Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2007, Article ID 83589, 7 pages
doi:10.1155/2007/83589

Research Article

Physical Layer Built-In Security Analysis and Enhancement Algorithms for CDMA Systems

Tongtong Li, Qi Ling, and Jian Ren

Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824, USA

Received 18 July 2006; Revised 23 December 2006; Accepted 20 January 2007

Recommended by Wei Li

Historically developed for secure communication and military use, CDMA has been identified as a major modulation and multiple-access technique for 3G systems and beyond. In addition to the wide bandwidth and low power-spectrum density which make CDMA signals robust to narrowband jamming and easy to be concealed within the noise floor, the physical layer built-in information privacy of CDMA system is provided by pseudorandom scrambling. In this paper, first, security weakness of the operational and proposed CDMA airlink interfaces is analyzed. Second, based on the advanced encryption standard (AES), we propose to enhance the physical layer built-in security of CDMA systems through secure scrambling. Performance analysis demonstrates that while providing significantly improved information privacy, CDMA systems with secure scrambling have comparable computational complexity and overall system performance with that of conventionally scrambled systems. Moreover, it is shown that by scrambling the training sequence and the message sequence separately with two independent scrambling sequences, both information privacy and system performance can be further improved. The proposed scheme can readily be applied to 3G systems and beyond.

1. INTRODUCTION

As people are relying more and more on wireless communication networks for critical information transmission, security has become an urgent issue and a bottleneck for new wireless communication services such as wireless mobile Internet and e-commerce [1]. Due to user mobility and the fact that there is no physical boundary in wireless environment, wireless communication networks are facing much more significant challenges compared to their data network counterparts.

Direct sequence spread-spectrum system, also known as code-division multiple access (CDMA), was historically developed for secure communication and military use. In CDMA systems, each user is assigned a specific spreading sequence to modulate its message signal. The spreading process increases the bandwidth of the message signal by a factor N, known as spreading factor or the processing gain, and meanwhile reduces the power-spectrum density of the signal also by a factor N. With large bandwidth and low power spectrum density, CDMA signals are resistant to malicious narrowband jamming and can easily be concealed within the noise floor, preventing from being detected by an unauthorized person. Moreover, the message signal cannot be recovered unless the spreading sequence is known, this makes it difficult for unauthorized person to intercept the signal.

Due to high spectrum efficiency and simplicity in system planning, CDMA is now finding widespread civilian and commercial applications such as cellular phones, personal communications, and position location. As it is well known, CDMA is used in the US digital cellular standard IS-95 and has been identified as the major modulation technique for third generation (3G) wireless communications and beyond.

Relying on the long pseudorandom spreading sequence generator, the operational CDMA system (IS-95) and the proposed 3G UMTS system can provide a near-satisfactory physical layer built-in security solution to voice centric wireless communications, which generally last only a very short period of time. However, the security features provided by these systems are far from being adequate and being acceptable when used for data communications. In literature, wireless security is generally considered from MAC layer and network layer, see [2], for example, and few thoughts have been given to the physical layer security enhancement. In this paper, we show that by combining cryptographic techniques and modulation techniques in the transmitter and receiver design, physical layer built-in security of wireless systems can be exploited to ensure wireless network security from both the physical layer and upper layers. In the following sections, first, security weakness of the existing CDMA airlink interfaces is analyzed. Second, instead of using the conventional scrambling method as in IS-95 or 3GPP UMTS, encrypted long code based on advanced encryption standard (AES) is proposed to be used in the scrambling process. It will be seen that ensured by AES, the proposed scheme can improve the physical layer built-in security of CDMA systems significantly. Moreover, it is shown that by scrambling the training sequence and the message sequence separately with two independent scrambling sequences, both information privacy and system performance can be further improved. The proposed scheme is easy to implement and can readily be applied to 3G systems and beyond.

2. PHYSICAL LAYER SECURITY EVALUATION OF IS-95 AND 3GPP UMTS CDMA SYSTEMS

In the operational and proposed direct-sequence CDMA (DS-CDMA) systems, as shown in Figure 1, each user's signal is first spread using a code sequence (known as *channelization code*) spanning over just one symbol or multiple symbols. The spread signal is then further scrambled using a pseudorandom sequence, to randomize the interference and meanwhile makes it difficult to intercept and detect the transmitted signal.

Consider a DS-CDMA system with M users and K receive antennas. Assuming the processing gain is N, that is, there are N chips per symbol. Let $u_j(k)$ $(j = 1, \dots, M)$ denote user j's kth symbol. Without loss of generality, let

$$\mathbf{c}_j = [c_j(0), c_j(1), \dots, c_j(N-1)] \tag{1}$$

denote user j's channelization code or spreading code. The spread chip-rate signal can be expressed as

$$r_j(n) = \sum_{k=-\infty}^{\infty} u_j(k) c_j(n - kN). \tag{2}$$

The successive scrambling process is achieved by

$$s(n) = r_j(n) d_j(n), \tag{3}$$

where $d_j(n)$ is the chip-rate scrambling sequence of user j.

Let $\{g_j^{(i)}(l)\}_{l=0}^{L-1}$ denote the (chip-rate) channel impulse response from jth user to ith antenna, the received chip-rate signal at the ith antenna $(i = 1, 2, \dots, K)$ can be expressed as

$$y_i(n) = \sum_{j=1}^{M} \sum_{l=0}^{L-1} g_j^{(i)}(l) s_j(n-l) + w_i(n), \tag{4}$$

where $w_i(n)$ is the additive noise.

From (4), we can see that it is impossible to recover the desired user's signal without knowing both the user's channelization code and scrambling code. This is known as the *built-in security* feature of the CDMA systems.

Since the channelization codes are chosen to be Walsh codes, which are easy to generate, the physical layer built-in security of CDMA systems mainly relies on the long pseudorandom scrambling sequence, also known as long code. In the following, we will analyze the maximum complexity to recover the long code of the IS-95 system and the 3GPP UMTS system.

2.1. Scrambling code recovery of the IS-95 system

In IS-95, the long-code generator consists of a 42-bit number called *long-code mask* and a 42-bit linear feedback shift register (LFSR) specified by the following characteristic polynomial:

$$\begin{aligned} x^{42} &+ x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} \\ &+ x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} \\ &+ x^{10} + x^{7} + x^{6} + x^{5} + x^{3} + x^{2} + x + 1, \end{aligned} \tag{5}$$

where the 42-bit long code mask is shared between the mobile and let the base station.

As shown in Figure 2, each chip of the long code is generated by the modulo-2 inner product of a 42-bit mask and the 42-bit state vector of the LFSR.

Let $M = [m_1, m_2, \dots, m_{42}]$ denote the 42-bit mask and $S(t) = [s_1(t), s_2(t), \dots, s_{42}(t)]$ denote the state of the LFSR at time instance t. The long-code sequence $c(t)$ at time t can thus be represented as

$$c(t) = m_1 s_1(t) + m_2 s_2(t) + \cdots + m_{42} s_{42}(t), \tag{6}$$

where the additions are modulo-2 additions.

As it is well known, for a sequence generated from an n-stage linear feedback shift register, if an eavesdropper can intercept a $2n$-bit sequence segment, then the characteristic polynomial and the entire sequence can be reconstructed according to the Berlekamp-Massey algorithm [3]. This leaves an impression that the maximum complexity to recover the long-code sequence $c(t)$ is $O(2^{84})$. However, for IS-95, since the characteristic polynomial is known to the public, an eavesdropper only needs to obtain 42 bits of the long-code sequence to determine the entire sequence. That is, the maximum complexity to recover the long-code sequence $c(t)$ is only $O(2^{42})$.

In fact, since $s_1(t), s_2(t), \dots, s_{42}(t)$ are the outputs of the same LFSR, they should all be the same except for a phase difference, that is,

$$s_{42}(t) = s_{41}(t-1) = \cdots = s_1(t-41). \tag{7}$$

Let $a = [a_1, a_2, \dots, a_{42}]$ denote of the coefficient vector of the characteristic polynomial in (5), then it follows from (7) that

$$\begin{aligned} s_i(t) &= a_1 s_{i-1}(t) + a_2 s_{i-2}(t) + \cdots + a_{42} s_{i-42}(t) \\ &= a_1 s_i(t-1) + a_2 s_i(t-2) + \cdots + a_{42} s_i(t-42). \end{aligned} \tag{8}$$

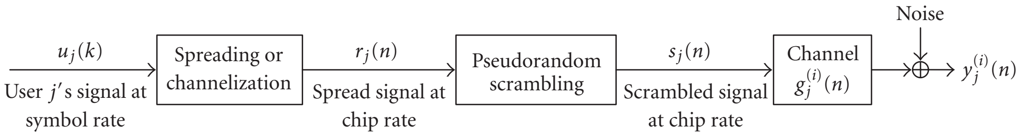
$u_j(k)$
User j's signal at symbol rate
Spreading or channelization
$r_j(n)$
Spread signal at chip rate
Pseudorandom scrambling
$s_j(n)$
Scrambled signal at chip rate
Channel $g_j^{(i)}(n)$
Noise
$y_j^{(i)}(n)$

Figure 1: Block diagram of a long-code DS-CDMA system.

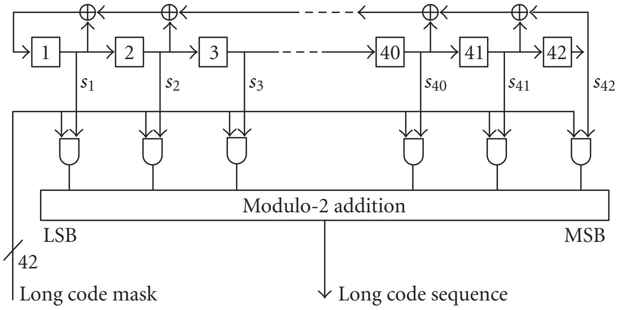

Figure 2: IS-95 long-code generator.

Substituting (8) into (6), we have

$$\begin{aligned} c(t) &= \sum_{i=1}^{42} m_i s_i(t) = \sum_{i=1}^{42} m_i \left(\sum_{j=1}^{42} a_j s_i(t-j) \right) \\ &= \sum_{j=1}^{42} a_j \left(\sum_{i=1}^{42} m_i s_i(t-j) \right) = \sum_{j=1}^{42} a_j c(t-j). \end{aligned} \tag{9}$$

Define

$$A = \begin{bmatrix} a_1 & 1 & 0 & \cdots & 0 \\ a_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{41} & 0 & 0 & \cdots & 1 \\ a_{42} & 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{10}$$

then it follows that

$$\begin{aligned} &[c(t), c(t-1), \dots, c(t-41)] \\ &\quad = [c(t-1), c(t-2), \dots, c(t-42)] * A. \end{aligned} \tag{11}$$

Let $C(t) = [c(t), c(t-1), \dots, c(t-41)]$, then for any $n \geq t$, from (11) we have

$$C(n) = C(t) * A^{n-t}. \tag{12}$$

Therefore, as long as $C(t)$ for a time instance t is known, then the entire sequence can be recovered. In other words, as long as an eavesdropper can intercept/recover up to 42 continuous long-code sequence bits, then the whole long-code sequence can be regenerated. Therefore, the long code sequence of IS-95 is vulnerable under ciphertext-only attacks as the maximum complexity to recover it is only $O(2^{42})$.

2.2. Scrambling code recovery of the 3GPP UMTS system

In the 3GPP UMTS standard, Gold codes generated from two generator polynomials of degree 18 are used as scrambling code, as shown in Figure 3.

Denote the states for the two LFSRs at time instance t as $r(t) = [r_{17}(t), r_{16}(t), \dots, r_1(t), r_0(t)]$ and $s(t) = [s_{17}(t), s_{16}(t), \dots, s_1(t), s_0(t)]$, where

$$\begin{aligned} r_{17}(t) &= r_7(t-1) + r_0(t-1), \\ s_{17}(t) &= s_{10}(t-1) + s_7(t-1) + s_5(t-1) + s_0(t-1). \end{aligned} \tag{13}$$

Then at time instance t, sequence I can be written as

$$I(t) = r_0(t-1) + s_0(t-1), \tag{14}$$

while sequence Q can be expressed as

$$Q(t) = \sum_{i=0}^{17} a_i r_i(t-1) + \sum_{i=0}^{17} b_i s_i(t-1), \tag{15}$$

where a_i and b_i are either 0 or 1 as shown in Figure 3.

Note that $r_0(t) = r_1(t-1) = \cdots = r_{17}(t-17)$ and $s_0(t) = s_1(t-1) = \cdots = s_{17}(t-17)$, we have

$$Q(t) = \sum_{i=0}^{17} a_i r_0(t+i-1) + \sum_{i=0}^{17} b_i s_0(t+i-1). \tag{16}$$

From (14) and (16), it follows that the maximum complexity to recover the scrambling code of the 3GPP UMTS system based on ciphertext-only attack is $O(2^{36})$.

This implies that the physical layer built-in security of the 3GPP UMTS is actually weaker than that of the IS-95 system, therefore, in the subsequent sections, we will focus on the IS-95 system and the results can be directly applied to 3GPP systems.

Once the long-code sequence is recovered, the desired user's signal can be recovered through signal separation and extraction techniques. If the training sequence is known, simple receivers, for example, the Rake receiver, can be used to extract the desired user's signal. Even if the training sequence is unknown, the desired user's signal can still be recovered through blind multiuser detection and signal separation algorithms, see [4–6], for example.

3. AES-BASED SECURITY ENHANCEMENT OF THE SCRAMBLING PROCESS

As can be seen from the previous sections, the physical layer security of CDMA systems relies on the scrambling process,

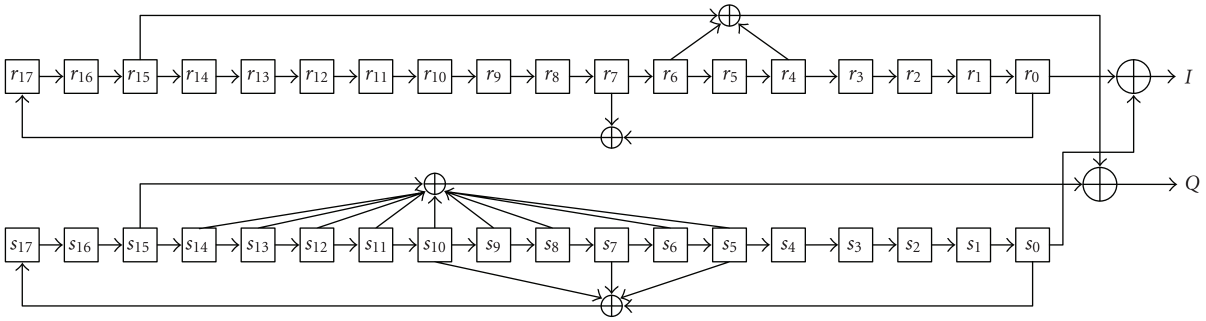

Figure 3: Scrambling sequence for 3GPP.

and the built-in information privacy provided by the operational and proposed CDMA systems is far from being adequate. In this paper, to enhance the physical layer built-in security of CDMA systems, we propose to generate the scrambling sequence using the advanced encryption standard (AES), also known as Rijndael.

Rijndael was identified as the new AES in October 2, 2000. Rijndael's combination of security, performance, efficiency, ease of implementation, and flexibility makes it an appropriate selection for the AES. Rijndael is a good performer in both hardware and software across a wide range of computing environments. Its low memory requirements make it very well suited for restricted-space environments such as mobile handset to achieve excellent performance. More details on AES can be found in [7].

As mentioned before, we will focus our discussion on IS-95 system as it has a stronger physical layer security and the results can be directly applied to 3GPP systems. The proposed secure scrambling scheme aims to increase the physical layer built-in security of CDMA systems, to prevent exhaustive key search attack, while minimizing the changes required to the existing standards. As shown in Figure 4, the proposed secure scrambling is essentially a counter-mode AES. In Figure 4, $s_0s_1s_2\ldots$ represents the output of the LFSR characterized by (5) as in the IS-95 system, K is the 128-bit common secret encryption key shared between the base station and the mobile station (K can also be 192 bits or 256 bits, as specified in the AES algorithm), and $M_0, M_1, \ldots, M_i$ denote successive message blocks with the same size as K, d is the shift between the successive inputs to the AES engine. If the input to the ith encryption block is $s_{t+id}, s_{t+1+id}, \ldots, s_{t+127+id}$ with initial delay t, then the input to the $(i+1)$th block is $s_{t+(i+1)d}, s_{t+1+(i+1)d}, \ldots, s_{t+127+(i+1)d}$. The selection of d should maximize the diversity between different inputs to the AES engine, which can be achieved by requiring d and $2^{42}-1$ to be relatively prime. In other words, d should not be divided by 3, 7, 43, and 127.

The secure scrambling process can be summarized as follows.

(1) The base station and the mobile station share a common initial state for the LFSR and an L-bit ($L = 128, 192$ or 256) common secret encryption key K.

(2) The long scrambling sequence is generated through encryption of a particular segment of the sequence generated from the LFSR using the shared secret key K.

(3) the scrambling process is realized by adding the scrambling sequence to the chip-rate spread signal.

For the 3GPP system, secure scrambling can be performed in the same manner by applying AES to the I, Q scrambling sequences separately. As described in [8, 9], the shared secret data between the mobile station and base station can be updated from time to time. To prevent malicious key reload, the key update request can only be initiated from the base station.

4. SECURITY OF THE PROPOSED SCRAMBLING PROCESS

In this section, we use data encryption standard (DES) [10] as a benchmark to evaluate the security of the proposed secure scrambling, which is essentially ensured by AES. We compare the number of possible keys of AES and that of IS-95 scrambling sequence. The number of keys determine the effort required to crack the cryptosystem by trying all possible keys.

The most important reason for DES to be replaced by AES is that it is becoming possible to crack DES by exhaustive key search. Single DES uses 56-bit encryption key, which means that there are approximately 7.2×10^{16} possible DES keys. In the late 1990s, specialized "DES cracker" machines were built and they could recover a DES key after a few hours. In other words, by trying all possible key values, the hardware could determine which key was used to encrypt a message [11]. Compared with DES, IS-95 has only 42-bit shared secret. The approximate number of keys is about 4.40×10^{12}, which is less than 10^4 of the number of DES 56-bit keys. This makes it possible to break the IS-95 long-code mask almost in real time through exhaustive key search.

On the other hand, AES specifies three key sizes: 128, 192, and 256 bits. In decimal terms, this means that approximately there are

(i) 3.4×10^{38} possible 128-bit keys;
(ii) 6.2×10^{57} possible 192-bit keys;
(iii) 1.1×10^{77} possible 256-bit keys.

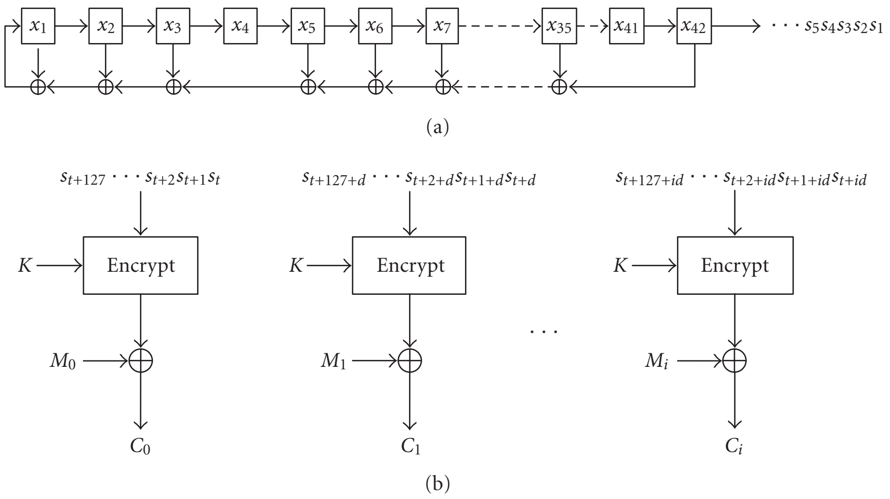
x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_{35}
x_{41}
x_{42}
$\cdots s_5 s_4 s_3 s_2 s_1$
(a)
$s_{t+127} \cdots s_{t+2} s_{t+1} s_t$
$s_{t+127+d} \cdots s_{t+2+d} s_{t+1+d} s_{t+d}$
$s_{t+127+id} \cdots s_{t+2+id} s_{t+1+id} s_{t+id}$
K
Encrypt
M_0
M_1
M_i
C_0
C_1
C_i
(b)

FIGURE 4: Proposed CDMA physical layer secure scrambling.

Thus, if we choose $L = 128$, then there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), as we can see, this is a very ambitious assumption and far from what we can do today, then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20-billion-year old.

Security measurement through the number of all possible keys is based on the assumption that the attacker has no easy access to the secret encryption key, therefore, the attacker has to perform an exhaustive key search in order to break the system. As it is well known, the security of AES is based on the infeasible complexity in recovering the encryption key. Currently, no weakness has been detected for AES, thus, exhaustive key search is still being recognized as the most effective method in recovering the encryption key and breaking the cryptosystem. In our case, in order for the attacker to obtain the scrambling sequence, the attacker needs to know the input sequence and encryption key. It is reasonable to require that the 42-bit initial secret of the LFSR in Figure 4 to be kept a secret together with the 128 bit encryption key. And the attacker will only have access to the scrambled message sequence, for which the secure scrambling sequence is generated from encryption of a 128-bit segment of the LFSR sequence using 128-bit shared secret key between the mobile station and the base station.

As pointed out in Section 2, for the IS-95 system, the entire scrambling sequence can be regenerated as long as 42 successive bits of the scrambling sequence are recovered. In the proposed procedure, even if one block of the scrambling sequence is intercepted, the attacker still needs to recover the secret key K and the input segments $[s_{t+id} \cdots s_{t+127+id}]$ in order to regenerate the entire scrambling sequence, that is, the attacker still needs to break AES.

The key update technique currently used can reduce the risk for the opponent to maliciously reload a new key since the process is controlled by the base station. However, it is still essential to protect the encryption key and to protect the mobile station from being hacked by the malicious attackers.

5. PERFORMANCE ANALYSIS OF CDMA SYSTEMS WITH SECURE SCRAMBLING

Pseudorandom scrambling in CDMA systems provides physical layer built-in user privacy for information transmission. However, from communication point of view, scrambling was originally designed to reduce interference of mobiles that use the same channelization code in different cells, and to ensure performance stability among user population by providing the desired wideband spectral characteristics, since the Walsh functions may not spread each symbol's power spectrum uniformly in the available frequency band [12, 13]. When applying secure scrambling, two natural questions arethe following.

(1) What effect does it have on system performance?
(2) Will it introduce significant computational complexity?

In this section, it will be demonstrated that while providing strong physical layer built-in security, secure scrambling has comparable computational complexity and system performance with that of the conventional scrambling process. It is also shown that by scrambling the training sequence and the message sequence separately with two independent scrambling sequences, both information privacy and system performance can be further improved.

5.1. Computational complexity

In this section, we compare the computational complexity of the proposed secure scrambling and conventional scrambling. For this purpose, we only need to compare the complexity of the two scrambling sequence generation methods. Note that they both use the same 42-bit LFSR as specified in (5). In IS-95, each bit of the long scrambling code is generated through

$$c(t) = m_1s_1(t) + m_2s_2(t) + \cdots + m_{42}s_{42}(t). \tag{17}$$

For the proposed secure scrambling, every 128-bit block of the scrambling sequence is generated through one AES encryption process. Here, we compare the number of instructions required by each method for every 128 bits, and also the time required for every 128 bits using a Dell computer with 1024 M RAM and 2.8 GHz CPU speed. The results are provided in Table 1. As can be seen, the computational complexity of secure scrambling is comparable with that of the scrambling process used in IS-95.

5.2. System performance and further improvement using separately scrambled training

Under the same spectral efficiency, in this section, we compare the input-output BER (bit-error-rate) performance of CDMA systems with conventional scrambling and secure scrambling, respectively. In practical systems, after spreading and scrambling, passband PAM (pulse amplitude modulation) is performed. Mapping information bearing bits to symbols, passband PAM is equivalent to a complex-valued baseband PAM system [14]. When BPSK or QPSK is chosen, the modulo-two addition between the message bits and the spreading sequence or the scrambling sequence is now equivalent to multiplying the message symbols using binary (± 1) sequences. In this paper, our discussion is based on the equivalent discrete-time baseband PAM model of CDMA systems, for which the spreading sequences and scrambling sequences are both binary antipodal sequences.

Based on (4), desired user's signal can be extracted through a two-stage procedure. First, training-based channel estimation is performed through correlation. Second, Rake receiver is applied to combine multipath components. It should be pointed out that currently, it is a common practice in industry to choose the chip rate training sequence be all 1's. The training sequence is put as a prefix to the chip-rate message sequence, and then it is scrambled using the long scrambling sequence. Channel estimation is therefore carried out based on the correlation property of the front part of the scrambling sequence.

This practice has two drawbacks: first, from security point of view, the front part of the scrambling sequence is exposed to attackers, which makes it possible to recover the whole scrambling sequence right away if secure scrambling is not used. This, at the meantime, illustrates the importance of secure scrambling, which can prevent the whole scrambling sequence being recovered based on the knowledge of part of it. Second, from the performance point of view, the correlation property of part of the scrambling sequence may not be ideal, and it can decrease the system performance due to nonaccurate channel estimation.

Separately scrambled training

To overcome these shortcomings, we propose to scramble the training sequence with an independent short scrambling sequence. The training sequence and its scrambling sequence are designed subject to the following constraints.

(1) The short scrambling sequence is independent of the long scrambling sequence.
(2) The short scrambling sequence has the same length as that of the training sequence.
(3) The scrambled training sequence is a Gold sequence.

Or equivalently, we can choose the training sequence be a Gold sequence and then no scrambling is necessary for it. At the meantime, the information sequence is scrambled with the long scrambling sequence. In other words, training sequence is separated from the information sequence in the scrambling procedure. As a result, the long scrambling sequence will not be exposed to malicious attackers and the channel estimation can be performed based on the low cross-correlation of Gold sequences. We term the proposed approach as "*separated training*," and denote the conventional practice by "non-separated training."

In the simulation, we choose the processing gain to be $N = 16$, and consider the single receiver case. It is assumed that QPSK signals are transmitted over four-ray multipath channels for each user, with the first path to be the dominant path. The multipath delays are uniformly distributed over the interval $[0, N - 1]$. That is, the maximum multipath delay L is allowed to be up to one symbol period, a reasonable assumption for wideband CDMA systems. The short scrambling sequence is chosen to be Gold sequences of length 63, and the training sequence is chosen to be a sequence of all 1's of the same length. Without loss of generality, user 1 is chosen to be the desired user. Figure 5 shows the bit error rate (BER) versus different signal-to-noise ratio (SNR) levels, assuming 4 equal power users in the system. SNR is defined as the chip SNR with respect to user 1. Multipath channels and information sequence consist of 1024 QPSK symbols are generated randomly in each Monto Carlo run, and the result is averaged over 100 runs.

As can be seen, system with secure scrambling has comparable performance with that of IS-95, and "*separated training*" delivers much better results compared to that of "non-separated training."

5.3. Discussions and extension to other wireless systems

From the previous two sections, we can see that with a slight increase in complexity, the physical layer built-in security of the CDMA systems can be improved significantly. Moreover, secure scrambling has the error-tolerant feature, that is, an individual error in the received message will have a limited local effect, it will not prevent the decryption of other parts of the message. This feature is very helpful under scenarios where retransmission is difficult or even impossible.

Table 1: Complexity comparison of the two generation methods of long scrambling sequences.

Method	Number of operations required for every 128 bits				Time (in seconds)
	AND	OR	BIT-SHIFT	TOTAL	
IS-95	5376	5248	5376	16000	0.0226
Secure scrambling	7096	6644	8640	22380	0.0536

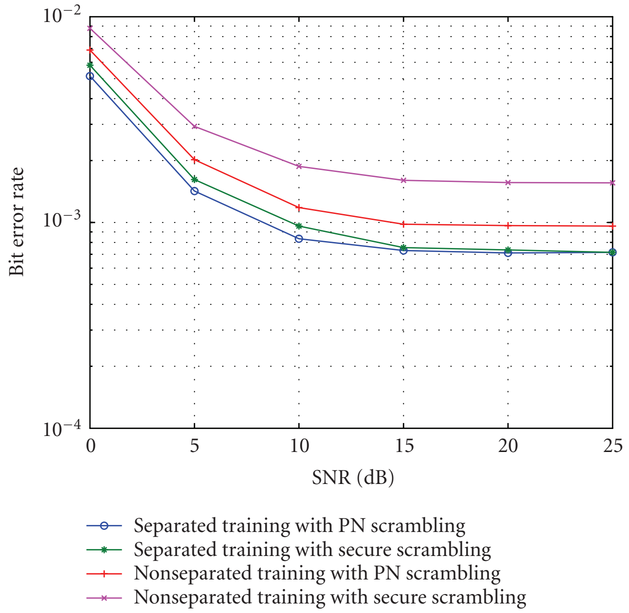

Figure 5: BER versus SNR, results from Rake receiver with no channel coding, 4-ray multipath channel, processing gain $N = 16$, number of users = 4.

Extension of the physical layer built-in security from CDMA systems to other wireless systems is partially possible. For example, the secure scrambling block can be implemented after the channel encoder in any wireless systems to introduce physical layer security. However, nonspread-spectrum system may not have the same antijamming features as the spread-spectrum systems, since the frequency domain diversity is not available anymore.

6. CONCLUSION

In this paper, security weakness of the operational and proposed CDMA systems is analyzed and an encryption-based secure scrambling process is presented. First, instead of using the long-code sequences generated by the LFSR directly, the scrambling sequences are generated through AES operations. As a result, the physical layer built-in security of the CDMA system is significantly increased with very limited complexity load. Second, it is shown that by scrambling the training sequence and the message sequence separately with two independent scrambling sequences, both information privacy and system performance can be further improved. Finally, error-tolerant decryption can be achieved through secure scrambling. The proposed scheme is very feasible and can readily be implemented for security enhancement in wireless networks.

ACKNOWLEDGMENTS

This paper is supported in part by MSU IRGP and Cyper Security Initiative.

REFERENCES

[1] R. Nichols and P. Lekkas, *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill Telecom Professional Series, McGraw-Hill, New York, NY, USA, 2002.

[2] IEEE, "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," November 1999.

[3] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[4] S. Bhashyam and B. Aazhang, "Multiuser channel estimation and tracking for long-code CDMA systems," *IEEE Transactions on Communications*, vol. 50, no. 7, pp. 1081–1090, 2002.

[5] C. J. Escudero, U. Mitra, and D. T. M. Slock, "A Toeplitz displacement method for blind multipath estimation for long code DS/CDMA signals," *IEEE Transactions on Signal Processing*, vol. 49, no. 3, pp. 654–655, 2001.

[6] A. J. Weiss and B. Friedlander, "Channel estimation for DS-CDMA downlink with aperiodic spreading codes," *IEEE Transactions on Communications*, vol. 47, no. 10, pp. 1561–1569, 1999.

[7] National Bureau of Standards, "FIPS Publication 197: Advanced Encryption Standard (AES)," November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[8] TIA/EIA/IS-95-B, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System," 1998.

[9] V. K. Garg, *IS-95 CDMA and cdma 2000: Cellular/PCS Systems Implementation*, Pearson Education, Upper Saddle River, NJ, USA, 1999.

[10] National Bureau of Standards, "FIPS Publication 81: DES Modes of Operation," December 1980, http://www.itl.nist.gov/fipspubs/fip81.htm.

[11] Electronic Frontier Foundation (EFF), "EFF DES Cracker Project," http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/.

[12] S. Parkvall, "Variability of user performance in cellular DS-CDMA-long versus short spreading sequences," *IEEE Transactions on Communications*, vol. 48, no. 7, pp. 1178–1187, 2000.

[13] T. S. Rappaport, *Wireless Communications: Principles and Practices*, Prentice-Hall, Upper Saddle River, NJ, USA, 2nd edition, 2002.

[14] J. Proakis, *Digital Communications*, McGraw-Hill, New York, NY, USA, 4th edition, 2000.