Revisiting the Passive Synchronization Method for Frequency Hopping Systems

Ganesh Yellapu
Central Research Laboratory,
Bharat Electronics Limited,
Bangalore, India-560013.
Email: ganeshyellapu@bel.co.in

Abstract

In wireless communications, especially in military communications, frequency hopping is a technique to combat against jamming where the carrier signal switches among various frequencies very rapidly. For frequency hopping systems, in order to have a successful communication session, the nodes of a wireless network must be synchronized. In literature, a passive synchronization method was proposed which does not require to transmit any synchronization information over a fixed frequency channel. The method works by forming a system of linear equations whose solution reveals the synchronization information. However, the criteria used to form the system does not always ensure a unique solution and as a result, the synchronization of nodes is not ensured. In this paper, the criteria is refined to form a system that ensures a unique solution and therefore, synchronization of nodes is always ensured.

Key words: Frequency hopping, linear feedback shift register, linear span, passive synchronization, rank, system of linear equations.

1 Introduction

Two fundamental problems in secure wireless communications are eavesdropping and jamming (deliberate interference). One way to defeat eavesdropping is encrypting the transmission signal. However, this is not effective against jamming. In literature, spread spectrum modulation techniques are developed for secure communication in wireless networks, especially for networks in hostile environments, to ensure that the transmitted signals are not eavesdropped and not jammed. Frequency hopping (FH) spread spectrum is one among them.

In frequency hopping systems, the carrier signal switches over a set of frequencies very rapidly. These frequencies are called hopping frequencies. The switching is de-

termined by a pseudo-random sequence. In literature, linear feedback shift registers (LFSRs) are used to generate these pseudo-random sequences as they are extremely fast and easy to implement in hardware. The hopping frequencies are stored in a look-up table (also called hop table), look at Table-1, and a binary number, formed by the contents of specific stages of the LFSR, is used to select a frequency from the look-up table.

Table 1: Hop Table: H

0	1	2	$\cdots$	i	$\cdots$	$m-1$
f_0	f_1	f_2	$\cdots$	f_i	$\cdots$	f_{m-1}

In FH systems, in order to have a successful communication session, the pseudo-random number sequence generators of the nodes [1] of a network must be synchronized. Otherwise, it is obvious that the communication is not possible. In literature, this synchronization is accomplished by transmitting the synchronization information on a predetermined fixed frequency channel [1]. Such methods are called Active Synchronization methods. The main disadvantages of the Active methods are one explicit fixed frequency channel must be reserved and more importantly, eavesdroppers can easily monitor this channel and can jam it.

In [1], a passive synchronization method is proposed which does not require to transmit any synchronization information over a reserved fixed frequency channel. The method works as follows: a node wishing to synchronize can choose any frequency from the set of hopping frequencies and monitors for (one or more) valid transmissions on this frequency. Each valid transmission on this frequency reveals some information about the contents of the stages of the LFSR which are used to select the frequency from the look-up table. This information is used to form a system of linear equations whose solution reveals the synchronization information i.e., the contents of all stages of the LFSR. In general, a system of linear equations $AX = b$, where A is a $n \times n$ binary matrix, b is a binary column vector and X is the unknown binary vector to be found, has a unique solution if the matrix A has rank n, equivalently A must be invertible. However, the criteria used in [1] to form the linear system does not always ensure the rank of matrix A is n.

In this paper, the criteria is refined to form a linear system that always has a unique solution. The rest of the paper is organized as follows: in section-II, linear feedback shift registers are briefly discussed, in section-III, the passive synchronization method is revisited and described, in section-IV, the criteria used to form the system is refined and section-V concludes the paper.

[1] A node in a network is a device that is capable of sending and/or receiving data generated by other nodes on the network.

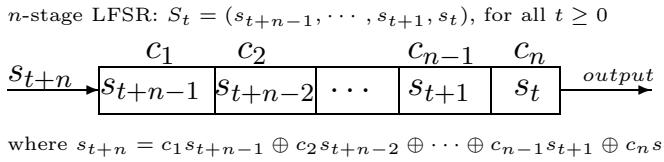

Figure 1: Linear feedback shift register

2 Linear feedback shift registers

A linear feedback shift register (LFSR) of length n [2], shown in Fig. 1, consists of n stages (or delay elements) numbered $0, 1, \ldots, n-1$, each is capable of storing one bit and, having one input and one output. At each clock, the following operations are performed:

1. the content of stage zero is output and forms part of the output sequence
2. the content of stage i is moved to stage $i-1$ for each i, $1 \leq i \leq n-1$ and
3. the new content of stage $n-1$ is the feedback bit s_i which is calculated by adding together modulo 2 the previous contents of a fixed subset of stages $0, 1, \ldots, n-1$.

These fixed subset of stages are determined by a polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$, called connection polynomial, of degree n where $c_i \in \{0, 1\}$. Clearly, maximum period of any output sequence of an LFSR of length n is $2^n - 1$. A pseudo-noise (pn) sequence is an output sequence of an n-stage LFSR with period $2^n - 1$. If $c(x)$ is a primitive polynomial of degree n over the field $\{0, 1\}$, the output sequence of the LFSR has period $2^n - 1$ for any nonzero initial state and the LFSR is called a maximum-length LFSR.

Given a LFSR with the connection polynomial $c(x)$ of degree n over $\{0, 1\}$, there is associated an $n \times n$ binary matrix L, called the state update matrix of the LFSR [3],

$$L = \begin{pmatrix} c_1 & c_2 & \cdots & c_{n-1} & c_n \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

For any $t \geq 0$, let $S_t = (s_{t+n-1}, s_{t+n-2}, \ldots, s_{t+1}, s_t)$ denotes the state of the LFSR at time t where $S_0 = (s_{n-1}, \ldots, s_1, s_0)$ is the initial state of the LFSR. Then,

$$S_t = L^t \cdot S_0^T, \forall t \geq 0$$

where L^0 is the $n \times n$ identity matrix, T represents the transpose of a matrix. In the passive synchronization method, the state update matrix L plays a prominent role.

Suppose the look-up table contains m frequencies $\{f_0, f_1, \ldots, f_{m-1}\}$ where the frequency f_i is stored in i^{th} location of the table for $i = 0, 1, \ldots, m-1$. Suppose $m = 2^n - 1$, for some n. Then, one can choose a maximum-length LFSR of length n to select frequencies from the table. Clearly, in one cycle of the LFSR, each frequency is selected exactly once. One problem with this method is, though m is large, (for example $m = 1023$, and hence $n = 10$), the hopping pattern is repeated very quickly. To overcome this, the table must contain huge number of frequencies, for example $m \geq 2^{16}$, which may not be feasible for concrete applications.

Suppose $m = 2^k$ for some k. In this case, an $n(> k)$-stage maximum-length LFSR can be used, and out of n stages, k stages of the LFSR can be designated to select the frequencies from the table. Clearly, in one cycle, each frequency is selected exactly 2^{n-k} times except f_0 which is at the table index zero and, the frequency f_0 is selected $2^{n-k} - 1$ times as a maximum-length LFSR does not visit the all-zero state. Further, if n is large, the hopping pattern will not be repeated quickly.

3 Revisiting the passive synchronization method

Consider a frequency hopping system that uses

1. $m = 2^k$ frequencies $\{f_0, f_1, \ldots, f_{m-1}\}$ stored in a table H such that $H[i]$ gives the frequency f_i for $i \in \{0, 1, \ldots, m-1\}$

2. a maximum-length LFSR of length n with the connection polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ of degree n.

Suppose out of n stages of the LFSR, k stages, numbered $i_0, i_1, \ldots, i_{k-1}$ where $i_* \in \{0, 1, \ldots, n-1\}$, are designated to select the frequencies from the table. For example, if the binary number formed by the contents of these k stages is denoted by i [2], the frequency $H[i] = f_i$ is selected from the look-up table.

Assume there is a node (call it as old node) in the network that is already transmitting some data. Suppose a new node is brought into the network. In order to communicate with the old node, the new node must be synchronized with the old node. Synchronizing the new node with the old node means, *at some time unit, the LFSR at new node must be initialized with the state of LFSR at the old node.* Once this is accomplished, both nodes are synchronized and hence, they can communicate to each other.

[2] Assuming i_0 as the least significant bit and i_{k-1} as the most significant bit

To achieve this, the passive method proposed in [1] forms a system of linear equations $AX = b$ (at new node) *whose solution reveals the state of the LFSR at old node at some time unit*. First, all elements of the coefficient matrix A and the vector b are set to zero. To form the system, the new node picks up a frequency from the table (does not matter which one) [1] and monitors for a valid transmission on this frequency. Suppose at time $t_0 + l_0$ where $l_0 = 0$, the first hit has occurred and, the state of the LFSR (at new node) at this time unit is denoted by $S_0 = (s_{n-1}, \ldots, s_{i_{k-1}}, \ldots, s_{i_1}, \ldots, s_{i_0}, \ldots, s_0)$. We call it as the initial state of the LFSR (at new node). Clearly, the first hit reveals the contents of the stages $i_0, i_1, \ldots, i_{k-1}$ of the LFSR (i.e., the binary values of $s_{i_0}, s_{i_1}, \ldots, s_{i_{k-1}}$) and helps in filling the k rows of the augmented matrix $[A, b]$ as below.

$$\begin{pmatrix} a_{0,0} & \cdots & a_{0,i_{k-1}} & \cdots & a_{0,i_1} & \cdots & a_{0,i_0} & \cdots & a_{0,n-2} & a_{0,n-1} \\ & & & & \vdots & & & & & \\ 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \\ & & & & \vdots & & & & & \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 & 0 \\ & & & & \vdots & & & & & \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 & 0 \\ & & & & \vdots & & & & & \\ a_{n-1,0} & \cdots & a_{n-1,i_{k-1}} & \cdots & a_{n-1,i_1} & \cdots & a_{n-1,i_0} & \cdots & a_{n-1,n-2} & a_{n-1,n-1} \end{pmatrix} \times \begin{pmatrix} s_{n-1} \\ \vdots \\ s_{i_{k-1}} \\ \vdots \\ s_{i_1} \\ \vdots \\ s_{i_0} \\ \vdots \\ s_0 \end{pmatrix} = \begin{pmatrix} b_{n-1} \\ \vdots \\ u_{i_{k-1}} \\ \vdots \\ u_{i_1} \\ \vdots \\ u_{i_0} \\ \vdots \\ b_0 \end{pmatrix} \quad (1)$$

where $u_{i_0}, u_{i_1}, \ldots, u_{i_{k-1}}$ are the contents of the stages $i_0, i_1, \ldots, i_{k-1}$ of the LFSR respectively. After the first hit, the LFSR at new node is updated at each time unit (i.e., after the first hit, at each time unit, LFSRs at both nodes are updated). Further, at each time unit t_0+l, for any $l > 0$, the state $S_l = (s_{l+n-1}, s_{l+n-2}, \ldots, s_{l+1}, s_l)$ of the LFSR at new node can be obtained as

$$S_l = L^l \cdot S_0^T$$

where $S_0 = (s_{n-1}, \ldots, s_{i_{k-1}}, \ldots, s_{i_1}, \ldots, s_{i_0}, \ldots, s_0)$ i.e., w^{th} row of L^l expresses $s_{l+n-1-w}$ as the linear combination of the bits of initial state, for all $w \in \{0, 1, \ldots, n-1\}$.

To fill the remaining rows of A, the new node monitors for some more valid transmissions on the same frequency. Suppose, the second hit occurs at time unit $t_0 + l_1$ where $l_1 > l_0 = 0$. Then at this time unit $t_0 + l_1$, once again contents of the stages $i_0, i_1, \ldots, i_{k-1}$ of the LFSR are revealed. Now, choose one row among the k rows of the matrix L^{l_1} corresponding to the stage numbers $i_0, i_1, \ldots, i_{k-1}$ that is satisfying the following criteria to fill the w^{th}-row of A (that is not yet filled):

1. it must not be identical with any of the non-zero rows of the incomplete coefficient matrix A

2. it must have a non-zero element at the w^{th}-column

Whenever a row, satisfying the above criteria, is found that is used to fill the w^{th}-row of the matrix A and the corresponding frequency selection bit is placed at w^{th}-row of the column vector b.

Suppose m^{th} hit occurs at time $t_0 + l_{m-1}$ where $l_{m-1} > \cdots > l_1 > l_0 = 0$ and after m^{th} hit, all rows of the augmented matrix $[A, b]$ are filled by using the above procedure. If this linear system of equations has unique solution, it can be solved using the gaussian elimination method to find the unknown initial state S_0 of the LFSR at new node. Observe that the state S_0 corresponds to the first hit which occurred at time $t_0 + l_0$ with $l_0 = 0$. Hence, $S_{l_{m-1}} = L^{l_{m-1}} \cdot S_0^T$ gives the state of the LFSR at time unit $t_0 + l_{m-1}$ and at this point, states of the LFSRs at old node and new node are identical. Thus the new node is successfully synchronized with the old node.

When the above criteria is used to fill the matrix A, it ensures that all rows of A are distinct and non-zero and, all diagonal elements of A are non-zero. The passive method in [1] believed that the matrix A formed by using this criteria has rank n. This may not be true. There are two problems in the passive synchronization method:

1. the coefficient matrix A formed by using the above criteria is not necessarily to have rank n. For example, the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

   has all distinct rows and all non-zero diagonal entries. However, rank of A is 2 as the last row is the linear combination of first two rows and hence, the matrix is not invertible.

2. if the new node monitors the frequency f_0 which is at the table index 0 (i.e., $H[0] = f_0$) then at each hit, the contents of the stages $i_0, i_1, \ldots, i_{k-1}$ of the LFSR are zero. This yields the linear system $AX = 0$. Hence, when the rank of A is n, we have the all-zero solution for the unknown initial state S_0 and when the rank of A is less than n, more than one solution is exist for S_0. In both cases, synchronization is not assured.

In next section, the above criteria is refined in order to have a unique non-zero solution for the system $AX = b$ where b is a non-zero (column) vector.

4 Refined criteria to form the system of linear equations

It is apparent that the new node must not choose the frequency f_0 which is at the table index zero to monitor. Instead, it can choose any other frequency from the

table. It ensures that b is always a non-zero vector as the contents of *all* k *stages* $i_0, i_1, \ldots, i_{k-1}$ of the LFSR are considered for the first hit.

Clearly, after the first hit, the filled k rows of A are linear independent. The notion behind filling the remaining rows of A is, whenever a subsequent hit occurs, choose a row from the matrix L^l, where $l > 0$, corresponding to one of the stage numbers $i_0, i_1, \ldots, i_{k-1}$ that is not in the linear span of the filled non-zero rows of A. However, in general, generating the linear span of a given set of n dimensional vectors over $\{0, 1\}$ and ensuring that a vector is not in that linear span is computationally intensive which is not feasible in concrete applications.

For this reason, to form the coefficient matrix A, the following criteria is used. Suppose r rows of the matrix A are successfully filled with r linearly independent vectors (for example, after the first hit, k rows of A are filled and, these k rows are clearly linearly independent). Then $n - r$ rows of A are yet to be filled and denote the indices of these rows by $w_0, w_1, \ldots, w_{n-r-1}$. Now, choose a row from the k rows of the matrix L^l, where $l > 0$, corresponding to the stage numbers $i_0, i_1, \ldots, i_{k-1}$ to fill the w_j^{th}-row of A that is satisfying the following criteria:

1. the row must have a non-zero element in the w_j^{th}-column.
2. the row must have zeros at columns $w_0, w_1, \ldots, w_{j-1}, w_{wj+1}, \ldots, w_{n-r-1}$.

This procedure is repeated until all rows of the matrix A are filled. When all rows of A are filled, the refined criteria ensures not only all diagonal elements of A are non-zero but also rank of A is n and therefore, the system $AX = b$ always has a unique solution. The solution can be found by using the gaussian elimination method.

Although existence of the matrix A is not discussed (i.e., in one cycle of the LFSR, whether all rows of A can be filled since the time unit $t_0 + l_0$), during simulations, it has been observed that the matrix A is found very likely for $n \leq 16, k = 4, 5, 6, 7$.

5 Conclusion

The passive synchronization method for frequency hopping systems has been revisited and described. The passive method works by forming a system of linear equations whose unique solution reveals the synchronization information. As the criteria used to form the system of equations does not always ensure a unique solution, the criteria is refined. Hence, once the system of equations is formed using the new criteria, the system always has a unique solution and the synchronization of nodes is always ensured.

References

[1] P. E. Atlamazoglou and N. K. Uzunoglu, "A passive synchronization method for frequency hopping systems," *Journal of Applied Mathematics & Bioinformatics*, vol. 3, no. 1, pp. 151–161, 2013.

[2] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. CRC Press, 1996.

[3] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. New York, NY, USA: Cambridge University Press, 2004.

[4] J. Huovinen, T. Vanninen, and J. Iinatti, "Demonstration of synchronization method for frequency hopping ad hoc network," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, Nov 2008, pp. 1–7.