Journal of Information Security, **2013, 4, 1-6**
http://dx.doi.org/10.4236/jis.2013.41001 Published Online January 2013 (http://www.scirp.org/journal/jis)

Frequency Hopping Spread Spectrum Security Improvement with Encrypted Spreading Codes in a Partial Band Noise Jamming Environment

Amirhossein Ebrahimzadeh, Abolfazl Falahati
Digital Cryptography and Coding Laboratory (DCCS Lab), Department of Electrical Engineering,
Iran University of Science and Technology, Tehran, Iran
Email: ebrahimzadeh_61@yahoo.com, afalahati@iust.ac.ir

Received June 17, 2012; revised October 25, 2012; accepted November 7, 2012

ABSTRACT

Frequency Hopping Spread Spectrum (FHSS) system is often deployed to protect wireless communication from jamming or to preclude undesired reception of the signal. Such themes can only be achieved if the jammer or undesired receiver does not have the knowledge of the spreading code. For this reason, unencrypted M-sequences are a deficient choice for the spreading code when a high level of security is required. The primary objective of this paper is to analyze vulnerability of linear feedback shift register (LFSRs) codes. Then, a new method based on encryption algorithm applied over spreading codes, named hidden frequency hopping is proposed to improve the security of FHSS. The proposed encryption security algorithm is highly reliable, and can be applied to all existing data communication systems based on spread spectrum techniques. Since the multi-user detection is an inherent characteristic for FHSS, the multi-user interference must be studied carefully. Hence, a new method called optimum pair "key-input" selection is proposed which reduces interference below the desired constant threshold.

Keywords: Frequency Hopping Spread Spectrum; Key Distribution Centre; Key Encryption Key; Linear Feedback Shift Register; Frequency Hopping Code Division Multiple Access; Direct Sequence Spread Spectrum

1. Introduction

Further employment of wireless communication system to exchange vital and critical electronic information requires an urgent attention to design reliable secure systems. This requirement is further strengthen for military communication systems where information transmission heavily relies upon wireless networks [1].

In fact the major advantage of a mobile set narrowband signal transmission is its efficient use of available frequency due to only a fraction of signal transmission frequency being used for a single subscriber. Indeed, a drawback is obvious, as it requires a well coordinated frequency allocation for different subscribers' signal which are now quiet vulnerable to signal jamming and interception.

In [2,3], the fundamental goal of spread spectrum system is considered as; to increase the dimensional characteristic of the signal, hence, to make eavesdropping and/or jamming more difficult since there are more dimensions of the signal to consider. In fact, the main method of increasing the dimensionality of the signal is to widen the signal's spectral occupancy [2,3].

In spread spectrum techniques, security against tapping and jamming is greater compared with narrowband spectrum techniques. Signals of spread spectrum are indistinguishable from background noise to anyone who does not know the coding scheme. The disadvantage of spread spectrum is its relatively high complexity of the coding mechanism which results in complex radio hardware designs and higher costs. Nonetheless, because of its remarkable advantages, spread spectrum has been adopted by many wireless technologies. For example, the IEEE 802.11b standard for wireless LAN employs DSSS over the 2.4-GHz free spectrum, whereas the Bluetooth standard uses frequency hopping spread spectrum (FHSS) for simplicity [1-3].

Furthermore, the main weakness of the wireless communication security system is the simplicity of accessing the communicating signal through the channel. Eavesdroppers can easily place an antenna in the desired field and after demodulation, the message bits can be obtained in the base-band form. If the messages are encrypted, after storing the encrypted messages with some cryptoanalysis methods, the original message can be smeared out. Now, if the received radio signals from the wireless channel is spread in a form that the intruder cannot ac-

cess the despread spectrum and receives only a signal similar to noise, a perfectly secure radio transmission channel is achieved [3-5].

Moreover, specifically the security of the frequency hopping code division multiple access (FH-CDMA) system mainly relies on the long-code generator that consists of a 42-bit long-code mask generated by a 42-bit LFSRs. However, if eavesdroppers can obtain 42 bits of plaintext-cipher-text pairs, the long-code mask can be recovered after dropping the transmission on the traffic channel for about one second [3,6,7].

The fast correlation attack method based on a recently established linear statistical weakness of decimated LFSR sequences for reconstruction of LFSR code is described in [8]. With this method eavesdropper can recover LFSR sequence that he knows the LFSR feedback polynomial. A method of blind estimation of PN code in multipath fading direct sequence spread spectrum systems is proposed in [9]. In this article a combed method is presented to estimate the unknown PN spreading sequence for direct sequence spread spectrum (DS-SS) signals in frequency selective fading channel. It is proven that LFSR codes are vulnerable to cipher-text-only attacks [10] and security weakness of white Gaussian sequence is investigated in [11].

This preface and further studies show that LFSR codes, white Gaussian sequences and other unencrypted codes have security weaknesses and can be recovered by eavesdroppers. So a method which can guarantee systems against the probable attacks is urgently required.

In this manuscript, a new method called hidden frequency hopping spread spectrum is proposed to augment the built-in security of FH-CDMA systems by applying cryptographic algorithm in the channelization code sequence.

2. Security Enhancement in FHSS System with Encryption Hidden within SS

In FHSS technique, several users spread their signal spectrum through available wideband frequency spectrum as narrowband sections with a special code which is called frequency hopping. These codes must have a low cross-correlation since other signals have little interferece over the desired signal. On the other hand, although M-sequences which are generated by LFSR have fair cross-correlation properties but they produce a weak security system for eavesdroppers to track the transmitted spread signals. Therefore, FH-CDMA uses a long-code to scramble the signal in wireless channels, thus the security is set up in the physical layer. The available security which is produced by this method is very low and not suitable for data communication considered. In this article, for security enhancement, a model is proposed that every user encrypts a special spreading code (e.g. a code that is made by the M-sequence generators) with his private key. The model is shown in **Figure 1**. Encrypted codes are then used as the spreading code in the channelization section. At destination, the receiver who knows his private key is able to regenerate the spreading code to de-spread the transmitted signal [3].

On the other hand, the security by the proposed method is related to the encryption algorithm, not to the LFSR complexity. If a suitable algorithm such as RC5, IDEA or any block cipher algorithm is chosen, then a desired high privacy can be obtained [12,13].

3. The Proposed System Model

Although spread spectrum systems are used for narrowband interference mitigation and have good efficiency in preventing intentional and unintentional channel interference, if jammer uses similar spreading codes method, it can be successful in deteriorating such techniques. The level of signal destruction depends on similarity between jammer and transceiver PN codes. This mechanism is different for FHSS and DSSS systems but FH systems are desired. In this method, jammer operates intelligently, after accessing the channel and receive spread signals, it finds spreading technique and PN sequence pattern. Then it generates similar PN pattern and can synchronize itself with the transceiver system to track the modulation type. It should be mentioned that jammer can be located between transmitter and receiver so to provide the man in the middle attack. So jammer can interfere with data signal or change receiver to a useless one and mask itself as an allowable user.

A proposed hidden frequency hopping method can be used to prevent sequence pattern disclosure. Therefore, complexity in this process solely depends upon encryptt ion complexity. Let's consider MFSK transceiver which employs FHSS with encrypted PN sequences, Gaussian noise power and partial band noise jamming function j(t). Suppose that jammer can access channel and obtain desired information from this system.

First a Key Distribution Centre (KDC) generates and transmits agreeable session key to receiver by secure procedure. Session key is a symmetrical key that BTS and SS know and its transmission would be performed by asymmetric pair public-privet key encryption. In this manner symmetric key encrypts SS public key and only SS can decrypt it. Then desired key is transmitted trough unsecure channel by secure process. Public asymmetric key is called Key Encryption Key (KEK). After key exchange, transmitter and receiver have the same encryption key to be able to encrypt PN codes that generate hidden narrow band frequencies. The transceiver system can now be synchronized, track encrypted PN codes, access hidden hopped frequencies and finally obtains

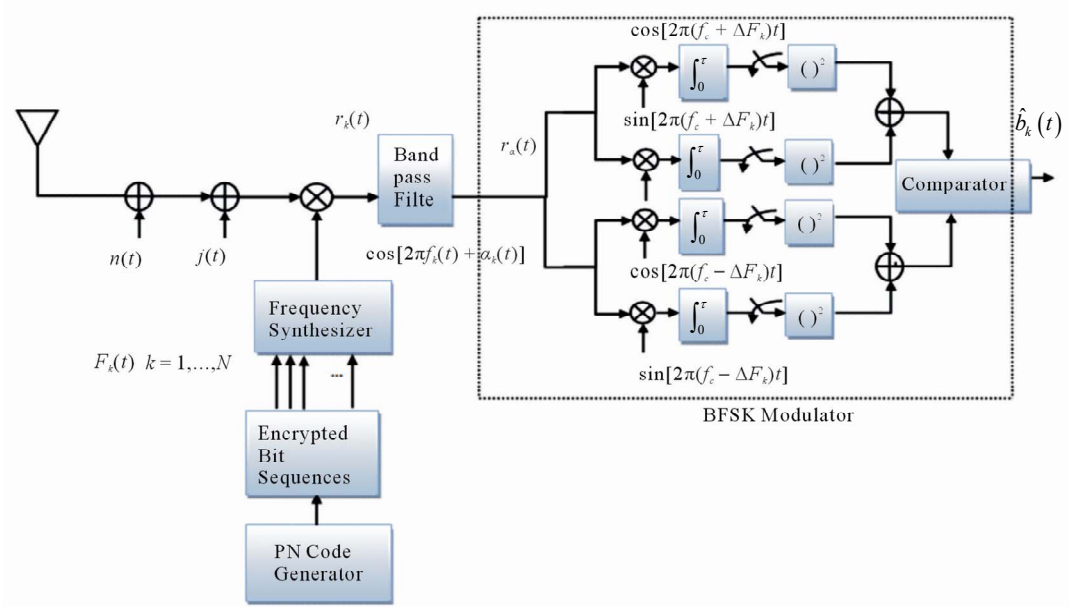

Figure 1. Proposed FHSS with hidden PN sequences for MFSK receiver (M = 2).

original data signals.

Therefore, the jammer applies interference power on narrow band hopped channels randomly and so the bit error rate can be computed as

$$\begin{aligned} &P_{\text{s-encrypted}} \\ &= P_S\left(\text{error}\middle|\text{hit}\right)\times P_{\text{hit}} + P_S\left(\text{error}\middle|\text{no-hit}\right)\times P_{\text{no-hit}} \end{aligned} \tag{1}$$

where P_S presents symbol error probability and P_{hit} is the probability of signal hitting the jammer.

Suppose that the transceiver and jammer have the same hop period T_H, the number of hoped channel N_H with different start signaling. Because jammer doesn't have session key, it can't obtain spreading codes, synchronize with transceiver and to know start transceiver signaling. Thus, the time of transceiver signaling is given by

$$T_{\text{sent-signal}} = T_H - t_{s_0} \tag{2}$$

where t_{s0} is the transceiver signalling start time. The jammer signalling time is

$$T_{\text{sent-signal}} = T_H - t_{s_0} \tag{3}$$

where t_{j0} is start time of jammer signaling, and $0 \le t_{s_0}$ & $t_{j_0} \le T_H$. So jammer and transceiver signal hit occurs in joint time hop period. This value can be expressed as

$$\alpha = \min\left\{T_{\text{sent-signal}}, T_{\text{sent-jammer}}\right\} \tag{4}$$

Figure 2 describes the transceiver signal and jammer signal collision behaviour. So within this behaviour, the probability of jammer and transceiver signal hit in *k*-th hop is

$$P_{\text{hit}} = \frac{\alpha}{T_H} \tag{5}$$

and

$$P_{\text{no-hit}} = 1 - P_{\text{hit}} \tag{6}$$

If jammer uses partial band noise jammer, with standard M-ary FSK modulation that uses one out of M frequencies each second, the bit error probability can be obtained as

$$\begin{aligned} &P_{\text{s-encrypted}} \\ &= \left(1-\frac{\alpha}{T_H}\right)\frac{1}{2(M-1)} e^{-\frac{lE_b}{2N_0}} \sum_{q=2}^{M}\binom{M}{q}(-1)^q e^{-\frac{lE_b(2-q)}{2qN_0}} \\ &+ \frac{\alpha}{T_H}\frac{1}{2(M-1)} e^{-\frac{lE_b}{2N_T}} \sum_{q=2}^{M}\binom{M}{q}(-1)^q e^{-\frac{lE_b(2-q)}{2qN_T}} \end{aligned} \tag{7}$$

where E_b is bit energy, N_0 is the one-sided noise spectral density, and N_T is the total AWGN and jammer noise.

Considering α is maximized by $t_{s_0} = t_{j_0} = t$ as

$$\alpha_{\max} = \min\left\{T_{\text{sent-signal}}, T_{\text{sent-jammer}}\right\}_{t_{s_0}=t_{j_0}=t} \tag{8}$$

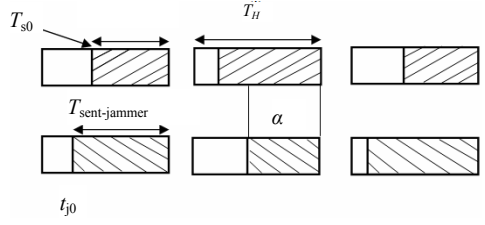

Figure 2. Collision of jammer and transceiver signals.

And maximum term for synchronization α_{Sync} can be given by

$$\alpha_{\text{Sync}} = \alpha_{\max} = \text{T}_{\text{H}} - \text{t} \tag{9}$$

In fact, this is obtained when jammer can synchronize itself with victim transceiver system. If jammer doesn't have session key, it can't access $\alpha_{\max}$.

The cross-correlation of some codes such as Gold and Kassami is lower than the encrypted codes, so a method must be used to optimize the input interference of the system to an acceptable extent. For this reason, an interference threshold is selected for the channel according to the channel interference average for 100 or 1000 times tests. In these tests the channel minimum value interference are calculated and a constant threshold is selected for a channel with a number of users, then the multi-user interference is estimated for each user who enters the network and this value is compared with the threshold level. If the result is less than threshold level, the optimum pair "key-input" is saved for new user and the data is sent confidently such that the interference do not exceed the threshold level. If the interference value is more than the threshold level, the user has to generate another PN and give it to the cryptographer for generating a frequency whose interference is not more than the threshold level. If p is probability of failure and (1 − p) is the probability of success, the probability of achieving the desired code after *k*-tries is

$$\text{P}(\text{A}) = \text{p}^k \times (1 - \text{p}) \tag{10}$$

4. Simulation Results

To perform simulation purposes, an averaging over different keys is employed to mitigate the dependency of BER results on the chosen keys. The simulation results given in **Figure 3** show that the mean value of interference among the encryption algorithm outputs is higher than the M-sequence codes. These values are estimated for 256 channel hops and 1000 iterations. It is dependent upon the selected keys and the encryption algorithm inputs. **Figure 4** represents the number of users trying to find optimum pair "key-input" for 32, 64, 128, 256 and 512 channel hops.

Figure 5 indicates the BER performance when the number of users is increased. This means that the interference is directly proportional to number of users. **Figure 6** represents the effect of FHSS system to mitigate the interference in multi-user channel for 64, 128, 256 and 512 channel hops. **Figure 7** compares m-sequence codes with encrypted codes considering both optimum and non-optimum key method in order to select pair input-key for 256 channel hop. This performance shows that the interference value for encrypted codes is higher

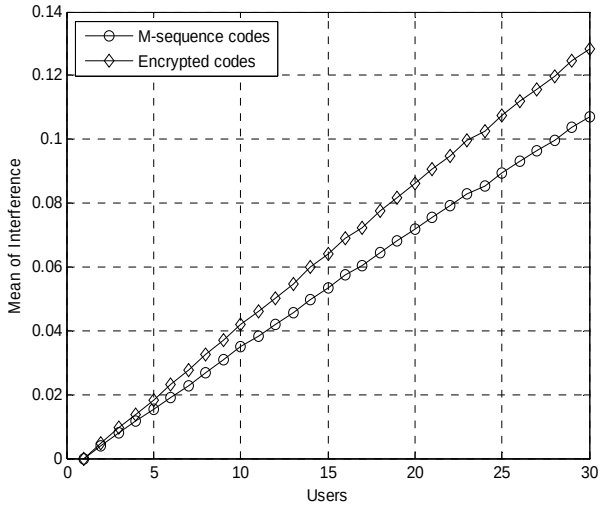

Figure 3. Comparing mean of interference M-sequence and encrypted codes in channel with 256 hop.

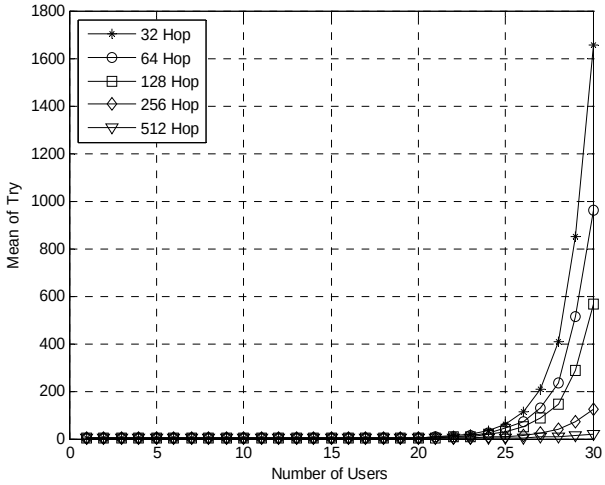

Figure 4. Calculation of mean try to access desired pair input-key with optimum interference.

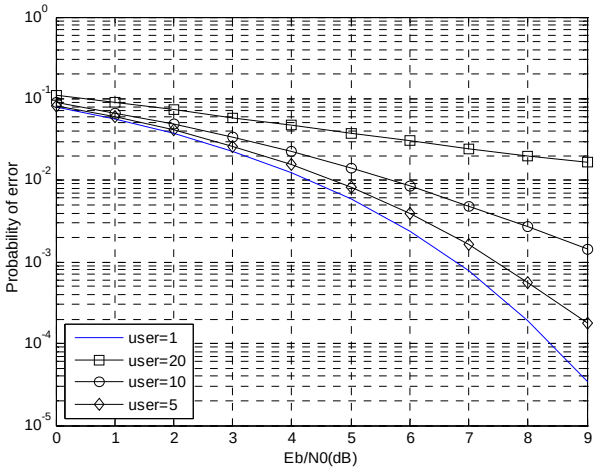

Figure 5. Probability of error for various number of users with 256 channel hop.

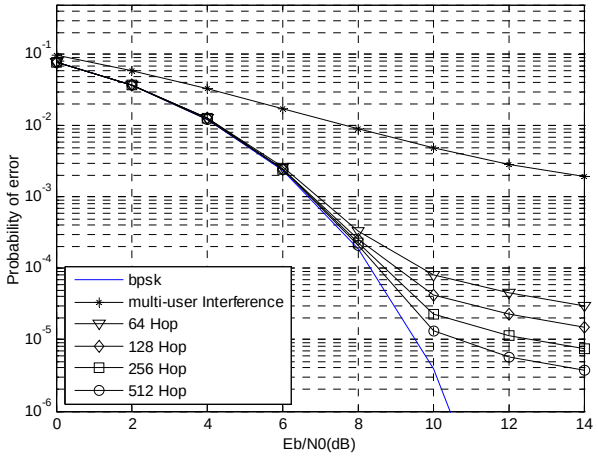

Figure 6. Probability of error for different channel hops in AWGN channel.

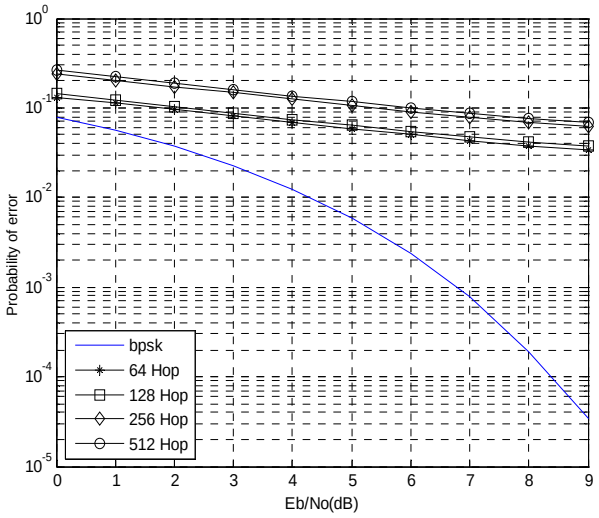

Figure 7. Comparing probability of error for M-sequence, encrypted and optimum encrypted code in 256 channel hop.

than unencrypted m-sequence codes and employing optimum method improves this value further.

Figure 8 represents the probability of decoding when wrong code is used. By comparing **Figure 6** with **Figure 8**, it's clear that if wrong codes are used, bit error rate becomes very high. In other words, if eavesdropper uses wrong code or key, it receives partial error frequency. To receive hidden frequencies, it must have access to a session key that victim transceiver employs.

5. Conclusions

A thorough investigation revealed security weaknesses of PN sequences. These drawbacks are challenged deploying a new method called hidden frequency hopping to augment the built-in security of FHSS systems. It is named hidden frequency hopping method since a known cryptographic algorithm is hidden within the PN codes.

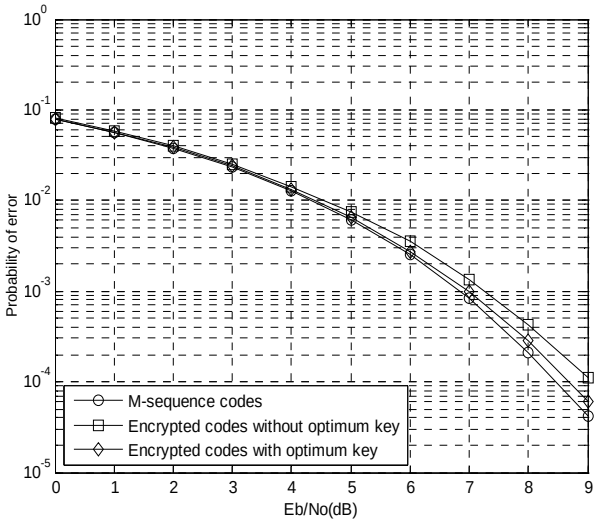

Figure 8. Uncertainty performance when a wrong key is inserted.

The jammer and transceiver signal hit occurrence in joint time hop period, the parameter α, is determined by analysis through the jammer and transceiver signalling start times. This value allows determination of the probability of the jamming signal colliding with the desired signal. It is found that, maximum value of α is reached when the jammer can determine the signalling start time to synchronize itself with the victim (a common un-encrypted method) and it is observed that with the proposed technique, the jammer can never reach maximum value to synchronize itself with the victim.

Simulation results show that when the proposed encrypted codes are utilized, the received channel interference increases. Naturally, this phenomenon makes the signal detection procedure more complex. Therefore, an optimum pair "key-input" algorithm is proposed to reduce the associated interference to the desired level. For instance, by employing codes with a good orthogonal behaviour, indeed, still algorithm can provide small amount of error but it also reduce the data transmission speed.

Furthermore, the performance of the encrypted FH/SS code is as good as unencrypted sequences when correct key is applied. When a wrong key is employed, system security is guaranteed.

6. Acknowledgements

Authors would like to thank the financial support of ITRC (Iran Telecommunication Research Company) for this project.

REFERENCES

[1] P. Zheng, L. Peterson, B. Davie and A. Farrel, "Wireless

Network Complete," Elsevier publisher, Amsterdam, 2009.

[2] Telecommunications Industry Association, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System," Telecommunications Industry Association, Arlington, 1998.

[3] M. Tafaroji and A. Falahati, "Improving Code Division Multiple Access Security by Applying Encryption Methods over the Spreading Codes," *IET Communication*, Vol. 1, No. 3, 2007, pp. 398-404. doi:10.1049/iet-com:20060295

[4] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Transactions on Information Theory*, Vol. 15, No. 1, 1969, pp. 122-127. doi:10.1109/TIT.1969.1054260

[5] I. Mansour, G. Ghalhoub and A. Quilliot, "Security Architecture for Wireless Sensor Networks Using Frequency Hopping and Public Key Management," *IEEE International Conference on Networking*, *Sensing and Control* (ICNSC), Delft,11-13 April 2011, pp. 526-531.

[6] V. K. Gray, "IS-95 CDMA and CDMA2000," Prentice-Hall, Upper Saddle River, 2000.

[7] J. K. Tugnait and T. Li, "Blind Detection of Asynchronous CDMA Signals in Multipath Channels Using Code-Constrained Inverse Filter Criteria," *IEEE Transactions on Signal Process*, Vol. 49, No. 7, 2001, pp. 1300-1309. doi:10.1109/78.928685

[8] J. Colic, "Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers, Information Security Research Centre," *EUROCRYPT'*95 *Proceedings of the* 14*th Annual International Conference on Theory and Application of Cryptographic Techniques*, Louvain-la-Neuve, pp. 248-262.

[9] X. Xu, "Blind Estimation of PN Code in Multipath Fading Direct Sequence Spread Spectrum Systems," 11*th IEEE International Conference on Communication Technology Proceeding*, Hangzhou, 10-12 November 2008, pp. 213-216.

[10] Q. Ling, T. Li and J. Ren, "Physical Layer Built-in Security Enhancement of DS-CDMA Systems Using Secure Block Interleaving," *Conference Record of the Thirty-Eighth Asilomar Conference on Signals*, *Systems and Computers*, Pacific Grove, 7-10 November 2004, pp. 1105-1109.

[11] L. Gang and A. Nakansu and M. Ramkumar, "Security and Synchronization in Watermark Sequences," 2002 *IEEE International Conference on Acoustics*, *Speech*, *and Signal Processing* (*ICASSP*), Orlando, 13-17 May 2002, pp. IV-3736-IV-3739. doi:10.1109/ICASSP.2002.5745468

[12] B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C," 2nd Edition, John Wiley & Sons, Hoboken, 1996.

[13] B. S. Kaliski, and L. Y. Yiqun, "On the Security of the RC5 Encryption Algorithm," RSA Laboratories Technical Report, Cambridge, 1998.

