ICWMMN2006 Proceedings

Rapid Long PN Sequence Acquisition Based on Fast Correlation Attacks*

Suling Wang, Hong Wen, Liang Zhou, Shumin Luo, Zhongpei Zhang

National Key Lab of Communication of UESTC, Chengdu 610054, China
E-mail: wang_suling@sina.com; {sunlike, lzhou}@uestc.edu.cn

Abstract: Fast correlation attacks algorithm (FCAA) is a well-known attacking method on stream ciphers. In this paper, we demonstrate that this method can be applied to PN sequence rapid acquisition as well. By this approach, we can acquire a long PN code with a short observation interval. To evaluate the performance of our method, we have performed some simulations. Simulation results show that the performance of FCAA search is close to that of iMPAs [3] search. This method is also significant in complexity reduction compared with full parallel search and serial search. Furthermore our approach needs not to extract the cyclic graphical models, so it can be applied to linear and nonlinear sequence acquisition.

Key words: Fast correlation attacks, PN sequence acquisition, iMPAs.

I. INTRODUCTION

The long period PN sequences are more desirable than the short one in spread spectrum technique applications to resist jamming or interception/detection. The very first step in the operation of a spread spectrum receiver is code acquisition and the long PN sequence acquisition is a critical necessity.

The most widely used and studied methods of PN acquisition are full parallel search, serial search [1], and hybrid search [2]. Full parallel search is the maximum-likelihood (ML) decision for the phase of the PN code based on a set of observations with the fastest speed but a relative more complex. Because the number of correlations needed in full parallel search is the period of the PN sequence, this method is infeasible for very long PN codes. Serial search is simple, but slow to acquire. Hybrid search provides a linear-scale tradeoff between these two extremes. M. Zhu and K. M. Chugg presented a new approach for the rapid PN code acquisition using iterative message passing algorithms（iMPAs）[3]. Although this approach provides suboptimal performance and significant complexity reduction, it must extract effective cyclic graphical models. However it is difficult to extract effective cyclic graphical models for many linear and nonlinear sequences and thus it makes a restriction to the application of iMPAs.

In this paper, we present a new method for achieving PN acquisition based on fast correlation attacks algorithm (FCAA)[4]. Our method is as fast as full- parallel search and the complexity and performance is very close to those of iMPAs acquisition. Furthermore, our approach need not use sparse graphical models, so it can be applied to linear and nonlinear sequence acquisition [5].

II. SYSTEM MODEL

In this paper, we will take linear feedback shift register (LFSR) sequences as example to show how the method of fast correlation attacks algorithm is applied to PN sequence acquisition.

A binary *r*-stage linear feedback shift register is shown in Fig.1. At time t, let y_t be the output, so that y_{t+i}, $0 \le i \le r-1$ is the value of the ith register and the constraint is

$$g_0 y_{t+r} \oplus g_1 y_{t+r-1} \oplus \cdots \oplus g_{r-1} y_{t+1} \oplus g_r y_t = 0 \qquad (1)$$

where $\oplus$ is modulo 2 addition and $g_i \in \{0,1\}, 0 \le i \le r$ are feedback coefficients. The *generating polynomial* is $g(y) = g_0 + g_1 y + \cdots + g_{r-1} y^{r-1} + g_r y^r$. The maximum achievable period of an *r*-stage LFSR is $N = 2^r - 1$ and is achieved for primitive $g(x)$ when the initial register contents $\boldsymbol{u} = (u_0, u_1, \cdots, u_{r-1})$, $u_i \in \{0,1\}$ are not all zeros.

The goal of code acquisition is to find the initial state $\boldsymbol{u}$ of the sequence presented in the received signal. In most practical scenarios with long PN codes, only part of this long

*This work is supported by the National Natural Science Foundation of China under Grant No. 60496313

sequence is observable, so the problem can be stated as: for a given number of M noisy observations $\boldsymbol{Z}=\{z_t\}$, $t=0,1,\cdots,M-1$ to estimate the initial state $\boldsymbol{u}$. A simplified model for these observations is

$$z_t=\sqrt{E_c}\,y_t(\boldsymbol{u})+n_t \tag{2}$$

where E_c is the signal energy per chip, $y_t(\boldsymbol{u})$ is the t-th output of the LFSR with initial state $\boldsymbol{u}$ and n_t is additive white Gaussian noise (AWGN) with zero mean and variance $N_0/2$. The model in (2) can be written in vector form as

$$\boldsymbol{Z}=\sqrt{E_c}\boldsymbol{Y}(\boldsymbol{u})+\boldsymbol{n} \tag{3}$$

where $\boldsymbol{n}=\left(n_0,n_1,\cdots,n_{M-1}\right)^T$ is a Gaussian vector with zero mean and covariance matrix $N_0/2\mathbf{I}_M$, where $\mathbf{I}_M$ is $M\times M$ the identity matrix.

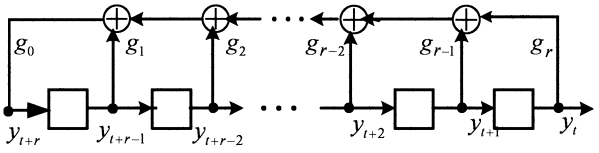

Fig.1. The generator diagram for an r-stage LFSR

III. ACQUISTION METHODS

Though the fast correlation attacks algorithm is an efficient stream cipher attacking algorithm, we can also view it as a decoding algorithm. The system model of fast correlation attacks acquisition is shown in Fig.2. We regard LFSR sequence $\boldsymbol{Y}(\boldsymbol{u})$ as input and $\boldsymbol{Z}$ as the corresponding channel output of $\boldsymbol{Y}(\boldsymbol{u})$. At the receiver, fast correlation attack algorithm is employed to obtain $\boldsymbol{Y}(\boldsymbol{u})$ and hence it recovers the initial state of LFSR.

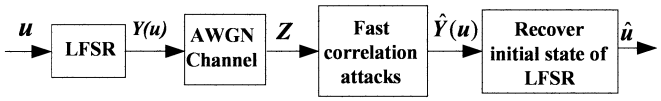

Fig.2. System model

For the purpose of reconstructing the LFSR-sequence $\boldsymbol{Y}(\boldsymbol{u})$ from $\boldsymbol{Z}$, the following principle[4] is essential to the algorithms: Every digit $y_t(\boldsymbol{u})$ of $\boldsymbol{Y}(\boldsymbol{u})$ satisfies several linear equations derived from the basic feedback relations, all of them involving l other digits of $\boldsymbol{Y}(\boldsymbol{u})$ if there are $l+1$ nonzero coefficients in $g(x)$. By substituting the corresponding digits of $\boldsymbol{Z}$ in these relations, we obtain a group of equations for each digit z_t, which may either hold or not hold. To test whether $z_t=y_t(\boldsymbol{u})$, we count the number of all equations that turn out to hold for z_t. Then the more of these equations hold, the higher the probability is for z_t to agree with $y_t(\boldsymbol{u})$. This can be justified by a statistical model, computing the corresponding conditional probabilities.

By iterating squaring of the generation polynomial, a variety of linear relations is generated for every digit $y_t(\boldsymbol{u})$. The average number M_n of relations obtained in this way can be computed as:

$$M_n=\log(M/2r)\times(l+1) \tag{4}$$

To give a more precise description we list the algorithm for BSC as follows:

Step 1: Determine M_n according to (4).

Step 2: Find the value of $h=h_{\max}$ such that $I(p,M_n,h)$ is maximum, where

$$\begin{aligned} I(p,M_n,h)=&\sum_{i=0}^{h}C_{M_n}^{i}(1-p)(1-S)^iS^{M_n-i}\\ &-\sum_{i=0}^{h}C_{M_n}^{i}pS^i(1-S)^{M_n-i}\end{aligned} \tag{5}$$

And $S=S(p,t)$ can be computed using the recursion

$$\begin{cases}S(p,t)=pS(p,t-1)+(1-p)(1-S(p,t-1))\\ S(p,1)=p\end{cases} \tag{6}$$

In (5), p is correlation probability which determined by BSC channel transition probability p_{ec} as:

$$p=1-p_{ec}, \tag{7}$$

Step 3: Initialize the iteration counter $i=0$.

Step 4: For every digit of $\boldsymbol{Z}$ calculate a new probability p^* for $z_t=y_t(\boldsymbol{u})$, given that h of M_n relations are satisfied.

$$p^*=pS^h(1-S)^{M_n-h}/(pS^h(1-S)^{M_n-h}+(1-p)(1-S)^hS^{M_n-h}) \tag{8}$$

Step 5: Calculate the thresholds P_{thr} and N_{thr}, where

$$\begin{cases}P_{thr}=\left(p^*(p,M_n,h_{\max}+1)+p^*(p,M_n,h_{\max})\right)/2\\ N_{thr}=U(p,M_n,h_{\max})\times N\end{cases} \tag{9}$$

where $U(p,M_n,h)$ is the probability that a digit z_t satisfies at most h of M_n relations,

$$U(p,M_n,h)=\sum_{i=0}^{h}C_{M_n}^{i}\left(pS^i(1-S)^{M_n-i}+(1-p)(1-S)^iS^{M_n-i}\right) \tag{10}$$

Step 6: Determine the number of positions N_w with $p^*<P_{thr}$. If $N_w<N_{thr}$ or $i<\alpha$, increase i and go to step 4.

Step 7: Make complement for those binary digits of $\boldsymbol{Z}$ with $p^*<P_{thr}$ and reset the probability of each digit to the original value p.

Step 8: If there exists digit of $\boldsymbol{Z}$ not satisfying the feedback relation then go to step 3.

Step 9: Terminate with $\boldsymbol{Y}(\boldsymbol{u})=\boldsymbol{Z}$.

IV. SIMULATION RESULTS

To evaluate the performance of our schemes, we have performed some simulations and compared the results of our approach with other three search methods over AWGN channel. We consider the m-sequence generated by an 15-stage LFSR with $g(y) = 1 + y + y^{15}$. The threshold for serial searches is determined using method in [1].

We do simulations with length M=256, M=512 and M=1024 respectively. As illustrated in Fig.3, when M=256, FCAA with 20 iterations provides approximately 0.4 dB degradation. From Fig.4 the improvement in E_c / N_0 for the FCAA to min-sum iMPA is about 0.5 dB when M=512 with 20 iterations, and more than 1 dB with 50 iterations. As observed in Fig. 5, when M=1024, FCAA with 20 iterations provides more than 0.5 dB improvement to min-sum iMPAs and about 0.8 dB with 50 iterations. It is reasonable to conclude that the length is longer, the performance of FCAA is better

V. CONCLUSIONS

In this paper, we have proposed a new approach for rapid pseudorandom long sequence acquisition using the method of fast correlation attacks. Simulation results show that fast correlation attacks performs close to that of iMPAs search method. Compared with full parallel and serial search, this approach also provides significant complexity reduction. Specifically our method suits not only for linear sequence acquisition, but also for nonlinear sequence acquisition. Furthermore our approach needs not to extract effective cyclic graphical models as in iMPAs search method.

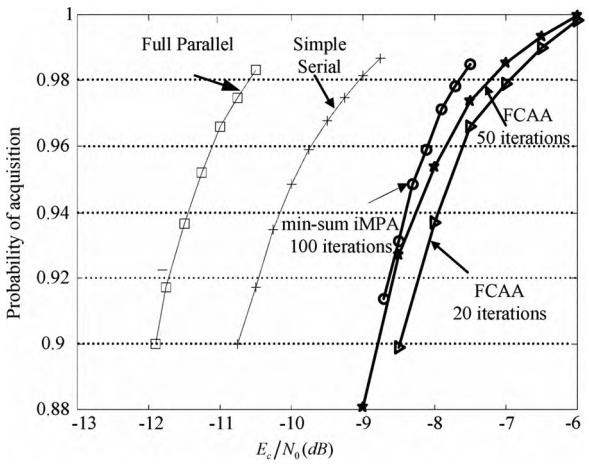

Fig.3. Comparison of acquisition performances of various approaches with $M = 256$ total observations

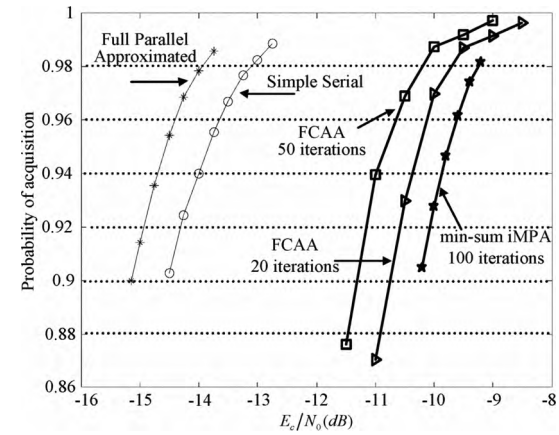

Fig.4. Comparison of acquisition performances of various approaches with $M = 512$ total observations

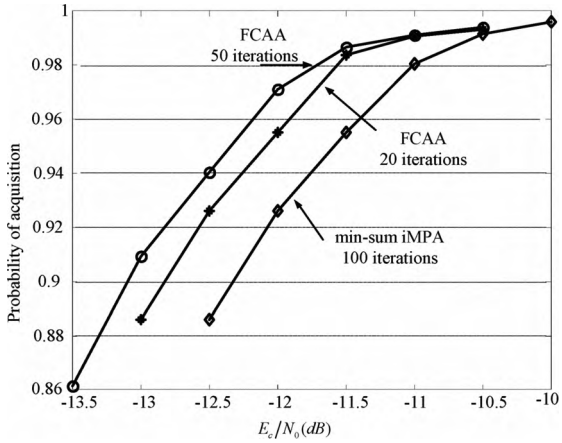

Fig.5. Comparison of acquisition performances of FCAA approaches with $M = 1024$ total observations

REFERENCES

[1] A.Polydoros and C. L. Weber, "A unified approach to serial search spread-spectrum code acquisition", *IEEE Trans. Commun.*, vol.32, NO.5, pp. 542-560, May 1984.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications Handbook. New York: McGraw-Hill, 1994.

[3] M. Zhu and K. M. Chugg, "A new approach to rapid PN code acquisition using iterative message passing techniques", *IEEE journal on selected areas in communications*, vol.23, NO.5, pp. 884-897, May 2005.

[4] W. Meier, and O. Staffelbach, "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, vol.1, 1989, pp. 159-176.

[5] Yang Li-zhen, Fu Xiao-tong, Xiao Guo-zhen and Chen Ke-fei, "Research on Correlation attacks on a nonlinear generator", Journal of Xidian University, Vol.28, No.5, pp. 566-568, Oct.2001.