International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

Lagrange Interpolating for Error Detection and correction in antijamming attack

Assistant Prof. Dr.AbdulKareem Merhej Radhi, College of Information Engineering, ,Nahrain University, Baghdad, Jadriya- Iraq.E-mail: kareem_m_radhi@yahoo.com, kareem_m_radhi@nahrainuniv.edu.iq

Abstract- Due to vulnerable signals in wireless channels or through jamming of one or multiple channels, Errors affected all transmitted data . Therefore errors detection and correction can be effective technique to reduce the effect of these errors. The proposed method in this research achieved using Lagrange Interpolating Polynomial to minimize the errors of transmitted data after detecting it. This technique produces Lagrange polynomials arranged in eight columns and rows. Using this technique will increase the probability of finding the correct data in less time comparing with other techniques. Moreover it reduces the spending time for error correcting. Proposed technique applied in raw data emitted through simulated channel using NS2 simulator.

Keywords: L.I.P. (Lagrange Interpolation Polynomial), NS2, jamming, Error Correction Code, Galois Field ,Packets, Shift Registers

Introduction

Various application domains such as environmental monitoring and surveillance wireless sensor networks were applied. Open transmission media, a sensor network may suffer from radio jamming attacks, which are easy to launch but difficult to defend. Attacked by jamming signals, a sensor network may experience corrupted packets and low network throughput.
In the real world scenario, jamming attacks may be very different in nature and may change over time. In addition, radio signals are unstable as many factors may cause jamming signal attenuated in different ways for different environments. As a result, different nodes suffer different degrees of radio jamming. Thus, it is inefficient for a whole sensor network simply to apply a single antijamming technique. This may result in poor performance of antijamming and/or still suffer serious performance degradation of energy consumption [1]. There are a variety of anti jamming techniques; some of them are suitable under a slight of antijamming conditions. The parameters of choosing proper antijamming technique are cost of energy saving and level of jamming signals. So, in a wireless sensor network, there are. For each node, there are n antijamming techniques available for different jamming conditions. For the node, each antijamming technique has different cost.

In A Mathematical Theory of Communication, Shannon proved that channel noise limits transmission rate and not the error probability. According to his theory, every communication channel has a capacity C (measured in bits per second), and as long as the transmission rate, R (measured in bits per second), is less than C, it is possible to design an error-free communications system using error control codes. The now famous Shannon-Hartley theorem, describes how this channel capacity can be calculated. However, Shannon did not describe how such codes may be developed. This led to a wide spread effort to develop codes that would produce the very small error probability as predicted by Shannon. There were two major classes of codes that were developed, namely block codes and convolutional codes[2].

Antijamming methods

Although jamming still an open problem to the wireless security community, there are several defense strategies and techniques used in the traditional computing to cope with this problem. Such strategies are: avoid jammed region (i.e. routing around jammed region), escape jammed channel (channel-hopping, frequency-hopping techniques), and spatial retreats.

Transmission Power Adjustment

With this technique, a sender node increases its transmission power, and thus increases the SNR at the receiver node [3]. This technique is suitable under a slight jamming condition, for example, at the periphery of the jamming area. In that area, the jamming signal is relatively weak, so the nodes usually only need to raise its transmission power by one or two levels. This technique introduces modest energy cost.

Error-Correcting Code

An error-correcting code is used for correcting some error bits that occurred during transmission [4]. Before transmission, the node encodes the packet. When the receiver has received the packet, the decoding process is capable of correcting some error bits by using the redundancy information contained in the encoded packet (under a certain condition, e.g., the number of error bits is smaller than a given threshold).

Applying error-correcting codes as an antijamming technique is energy efficient as it largely relies on computation and transmission of extra bits. Many detecting and error-correcting codes have been used as Reed-Solomon, forward error correction, hamming codes, and cyclic redundancy code, etc.

Channel Hopping

With this technique, a sensor node will change the working channel when it detects strong jamming signals in the current channel [1]. As shown in Figure (1), node B in the shaded area is jammed. Node A is an intermediate node which works on two channels. It switches between the two channels, so it can keep the network connected. When it changes its working channel, it will notify its neighbor working on the same frequency immediately.

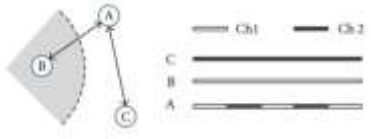

Figure [1] Illustration of the channel hopping technique.

General Errors and polynomials

The information sent by the internet, where the information (say a file) is broken up into packets, and the unreliability is manifest in the fact that some of the packets are lost during transmission: Suppose that the message consists of n packets and suppose that at most k packets are lost during transmission. Note that in this setting the packets are labeled and thus the recipient knows exactly which packets were dropped during transmission. The contents of the packet might be a 32-bit string and can therefore be regarded as a number between 0 and 2^{32-1}. The properties of polynomials over GF(q) (i.e., with coefficients and values reduced modulo q: q a prime number) are perfectly suited to solve this problem and are the backbone of this error-correcting scheme. To see this, let us denote the message to be sent by $m_1,...,m_n$ and make the following crucial observations: 1) There is a unique polynomial P(x) of degree n−1 such that P(i) = mi for $1 \leq i \leq n$ (i.e., P(x) contains all of the information about the message, and evaluating P(i) gives the contents of the i-th packet). 2) The message to be sent is now $m_1 = P(1),...,m_n = P(n)$[5][6].

Lagrange Interpolating Polynomial

The proposed algorithm introduces and modifies Lagrange Interpolating polynomial and its useful specification to construct simulated polynomials for transmitted and received data of emitted packets. The algorithm reduces the error bits for redundant and jammed packets compared with other techniques. Moreover, in spite of increasing errors in transmitted data, the researcher find with this technique there is increasing the probability of finding correct data and reduce the spending time for errors correcting.

Polynomial Interpolation Theory

Let *A* be a finite set of the values of unknown function *f(X)* such that $A = \{f(X_0), f(X_1, \ldots, f(X_n)\}$ and we want to find an approximation to the value of f(X^*). if $X^* \in \{X_0, X_1, \ldots X_n\}$ then this process is called interpolation. While if $X^* \notin \{X_0, X_1, \ldots X_n\}$ then this process called Extrapolation. Practically, the above process is always called interpolation [7].

One of the most useful and well-known classes of functions mapping the set of real numbers into itself are the algebraic polynomials, the set of functions of the form:

$$P_n(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ldots (1)$$

Where n is a nonnegative integer and $a_0, a_1, \ldots, a_n$ are real constants. One reason for their importance is that they uniformly approximate continuous functions. This result is expressed precisely in the Weierstrass Approximation Theorem as shown in Figure (2).

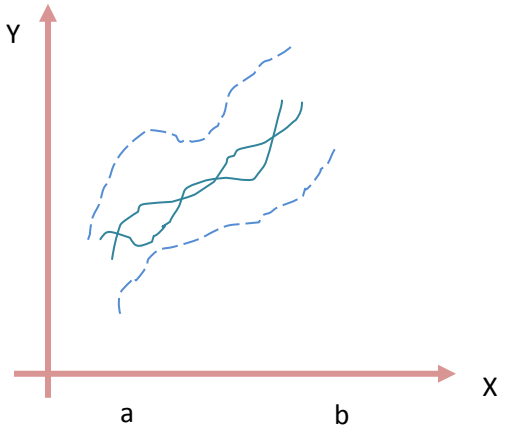

Figure [2] bounded Polynomials

Weierstrass Approximation

Suppose that f is defined and continuous on [a,b]. For each ε > 0, there exists a polynomial P(x), with the property that

$$|f(x) - P(x)| < \varepsilon \quad \forall\, x\ in\ [a,b] \ldots (2)$$

Interpolated Polynomial

If $X_0, X_1, \ldots X_n$, *are n+1* distinct numbers and f is a function whose values are given at these numbers, then a unique polynomial P(x) of degree at most n exists with

$$F(X_k) = P(X_k) \quad \forall\, k = 0,1,2, \ldots . n$$

This polynomial is given by:

$$P(X) = F(X_0)L_{n,0}(X) + \ldots\ldots + F(X_n)L_{n,n}(X)$$

$$= \sum_{k=0}^{n} F(X_k)L_{n,k}(X) \ldots\ldots\ldots (3)$$

Where, ∀ k = 0, 1... , n

$$\boldsymbol{L_{n+k}(X) = \frac{(x-x_0)(x-x_1)\ldots\ldots(x-x_{k-1})(x-x_{k+1})\ldots\ldots(x-x_n)}{(x_k-x_0)(x_k-x_1)\ldots\ldots(x_k-x_{k-1})(x_k-x_{k+1})\ldots\ldots(x_k-x_n)}}$$

$$= \prod_{\substack{i=0 \\ i \neq k}}^{n} \frac{(X-x_i)}{(x_k-x_i)} \ldots\ldots\ldots\ldots\ldots \textbf{(4)}$$

Proposed Algorithm

This challenge of antijamming technique which is presented in this research formulated by combining L.I.P and binary search method. With NS2 simulator, the researcher simulates various transmitter and receiver nodes with different packets. Proposed ECC used to correct error bits that occurred during transmission after the encoding process. The block diagram of the proposed algorithm can be shown in figure [3] .

Matrix constructed frame performed in GF(8) using Equation (4), where the tuples value are 8th Interpolated Lagrange Polynomials, while the final attributes involve the precise numerical value of I.L.P, after powered the content of each position by the multiple of 2 in ascending order, as shown in table[1].

Single parity check bit (S.P.B) shown in table (1) be performed and allocated in column number 10 to monitor the data packet as additional policy for detecting errors in data transmitted, while constructed Lagrange polynomial be the first check guard.

Table [1] Matrix Tabular Polynomial of GF (8)

Index	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	*S. P. B.*	*L.I.P*
0	1	0	0	0	0	0	0	1	*0*	N_0
1	0	1	0	0	0	0	1	1	*1*	N_1
2	1	0	.1	0	0	0	0	1	1	N_2
-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-
254	0	1	1	0	1	1	1	0	1	N_{254}
255	1	1	1	1	1	1	1	1	.	N_{255}

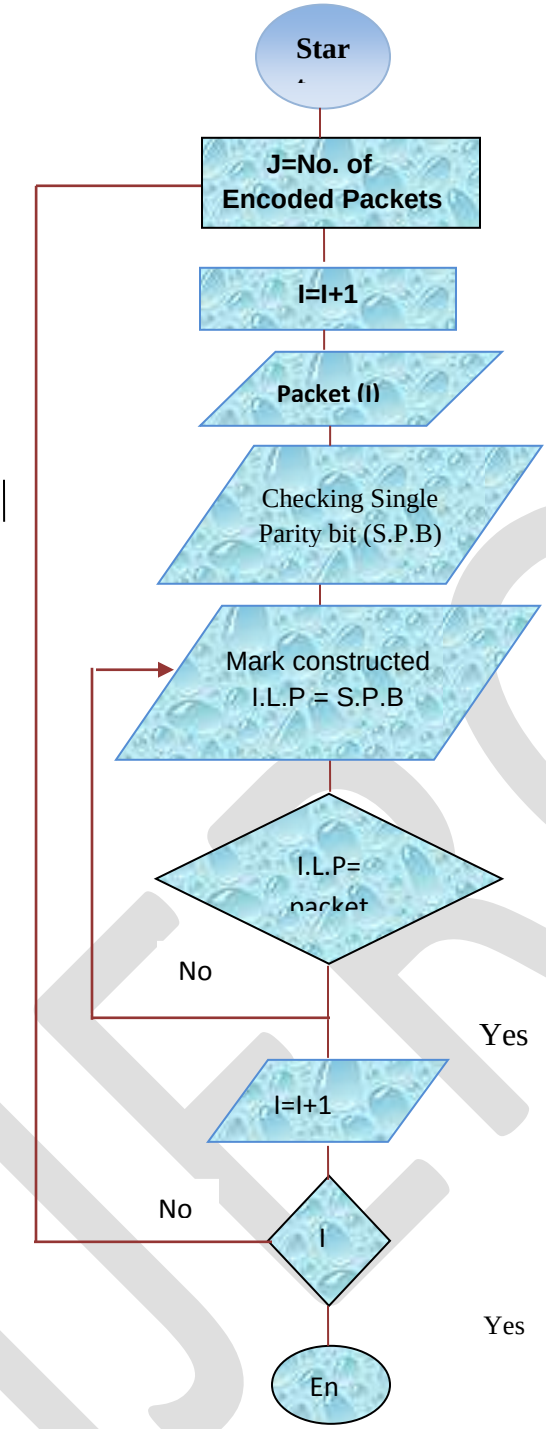

Figure [3] Block Diagram of the Proposed Algorithm

Moreover, in the proposed algorithm, the generated packets can be simulated using logical circuits containing eight stages of shift registers with (XOR) gate. Each shift register contains one binary bit, where the contents of the second and fourth shift registers are xored to feed the first shift register. Figure [4] depicts the architecture of this design.

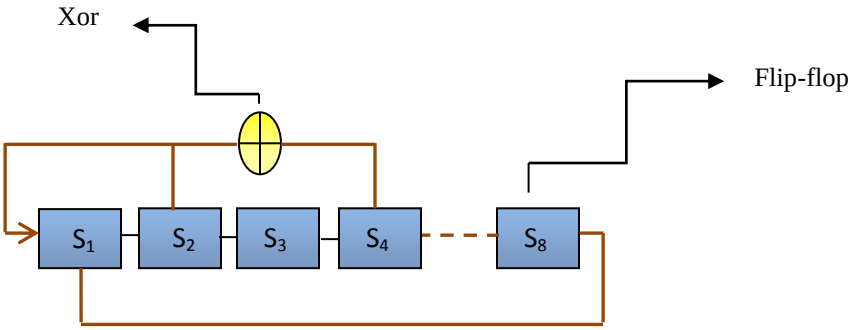

Figure [4] simulated of the generated Packets

So the simulated logical circuits and its output can be represented in Figure [5] by the following p(x) matrix. Where the left hand side of each equation represent single parity bit.

$$P(x)= \begin{bmatrix} C_1 \oplus & & & & & & C_8=0 \\ C_2 & \oplus & & & & & C_8=0 \\ C_2 & \oplus & C_4 & & \oplus & & C_8=1 \\ C_3 & \oplus & C_4 & \oplus & C_8=1 & & \\ C_3 & & \oplus & C_5 & & \oplus & C_8=1 \\ C_4 & & & & \oplus & & C_8=0 \\ C_1 & & \oplus & C_5 & & \oplus & C_7=1 \\ C_2 & & \oplus & C_7 & & \oplus & C_8=1 \end{bmatrix}$$

Figure [5] Simulated Shift Register Matrix

ACKNOWLEDGMENT

I would like to thanks the people who helped me in this work . Also I would express thanks to the stuff of laboratory in my university for their helpful efforts in this work.

CONCLUSION

Minimizing errors in data transmitted through vulnerable channels is an important case. Using any technique should increase the probability of finding the correct data in less time. So this work overcome the errors in transmitted data using Lagrange interpolating polynomials. Comparing the results of this work with previous techniques, we can find more accurate data in a less time.

REFERENCES:

[1]. Yanmin_Zhu,[1,2] Xiangpeng_Li, and Bo_Li, "Optimal Adaptive Antijamming in Wireless Sensor Networks", Shanghai Jiao Tong University,2012.

[2]. Vikas Gupta , Dr. Chanderkant Verma, ," Error Detection and Correction: An Introduction", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 11, November 2012

[3]. W. Xu, "On adjusting power to defend wireless networks from jamming," in Proceedings of the 1st Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems, pp. 1–6, 2007.

[4]. G. Balakrishnan, Y. Mei, J. Yingtao, and K. Yoohwan, "Performance analysis of error control codes for wireless sensor networks," in Proceedings of the 4th International Conference on Information Technology-New Generations (ITNG '07), pp. 876–879.

[5] Rao Satish, Tse David, " Discrete mathematics and Probability Theory" , CS 70 Springer 2009.

[6]. W. Xu, W. Trappe, and Y. Zhang, "Defending wireless sensor networks from radio interference through channel adaptation," ACM Transactions on Sensor Networks, vol. 4, no. 4, article 18, 2008.

[7] Burden L, Richard, and j. Faires, Douglas, 9th edition, 2011