A Novel Frequency Hopping Scheme for Secure and Reliable Communication Systems

Wassim Itani[a], Ayman Khalil[b], Diana Sidani[c], Lina Agha[d]
[a] Department of Computer and Communications Engineering, RHU, Meshref Lebanon
wassim.itani@hotmail.com
[b] Associate Professor, Department of Computer and Communications Engineering, RHU, Meshref Lebanon
khalilah@rhu.edu.lb
[c] Department of Computer and Communications Engineering, RHU, Meshref Lebanon
diana_sidani@hotmail.com
[d] Department of Computer and Communications Engineering, RHU, Meshref Lebanon
linaagha@live.com

Abstract. Societies nowadays are far more dependent on technology mediated communication than before. The increasing importance of information and communication has brought with it an attempt by the military and other powerful organizations to maintain their dominance by asserting control over communication. Secure communication has grown to be vitally important (ictregulationtoolkit.org).
This paper studies a novel frequency hopping schema that assures secure transmission of real and non-real data transmission. The paper proposes the usage of chaotic functions, logistic mapping and tent mapping, in addition to matrix operations in order to define hopping sequences. A tree algorithm is used in order to combine the above generated frequencies. The paper proposes a novel system that increases the complexity of existing algorithms and makes it very hard to predict using a frequency analyzer. The paper forms a solid ground to a secure Radio Frequency (RF) communication that can be used in real-life applications that seek security in their communications such as military applications.

Keywords: Secure Transmission, Radio Frequency Systems, Chaotic Frequency Hopping, Tent Mapping, Logistic Mapping, Tree Algorithm.

1. Introduction

1.1 General Background

Frequency hopping is the easiest spread spectrum modulation to use. Frequency hopping spread spectrum (FHSS) divides the existing frequency band into a chain of small sub channels. In general, frequency hopping is a radio transmission technique where the signal is divided into multiple parts and then sent across the air in random pattern of hopping frequencies.

Generating the FH sequence is one of the key technologies of FH communication systems. The FH sequence must have several properties in order to be categorized as a good sequence.

In military use, frequency hopping provides great protection against eavesdropping. Moreover if the communication is using spread spectrum frequency hopping provides an anti-jamming solution (Komo andSoutheastcon 1989).

In civilian use, frequency hopping is used in the unlicensed bands declared by the Federal Communication Commission (FCC), which are 900MHz and 2.4GHz. Frequency hopping is used by many devices such as walkie-talkies, and some radio services such as eXtreme Radio Service (eXRS) (wikipedia.org).

In commercial communication systems, frequency hopping is used in applications such as "Bluetooth" technologies and ultra-wideband (UWB) communication systems.

1.2 Problem Statement

Whether using the basic sequences, which mostly use linear functions, or using chaotic sequences, one is not able to attain high level of security. Basic sequences are easily discovered using linear functions. Using chaotic sequences allows the user to increase the complexity of the system, yet with the development of computation technology as well as nonlinear theory, the reconstruction of these sequences became possible. This leads to exposing the sequence to eavesdropping and eliminating the security of the system. Moreover, it is known that chaotic sequences, along with some none chaotic sequences, are sensitive to initial conditions. Therefore, choosing the right initial values allows one to add more security to the system.

Statement: the problem of present sequences lies in the ability of reconstructing the whole sequence from a partial sequence, thus allowing the prediction of upcoming frequency hopes after a certain time. The presence of one function, whether basic or chaotic, is a main factor to this problem.

2. Survey of Existing Studies

2.1 Introduction

Johannes Zenneck's book *Wireless Telegraphy* (German, 1908, English translation McGraw Hill, 1915) was possibly the earliest mention of frequency hopping in the open literature. Nowadays, several frequency hopping sequences are implemented in variable systems, these sequences are categorized into chaotic and none chaotic sequences.

2.2 Basic Sequences (None Chaotic):

2.2.1 M-Sequence

The M-Sequences have been widely used in many areas such as telecommunication, cryptology, navigation and radar. It is one way to achieve frequency-hopping sequences having acceptable random properties and good autocorrelation properties (Komo and Southeastcon 1989).

2.2.2 Reed-Solomon Sequence

On January 21, 1959, Irving Reed and Gus Solomon proposed a paper to the Journal of the Society for Industrial and Applied Mathematics (Wicker and. Bhargava 1994). In the last half of the twentieth century, Reed-Solomon codes have been an essential element of the telecommunications revolution.

2.2.3 Bent Sequence (Kumar 1988)

In the mathematical field, a bent function is a special type of Boolean function. . In frequency-hopping spread-spectrum multiple-access communication systems, bent functions and sequences have good Hamming correlation properties and large period, and are also derived from sequences having large linear span.

The problem in the above three sequences is that they have low complexity and poor security. It is easy to reconstruct such systems using linear functions and algorithmic relations. Thus these sequences cannot be used in systems that require very high level of security. Moreover, these sequences having short linear span are potentially weak when the threat of intelligent jamming exists.

2.3 Chaotic Sequences (Xiangdong Liu, Xiqin He, Xueye ANG, Nan Jiang 2011)

This is more secure than non-chaotic sequences and thus it is adapted by modern military communication systems and civilian multiple access mobile communication. It has many advantages; one of them is that it has a very low probability of intercept.

One of the key challenges of FH is generating good FH sequences. The sequence should have a complex structure and long period to make it difficult to repair whole sequence from any partial sequence. To overcome the limitations of non-chaotic sequences, chaotic systems are used to construct large number of wide spectrum sequences in a number of ways efficiently due to their sensitivity to initial conditions. Chaotic methods have become well-known and adapted methods for generating spreading spectrum sequences and frequency hopping sequences. Overall, there are strong nonlinear relationships between the conditions of chaotic sequences, and they are too complicated to predict by linear method, this is the origin of chaotic secret communications. After the extreme development in communication, some efficient nonlinear methods are developed to restore whole chaotic sequences from any partial sequences, such as phase space reconstruction.

3. Requirements and Simulation Study

3.1 Introduction

The design of the proposed system is formed of two main parts, the functions and the algorithm. These two parts are side by side responsible to form the frequency generator, which defines the frequencies and hopping sequence to be used. Along with these two main parts the choosing of variables for the functions is an essential subpart to be discussed.

3.2 Functions

Linear functions are widely used to generate the frequencies, a good example of these functions are the m/M sequence function, Bent sequence function, Reed-Solomon sequence function, etc… Yet these functions are easy to predict using linear algorithms thus providing the whole sequence from partial sequence; this leads to the rise of the importance of chaotic functions. In this system there is not one function applied, but several functions, in order to assure the security of the system. This study uses the logistic mapping and tent mapping chaotic functions along with a novel matrix operation named DWL.

Figure 1: The time series and staircase diagram for logistic map where r equal to 4

3.2.1 Logistic Mapping

The logistic mapping has the following equation (wikipedia.org):

$$x_{n+1} = r x_n (1 - x_n)$$

X_n is the mapping between zero and one; X_0 is the initial condition;

n is the number of iterations;

r is the positive number that defines the function;

Behavior (Wiens)

The behavior of the logistic map depends mostly on one factor "r". Note that the function's outcome varies significantly when a slight change in the initial conditions takes place. With r<4, the system has no chaotic effect and revolves around a fixed point. With r=4, the system shows chaotic characteristics. Yet with r>4, the system diverges to infinity.

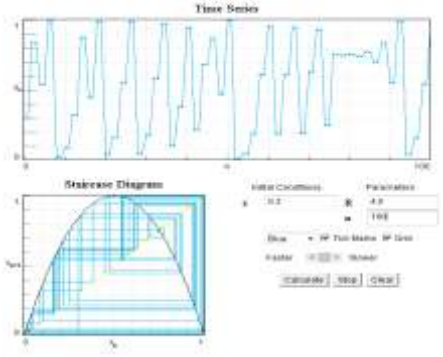
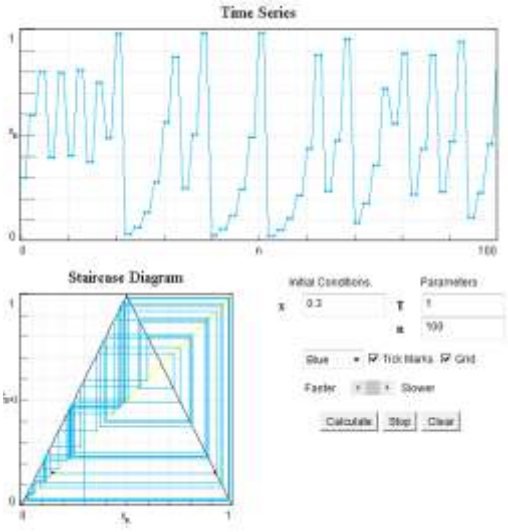


Figure 2: The time series and staircase diagram for Tent map where μ equal to 2.



3.2.2 Tent Mapping

The tent map has the following equation (Wikipedia):

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu x_n & \text{for } x_n < \frac{1}{2} \\ \mu(1 - x_n) & \text{for } \frac{1}{2} \leq x_n \end{cases}$$

The tent map took its name from its tent-like graph that occurs when μ is between 0 and 2. For the same values of μ the function fμ maps the unit interval [0, 1] onto itself. Yet at μ equal to 2, the case of the tent map is a non-linear transformation of the logistic map with r=4. With μ greater than 2 the tent map diverges to infinity.

3.2.3 DWL Function

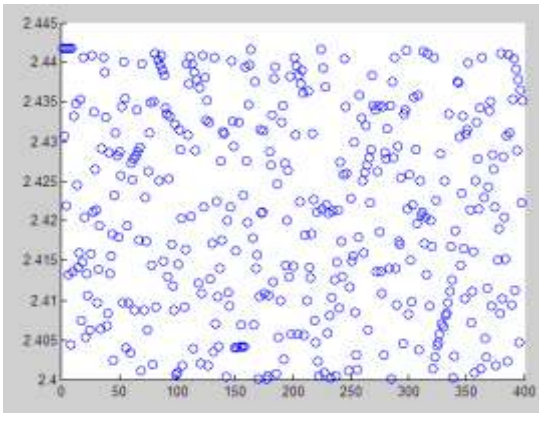


Figure 3: Scatter for frequencies resulting from DWL with initial variable from 1.1 to 1.5

The DWL function is summarized as follows:

The function is formed of the multiplication of 2 matrices. Matrix D of dimension 11x11 is multiplied by matrix L of dimension 11x1 to result in a matrix W of dimension 1x11, that represents the 11 frequencies.

To fill matrix D we apply the following function $F(x) = x^2$

Consider d[i] [j], to be the current space to be filled of the matrix, where I represents the number of rows, and j represents the number of columns.

If row is even and column even, d[i] [j] = F(x-j) -i
If row is even and column is odd, d[i] [j] = F(x+j) –i
If row is odd and column is even, d[i] [j] = F(x-j) +i
If row is odd and column is odd, d[i] [j] = F(x+j) +i
To fill the matrix L we apply the following function G(x) = 1/x

Consider l[i], to be the current space to be filled of the matrix, where i represent the number of rows.
If row is even, l[i] = G(x-i)
If row is odd, l[i] = G(x+i)

After multiplying the two matrices, we obtain matrix W. The values of matrix W are mapped by a simple linear mapping to be within the range needed.

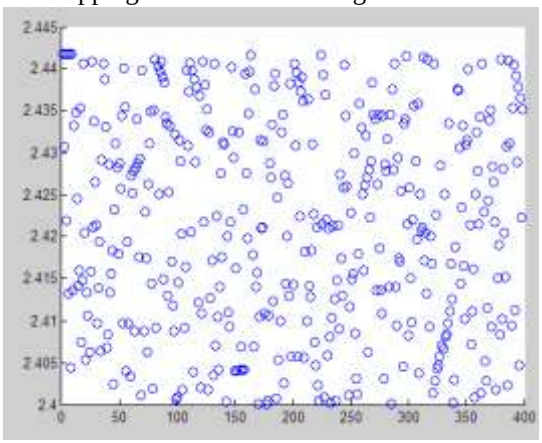


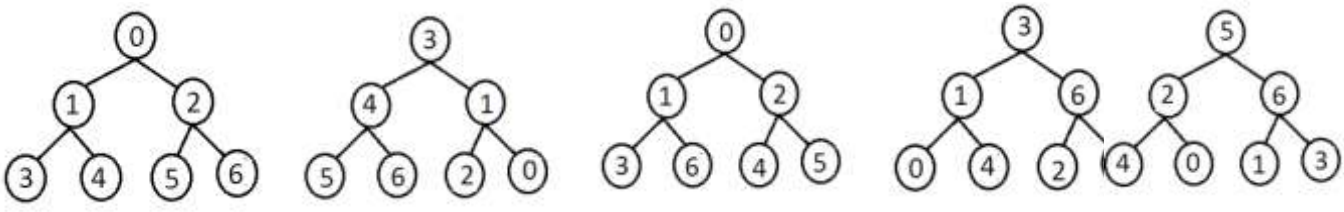
Figure 4: Scatter for frequencies resulting from functions 1&2&3.

All together, the logistic map, tent map, and DLW matrix, form the system's three functions that are used to generate new frequencies to hop to. Each function is designed to form a cycle of 10 iterations that will generate 10 frequencies, except the last function which will generate 11 frequencies. This cycle repeat itself as long as the communication is taking place.

3.3 Algorithm

Now, the system needs to permute the 31 frequencies that were obtained in order to add more security. For this task, the study proposes a new algorithm based on "trees"; this algorithm constitutes four methods: LRC (left - right-current), RCL (right-current-left), RLC (right-left-current), and LCR (left-current-right). To remove the risk of repetition, we proposed a way to use these tree algorithms efficiently. The system will use each set of 31 frequencies only once. These frequencies are randomized according to LRC, and then new set of 31 frequencies is generated. Now these frequencies will be permuted by another technique, say RLC, and so on. This method proved to give the best results of the algorithm.

Figure5: 7 array undergoing LRC, RCL, LCR, and RLC



3.4 Variables

Adapting simple frequency hopping is not enough. We need to use strategies for dynamic adaptation of the variables of frequency hopping functions. Some initial variables that can be used in our three functions are:

1. Stocks for 33 very popular companies
2. Number of pages/people/Shares on Face book:
3. Time in 33 different apply the following formula:

VARIABLE=HOURS+MINUTES+ (SECONDS) ^4

In the above three methods, we discussed dynamic variables that could be known and directly used at the transmitter and sender at the same time.

4. Temperature: This variable is different from the above three; it is not a global variable that can be known at the sender and receiver without being sent. To use Temperature, we place a sensor at the sender's side and record the values. Then, we have to send these values to the receiver, but it can't be that simple. We apply Diffie-Hellman to send these temperatures in a secure way.

3.5 Results and Interpretations

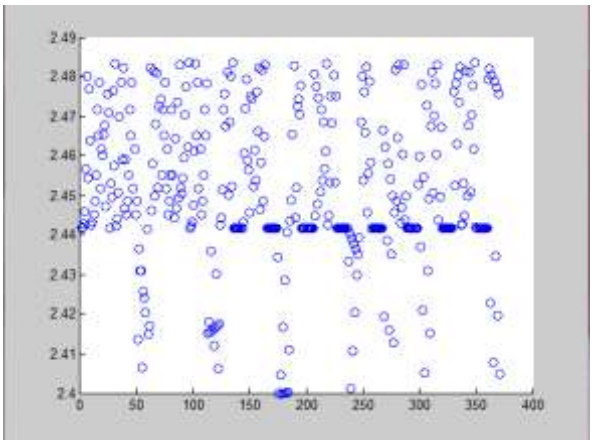


Figure 6: Scatter for frequencies resulting from functions 1&2&3 after using tree algorithm.

Upon combining the logistic function, tent function, and DWL function, and permuting them with the tree algorithm positive results appeared.

The obtained results showed great advantages of the system, thus allowing the system to reach its desired purpose. The positive results of the system are presented below:

A) Maintaining Chaotic Properties of the System:

The system has maintained its chaotic properties; this was shown in the results. The results show that after several iterations, new unique frequencies are generated. Moreover, these frequencies show no pattern and show randomness in all aspects.

Thus the generated sequence is set to be chaotic.

In addition to this, the system does not tend to infinity or to diverge to any fixed point no matter how large the iteration is. The system maintains its chaos and maintains evolving in orbits of sets.

Furthermore, upon changing initial conditions, the system's outcome changes significantly. Thus the change of initial conditions leads to closer points of totally different future trajectories. This shows that the "Sensitivity to initial conditions" property of the

chaos theorem is present in the obtained results. This property states that each point in the system is arbitrarily approximated by other points with significantly different future trajectories.

B) Advantages Shown by the Usage of the Algorithm:

Unlike other chaotic systems, this system is equipped with an algorithm that alters between the present chaotic functions. This alteration shows great advantages.

The alteration causes frequencies having close outcome to be separated. According to the chaos theory, any chaotic system shows close outcome at the first stages of the system. Yet this thing changes after several levels of the system. This is not the case in our system. This system due to the algorithm present in it separates the outcome in such a way that even if one uses one chaotic function, he will not get close outcome in the initial stages. Moreover, this system uses more than one function which makes the result even more chaotic. The results have showed the repetition of a certain frequency (2.44) for 3 initial iterations on function 1, and the repetition of another frequency (2.46) in the initial iterations of function 2 without the usage of the tree algorithm. Upon the usage of the tree algorithm these frequencies are separated.

C) Combination of Several Chaotic Frequencies Effect:

The combination of several chaotic functions serves in increasing the states of the system with the consequent increase of the period of repetition. It also serves in increasing the security of the system (Herrero, Cochado, Redondo and Alonso 2010).The results, indicates the braking of the trajectory of the both maps, the logistic and the tent. The combination of these two frequencies, along with the third, makes it extremely difficult and nearly impossible to make an individualized analysis of the sequence generated by each chaotic map

4. Communication System Design

4.1 Introduction

A frequency hopper is constructed by a pseudo noise (PN) code generator that selects the frequencies to hop to. A frequency de-hopping takes place at the receiver side using pseudo noise code generator that drives the receiver's local oscillator frequency synthesizer.

Figure 7: The basic frequency hopping system

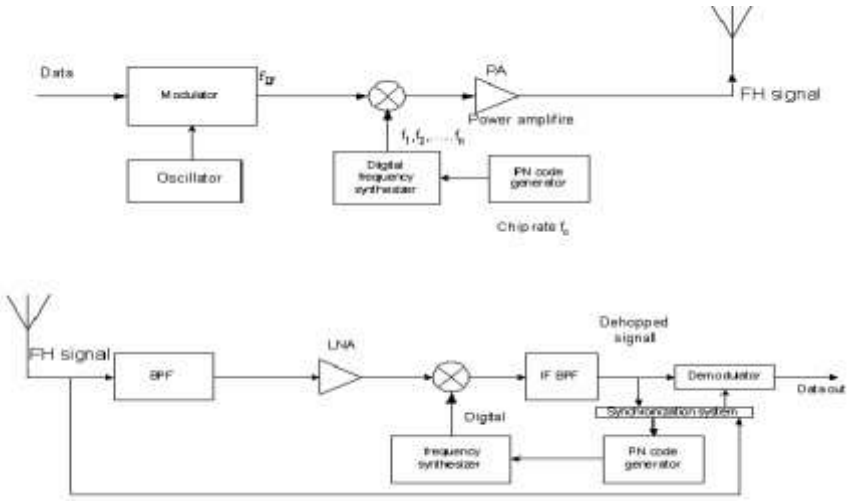
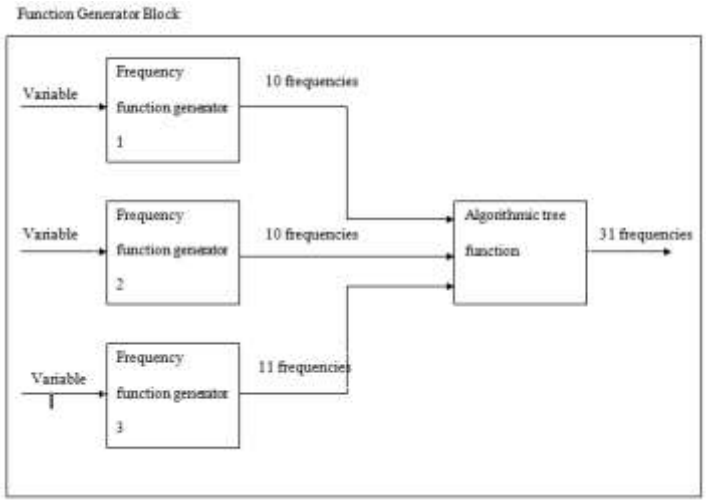


Figure 8: Function generator block



4.2 Design of the system

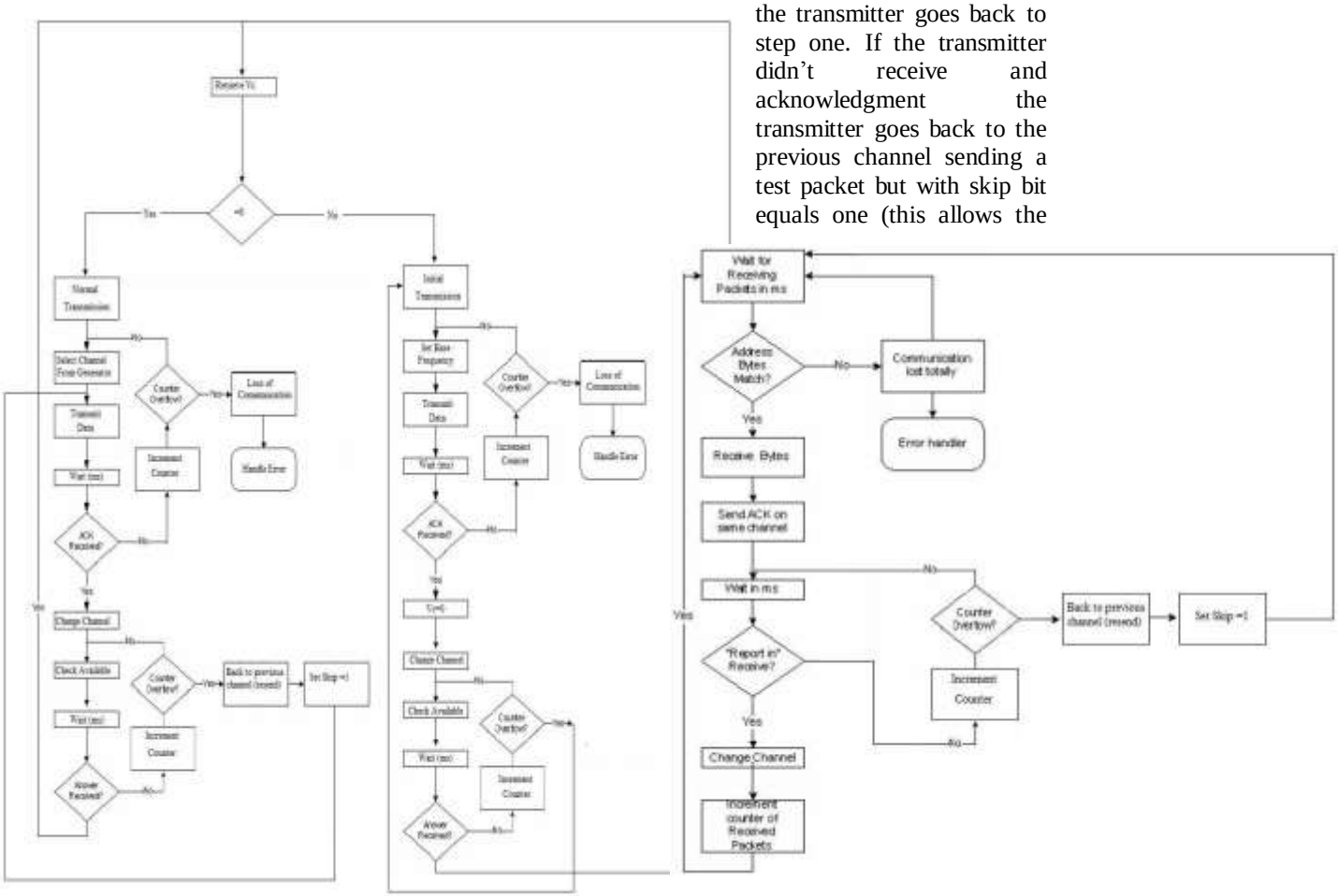
4.2.1 Frequency generator

The frequency generator was discussed in details in the previous sections. This generator generates frequencies in sets from each function. Then it manipulates the produced frequencies using a specific algorithm. This outcome is stored in an array of 31 frequencies.

4.2.2 Hopping schema

There are two main schemas for transmission, the "Normal Transmission" and the "Initial Transmission". The initial transmission takes place on a base station that is known to both the transmitter and receiver. In this transmission the message sent doesn't contain any data, in this transmission, the sender and receiver share initial variables needed for the frequency generator. Nonetheless, the transmission of the message data takes place in the normal transmission mode.

Each time the transmitter sends a packet data it waits for an acknowledgment packet from the receiver on the same channel. If the transmitter receives the acknowledgment within the predefined time-out, it selects a new frequency and sends a test packet, if acknowledgment is received the transmitter goes back to step one. If the transmitter didn't receive and acknowledgment the transmitter goes back to the previous channel sending a test packet but with skip bit equals one (this allows the



receiver to jump over the next frequency). If the transmitter didn't receive an acknowledgment packet for the data packet within the predefined time-out, the transmitter resends the packet data and increments the resend counter. If the counter is overflowed then an error occurs. As for the functionality of the receivers it mirrors that of the sender.

Figure 9: Message communication flow chart at the transmitter.

Figure 10: Message communication flow chart at the receiver.

4.2.3 Message Type

The messages in the system are divided into 5 main types:

i- Data Message (message containing the data)

ii- Acknowledgment Message (message sent by the receiver)

iii- Test Message (message sent to test the next hop)

iv- Initialization Message (message used to determine the variables) The format of the message is shown below.

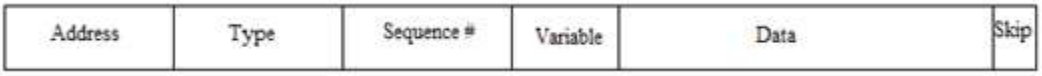


Figure 11: The message divided into 6 parts.

(1) Address:

The address bits of the packet data indicate the destination address of the receiver. This may come in hand in case of a multi-user network.

(2) Type:

The type bits of the packet data indicate the type of the message, whether it is a data message or an acknowledgment message, or an initialization message, or a test message.

(3) Sequence Number

The sequence bits of the packet data indicates the number of the packet that are received by the receiver, the bits are incremented each time the receiver receives a data message.

(4) Variables

The variables bits of the packet data contain 4 variables. The first variable V_C indicates whether to start the algorithm from the beginning with the initialization schema. The V_1, V2, V_3, are always set to zero except in the initialization state where they are set as initial values for the frequency generator.

(5) Data

The data bits of the packet data contains the message that is to be sent

(6) Skip

The skip bit of the packet data informs the receiver that it should skip the next frequency and go to the one after.

5. Summary and Conclusion

The system that was demonstrated in this paper has proved its theoretical efficiency. This paper has provided a secure communication system based on frequency hopping technology and using 3 basic functions, out of which 2 are chaotic and one is a novel matrix operation. Along with the three functions the system consists of a tree algorithm that is used to shuffle between the frequencies. The usage of these functions along with algorithm has yielded an unpredictable sequence that is impossible to regenerate using regular methods. The system, with its theoretical efficiency, has not been tested in a hardware manner, due of unfeasible material at the time. The authors of this paper, recommend, anyone capable of applying this system, to a hardware application to do so, for further study and improvement.

References

Website: http://www.ictregulationtoolkit.org/en/Section.2467.html

Website: http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

Komo, J.J. ,” Southeastcon '89. Proceedings. Energy and Information Technologies in the Southeast”. IEEE TRANSACTIONS, April 12, 1989

Stephen B. Wicker, Vijay K. Bhargava, “An Introduction to Reed-Solomon Codes”,1994

Kumar, P.V. , “Frequency-hopping code sequence designs having large linear span”, Jan 1988

Xiangdong Liu, Xiqin He, Xueye ANG, Nan Jiang, “A New Chaotic FH Sequences Generator based On Dynamic Quantization”, April 2011

Website: http://en.wikipedia.org/wiki/Logistic_map

Elmer G. Wiens, “Egwald Mathematics: Nonlinear Dynamics, THE LOGISTIC MAP AND CHAOS”

Website: http://en.wikipedia.org/wiki/Tent_map

Alvaro Herrero, Emilio Corchado, Carlos Redondo, Angel Alonso, “Computational Intelligence in Security for Information Systems 2010”