Performance Analysis of Cyclic Redundancy Check (CRC) Error detection Technique in the Wireless Sensor Network

Michael O. Ezea[1], Henry O. Osuagwu[2], Mamilus A. Ahaneku[3]

[1, 2]PG Student, Department of Electronic Engineering, University of Nigeria, Nsukka, Enugu State, Nigeria
[3]Assistant Professor, Department of Electronic Engineering, University of Nigeria, Nsukka, Enugu State, Nigeria

Abstract - *With the increase in the need for data transmission from one point to another, and hence sources of noise and interference, developing an efficient and reliable techniques for error detection in wireless sensor network has been a thing of priority for engineers. In data communication, transfer of data from a source to a sink involves many steps which are subject to errors. Realizing an efficient and a reliable error detection technique is important in the deployment of wireless sensor networks (WSNs). This work investigates the divisor bits of a CRC-4 error detection technique that gives the minimum undetected erroneous packets when used as a divisor bits in the WSN. In our approach, we generated the possible 5 CRC divisor bits of CRC-4. Through simulation, the performance of these divisor bits in terms of number of erroneous frames that is undetected was demonstrated using MATLAB. The results show that when 100000 frames of which each frame containing 32 bits was sent, there were a minimum undetected erroneous frame when 10011 was used as a divisor bit in the CRC-4.*

Key Words: **WSN, CRC, Error Detection, Bits, MATLAB**

1. INTRODUCTION

The physical environment is made up of different information sources, such as light, temperature, pressure, motion, and many others. One can understand the environment better by getting information about the environment from multiple sources. One of the promising technologies that is widely used in capturing and relaying such information is wireless sensor network (WSN) [1]. WSN is currently receiving global acceptance for data procurement due to its cost effectiveness and flexibility [2]. In this type of infrastructure, sensors are incorporated into various devices, machines, and environments. These sensors capture the information about the physical environments and reports appropriately so that further action could be taken.

We can define wireless sensor networks as a self-organized networks that can help to keep surveillance of the situations of the environment such as temperature, sound, vibrations, pressure, etc. and then transmit the data through the network to the sink where the examination and analysis of the data take place[3]. Wireless sensor network is made up of numerous wireless sensor nodes spread in an area of interest with some base stations where data is collected. These sensor nodes with the help of radio signal communicate among themselves. A wireless sensor node has a built-in device for sensing and computing, radio transceivers and power components. [2], [4], [5], [6]. The data obtained and collected from the wireless sensor network is usually affected by noise, errors, missing values and malicious attacks on the network which often make the data unreliable [7], [8].

When errors in data communication are undetected, it could lead to misinterpretation of transmitted packet by the receiver, transfer of the erroneous data from source to sink, and can also cause a fatal failure in the system [9]. For instance, when data is transmitted through a communication network, it is expected that the receiver should receive exactly what the transmitter transmitted. To determine if the received message is the same as the sent message without having a copy of the original message is termed error detection [10]. The reason for error detection technique is to enable the receiver of a message to ascertain if a message transmitted through an unreliable channel is error free or not [9].

For wireless sensor network, detecting and correcting errors are usually carried out at the data link and the transport layers in the OSI model [4]. Generally, in error detection, redundant bits are added to the total transmitted data. The receiver uses these additional bits to check for error on the sequence of the bits that are received during transmission. Some error detection schemes could be applied to correct the error, which is called error correction scheme. However, the number of bits in error that can be detected may be different depending on the scheme.

The rest of this paper is organized as follows: Section 2 presents the related literature on different error detection mechanisms used in WSN. Section 3 provides an overview of CRC scheme and CRC model presentation. Section 4 presents the performance analysis and the simulation results. The relevant conclusions are presented in section 5.

2. RELATED WORKS

To transfer data from the transmitting station to a receiving station, many stages are involved in the process and each is subject to error. For reliable communication, error must be detected and corrected. With the error control process, we can be assured that the transmitted and received data are the same. Error is said to have occurred when the input data is not the same with the output data. During transmission, noise could corrupt digital signals, thereby introducing errors in the binary bits moving from one system to another. That means a 0 bit may change to 1 or a 1 bit may change to 0. To reduce the rate of occurrence of this error, error detecting schemes have been suggested. In [11], the researcher introduced harming code error detection techniques. This technique can detect two bits error and correct one-bit error. This type of error detection techniques is suitable in a situation where there is few randomized mistakes. Harming is to do the process of error detection, then correct the errors so that the arrangement of the bits will be in its planned sequence before sending the data [12]. It is a technique developed by R.W. Harming for error detection and correction [13]. Hamming Code method inserts (n + 1) check bits into 2n data bits. This method uses XOR (Exclusive - OR) in the error detection process [11].

In [7], the researcher used outlier to detect the presence of error in the wireless sensor network. According to [7], [14], This technique targets the arrangements in data that does not follow the predicted behavior. It is an observation that is not consistent with the set data. In the WSN, we can define outliers as those measurements that do not follow the normal patterns of a sensed data due to the presence of error. The disadvantage of this is the trouble associated with defining the normal behavior or a normal region.

According to [15], [16], parity bit is the most common method of detecting bits errors with asynchronous character. The method of error detection using parity bit involves attaching an extra 0 or 1 bit to a codeword at the transmission point. For example, the codeword (i.e., the transmitted sequence) 1001 may be incorrectly received as 1101. A parity bit is often used to detect such errors. If the data to be transmitted is 7-bits and the parity bit is used to detect the error, the 8th bit is the parity bit. Parity bits is categorized into two: the even Parity check and the odd parity check [15]. For even parity method, the parity bit is chosen to make the total number of 1s in the codeword even. For example, if 110011 is the dataword to be transmitted, the parity bit to be appended should be 0 so that the codeword would be 0110011 which is even parity of 1. To transmit 11001 dataword, the parity bit to be attached would be 1 so that the codeword becomes 111001 which is even parity of 1s. For the odd parity, the parity bit is chosen so as to make the total number of 1s odd. Error is said to have occurred if the data received from the receiver does not give the expected parity. The receiver will detect the error and request for retransmission. Single bit errors can be checkmated by parity check method. Parity bit can also checkmate burst errors provided the errors in each unit data that occurred is even or odd depending on the type of parity bit applied. For example, even parity method cannot detect burst errors if the errors in the unit data is even and odd parity bit method cannot detect burst errors if the errors in the unit data is odd.

In [17], the researcher discussed effectiveness data transmission error detection using check sum error detection techniques. The checksum technique involves summing up the data to be transmitted, finding the complement, appending the complement and then transmitting them together. Just like CRC, checksum is based on the concept of redundancy. During transmission, checksum generator segments the data unit into equal segments of n bits (usually 16). We then add these segments of data using one's complement arithmetic. After summing, the total sum is appended to the original data unit as redundancy bits to the codeword. The codeword is then transmitted through the network. The receiver receives the information and then performs the same calculation, output of 0 implies that the information was not corrupted during transmission and therefore error free else, the data is discarded. This type of error detection technique cannot detect the errors if the increment in the value of one word is the same with the decrement in the value another. Since the sum and checksum did not change, the detection of the two errors using checksum scheme becomes impossible

In [18], The researcher used temporal correlation in sensor data set to detect and correct errors at receiver nodes. This method uses predictions generated for future data during execution by applying the knowledge of correlation and comparing sequences of these predictions with observed data within a decision tree. The properties of this correlation is contained in the data models which makes it possible to generate predictions based on the recent history of observations. This method is based on predictions which are not reliable.

During data transmission, errors are introduced which do affect the data being transmitted. This has made scientists and researchers propose so many methods of detecting and possibly correcting such errors. Some of these techniques are capable of detecting only single bit errors, all unidirectional errors, some can detect only burst errors. Since none of the error detection mechanism currently used in communication networks is capable of detecting all types of error (one may be good in single error but will not be good in burst error, another may be good in burst error but will not be good in multiple error) but cyclic redundancy checks (CRC) outperforms other schemes in terms of error detection. In this paper, we focused on CRC-4 divisor bits that gives the minimum undetected erroneous packets (i.e. that gives the best performance) when data is transmitted in the wireless sensor network.

3. OVERVIEW OF CRC SCHEME

Cyclic redundancy check is a technique for detecting errors in a digital data during the time of production, transmission and storage [19], [20]. In CRC, extra 0 bits are appended to the actual message to be transmitted. A predetermined binary number also known as divisor bits is used to perform a binary division on the data. The remainder after the binary division which is known as the cyclic redundancy check bits are appended to the actual message to be transmitted. At the receiver end, the same binary operation is also performed on the incoming data unit. A remainder of zero indicates that the no error was introduced transmission and the data was received uncorrupted. Else, the data was corrupted during transmission and therefore is rejected at the receiver and retransmission request made. The system block diagram is shown in figure 1.

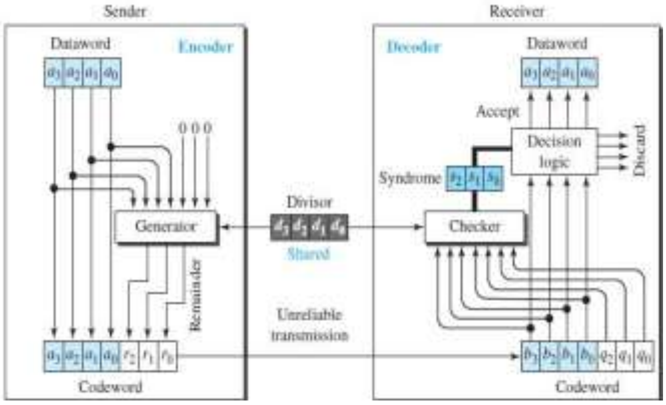

Figure 1: System Block Diagram [21]

Cyclic redundancy check codes are usually used to detect errors over frames of a certain length. The frame is usually expressed as a polynomial in x, where the exponent of x is the place marker of the coefficient. The vector $b=b_{L-1}\, b_{L-2} \ldots b_1 b_0$ length L is represented by the degree L-1 polynomial.

$$b(x) = \sum_{i=0}^{L-1} b_i\, x^i$$

$$= b_{L-1}\, x^{L-1} + b_{L-2}\, x^{L-2} + \cdots + b_1 + b_0 \qquad (1)$$

3.1 CRC Error Detection Procedure

Let the data to be transmitted consist of a length k binary vector, and represent it by the degree k - 1 polynomial.
Let the length of the data to be transmitted be k binary vector, and represented by degree k - 1 polynomial.

$$dx = d_{k-1}x^{k-1}$$

$$= d_{k-2}x^{k-2} + \cdots + d_1 x + d_0 \qquad (2)$$

At the encoding part of the system block diagram, there are *k* bits of the data word (the message) while the code word has *n* bits. *(n – k)* 0s is added to the right side of the data word to augment it. We can represent redundant bits, which are the CRC bits by the degree n-k-1.

$$r(x) = d_{n-k-1}x^{n-k-1}d_{n-k-2}x^{n-k-2} + \cdots + d_1 + d_0 \qquad (3)$$

The polynomial for the code word is written as follows:

$$c(x) = d(x)x^{n-k} + r(x)$$

$$= d_{k-1}x^{n-1} + \cdots + d_1 x^{n-k+1} + d_0 x^{n-1}$$

$$+ r_{n-k-1}x^{n-k-1} + \cdots \quad + r_1 + r_0 \qquad (4)$$

The generator then uses a predefined and agreed divisor bits of size *n* – *k* + 1. The generator divides the augmented data word by the divisor (modulo-2 division). The result (i.e., the quotient) of the division is discarded while the remainder is appended to the dataword to create the codeword. The decoder receives the codeword (possibly corrupted in transition). A checker which is a replica of the generator is now used to evaluate a copy of the *n* bits fed into it, the checker produces syndrome bits of *n* – *k* bits, which is now fed to the decision logic analyzer, and the analyzer has a simple function. If the syndrome bits are all 0s, the leftmost bits of the code word are error free and therefore accepted as the dataword (interpreted as no error); else, the bits are said to have been corrupted during transmission and therefore discarded (error). CRC is an effective method of error detection. The error detection capability of CRC depends on the chosen divisor bits [22].

3.2 Model Presentation

The system block diagram of figure 1 was modeled in MATLAB version R2013a Simulink environment. MATLAB is preferred due to its cost effective and has been identified as one of the effective methods to provide a simpler and quicker method to resolve this problem. The model is used to evaluate the performance of the divisor bits in CRC-4 wireless sensor network error detection. Their performances are compared to identify the one with the highest performance. The MATLAB model is made up of Bernoulli binary generator, CRC encoder, binary symmetrical channel, and CRC decoder.

The Bernoulli binary generator block, randomly generates binary numbers using a Bernoulli distribution [23]. For each input data frame, the CRC generator block generates cyclic redundancy code (CRC) bits and appends them to the frame. Binary symmetrical channel block brings in binary errors to the transmitted signal through this channel. The input port signifies the binary signal that is transmitted. A scalar or vector input signal can be recognized by this block. The block processes each vector element independently, and introduces an error in a given spot with error probability.

CRC syndrome detector block, computes checksums for its entire input frame. It accepts a binary column vector input signal. The block's second output is a vector whose size is the number of checksums, and whose entries are *0* if the checksum computation yields a zero value and *1* otherwise. The first output is the data frame with the CRC bits removed and the second output indicates if an error was detected in the data frame.

The MATLAB function block contains a code which compares the output of the Bernoulli binary generator, first output of general CRC detector and the second output of general CRC detector. If the output of Bernoulli binary generator is not equal to the first output of general CRC detector and the second output of general CRC detector is zero, the error is not detected then the counter counts it as an undetected error. Figure 2 shows system simulation model and how the functional blocks are connected. The display shows the number of undetected errors when 100000 frames are sent.

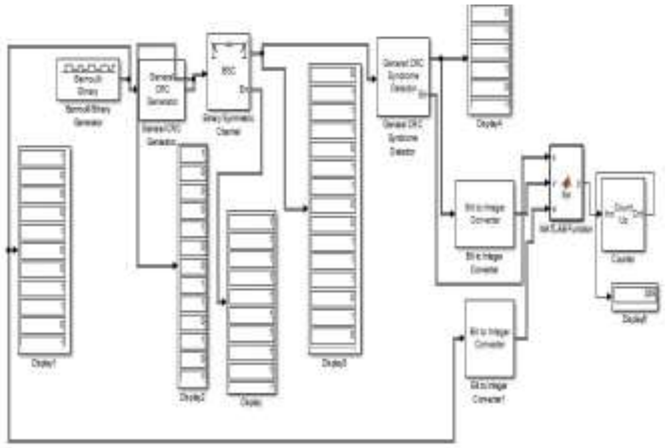

Figure 2: System Simulation Model

4.0 PERFORMANCE ANALYSIS OF CRC-4

Table 1 shows the possible CRC-4 divisor bits. The bits were generated in the MATLAB using the following codes:

```
  for s=16:30
  x=s+1;
  y= mod(x,2);
  z= decimal ToBinaryVector(x);
  if y==1
  disp(z)
  end
end
```

Table 1: Possible five bits (CRC-4) divisor bits

1 0 0 0 1
1 0 0 1 1
1 0 1 0 1
1 0 1 1 1
1 1 0 0 1
1 1 0 1 1
1 1 1 0 1
1 1 1 1 1

Each of the divisor's performance is tested in MATLAB Simulink in other to deduce the divisor that has best performance in error detection when used in wireless sensor network.

4.1 Simulation Results

When five bits are used as CRC divisor code, the following results were obtained, with number of undetected erroneous frames plotted against channel error probability. Figure 3 to 10 shows the performance of different five bits CRC divisors. They show the number of undetected errors at various channel error probability.

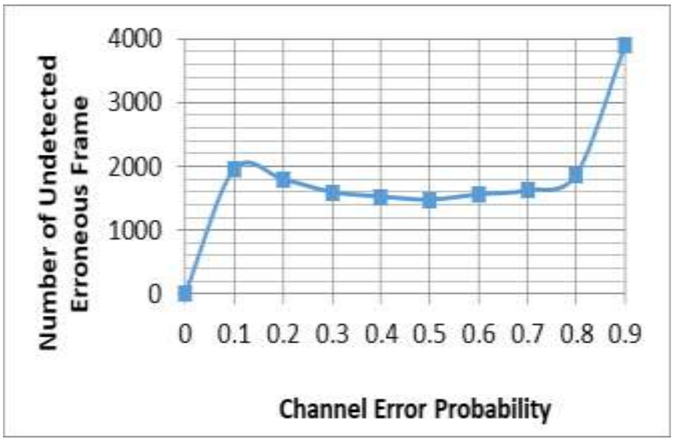

Figure 3: Performance of 1 0 0 0 1 when used as CRC Divisor

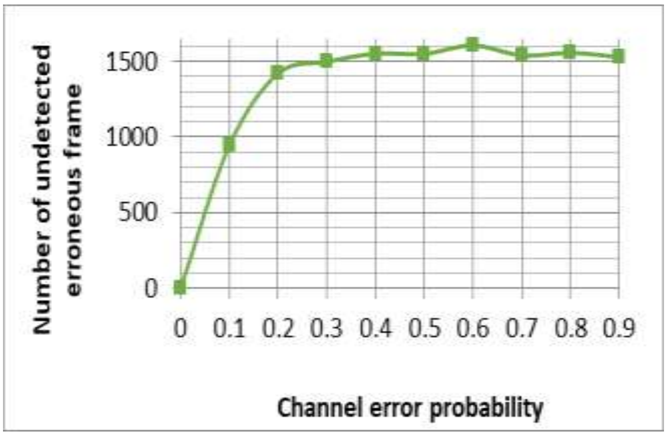

Figure 4: Performance of 1 0 0 1 1 when used as CRC Divisor

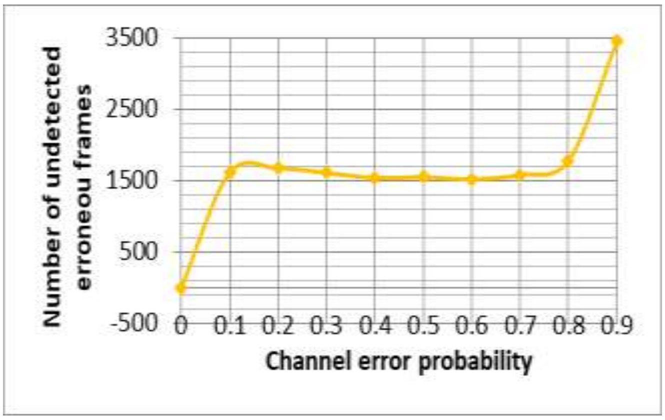

Figure 5: Performance of 1 0 1 0 1 when used as CRC Divisor

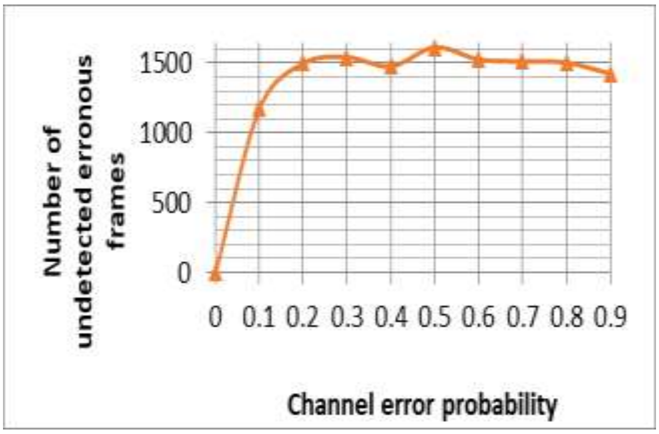

Figure 6: Performance of 1 0 1 1 1 when used as CRC Divisor

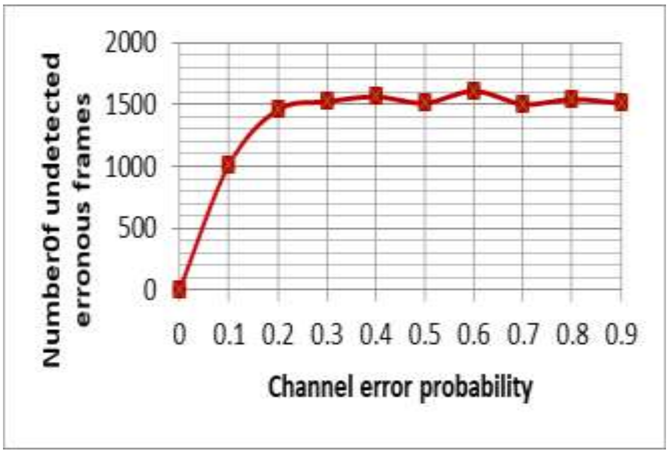

Figure **7:** Performance of 1 1 0 0 1 when used as CRC Divisor

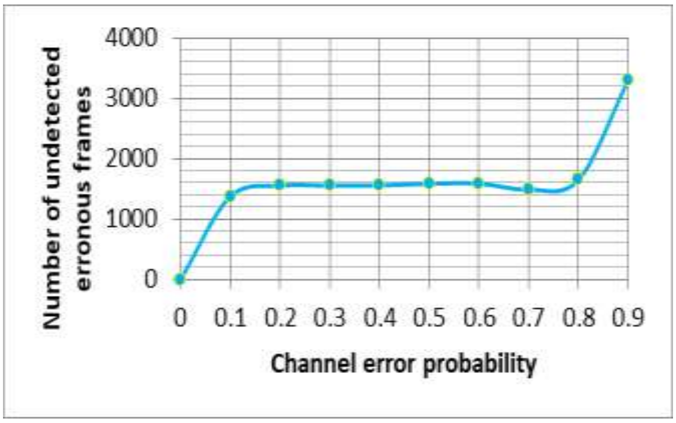

Figure 8: Performance of 1 1 0 1 1 when used as CRC Divisor

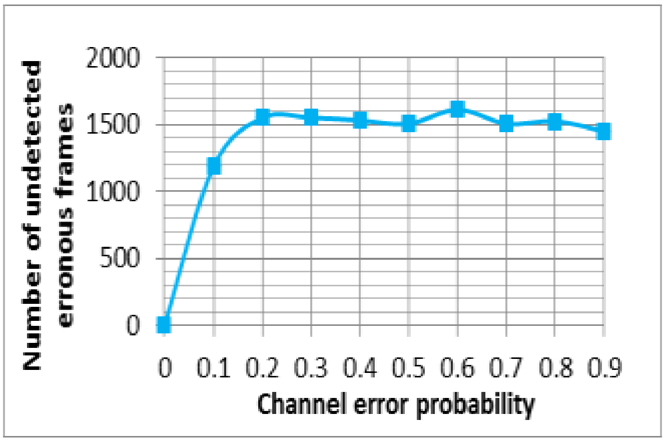

Figure 9: Performance of 1 1 1 0 1 when used as CRC Divisor

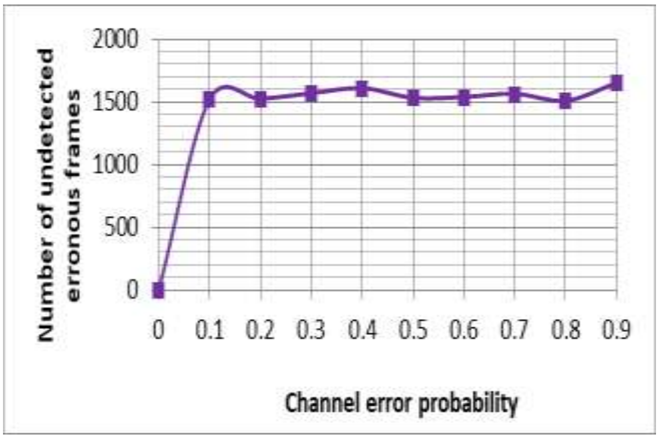

Figure 10: Performance of 1 1 1 1 1 when used as CRC Divisor

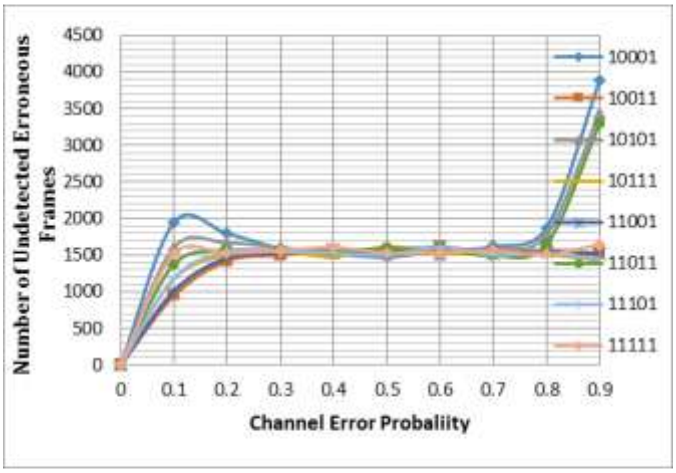

Figure 11: Comparison between different Five bits CRC Divisor

Figure 11 shows the performance comparison of different five bits CRC divisor bit, it can be shown that 10011 has the minimum undetected erroneous frames at average and therefore, gives the best performance in error detection when used as CRC divisor bit.

5.0 CONCLUSION

Reliable communication is one of the most important aspects of both wired and wireless communication. Data transmitted and collected by WSNs is repeatedly unreliable. To guarantee the reliability of a sensor data becomes difficult, as limitations on transmission power due to stern energy constraints make them more susceptible to noise and interference. There are numerous techniques used for error detection at data link layer, among which CRC provides desirable efficiency. In this paper, an analysis has been carried out on cyclic redundant check (CRC4) in other to determine the string of divisor bits that will perform better when used as cyclic redundant check divisor bits, from the graphs, it can be shown that 10011 has the best performance when compared with other five bit divisors since it has the lowest undetected erroneous frames.

REFERENCES

[1] L. Tang, M. Liu, and K. Wang, "Study of path loss and data transmission error of IEEE 802 . 15 . 4 compliant wireless sensors in small-scale manufacturing environments," no. November, 2012, doi: 10.1007/s00170-012-3928-3.

[2] P. Capabilities, "An Overview of Wireless Sensor Networks," pp. 1–23, 2014.

[3] L. In and W. Sensor, "Review of Nature Inspired Technique for Minimize Energy Consumption in Wireless Sensor Networks," vol. 4, no. 05, pp. 505–506, 2016.

[4] M. Roshanzadeh and S. Saqaeeyan, "Error Detection & Correction in Wireless Sensor Networks By Using Residue Number Systems," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 2, pp. 29–35, 2012, doi: 10.5815/ijcnis.2012.02.05.

[5] R. Aggarwal, "A Review of Fault Detection Techniques for Wireless Sensor Networks.," *... J. Comput. Sci. Issues (IJCSI ...*, vol. 10, no. 4, pp. 127–138, 2013.

[6] P. J. M. Havinga, "Ensuring high sensor data quality through use of online outlier detection techniques Yang Zhang *, Nirvana Meratnia and," vol. 7, no. 3, 2010.

[7] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 12, no. 2, pp. 159–170, 2010, doi: 10.1109/SURV.2010.021510.00088.

[8] A. R. Kumar, M. Ashok, and R. P. Sam, "Error Detection and Cleaning for Big Data Sets from Sensor Network Systems on Cloud," vol. 4, no. 5, pp. 261–265, 2016.

[9] D. N. Owunwanne, "Analysis Of The Effectiveness Of Error Detection In Data Transmission Using Polynomial Code Method," *Int. J. Manag. Inf. Syst.*, vol. 14, no. 2, pp. 105–112, 2011, doi: 10.19030/ijmis.v14i2.835.

[10] P. S. Helode, Dr. K. H. Walse, and Karande M.U., "An Online Secure Social Networking with Friend Discovery System," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 5, no. 4, pp. 8198–8205, 2017, doi: 10.15680/IJIRCCE.2017.

[11] A. Fauzi and R. Rahim, "Bit Error Detection and Correction with Hamming Code Algorithm," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 3, no. 1, pp. 76–81, 2017.

[12] W. Fitriani and S. Sikambing, "Single-Bit Parity Detection and Correction using Hamming Code 7-Bit Model," vol. 154, no. 2, pp. 12–16, 2016.

[13] "The Bell System Technical Journal," vol. xx, no. 2, 1950.

[14] K. Singh and M. Cantt, "Outlier Detection: Applications And Techniques," *Int. J. Comput. Sci. Issues*, vol. 9, no. 1, pp. 307–323, 2012.

[15] R. Alsaqour, M. Uddin, and M. Al-hubaishi, "Review of error detection of data link layer in computer

network," no. April 2016, 2014, doi: 10.5829/idosi.mejsr.2013.18.7.11805.

[16] S. Singh, N. Gupta, and R. Gupta, "Implementation of Various Error Detection," pp. 10201–10209, 2018, doi: 10.15680/IJIRSET.2018.0710004.

[17] N. Doukas, "Effectiveness Data Transmission Error Detection using Check Sum Control for Military Applications," no. January, 2008.

[18] S. Mukhopadhyay, S. Member, and C. Schurgers, "Model-Based Techniques for Data Reliability in Wireless Sensor Networks," vol. 8, no. 4, pp. 528–543, 2009.

[19] N. P. Mathew and A. Mohan, "Matrix Code Based Error Correction for LUT Based Cyclic Redundancy Check," *Procedia Technol.*, vol. 25, no. Raerest, pp. 590–597, 2016, doi: 10.1016/j.protcy.2016.08.149.

[20] E. O. Bartholomew and E. A. Oscar, "Error Detection in a Multi-user Request System Using Enhanced CRC Algorithm," *Int. J. Inf. Technol. Comput. Sci.*, vol. 6, no. 9, pp. 14–23, 2014, doi: 10.5815/ijitcs.2014.09.02.

[21] B. Aforouzan, Data Communication and Network: Fourth Edition, 2014. pp. 267-297

[22] I *et al.*, "We are IntechOpen , the world ' s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %," *Intech*, vol. i, no. tourism, p. 13, 2012, doi: 10.1016/j.colsurfa.2011.12.014.

[23] The Bernoulli Experiment and the Distributions it generates" [online]. Available http://www.engr.colostate.edu.ECE303/FA07/matlab/EE303_Lab2_Text.pdf