Communications". *University of Waterloo*.

[24] M. Spreitzer, M. Theimer. "Scalable, Secure, Mobile Computing with Location Information". *Communications of the ACM*, July 1993.

[25] L. Tancevski, I. Andonovic, M. Tur, J. Budin, "Massive Optical Lan's Using Wavelength Hopping/Time Spreading with Increased Security", IEEE Photonics Technology Letters, Vol. 8, No. 7, July 1996.

[26] M. Tatebayashi, N. Matsuzaki. "Key Distribution Protocol for Digital mobile Communication Systems". *Proceedings of CRYPTO'89*, Springer-Verlag.

[27] Francisco Javier González-Serrano, Juan José Murillo-Fuentes, "Adaptive Nonlinear Compensation for CDMA Communication Systems", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 50, NO. 1, pp. 34 – 42, JANUARY 2001

[28] J. E. White. "Telescript Technology: The Foundation for the Electronic Marketplace". *General Magic, Inc.*, Mountain View, CA. 1994.

[29] Sung-Shik Woo, Heung-Ryeol You, Tae-Gun Kim, "The Position Location System Using IS-95 CDMA Networks", IEEE, 2000.

[30] M. Wooldridge, R. Jennings. "Intelligent Agents: Theory and Practice". *Knowledge Engineering Review*. October 1994.

[31] Weiping Xu, Laurence B. Milstein, "On the Use of Interference Suppression to Reduce Intermodulation Distortion in Multicarrier CDMA Systems", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 49, NO. 1, JANUARY 2001.

Dae-Hyun Ryu (dhryu@hansei.ac.kr)
Prof. Dae-Hyun Ryu received his B.S. degree, M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Busan National University in 1983, 1985 and 1997, respectively. From 1987 to 1998, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 1998, he joined the department of IT, Hansei University, Korea. His research interest is in the area of Digital image processing, Digital watermark and Information security system design.

Seung-Ju, Jang received a B.Sc. degree in Computer Science and Statistics, and M.Sc. degree, and his Ph.D. in Computer Engineering, all from Busan National University, in 1985, 1991, and 1996, respectively. He is a member of IEEE and ACM. He has been an associate Professor in the Department of Computer Engineering at Dongeui University since 1996. He was a member of ETRI(Electronic and Telecommunication Research Institute) in Daejon, Korea, from 1987 to 1996, and developed the National Administration Multiprocessor Minicomputer during those years. His current research interests include fault-tolerant computing systems, distributed systems in the UNIX Operating Systems, multimedia operating systems, security system, and parallel algorithms.