Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 151-161
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

A Passive Synchronization Method for Frequency Hopping Systems

Prodromos E. Atlamazoglou[1] and Nikolaos K. Uzunoglu[2]

Abstract

Frequency Hopping is a modulation technique where the signal is repeatedly switching frequencies during communication, minimizing thus the probability of jamming and detection. A major challenge encountered in the design of Frequency Hopping Systems is the achievement of synchronization between spatially separated communication nodes. In the open literature, this challenge is addressed by transmitting synchronization data on a fixed frequency channel,a technique vulnerable to eavesdropping and interference. In order to address this vulnerability, a Passive Synchronization method is presented that does not require the broadcasting of any information about the current state of the frequency hopping system. The proposed method is based on monitoring one of the system frequencies by the stations not yet synchronized. Using the detection of valid transmissions on this frequency, the time intervals between them are measured. Capitalizing on the information gathered

[1] Infrastructure Directorate, Hellenic Army General Staff, Athens, Greece, e-mail: prodrom@central.ntua.gr

[2] Department of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece, e-mail: nuzu@cc.ece.ntua.gr

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
Published online : March 30, 2013

this way, a Boolean linear system of equations is formulated, with unknowns that directly correspond to a specific position in the period of the hopping pattern. This system is then solved using a Boolean version of the Gaussian Elimination numerical solution technique.

Mathematics Subject Classification: 94A55, 94A60
Keywords: Synchronization; Frequency Hopping; Boolean Algebra; LFSR

1 Introduction

The fundamental weakness of conventional fixed frequency wireless communications lies in the fact that the transmission medium (free space) is equally accessible to both allied and enemy forces. This makes them vulnerable to both interception and jamming. Interception is the unauthorized monitoring of radio traffic, whereas jamming is the deliberate disruption of communication by operating a transmitter (jammer) on the same frequency as the legitimate radio traffic. Whilst encryption [1] may provide some degree of resistance to the threat of interception, it is obviously ineffective against jammers. This was the motivation behind the development and adoption of the Frequency Hopping Technique, which constitutes the only effective counter measure to both interception and jamming.

Frequency Hopping was first employed during the Cuban Crisis and it is nowadays implemented even in the 802.11b protocol (Wi-Fi) where it enables the operation of more than one wireless networks in the same area. It is a modulation technique where the signal is repeatedly switching frequencies during communication.

The order, in which the hopping system transmits in the frequencies available to it, must ensure that every frequency is being used in a balanced way. Furthermore this order must not be obvious to eavesdroppers. It must appear random while being totally deterministic. In other words it must be pseudorandom.

Many methods exist for the generation of pseudorandom sequences, but the most popular is the use of Linear Feedback Shift Registers. LFSRs are simple, easy to construct circuits made up from Flip-Flops connected in line and clocked by the same time source. At each pulse of this source, the contents of each Flip-Flop shift to the one placed to the right of it. The first Flip-Flop in the line is filled with the result of a Boolean Function (usually XOR) with inputs the contents of some of the inner Flip-Flops. This constitutes the Feedback mentioned in the name of these circuits. LFSRS offer excellent pseudorandomness in their output, and that is why they are typically employed as structural elements in stream cipher cryptography [2]. Frequency Hopping systems use the binary number formed by the contents of a specific subset of the registers of an LFSR to select with the help of a lookup table the frequency for transmission at each hop.

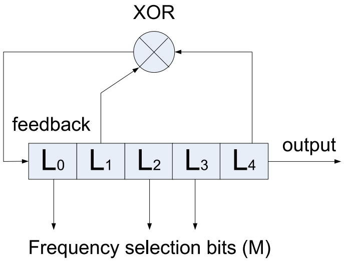

Figure 1: Linear Feedback Shift Register

For the Frequency Hopping systems to function correctly, it is essential that the pseudorandom generators of the various communication stations are completely synchronized to each other. Otherwise, it is obvious that communication is impossible. But it is evident that the synchronization of pseudorandom generators in distant stations, that most probably have started functioning at different times, is far from a trivial task.

In open literature the way this synchronization is achieved is based on the transmission of synchronization signals on a predetermined fixed frequency channel [3]. These are the so called Active Synchronization methods. In these methods, the transmitter sends out a beacon frame to announce its presence. This frame has a timestamp, along with sync field (alternating zero one sequence) that provides the transmitter clock value. The Receiver after accepting the timestamp and adding a small offset value for transmission delay, adjusts its own timer to coincide with the transmitter.

The Active synchronization methods although widely used, are characterized by several disadvantages. Among these is the requirement for an additional non-hopped channel, the need for establishing universal system time, the fact that they are extremely time consuming and that they even consume bandwidth. But the most important of these shortcomings is the fact that transmitting the synchronization signals in a fixed frequency channel, essentially reduces the security offered by Frequency Hopping. This is because eavesdroppers can easily monitor this fixed channel, and jam it or even transmit their own fake sync signals in an active attack scenario, making legitimate synchronization impossible.

The method proposed in this paper doesn't require the transmission of any synchronization signal. That's why we call it a Passive Synchronization method and the reason it doesn't suffer from any of the shortcomings of the Active Methods mentioned in the previous paragraph.

According to the proposed method, each station wishing to synchronize has to monitor one of the hopping frequencies (doesn't matter which one) and record the temporal distances between detecting valid transmissions using it.

When the station has collected sufficient information from this monitoring, it processes the gathered data mathematically in a way that will be described in the following section, and deduces the current contents of the LFSR used by the transmitting station. From that moment on, synchronization has been achieved and the receiver can accept as well as send messages without any problem.

2 Description of the Method

We consider a Frequency hopping system that uses as a pseudorandom generator an LFSR with N registers. M of these are used for frequency selection. They are those with indices J_k, where $k = 0, ..., M - 1$. The contents of these registers that correspond to the selection of the frequency monitored by the proposed method are $F_k = L_{Jk}(t_H)$. The times that we detect valid transmissions in this frequency are denoted by t_H and we call these detections hits. The indices of the registers used for feedback are given by R_P, where $p = 0, ...D-1$. D is the number of the registers that participate in the feedback operation.

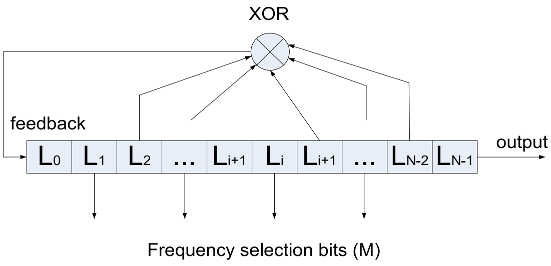

Figure 2: LFSR with N registers and M frequency selection bits

If initially we fill the registers of the LFSR with $L_i(0)$, $(i = 0, \ldots, N-1)$, the temporal evolution of its contents can be seen on Table 1. At time step 1, the content of each register shift to one on its right, while the first register is being fed the XOR of the D registers with indices R_P, where $p = 0, ...D-1$. The remaining lines of the table are filled in a similar way.

Table 1: Contents of the LFSR at consecutive time steps

time step	$L_0(t)$	$L_1(t)$	$L_2(t)$	$\ldots$	$L_{N-1}(t)$
0	$L_0(0)$	$L_1(0)$	$L_2(0)$	$\ldots$	$L_{N-1}(0)$
1	$\bigotimes_{p=0}^{D-1} L_{Rp}(0)$	$L_0(0)$	$L_1(0)$	$\ldots$	$L_{N-2}(0)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
t_{H1}	$\bigotimes_{p=0}^{D-1} L_{Rp}(t_{H1}-1)$	$L_0(t_{H1}-1)$	$L_1(t_{H1}-1)$	$\ldots$	$L_{N-2}(t_{H1}-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
t_{H2}	$\bigotimes_{p=0}^{D-1} L_{Rp}(t_{H2}-1)$	$L_0(t_{H2}-1)$	$L_1(t_{H2}-1)$	$\ldots$	$L_{N-2}(t_{H2}-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$

The combination of the contents of the frequency selection registers, that correspond to the selection of the monitored frequency, occurs for the first time at time step t_{H1}, (first hit) and then again at time t_{H2}, (second hit). Many more reappearances of this combination will take place in subsequent time steps.

The information contained in Table 1, is fully available only to the transmitter and the already synchronized with it receivers. The non synchronized receivers know considerably less.

What these receivers actually know can be seen at Table 2. Initially they only know the contents of the LFSR assigned for frequency selection at the time steps when a valid transmission is detected in the monitored frequency. If all the contents of all the LFSR were known for all time steps, the prdiction of the frequency used at any moment would be a trivial issue, and the receiver possesing this knowledge would be already synchronized.

Table 2: The view from the side of a station that attempts to synchronize

time step	…	$L_{J0}(t)$	…	$L_{JM-1}(t)$	…
0	…	?	…	?	…
1	…	?	…	?	…
$\vdots$		$\vdots$		$\vdots$	
$t_{H1}-1$	…	-	…	-	…
t_{H1}	…	F_0	…	F_{M-1}	…
$t_{H1}+1$	…	-	…	-	…
$\vdots$		$\vdots$		$\vdots$	
$t_{H2}-1$	…	?	…	?	…
t_{H2}	…	F_0	…	F_{M-1}	…
$t_{H2}+1$	…	?	…	?	…
$\vdots$		$\vdots$		$\vdots$	

But contrary to what one might suppose, what a not yet synchronized receiver, really needs to know is much less than the period of the output of the LFSR times the number of the frequency selection registers. This is because of the way a LFSR is structured and functions, if the contents of all of its registers are known for only one time step, then it is trivial to compute its contents for any other time step preceding or following it. Thus the real number of unknowns is N. All the remaining unknowns in Table 2 are dependent on these and can be computed from them if necessary in a completely deterministic way.

From what we just mentioned it becomes clear that it doesn't really matter for which time step the contents of the LFSR are chosen as unknowns. But while all the time steps are mathematically equivalent, it is more convenient to pick one of the time steps for which a valid transmission on the monitored frequency is detected. The reason for this is that in this way some of the equations of the system needed to be solved for finding the unknowns are easier to formulate. That's why in the proposed method we use as unknowns the contents of the LFSR at the instance of the first detection of valid signal on the monitored frequency (first hit).

In order to find the N unknowns an algebraic system of N equations is needed. The $N \times N$ coefficient matrix of the system is denoted by A, the vector of unknowns by H and the right hand side vector by b.

$$H_k = L_k(t_{H_1}), k = 0, \ldots, M-1 \tag{1}$$

$$[A] \cdot [H] = [b] \tag{2}$$

$$\begin{bmatrix} A_{00} & \ldots & A_{0(N-1)} \\ \vdots & & \vdots \\ & \ddots & \\ \vdots & & \vdots \\ A_{(N-1)0} & \ldots & A_{(N-1)(N-1)} \end{bmatrix} \cdot \begin{bmatrix} H_0 \\ \\ \vdots \\ \\ H_{N-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ \\ \vdots \\ \\ b_{N-1} \end{bmatrix}$$

Thanks to the convenient selection of unknowns, the first M equations are very easily found. For formulating them one just need to equate the unknowns corresponding to the frequency selection registers to their contents when the monitored frequency is selected. By expanding these simple equations (using zero coefficients for the remaining unknowns), we get the following M equations of M unknowns each. Substituting them to the lines of the system corresponding to the frequency selection registers we get

$$H_{Jk} = L_{Jk}(t_{H_1}) = F_k, k = 0, \ldots, M-1 \tag{3}$$

$$\{H_{J0}, \ldots, H_{JM-1}\} = \{L_{J0}(t_{H_1}), \ldots, L_{JM-1}(t_{H_1})\} = \{F_0, \ldots, F_{M-1}\} \tag{4}$$

$$H_{J0} = F_0 \Rightarrow 0 \cdot H_0 \oplus \cdots \oplus 1 \cdot H_{J0} \oplus \cdots \oplus 0 \cdot H_{N-1} = F_0 \tag{5}$$

$$\vdots \tag{6}$$

$$H_{JM-1} = F_0 \Rightarrow 0 \cdot H_0 \oplus \cdots \oplus 1 \cdot H_{JM-1} \oplus \cdots \oplus 0 \cdot H_{N-1} = F_{M-1} \tag{7}$$

$$\begin{bmatrix} A_{00} & \ldots & A_{0J0} & \ldots & A_{0J(M-1)} & \ldots & A_{0(N-1)} \\ & \ddots & & & & & \\ 0 & \ldots & 1 & \ldots & 0 & \ldots & 0 \\ & & & \ddots & & & \\ 0 & \ldots & 0 & \ldots & 1 & \ldots & 0 \\ & & & & & \ddots & \\ A_{(N-1)0} & \ldots & A_{(N-1)J0} & \ldots & A_{(N-1)J(M-1)} & \ldots & A_{(N-1)(N-1)} \end{bmatrix} \cdot \begin{bmatrix} H_0 \\ \vdots \\ H_{J0} \\ \vdots \\ H_{JM-1} \\ \vdots \\ H_{N-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ \vdots \\ F_0 \\ \vdots \\ F_{M-1} \\ \vdots \\ b_{N-1} \end{bmatrix}$$

We are missing $N - M$ more equations, $N - M$ more lines of the system.

Finding these is considerably more complex. What needs to be done, is to express the contents of the registers of the LFSR for the time steps following the first hit (t_{H1}), as functions of the (unknown) contents of the LFSR for that first hit. In other words, to express them as functions of the N unknowns of our system. So at time step $t_{H1}+1$, the content of the 1st register of the LFSR is

$$L_0(t_{H1}+1) = \bigotimes_{p=0}^{D-1} L_{Rp}(t_{H1}) = \bigotimes_{p=0}^{D-1} H_{Rp} = H_{R0} \otimes \cdots \otimes H_{RD-1}. \tag{8}$$

The contents of the remaining registers for time step $t_{H1}+1$ are found by shifting to the right the contents of the registers of time step t_{H1}.

$$L_i(t_{H1}+1) = L_{i-1}(t_{H1}) = H_{i-1}, i = 1, \ldots, N-1. \tag{9}$$

The contents of the LFSR for the subsequent time steps $(t_{H1}+1, t_{H1}+2, \ldots)$, are found in a similar manner by expressing them using binary logical operations as linear functions of the original unknowns (H_i). In this way we arrive at time step t_{H2}, when the second hit is detected.

$$L_0(t_{H2}) = L_0(t_{H1}+t_d) = \bigotimes_{p=0}^{D-1} L_{Rp}(t_{H2}-1) = f_0(H_0, \ldots, H_{N-1}). \tag{10}$$

$$L_i(t_{H2}) = L_i(t_{H1}+t_d) = L_{i-1}(t_{H2}-1) = f_i(H_0, \ldots, H_{N-1}), i = 1, \ldots, N-1. \tag{11}$$

For this new hit (t_{H2}), we know once more the contents of the registers of the LFSR that are employed for frequency selection. So if we equate the expressions of these contents in terms of the original unknowns, to the pattern corresponding to the selection of the monitored frequency, we get M new equations with the same N unknowns.

We select those that are not identical to the equations we already have (meaning they are linearly independent of them) and place them in the lines of the system that are unknown to us. This placement is done in a way, that the diagonal elements of the coefficient matrix are always non-zero, so that this matrix is invertible and the associated linear system solvable.

When (after N/M hits) we have N equations for our N unknowns, we can use the Gaussian Elimination numerical method for solving linear systems will be used adapted for the Boolean algebra. The details of this adaptation lie beyond the scope of this short paper, but suffice it to say that multiplication is substituted by the logical operation AND, and addition by XOR.

In order to fill in a systematic way the matrices of the linear system of equations required by the proposed method, the following technique is used. First all the elements of the coefficient matrix and the right hand side vector are set to zero.

The filling of the elements (assembly) of the matrices of our system will take place in stages. M lines at a time. At each stage we can check if a line has been filled, by looking at its diagonal element (that is the one with equal column and line indices). If this is non-zero then the line is already filled (from a previous stage). Otherwise it isn't, as the diagonal elements of the coefficient matrix of the system are not allowed to be zero.

After the first hit, (t_{H1}) we get our first M Boolean equations. They are the ones resulting from equating the contents of the frequency selection registers with the bits corresponding to the monitored frequency.

This way, we can fill M lines of the coefficient matrix and M elements of the right hand side vector. At the M elements of the right hand side vector we place the bits corresponding to the monitored frequency, while at the lines of the coefficient matrix A with indices those of the frequency selection registers we set their zero diagonal elements to 1. All other elements remain zero.

In order to track the evolution in time of the correlations of the unknown contents of the LFSR, we introduce a auxiliary matrix. Denoted by C, it is a binary $N \times N$ matrix.

Initially all of its elements are set to zero. Then at the time step after the first hit we fill with 1s the elements of the first line with column indices equal to the indices of the registers that are employed in the feedback of the LFSR. At the remaining lines (after the first) we put ones at their pre-diagonal elements (those with column index equal to their line index minus one). In this way we encode in binary the operation and function of the LFSR. The first line of the auxiliary matrix encodes the feedback operation, while the rest encode the shifts to the right.

The lines after the first are filled with the contents of the previous time step for the line situated above them. It is obvious how this encodes the shifts to the right of the contents of the LFSR. In order to avoid errors, this change must start from the bottom line and work its way up to the second (that will be filled with the contents of the first line from the previous step, which must be temporarily stored before the application of the aforementioned changes).

In the steps that follow the transformation of the contents of the auxiliary matrix take place in the following way: The contents of the first line are substituted by the results of the XOR of the corresponding elements of the lines with indices those of the registers that are employed in the feedback. In that way we continue to encode in binary the process of feedback for the steps that follow that of the first hit (t_{H1}).

Then when we detect again another hit, then and only then from the M lines of the matrix C with indices those of the frequency selection registers, we choose the ones that fulfill the following criteria:

- They are not identical with any of the already nonzero lines of the incomplete coefficient matrix A (those with non-zero diagonal element). In this way we ensure that the equations of our system will be linearly independent.

- The chosen lines must have a non-zero element on a column with index equal to the line index of a zero line of the incomplete A. This criterion guarantees that the A matrix will have non-zero diagonal elements and our system will be solvable.

When the above three criteria are satisfied we take the lines that satisfy them and we place them at the positions of the zero lines of the incomplete A, ensuring that each new line will go in such a position that its diagonal element will be non-zero. This is what the second criterion makes possible.

When using the above criteria, we choose a line from C (let that be the line i), in order to place it at the position of the line j of the incomplete A, then we also take the content of the corresponding frequency selection bit and place it at the position of the element of the incomplete right hand side b with index j.

In this way we assemble the coefficient and the right hand side matrices of our system, and after N/M hits the matrices of our system will be complete.

3 Conclusion

The proposed method is simple easy to implement, efficient and offers speed, accuracy and above all security as it does not require a fixed frequency synchronization channel.

An additional advantage of the method that we have presented is that it allows to a central station to choose which peripheral stations will be receiving a certain message and which will be excluded. This can be done by assigning a different monitored frequency to each peripheral station, and when one station doesn't need or shouldn't read a certain transmission the central station will not use this particular frequency in its hops. Then the temporarily excluded station won't be able to synchronize.

References

[1] B. Schneier, *Applied Cryptography*, John Wiley & Sons, 1996.

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

[3] J. Huovien, T. Vanninen and J. Iinatti, Demonstration of synchronization Method for Frequency Hopping Ad Hoc Network, *Proceedings of the 2008 IEEE Military Communications Conference*, (MILCOM 2008), (2008), 1794–1800.