http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (7): 1325-1333, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1325.1333

Anti-Detection Performance of Code-Hopping Direct Sequence Spread Spectrum System

Li Dezhi, Gu Xuemai and Guo Qing
Communication Research Center, Harbin Institute of Technology, Harbin,
150080, People Republic of China

Abstract: In wireless communications especially satellite communications, as blind detection technologies developing, traditional Direct Sequence Spread Spectrum (DSSS) system is no longer secure enough. Code-Hopping (CH) DSSS system is considered as an evolution for its dynamization. CH-DSSS system gets rid of periodical cycle characteristic with its variable and unpredictable spreading sequence. Therefore, CH-DSSS signal is harder to be detected unauthorized. Theoretical analysis and simulations are carried out on both signal parameters and data demodulation. Results indicate that the anti-detection performance of CH-DSSS system improves logarithmically as the number of hopping codes increases. Considering the limited code sequence resource, the performance curve is given, from which a cost-effective codes number could be chosen.

Key words: Direct sequence spread spectrum (DSSS), code-hopping (CH), anti-detection, estimation-based time-domain sliding correlating accumulation ETSCA, data encryption

INTRODUCTION

Our daily lives become more and more dependent on satellite communications. However, satellite communication is easily to be jammed or intercepted for its openness. Not only military satellite systems need secure protection but also civil systems. For Pay-TV broadcasting, security problems cause massive financial losses to the providers. Private and business users expect secure transmission of their data (Hermanns *et al*., 2005).

Today, no special effort is done in civil satellite communications to secure the transmission on the physical layer. Even some military communications need more solutions to prevent jamming and interceptions. The exiting anti-detection and anti-interception methods in physical layer could be sorted into four kinds. They are space-domain, frequency-domain, time-domain and code-domain. In space-domain, the main idea is beam narrowing. The anti-detection performance is realized by precise directional communication. However, the detector could still be placed just in the beam or closely enough to the transmitter. In frequency-domain, frequency hopping technique is so costly and complicated that civil wireless communications can not afford. In time-domain, though many methods are proposed to increase the difficulty of detection, the benefit is limited. Some mixed modes are also proposed like space-time code scheme (Mingxin *et al*., 2008).

In code-domain, Direct Sequence Spread Spectrum (DSSS) systems were thought to be secure but all the secure performance is based on the assumption that the code sequence is unknown for interceptors. However, this assumption is not the truth any more. Most DSSS systems are using vulnerable Linear Feedback Shift Register (LFSR) generators to create the spreading sequences. According to the research, the hidden 42-bit LFSR mask value of IS-95 mobile phone communications can be revealed in about 1 sec of interception. The argument of CDMA-based voice privacy in IS-95 is weakened by this (Hermanns *et al*., 2005). DSSS systems which do not use LFSR could be cracked too with more time and calculations.

Despite wireless communications, DSSS communication system also has applications in optical LAN to transmit private data (Britto and Sankaranarayanan, 2006). Its security mechanism will be broken either when the code is decrypted.

Many detection and interception algorithms are developed. Some of them base on the energy detection. Some utilize autocorrelation of spreading code (Polydoros and Holmes, 1983). Others focus on the higher order spectral features, as well as cepstrum and periodic spectrum. Even matrix calculation is used. Except energy detection, almost all of these algorithms use periodical cycle characteristic. Though the periodical cycle characteristic may be covered by data modulation, it could be extracted by methods like autocorrelation and periodic spectrum. Particularly, algorithms using autocorrelation of DSSS signal are more and more popular.

DSSS detection using second order moment estimators was presented in 2002 (Burel *et al*., 2001). Because the fourth-order moment chip is blind to the

Corresponding Author: Li Dezhi, Communication Research Center, Harbin Institute of Technology, Harbin, 150080, People Republic of China

arbitrary Gaussian noise, the detection method based on the quadratic fourth-order moment chip of DS-CDMA was proposed (Zhijin and Junjie, 2009). Advanced detection method based on fluctuating observation of second order statistic estimator was presented in 2010 (Khodadad *et al*., 2010).

Self-Organizing Feature Map (SOFM) neural network algorithm was presented to detect and identify the PN sequence (Hao *et al*., 2006). Singular Value Decomposition (SVD) plus Digital Phase Lock Loop (DPLL) was presented to solve the problem of blind Pseudo-Noise (PN) sequence estimation for low signal to noise ratios (SNR) DSSS signals in dynamic environments (Zhang *et al*., 2008).

Autocorrelation techniques for FH/DS signals detection was presented since 1983 (Polydoros and Holmes, 1983). Segment correlation and amplitude accumulation method was presented by Sun *et al*. (2006). A long PN code sequence estimation and synchronization algorithm by subsection technique was proposed by Yong *et al*. (2007). A combination method was presented to estimate the unknown PN spreading sequence for DSSS signals in frequency selective fading channel (Xu, 2008). Communication signals are appropriately to be modeled as cyclostationary stochastic processes. Method based on second order cyclostationary statistics was adopted to detect whether the modulated signal exists in background noise (Yu *et al*., 2008).

DSSS systems have good anti-interference performance both on data transmission and telemetry tracking and control (Wu *et al*., 2010). To exploit the power of DSSS system for anti-jamming and low probability of intercept, dynamic spreading codes have to be developed, i.e., Code-Hopping (CH) DSSS systems.

Code hopping technique eliminates periodic cycle which is the most important characteristic for unauthorized detection. Interception and eavesdropping renders impossible for unpredictable and non-circulating spreading codes. At negative SNR, the signal disappears in noise and the attacker can not even detect a signal. The advantages of CH-DSSS grow with the signal bandwidth. Best are modern ultra-wideband (UWB) transmission systems. And the hopping code generation could be supported by fast spread sequence generation technology (Chen *et al*., 2010; Tong *et al*., 2011).

Estimation-based Time-domain Sliding Correlating Accumulation (ETSCA) algorithm is based on estimation and weighted accumulation (Li *et al*., 2010). ETSCA algorithm can successfully detect DSSS signal information in SNR lower than -15 dB when the PN code used is only 15 bits long. SNR required could be even lower when code length increases. ETSCA Algorithm can also estimate data transmitted with good BER performance. In particular, this algorithm could be used to detect CH-DSSS signal with small change. With this method, the Anti-detecting performance of non code-hopping (NCH) DSSS and CH-DSSS systems are compared. Theoretical analysis and simulation lead to a conclusion that CH-DSSS system is more secure than NCH-DSSS system.

SYSTEM DESCRIPTION

DSSS system block diagram is shown in Fig. 1.

For simplicity, ignore the fading. Received signal S (t) which is modulated by BPSK can be expressed as:

$$S(t) = d(t).c(t).\sin(\omega t)+n(t) \quad (1)$$

S_i (t) stands for one symbol segment of S (t), it can be expressed as:

$$S_i(t) = d_i(t).c(t).\sin(\omega t)+n_i(t),\ i = 1, 2,... \quad (2)$$

where, d_i (t) is data transmitted, c (t) is the Pseudorandom Noise (PN) code, ω is angular frequency and n_i (t) is Additive White Gaussian Noise (AWGN).

The main difference to traditional NCH- DSSS systems is the dynamization of secure pseudo noise spreading code. CH-DSSS system block diagram is shown in Fig. 2. The PN code generators are controlled by Code Hopping Control (CHC) module. That makes the actual spreading code unpredictable but can still be synchronized by key mechanism. Spreading code can be realized in hardware by Advanced Encryption Standard (AES) blocks in Open for Business (OFB) mode. Simple variants with basic LFSR generators are possible to reuse existing CDMA hardware. By dynamically re-seeding the LFSR, attacks become much harder.

Signal in CH-DSSS system modulated by BPSK can be expressed as:

$$Sch_i(t) = d_i(t).c_i(t).\sin(\omega t)+n_i(t),\quad c_i \in \{c_{[j]}, j = 1, 2,..., R\} \quad (3)$$

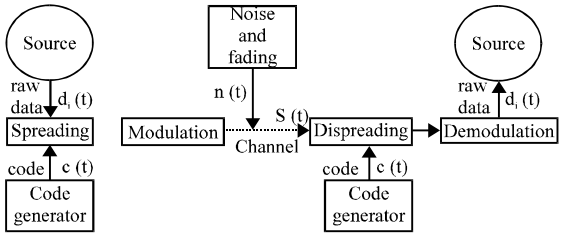

Fig. 1: NCH-DSSS system architecture

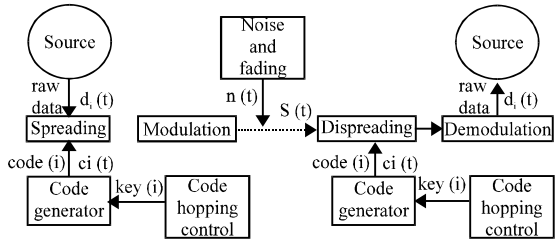

Fig. 2: CH-DSSS system architecture

where, $c_{[j]}$ (t) is the hopping code, R is the number of hopping codes and c_i (t) is determined by code hopping table. Comparing Eq. 3 with Eq. 2, the only difference is code c_i (t) in (3) is variable as data symbol changing.

ETSCA METHOD

Most of detecting methods for DSSS signal make use of the cycle repeated feature. ETSCA (Estimation-based Time-domain Sliding Correlating Accumulation) method has good detecting performance and portability. The method can detect DSSS signal period and synchronization in SNR lower than generally working. It can estimate data with BER closed to theoretical BER.

Estimation model: The modulated code Cm (t) can be expressed as:

$$Cm(t) = c(t).\ Sin(\omega t) \tag{4}$$

Then:

$$\begin{aligned} &S_i(t)\cdot Cm(t)\\ &=[d_i(t)\cdot c(t)\cdot \sin(\omega t)+n_i(t)]\cdot[c(t)\sin(\omega t)]\\ &=d_i(t)\cdot c^2(t)\sin^2(\omega t)+n_i(t)c(t)\sin(\omega t)\\ &=d_i(t)\left(\frac{1+\cos(2\omega t)}{2}\right)+n_i(t)c(t)\sin(\omega t)\end{aligned} \tag{5}$$

So d_i (t) can be acquired by integration in code period T_p:

$$d_i=\frac{2}{T_P}\int_0^{T_P} \mathrm{LPF}[S_i(t)Cm(t)]dt \tag{6}$$

where, S_i (t) is one segment of DS signal in T_p. LPF [S] means signal S passes low pass filter. For the lack of C_m (t) we use estimated code Cm_E (t) instead. Cm_E (t) can be expressed as:

$$Cm_E(t) = c(t)\sin(\omega t)+n_E(t) \tag{7}$$

where, n_E (t) is estimation noise. Then estimated data d_{Ei} (t) could be acquired as follow:

$$d_{E,i}=\frac{2}{T_P}\int_0^{T_P} \mathrm{LPF}[S_i(t)\ Cm_E(t)]\ dt \tag{8}$$

The accuracy of d_{Ei} (t) is determined by accuracy of Cm_E (t). Cm_E (t) could be calculated by:

$$\begin{aligned} &Cm_E(t)\\ &=\frac{1}{M}\sum_i^M d_{Ei}(t)\ S_i(t)\\ &=(2P-1)c(t)\sin(\omega t)+\frac{1}{M}\sum_i^M d_{Ei}(t)\ n_i(t)\end{aligned} \tag{9}$$

where, M is the total number of segments, P is the probability of d_{Ei} (t) equaling to d_i (t). P tends to 1 when the estimation is accurate. The second item in tends to be 0 when M is large enough.

Equation 8 and 9 indicate that we can calculate d_E (t) from Cm_E (t), then reversely refresh Cm_E (t) using d_E (t). As this process continuing, the power of estimated noise is reduced gradually. When the actual application, it could choose any signal segment S_i (t) as the initial value of estimated code $Cm_E(t)_{(0)}$. Simulation results show that the value of d_E (t) and Cm_E (t) will be available after 3 to 5 circular processes.

Parameter detection: ETSCA method adopts time-domain sliding correlation algorithm detects code period and code synchronization. According to this algorithm, signal samples are divided into several segments with the same length by a dividing window. which the size of is T. The dividing window slides to search synchronization position and the sliding offset is P_{syn}. the final output V (T, P_{syn}) is as follow:

$$\begin{aligned} &V(T,p_{syn})\\ &=\sum_t^T\left(\frac{1}{M}\sum_i^M Cm_E(t)_{(n-1)}\ S_i^{T,p_{syn}}(t)\cdot d_{Ei}(t)_{(n-1)}\right)\\ &=\frac{1}{2}\sum_t^T(2P_{(n-1)}-1)(2P_{(n)}-1)\end{aligned} \tag{10}$$

where, n is the times of refreshing moves and $S_i^{T,p_{syn}}$ (t) is one of the segments divided by parameters T and p_{syn}. V (T, p_{syn}) gets its maximum value when T equals to code period T_p and p_{syn} is just the position where code synchronized. If T and p_{syn} do not match the true value, there will be no spreading gain. Then because of the powerful noise, the estimation is nearly a random guess. It means that the accuracy probability tends to 50% and V (T, p_{syn}) will be 0.

Figure 3 is a mesh plot of V (T, p_{syn}). In this simulation, 15 bits code is used and the SNR is -3 dB. Units of both T axis and p_{syn} axis are sample time T_S. Figure 1 indicates that there is a series of peaks forming a wall at 480 T_S in T axis (where T_p is). The coordinate of the

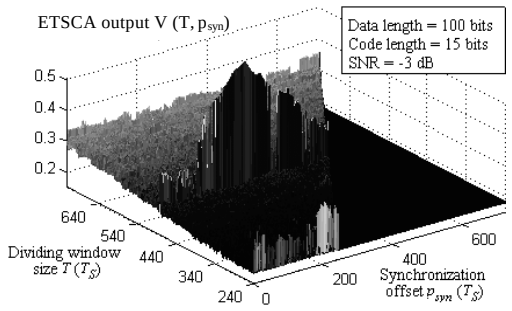

Fig. 3: Mesh plot for simulation results V (T, p_{syn})

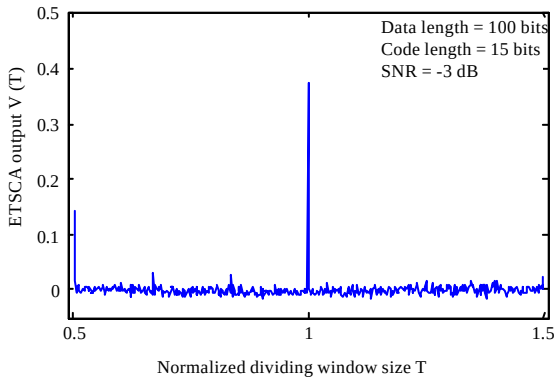

Fig. 4: Projection on T plane

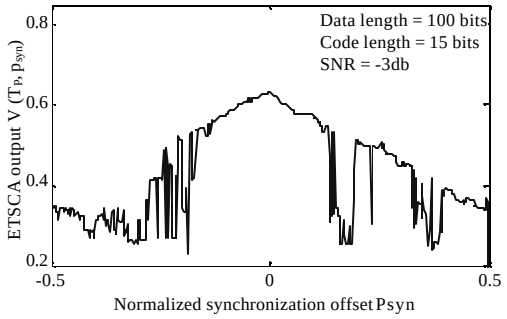

Fig. 5: Section when T equals to T_p

wall's highest peak are just code period and synchronization position which we are searching for.

Define V (T) as the maximum V (T, p_{syn}) for each T. That is the projection on T plane. Figure 4 shows the curve of V (T) which has a clear period spectrum. For convenience, the abscissa is T normalized with code period T_p.

Figure 5 is the Section when T equals to T_p. It's where the peak wall is. The p_{syn} axis has been normalized by code period T_p. "0" means it's just the synchronization position and "1" means the sliding offset is one code period. Figure 4 has clearly shown where the synchronization position is.

DETECTION ON CH-DSSS SYSTEM

CH-DSSS system is developed from NCH-DSSS system. The only difference between them is code sequence in CH-DSSS system is dynamic. Do the same processing with NCH-DSSS system, define:

$$\begin{aligned} Cmch_E(t) = \frac{1}{R}[c_{[1]}(t) + c_{[2]}(t) + \\ \cdots + c_{[R]}(t)]\sin(\omega t) + n_E(t) \end{aligned} \tag{11}$$

then:

$$\begin{aligned} & Sch_i(t) \cdot Cmch_E(t) \\ & = [d_i(t)\, c_i(t)\sin(\omega t) + n_i(t)] \cdot \\ & \left\{\frac{1}{R}\sum_{j=1}^{R} c_{[j]}(t)\sin(\omega t) + n_E(t)\right\} \\ & = d_i(t)\frac{1+\cos(2\omega t)}{2}\frac{1}{R} \cdot \\ & \left[1 + \sum_{j=1, c_{[j]} \neq c_i}^{R} c_i(t)\, c_{[j]}(t)\right] + Noise(t) \\ & = \frac{d_i(t)}{2R} + \frac{\cos(2\omega t)\, d_i(t)}{2R} + A(t) + Noise(t) \end{aligned} \tag{12}$$

Where:

$$\begin{aligned} Noise(t) = d_i(t)\, c_i(t)\sin(\omega t)\, n_E(t) + \\ \frac{n_i(t)}{R}\sum_{j=1}^{R} c_{[j]}(t)\sin(\omega t) + n_i(t)\, n_E(t) \end{aligned}$$

$$A(t) = \frac{[1+\cos(2\omega t)]d_i(t)}{2R}\sum_{j=1, c_{[j]} \neq c_i}^{R} c_i(t)\, c_{[j]}(t)$$

Dealing with integrator and LPF, 3 items behind in tend to be 0. Thus:

$$d_{Ei} = \frac{2R}{T_P}\int_0^{T_P} LPF[Sch_i(t)\, Cmch_E(t)]\, dt \tag{13}$$

Comparing Eq. 12 with Eq. 5, it could be found that noise in Eq. 12 is larger than which in Eq. 5 . The coefficient of data item d_i in Eq. 12 is smaller too because of the exiting of R. Similarity with, Eq. 9, consider:

$$\begin{aligned}
&\frac{1}{M}\sum_{i=1}^{M} d_{Ei}(t)\,Sch_i(t)\\
&=\frac{1}{M}\sum_{i=1}^{M}\left[d_{Ei}(t)\,d_i(t)\,c_i(t)\sin(\omega t)+d_{Ei}(t)\,n_i(t)\right]\\
&=\frac{1}{M}\sum_{j=1}^{M(2P-1)} d_j(t)\,d_j(t)\,c_j(t)\sin(\omega t)+\\
&\frac{1}{M}\sum_{i=1}^{M} d_{Ei}(t)\,n_i(t)\\
&=\frac{1}{M}\sin(\omega t)\sum_{j}^{M(2P-1)} c_j(t)+\frac{1}{M}\sum_{i=1}^{M} d_{Ei}(t)\,n_i(t)
\end{aligned} \tag{14}$$

Assume the distribution of hopping code is uniform. Then Eq. 14 will comes to:

$$\begin{aligned}
&\frac{1}{M}\sum_{i=1}^{M} d_{Ei}(t)\,Sch_i(t)\\
&=\sin(\omega t)\frac{(2P-1)}{R}\sum_{i=1}^{R} c_{[i]}(t)+\frac{1}{M}\sum_{i=1}^{M} d_{Ei}(t)\,n_i(t)\\
&=(2P-1)\left(\frac{1}{R}\sin(\omega t)\sum_{i=1}^{R} c_{[i]}(t)+\right.\\
&\left.\frac{1}{M(2P-1)}\sum_{i=1}^{M} d_{Ei}(t)\,n_i(t)\right)\\
&=(2P-1)\,Cmch_E(t)
\end{aligned} \tag{15}$$

When SNR is high, P tends to be 1. Then:

$$Cmch_E(t)=\frac{1}{M}\sum_{i=1}^{M} d_{Ei}(t)\,Sch_i(t) \tag{16}$$

Although the above derivation assumed the inner products of non-relevant items are 0. But in fact, these items are not absolutely relevant. The correlation value can not be ignored when the code length is short. This is equivalent to adding noise with fixed SNR. Especially, this part of the noise can not be depressed by increasing accumulated data length.

SIMULATION

The simulation includes two parts. One is signal parameters anti-detecting performance simulation. In this part, the main work is on weather the detecting method could recognize the signal parameters rightly.

The other part is data demodulation test. After acquiring the signal period and synchronization, the original data transmitted could be demodulated. System using code hopping will get an extra anti-detecting gain in this step.

Parameter anti-detection simulation: in the simulation, 400 bits data have been spread by 15 bits PN code. The filter band is 4 times wide of signal band and the SNR is -6 dB. Figure 5 shows the results V (T) when R is 1, 2, 4 and 8, respectively.

Table 1: Judgment factors when data length is 400 bits

R	$\sigma_{Y,first}$	$\sigma_{Y,second}$	γ_Y
1	52.6334	7.101	7.4121
2	53.5802	9.6783	5.5361
4	35.241	5.2162	6.7563
8	9.2133	4.7301	1.94784

Figure 6 points out the signal's main spectrum falls when increasing the number of hopping codes. In another word, the anti-detecting performance gets better when hopping-code number increased.

In order to quantitatively determine whether the maximum spectrum is the real signal, define γ_Y named peak ratio. Firstly, define the maximum peak factor $\sigma_{Y,first}$ and the second maximum peak factor $\sigma_{Y,second}$ of vector Y as follows:

$$\sigma_{Y,first}=\frac{Y_{max}-Mean(Y)}{Mean(|Y-Mean(Y)|)} \tag{17}$$

$$\sigma_{Y,second}=\frac{Y_{submax}-Mean(Y)}{Mean(|Y-Mean(Y)|)} \tag{18}$$

where, function "Mean (Y)" is to calculate the average value of Y, T_{max} is the maximum value of Y and Y_{submax} is the second maximum value of Y. Then define γ_Y as:

$$\gamma_Y=\frac{\sigma_{Y,first}}{\sigma_{Y,second}} \tag{19}$$

Table 1 shows γ_Y of V (T). It can be seen that, the maximum spectrum is really signal code period spectrum when $\sigma_{Y,first}$ and γ_Y is large.

Data anti-demodulation simulation: In the same time of recognizing period spectrum, code synchronization information could be obtained by intercepting the p_{syn} plane including period spectrum in mesh plot.

For NCH-DSSS system, ones making sure the code period and synchronization position, d_{Ei} (t) could be directly output as blind detection results. Figure 7 gives out BER of d_{Ei} by different SNR, the theoretical value presents either. It is shown that detecting methods could easily get the original data transmitted.

While in CH-DSSS system, there is a protection from demodulating uncooperative. That is detectors have no idea of the pole of the code. This problem does not exit in NCH-DSSS system, because you can get the right data sequence or the totally opposition which is usable either.

The demodulation results in CH-DSSS system is permutation and combination of hopping codes. It causes fixed bit error according how many hopping codes are used. For example, there are two hopping codes, both demodulation results of two data sequences are the same

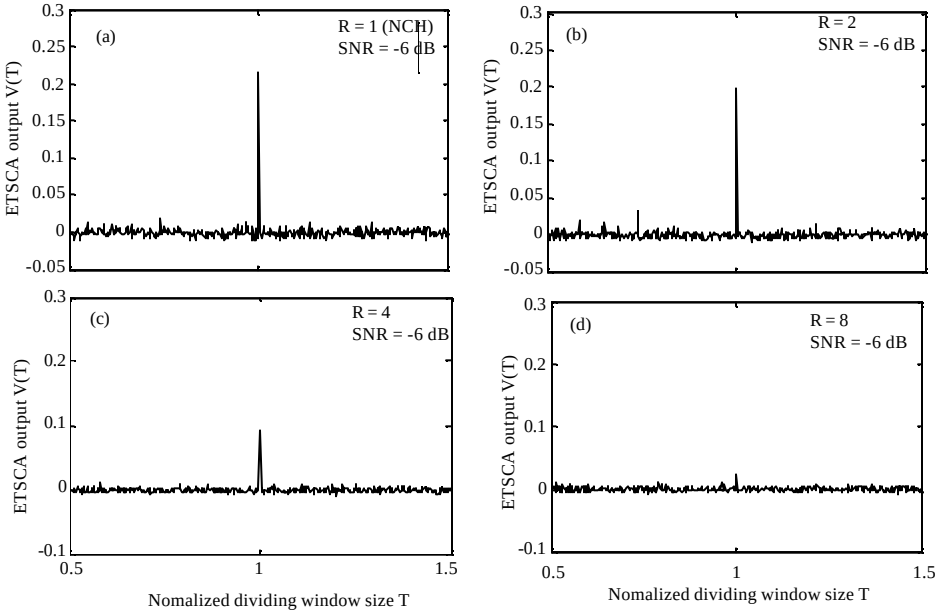

Fig. 6: Results for different number of codes, (a) NCH system, (b) CH system when R = 2, (c) CH system when R = 4 and (d) CH system when R = 8

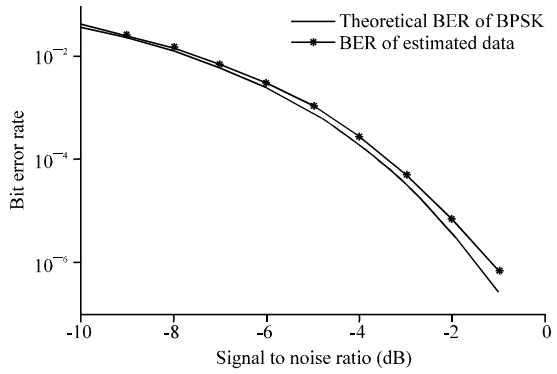

Fig. 7: BER of estimated data d_{Ei} (t)

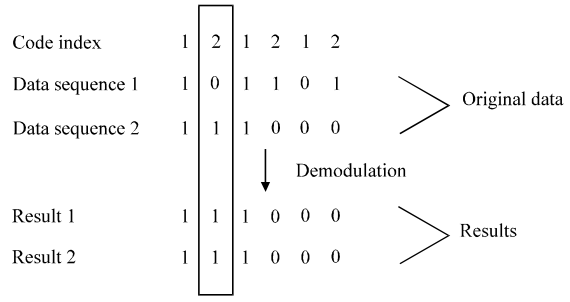

Fig. 8: Demodulation of 2 codes hopping system

as shown in Fig. 8. Noticing data spread by code 2 in the rectangular, either 0 or 1 ill be considered as 1. Therefore, code hopping encrypts the raw data. The more hopping codes, the deeper data are encrypted. Thus intercepting demodulation will have a high ABER (average bit error rate).

However, interceptor could still get right data by decryption like code separation or just has a good luck. When the demodulated results have the same polarity with original data, it is called consistent situation. And the BER in consistent situation is called CSBER.

In simulation, ABER is got by directly demodulating CH signals by ETSCA method. And CSBER is got by using special1 data instead of random data to artificially create consistent situation.

RESULTS ANALYSIS

Parameter anti-detection analysis: It is indicated by Eq. 10 and 15 that the precision of estimation is related to the SNR. As SNR decreasing, the signal's main spectrum in T plane projection is gradually submerged in noise. It is also reflected as the decreasing of γ_γ. Generally, detection fails when γ_γ is less than 2. Define the SNR is the lowest working SNR when γ_γ equals to 2. The lowest working SNR for different number of hopping codes is shown in Fig. 9.

Anti-detection performance of CH signals is related to the cross correlation of hopping codes adopted. The less cross correlation is, the more efficient the hopping

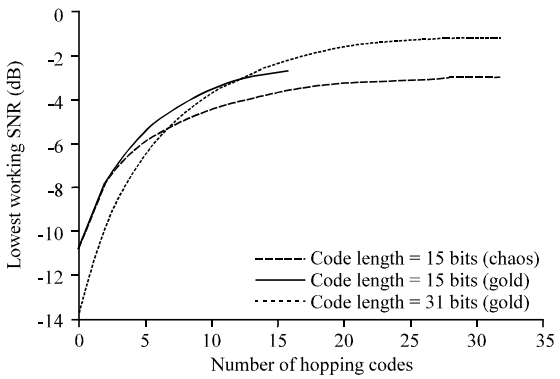

Fig. 9: Lowest working SNR

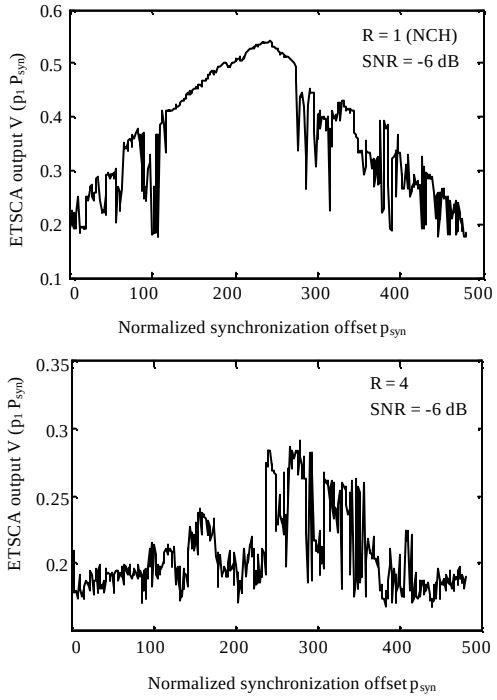

Fig. 10: Synchronization detection on NCH system and CH system

codes are. That is why the curve of Lowest working SNR for codes 31 bits long is higher than that for codes 15 bits long. For chaos codes and gold codes which are both 15 bits long, anti-detection performance of gold codes is better than that of chaos codes for the same reason.

The curve of lowest working SNR rises logarithmically as the number of hopping codes increasing. The curvature is related to the cross correlation. The curve rises faster when the cross correlation is smaller. Generally, the curve approaches a horizontal line when R is bigger than code length. The anti-detecting efficiency is high when the number of hopping codes is below 1/3 code length.

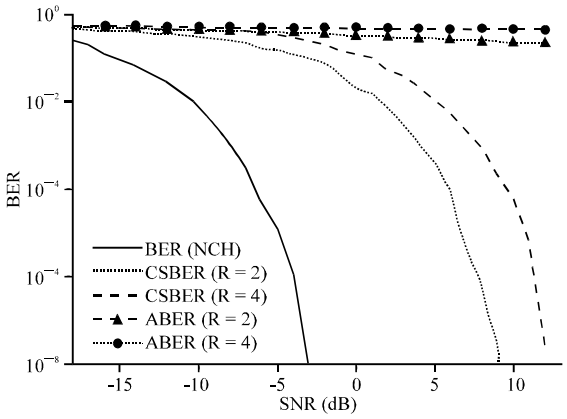

Fig. 11: BER of CH system (BPSK, 31 bits gold codes)

Code hopping system also makes it hard to get synchronization position in p_{syn} plane which is shown in Fig. 10. We could easily find synchronization position in NCH system's p_{syn} plane projection. But it could only get an approximately position in CH system's projection.

Data anti-demodulation analysis: Demodulation results are shown in Fig. 11. The modulation is BPSK mode. The spreading sequence is gold code and the code length is 31 bits.

In the consistent situation, the encryption offered by different hopping codes is gone, so CSBER is lower than ABER. But these hopping codes also provide another protection-the inter-code interference. For interceptors, unpredictable hopping codes undoubtedly add a lot of noise. So CSBER will be higher than normal BER.

BER of CH system is further bigger than the BER of NCH system. It proves the secure performance of CH system is better. CH signals gets about 12 dB anti-demodulation gains while R is 2. The anti-demodulation gain increases when R grows. In fact, as R growing, the probability of consistent situation decreases quickly. And it's hardly to separate hopping codes when R is big.

CONCLUSION

Research shows NCH-DSSS signals is indeed insecure. It could be easily detected and even be demodulated. Cycle repeated feature is NCH-DSSS system's biggest weakness which is used by detecting methods. CH-DSSS system eliminates this weakness efficiently by unpredictable hopping codes.

CH-DSSS system has not been applied widely in wireless communication. Thus there is few detecting or intercepting research against CH-DSSS communication system. Separating hopping codes may improve the detecting performance. But it is really hard to distinguish unknown and mixed codes with low SNR.

CH-DSSS system has stronger anti-detection performance in both signal parameters and data demodulation. Increasing hopping codes will be efficient if the cross correlation of hopping codes is small and the number of hopping codes is smaller than 1/3 code length. As the number of hopping codes rising, the efficiency falls down. And when the number of hopping codes is larger than the code length, there will be little improvement.

Hopping codes will also encrypt the raw data and add inter-code interference into interceptors' demodulation. The anti-demodulation gain is more than 12 dB and will become bigger when increasing the number of hopping codes.

The cost of increasing anti-detection performance is the system complexity. To improve NCH-DSSS system into CH-DSSS system, NCH-DSSS system needs to add CHC module. Additional requirement of spreading code resources is an important issue. Real-valued direct sequences (Jiang and Lu, 2009) and chaotic PN sequences (Leon *et al*., 2001) have been developed to solve this problem. The CH synchronization and management of CHC key also need to be studied.

In conclusion CH-DSSS system has good anti-detection performance and should be developed to instead of NCH-DSSS system in secure communications.

ACKNOWLEDGMENT

This study was supported by the National major special science and technology project of China (2009ZX03005-003).

REFERENCES

Britto, K.S.S. and P.E. Sankaranarayanan, 2006. CDMA based optical lan. Inform. Technol. J., 5: 673-678.

Burel, G., C. Bouder and O. Berder, 2001. Detection of direct sequence spread spectrum transmissions without prior knowledge. IEEE Global Telecommun. Conf. USA., 1: 236-239.

Chen, F., J. Hua, C. Zhao and S. Zhou, 2010. Fast generation of bent sequence family. Inform. Technol. J., 9: 1397-1402.

Hao, C., G. Wei and Y. Jingdong, 2006. DSSS signal parameter detection and PN sequence estimation based on SOFM neural network. Proceedings of the 6th International Conference on ITS Telecommunications (ITS'06), Chengdu, pp: 1275-1277.

Hermanns, F., S.H. Cruickshank and S. Iyengar, 2005. Protection of the European space infrastructure. Proceedings of the 14th IST Mobile ans Wireless Communications Summit, June 19-23, Dresden, Germany, pp: 1-5.

Jiang, X.Y. and J.H. Lu, 2009. Code hopping communications with real-valued direct sequences for anti-interception. Proceedings of the IET International Communication Conference on Wireless Mobile and Computing, Dec. 7-9, Shanghai, China, pp: 125-128.

Khodadad, F.S., F. Ganji and A. Safaei, 2010. A robust PN length estimation in down link low- SNR DS-CDMA multipath channels. Proceedings of the 12th International Conference on Advanced Communication Technology, Feb. 7-10, Phoenix Park, pp: 951-955.

Leon, D., S. Balkir, M.W. Hoffman and L.C. Perez, 2001. Robust chaotic PN sequence generation techniques. IEEE Int. Symp. Circuits Syst., 4: 53-56.

Li, D., X. Gu and Q. Guo, 2010. Estimation-based blind detection in low SNR on direct-sequence spread spectrum signal. Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing, Sept. 23-25, Chengdu, pp: 1-4.

Mingxin, Z., R. Wenhui, X. Feng, Z. Yatong, J. Shen and Z. Yaling, 2008. A novel CDMA-BLAST space-time code scheme. Inform. Technol. J., 7: 1067-1071.

Polydoros, A. and J.K. Holmes, 1983. Autocorrelation techniques for wideband detection of FH/DS waveforms in random tone interference. Proceedings of thr Military Communications Conference, Oct. 31-Nov. 2, Washington, DC., pp: 781-785.

Sun, J., Q. Shen and L. Yuan, 2006. A new segment correlation and amplitude accumulation method of direct sequence spread spectrum signal pseudoradom code period. Modern Defence Technol., 34: 73-75.

Tong, L., F. Chen, J. Hua, L. Meng and S. Zhou, 2011. Correlation analysis and realization of gordon-mills-welch sequences in advanced design system. Inform. Technol. J., 10: 908-913.

Wu, Z., N. Zhao, G. Ren and T. Quan, 2010. Anti-interference strategies review of unified spread spectrum telemetry tracking and control system. Inform. Technol. J., 9: 979-983.

Xu, X., 2008. Blind estimation of PN code in multipath fading direct sequence spread spectrum systems. Proceedings of the 11th IEEE International Conference on Communication Technology, Nov. 10-12, Hangzhou, pp: 213-216.

Yong, Z., L. Ming and T. Bin, 2007. Blind estimation of long PN code sequence. Proceedings of the International Conference on Communications, Circuits and Systems, July 11-13, Kokura, pp: 705-708.

Yu, M., S, Li, H, Feng and Z. Yang, 2008. Blind detection and parameter estimation of multiuser and multipath DS-CDMA signal using cyclostationary statistics. Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, Oct. 12-14, Dalian, pp: 1-5.

Zhang, T., S. Dai, W. Zhang, G. Ma, 2008. Blind estimation of the PN sequence for weak DS-SS signals in dynamic environments. Proceedings of the 11th IEEE International Conference on Computer System, Nov. 19-21, Singapore, pp: 470-474.

Zhijin, Z. and P. Junjie, 2009. A detection method of DS-CDMA signal based on the quadratic fourth-order moment chip. Proceedings of International Conference on Networks Security, Wireless Communications and Trusted Computing, Apr. 25-26, Wuhan, Hubei, pp: 759-762.