I. J. Computer Network and Information Security, 2017, 11, 17-26
Published Online November 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.11.02

Error Prone Transmission System to Resist Data Loss in a Wireless Sensor Network

Sunil Kumar
Research Scholar, I. K. Gujral Punjab Technical University, Kapurthala (Punjab), India.
E-mail: sunilymca2k5@gmail.com

C. Rama Krishna
Department of Computer Science and Engineering, NITTTR, Chandigarh, India.
E-mail: rkc_97@yahoo.com

A. K. Solanki
Department of Computer Science and Engineering, BIET, Jhansi (U.P.), India.
E-mail: solankibiet13@gmail.com

Received: 06 June 2017; Accepted: 07 August 2017; Published: 08 November 2017

Abstract—Data losses in wireless sensor network (WSN) commonly occur due to diverse transmission errors such as hardware or software limitations, channel congestion, network coverage constraint and transmission delay. Another important cause for data loss is distinct security attacks caused by illegal interferences of illicit third parties. Apart from that data loss may occur due to some unforeseen causes too. A number of efforts have been made in WSN to control such types of data loss during the transmission process individually or along with various combinations. However, none of them are capable of addressing each of the mentioned cause of data loss in WSN environment. Henceforth, we have proposed an error resistant technique for WSN to address all of the mentioned causes for data loss. The proposed technique also offers a backup system for the accidental data losses. The experimental results shows that the proposed technique offers minimum data loss during the communication process by offering higher *Signal to Noise Ratio (SNR)* and low *Information Loss* compared to the other existing error control techniques. The time efficiency can also be justified by its high *Throughput* and complexity can be verified by measuring *Cyclomatic Complexity*.

Index Terms—Transmission errors, security attacks, data loss, backup system, Signal to Noise Ratio, information loss, throughput, Cyclomatic Complexity.

I. Introduction

The most significant security issue in any data conveying system is unwanted data loss which occurs due to various limitations of used data transmission system. According to Yin et al. (2015)[1], repetition of transmitted message in the form of cyclic redundancy code (CRC), forward error coding (FEC), longitudinal redundancy check (LRC), automatic repeat request (ARQ) and vertical redundancy check (VRC) are the most popular error control techniques for any communication system. However, these techniques are incapable of detecting the position of particular single or multiple-bits error whether they are in discrete or continuous form (Ferng et al. (2014)[2] and Mancheno et al. (2015)[3]). These types of redundancy codes replace the erroneous messages by the redundant transmitted fresh messages at the receiving end or during the communication process. Conversely, these types of redundant error coding techniques employ immense data overhead on the communication channel which is not affordable for various tiny communicating devices used in WSN (A. Karthikeyan (2015)[4] and Kesuma et al. (2016)[5]).

According to Cui et al. (2016)[6], in wireless sensor network, during transmission of data, the transmitted data can be erroneous due to several reasons such as limitations of transmission channels, security attacks, channel noises and high complexities of the transmission system in terms of time and space. The transmitted data bits get corrupted due to these reasons in discrete or continuous form. These errors are sometime very large in size. Generally, data link layer is responsible for controlling various transmission errors. However, when the errors are discrete in nature and large in number then the data link layer cannot control such errors. Henceforth, special care is needed to handle the large and discrete data errors at the application layer. Error detection is one of the important aspects for controlling data errors. A number of techniques have been used so far to detect such types of data errors. The parity coding and checksums are the most popular error detecting techniques. However, these techniques cannot detect more than one bit error. Among the various error control codes, use of Hamming code and Hash function can detect position of error bits; however they have distinct limitations too. Hamming code can detect only single-bit

error whereas Hash function can detect maximum eight bits of discrete or continuous bit errors (Udgata et al. (2011)[7]. However, among the current error control techniques, no one can detect more than eight bit errors in WSN environment (Miyaji et al. (2011)[8], Liu et al. (2013)[9] and Asaduzzaman et al. (2015)[10]).

As data overhead for tiny devices in WSN is one of the biggest challenges. However, the existing error control techniques are not capable of addressing more than eight bit errors during the communication process. Mostly the repetitive transmission of error control codes are used to address the distinct large size of transmission errors. However, these techniques are imposing a huge data overhead during the transmission process which is not affordable for the tiny communicating devices used in WSN infrastructure. Therefore, to address each individual error bit, we have designed an error control technique which imposes minimal amount of data overhead. Thus, the proposed technique solves the requirement of tiny communicating devices, used in wireless sensor network (Ferng et al. (2014)[2], Nisar et al. (2008)[11] and Berger et al. (2016)[12]). Apart from that it minimizes data loss and offers time efficiency as compared to existing error control techniques. It can detect and correct any numbers of error bits whether they are discrete or continuous which is the primary strength of the proposed error control technique. Apart from that the proposed technique is capable of regenerating original message if data loss occurs due to any unforeseen circumstances. Thus, the proposed technique offers a backup system for accidental data loss during the communication process. The particular objective of this research is to facilitate WSN with,

- To minimize transmission errors during the message communication with minimal data overhead.
- To reduce data loss caused by various transmission errors and offering a backup system for unintentional data loss.
- To provide less time complexity by offering higher processing speed during the execution of proposed technique.

Rest of the paper is arranged as follows: Section II comprises related works to examine research gap by analyzing the strengths and weaknesses of various existing security techniques, Section III displays the detail description about the proposed technique and its functionality, Section IV includes assessment platform to define some important parameters for justifying performances of proposed technique, Section V includes result section to examine performances of the proposed technique in distinct aspects, Section VI contains the conclusions to analyze the strengths and weaknesses of the proposed technique and also proposes a future work for improving its performance.

II. Related Works

Number of efforts has been made to resolve various current issues regarding the transmission errors in wireless sensor network. Among such efforts, few are used to detect and correct distinct transmission errors whereas few are used either for detecting or correcting such errors. Arvaree et al. (2011)[13], proposed an application to verify the competence of error control codes. According to authors, the matter and issues related to competence of an error control code can be covered by software metrics. This research defines how software metrics can be applied for examining competence of the established code in the initial phase of expansion. In this work, a tool was assigned for activating an assumed code. It examines the productivity level and generates productivity information. However, this code is not usable for the external codes. Apart from it, compiler is application specific; henceforth, it cannot be executed in any other environment (Lim et al. (2010)[14], Csoka et al. (2015)[15], Al-Riyami et al. (2016)[16] and Kaur et al. [26]).

Macian et al. (2012)[17] and Ibrahim et al. [27], proposed a method to exploit the probability of sensing corresponding errors using Hamming codes. By selectively employing bits in memory, clear result is attained such that errors corresponding to it produce a disorder that does not match any of those that are adjacent to a single error. This work is verified and applied with diverse nature of input file such as structured or unstructured. However, this method is not suitable for detecting and correcting a large number of discrete or continuous data errors. On the other hand, this technique is not suitable for the tiny devices as it has high time complexity.

According to Cui et al. (2014)[18], Mittal et al. [28], Mancheno et al. (2015)[3], Jamalabdollahi et al. (2016)[19] and Yussoff et al. [29], due to space usage, change in state of an element inside a device or system or single-event upset (SEU) is one of the significant reason of disaster or even fault of system-on chip (SOC), error-detection and correction (EDAC) method frequently accepted to defend memory lockups in SOC contrary to error of SEU. In this work, grouping Hamming code algorithm is applied which uses about 32-bit input data and enhances the capability of EDAC as well as it reduces the region overhead of storing check-bits. Here, every 32-bit data is separated into two groups; each of the groupings embraces a distinct error correction and double error detection (SEC-DED) by using Hamming codes. However, this work requires high amount of execution time to process 32-bits data which makes it unusable for small devices. Apart from that, during the execution, devices consumes huge amount of power which makes it unusable for low-life battery enabled devices.

Wells et al. (2010)[20], proposed a soft error resistant video encoder design which customs the intrinsic construction of current video encoders as a basis for construction of a checksum based error detection appliance. The proposed technique can investigate handling of video frames in parallel with negligible extra

price. It can importantly recover superiority of coded video in occurrence of lenient errors. However, retrieval process of original video frames from the encoded video frames suffers with the conversion error. So, the proposed technique is not capable of removing all soft errors from the video frames during communication.

Nisar et al. (2008)[11], proposed small charge codes for sensing called checksum codes and reimbursing of recurrent errors because of voltage over scaling in linear digital filters. According to authors, in the theory of conventional coding, a key issue is analyzing data errors and experiencing important latency as well as computation rates. Hence in this work, latches of low precision shadow have been introduced to classify errors sources because of power over-scaling. The main strength of proposed technique is that it does not require any training and this system acclimatizes energetically to save power, keeping system presentation within satisfactory range. However,in this technique, data errors can be incorporated due to power-fault during the execution of entire process. Apart from that, data loss may also occur due to electrical leakage.

According to Reviriego et al. (2012)[21] and Csoka et al. (2016)[22], single error correction (SEC) code is one of the traditional memory error correction code. Apart from that, further progressive error correction codes (ECC) are normally used when extra protection is necessary. These types of error correction codes should have capabilities to detect the errors as well; however, this feature is normally absent in such kind of error correction codes. Consequently, as per authors, currently available ECCs and SECs are more advanced as they can correct double or triple bits memory errors. Nevertheless, these types of codes offer high execution complexities which liquefy their importance. Henceforth, authors proposed an advanced difference set code to correct as well as to detect distinct errors which are more than single bit along with low complexities. This mutual error detection and correction competency makes the proposed scheme a favorable choice for memory application. However, the proposed technique cannot detect and correct a large number of discrete or continuous error bits. Subsequently, it offers high latency time during the execution which makes it unusable for tiny devices.

Singh et al. (2012)[23], introduced the forward error correction (FEC) code for wireless sensor network. According to authors, lifespan of any wireless sensor network directly relies on effectual usage of its power requirements. Power is mainly used up during wireless communication and reaction. As power maintenance is a key problem of concern in WSN, replication of transmission is not a reliable choice and FEC would be favored over Automatic Repeat Request (ARQ). In this research effort, a well-organized FEC technique for WSNs has been used to escape from retransmission which is not only protects power but also spreads its efficiency and allows it to tackle multi-bit burst error. This error correction technique is efficient for minimizing burst error of even 8-bits. However, this technique is not capable of correcting more than eight bit (discrete or continuous) errors.

Hong et al. (2010)[24], proposed a quick error-detection (QED) technique for actual post silicon authentication for detecting multiple-bit data errors. This technique is mainly introduced for the tiny devices. It converts current post silicon endorsement trials into newfangled authentication checks which expressively decrease error detection latency. QED alterations permit elastic adjustments between attention, error-detection latency and difficulty and can be applied in software with slight or no hardware deviations. However, this technique cannot solve distinct logical bugs during the execution process. This technique is also not effective in the wide range communications.

Henceforth, from so far discussion, we have seen that the present error control techniques are fail to offer any concrete solution for detecting and correcting large data errors with low time and space complexities. These error control techniques need further improvement to enhance their efficiencies. Current literature shows that there is no error control technique available which can detect as well as correct more than eight-bit discrete or continuous errors in WSN environment. Therefore, when a large number of error bits are incorporated within the transmitted data during the communication process, it is very hard or nearly impossible to remove them. Henceforth, in this paper, we have proposed a new error control technique which can detect and correct any number of error bits (whether discrete or continuous).

III. Proposed Technique

From the existing literature we have seen that existing error control techniques are not able to resolve a large number of discrete or continuous errors. Henceforth, we have proposed an error correction technique to control any number of discrete or continuous error bits. First sub-section provides the description of error control bit generation and incorporation within the original input data and the second sub-section describes the working principle of the proposed error control technique.

A. Error Control Bit Generation and Incorporation

The proposed technique involves two rounds of error control-bit incorporation operation.

In the first phase, error control system is included for providing a backup system to avoid accidental data loss. Consequently, second round of error control technique is applied for addressing each and every error bits individually. The overall structure of proposed error control technique is shown in Fig.1. Fig. 1 clearly shows the dual phases of proposed error control bit incorporation technique. The first phase started with splitting input pair of 8-bit binary strings. After splitting, each pairof 8-bit strings are taken and after that lower valued string is subtracted from the higher valued string. These two continuous strings and subtracted string are then concatenated into single string and completed the first phase of error control bit incorporation. In second

phase, concatenated sting is taken and performed binary addition of each pair of continuous bits and the resultant bits are placed after each pair of input bits. The proposed algorithm is described by Algorithm-1.

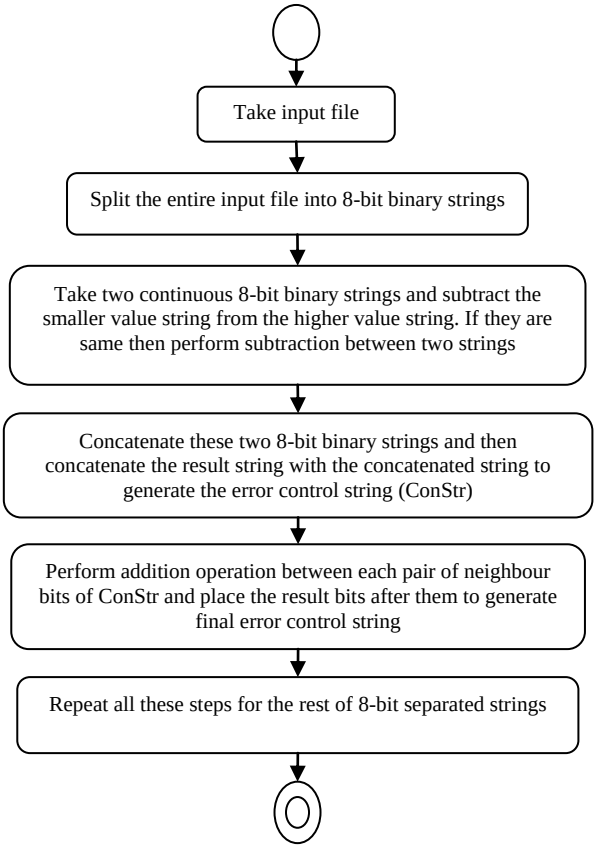

Fig.1. The Proposed Error Control Model

Algorithm-1: Proposed error control bits integration technique

//First phase of error control bit incorporation

a) Split the input file into n numbers of small 8-bit binary strings.

b) Let the two 8-bit input strings are $Str1$ and $Str2$. Calculate the decimal values of $Str1$, $Str2$ and store them in $num1$ and $num2$ as,

$$num1 = \sum_{i=0}^{7} (Str1_i \times 2^i),$$

$$num2 = \sum_{i=0}^{7} (Str2_i \times 2^i)$$

Here, i is the bit position.

c) Perform the subtraction between $num1$ and $num2$ and store the subtracted values in string variable $sub1$ as, if ($num1 \geq num2$)

$$sub1 = num1 - num2$$

Else

$$sub1 = num2 - num1$$

//Conversion of 8-bit string

d) Convert $sub1$ into binary string as,

$$\left.\begin{array}{c} x = sub1 \; modulo 2^i \\ y1 = \dfrac{sub1}{2^i}, \quad where 0 \leq i \leq 7 \\ s' = z \times (10)^{l(x)} + x, where \; l(x) = \lfloor log_{10}^{x} \rfloor + 1 \end{array}\right\} if y1 \neq 1$$

Here $x, y1$ and z are the ordinary integer variables and s' is a string variable where i represents the bit sequences of s'.

e) If s' is of 8-bit length then put it in the string array sub' as $sub' = s'$

Else make s' 8-bit by concatenating zero (0) at MSB (Most Significant Bit) position of s' and put it in the two-dimensional string array sub' as $sub' = s'$.

f) Concatenate $Str1$, $Str2$ and sub' into $ConStr$ as,

$$ConStr = (Str1 \times (10)^{l(Str2)} + Str2) \times 10^{l(sub')} + sub'$$

Where, $l(Str1) = (\lfloor log_{10}^{Str1} \rfloor + 1)$,
$l(Str2) = (\lfloor log_{10}^{Str2} \rfloor + 1)$ and
$l(sub') = (\lfloor log_{10}^{sub'} \rfloor + 1)$.

//Second phase of error control bit incorporation

g) Perform addition between each pair of consecutive bit of $ConStr$ and incorporate the dual results bit after them as

g1) If $x1$ is any ordinary variable then perform,

$$x1 = ConStr_i + ConStr_{i+1}$$

g2) If the length of $x1$ is 1-bit then add 0 at MSB (Most Significant Bit) position of $x1$.

g3) Concatenate $ConStr$, $ConStr'$, and $x1$ into a single string variable C' where initial length of C' is $\emptyset$,

$$C' = \left(\left(\left(\left((C' \times 10) + ConStr_i\right) \times 10\right) + ConStr_{i+1}\right) \times 100\right) + x1, \quad \text{Where } 0 \leq i < 8.$$

h) Repeat steps (a-g) for rest of the dual consecutive 8-bit strings and concatenate all of them into a single string.

In Algorithm-1, step (a) splits the entire input file into 8-bit binary strings. After splitting the input file into several small strings, dual consecutive 8-bit strings are taken from the split strings and assigned to string variables $Str1$ and $Str2$ for initial phase of error control bit incorporation using step (b). Step (b) also calculates the decimal values of $Str1$ and $Str2$ and store them to $num1$ and $num2$ integer variables. Step (c) subtracts $num2$ from $num1$ when $num1$ is greater than or equal to $num2$. Consequently, step (c) subtracts $num1$ from $num2$ when $num2$ is greater than $num1$. The subtracted result is stored into $sub1$ by the step (c) too. Steps (d) and (e) convert the subtracted values into 8-bit binary string (s') and put it to a string variable sub'. Step (f) concatenates $Str1$, $Str2$ and sub' into a single string and stores the concatenated string into string variable $ConStr$. Thus, with step (f), first phase of error control bit generation as well as incorporation operations is completed. In second phase, step (g), adds the two consecutive bits of $ConStr$ in the dual bit format to represent sum and carry bits. The sub-step (g1) adds the two each pair of consecutive bits and outcome is stored into variable $x1$ and the sub-step (g2) checks length of.

$x1$ and if it is single bit, then, it adds 0 at the MSB (Most Significant Bit) position. Sub-step (g3) concatenates the resultant binary string $x1$ with $ConStr$ to include final error control bits. Step (h) repeats all these steps (a-g) for rest of the 8-bit separated strings wherein with the each iteration; two 8-bit consecutive strings are taken as input

B. Workings of the proposed error control technique

After receiving the complete string on the other end, it is used as input to detect and correct the transmission errors. The proposed error control technique is then applied to the received string to detect and correct erroneous bits with referenced error control bits. The vivid working of the proposed error control operation is described by Algorithm-2.

Algorithm-2: Workings of proposed error control operation

//First round of error control operation

a1) Take received string and store it into the string variable Str where $\langle Str_i \rangle$ represent the bit sequence of Str. Let $AddStr$ as well as Ori are ordinary string variables and if n is the total length of received string (Str) then perform,
for $(i = 0; i \leq n; i + 4)$
$$AddStr = (Str)_i + (Str)_{i+1}$$

a2) If $AddStr$ is single bit string, then,
Add 0 at MSB position of $AddStr$
End if

a3) Match each bit of $AddStr$ with $\langle Str_{i+2} Str_{i+3} \rangle$

a4) If all bits of $AddStr$ matched with $\langle Str_{i+2} Str_{i+3} \rangle$, then perform
$$Ori = \Big(((Ori \times 10) + Str_i) \times 10\Big) + Str_{i+1},$$
Where, Ori is a string variable and initial length of Ori is $\emptyset$.
End If

a5) If match is not done then generate the original string by performing subtraction between Str_i and $\langle Str_{i+2} Str_{i+3} \rangle$ or Str_{i+1} and $\langle Str_{i+2} Str_{i+3} \rangle$.
Perform the following operation to eliminate $\langle Str_{i+2} Str_{i+3} \rangle$,
$$Ori = \Big(((Ori \times 10) + Str_i) \times 10\Big) + Str_{i+1}$$
End If
End for

// Second round of error control operation

a6) Let the length of Ori is m, where $m < n$. Take Ori as input and separate each 8-bit string from it and store them into a two-dimensional string array EC.

a7) Perform subtraction between EC_j and EC_{j+1} according to the Algorithm-1 and compare the subtracted result with the EC_{j+2} where $0 \leq j \leq (m \div 8)$.

a8) If match is done,
Eliminate EC_{j+2} with the help of step (a4) or (a5)
End If

a9) If match is not done, replace corrupted bit using EC_{j+2} and EC_j or EC_j and EC_{j+1} by performing,
$sub1 = EC_{j+2} + EC_j$, $sub2 = EC_{j+2} - EC_j$, $sub3 = EC_j - EC_{j+2}$
$sub1' = EC_{j+1} + EC_j$, $sub2' = EC_{j+1} - EC_j$, $sub3' = EC_j - EC_{j+1}$
Match among $(sub1, sub2, \ldots sub1', \ldots sub3')$ and take maximum matched positive result from the list.
Eliminate EC_{j+2} with help of step (a4) or (a5)
End If

a10) Repeat step (a7) to (a9) for the rest of the elements of EC.

a11) After eliminating all error control bits from EC by repeating step (a8) or (a9), reform the output file as same as the input file format.

In Algorithm-2, step (a1) declares some string variables for presenting the proposed error control algorithm. Step (a1) also stores the entire received string into the string variable Str and adds each pair of consecutive bits of Str into another string variable $AddStr$. Step (a2) checks the length of $AddStr$ and if the length of $AddStr$ is single bit then this step adds a 0 at the MSB position of $AddStr$. Step (a3) compares $AddStr$ with the combination of next two bits of Str which are the error control dual reference bits. If match is done then step (a4) eliminates the extra error control reference bits and stores the original bits in a string variable Ori where the initial length of Ori is $\emptyset$. If the match is not done, step (a5) detects the corrupted bit with the help of referenced error control bit and replaced the corrupted bit by regenerating the original bit. Step (a5) eliminates the dual reference error control bits after correcting the erroneous bit. Step (a5) further puts the original bits into the string variable Ori after eliminating dual reference error control bits. Steps (a1-a5) are repeated for other bits of received strings (Str) to correct all individual bit errors and for eliminating referenced error control bits. With the elimination of referenced error control bits, first round of error control operation is accomplished.

In the second round of operation, newly generated string Ori is taken as input where the length of Ori is m. Step (a6) separates ($m/8$) numbers of 8-bit strings from m and stores them in two-dimensional string array EC. Step (a7) subtracts each of the two consecutive elements (i.e. 8-bit strings) of string array EC . The subtracted string is then compared with the next 8-bit string EC which is a reference 8-bit error control string. If the match is done, step (a8) eliminates the reference error control string. If match is not done then, step (a9) modify the corrupted string with the help of reference error control string and after removing all errors, step (a9) eliminates the reference error control string from the EC. Step (a10) repeats the steps (a7-a9) for the rest elements of EC. After eliminating all the reference error control string, retrieved original strings are concatenated and forms the output file in the same format of input file using step (a11). Thus, the original file is retrieved at the receiving end after performing the proposed error control operation to remove any number of discrete or continuous error bits.

IV. Assesment Platform

This section basically includes the description of

experimental setup, data preparation for our experiment and few important parameters which will be used during the result analysis in the next section to justify the performances in distinct aspects and to justify our objectives.

A. Experimental Setup and Data Preparation

The implementation and the performance testing of the proposed error control technique have been done in the Linux environment. Java is used as programming language during the implementation of proposed error control technique. The wpa_suppliment software tool (provided by the Linux) and DHCP client component is used for testing the performance of proposed error control technique in WSN environment. We have tested with distinct kind of input files which are suitable for tiny or small devices that are mostly used in WSN. We have tested with the text data, image and video files to maintain the diversity of input files.

B. Some Important Definition

During result analysis, performances of proposed error control technique in different aspects are represented with the help of few parameters. Henceforth, this section defines these parameters to justify their relationship with the proposed technique.

1) Signal to Noise Ratio (SNR_{dB})

Signal to noise ratio is the sample length of digital data relative to number of incorporated errors. It can be expressed logarithmically in decibels (dB). If SNR of any sample is high, it signifies that the sample is less erroneous. In the equation (1), $x(n)$ is the length of input samples, whereas $y(n)$ is the length of output sample. It can be formulated by using equation 1,

$$SNR_{dB} = 10 \times Log_{10}^{\{\sum_n x^2(n)/\sum_n [x^2(n)-y^2(n)]\}} \quad (1)$$

2) Information Loss (IL)

Fewer, during the transmission, some portions of transmitted information are modified or corrupted by the channel noise or some unwanted circumstancessuch as interference of illicit third party, limitations of transportation system. Mostly this information cannot be retrieved at the receiver end, i.e., it gets permanently lost. Such phenomena are known as information loss (*IL*). It can be formulated by using equation 2,

$$IL = \frac{Actual\ file\ Size - Retrieved\ file\ size}{Actual\ File\ size} \times 100 \quad (2)$$

Any data transmission system is considered highly secure and robust when the information loss occurred during the transportation is very small. In our proposed model, information loss is calculated for justifying the effectiveness of proposed scheme against data errors and various security attacks.

3) Throughput (TP):

Throughput or TP is the amount of work done in a given time. It is measured to calculate the time efficiency of a certain technique. The throughput produced by any technique can be calculated by using equation 3,

$$TP = \left(\frac{Output\ file\ size}{Total\ execution\ time}\right) \quad (3)$$

As we know that, time requirement is inversely proportional to the processing speed of a computing system i.e. with the increment of processing speed, time requirement to accomplish a job decreases. So in these circumstances throughput is increased with the increment of processing speed.

4) Cyclomatic Complexity (CC):

Cyclomatic Complexity (CC) is a measure of source code complexity that has been correlated to the number of coding errors. It is calculated by producing a control flow graph (CFG) of the code that is used to find the number of linearly-independent paths throughout a program unit. The Cyclomatic Complexity of any technique or algorithm can be determined by equation (4). In equation(4), *M* denotes the Cyclomatic Complexity of any technique, *E* denotes number of edges, *N* is the number of vertices or nodes, and *P* is number of predicate nodes (node that contains condition) of control flow graph.

$$M = \left(E - N + (2 \times P)\right) \quad (4)$$

If CC of any technique is high, it is considered as highly time complex ((Mieee B. Nkom et al. (2011)[25]. A range of Cyclomatic complexities and their corresponding analysis are given in Table 1.

Table 1. Cyclomatic Complexity Range

Cyclomatic Complexity	Evolution
1-10	Simple, low risk and highly capable
11-20	Complex, risk and reasonable efficiency
21-50	Highly Complex, risk and less efficiency
> 50	Unstable, inefficient and unreliable

V. Result Analysis and Discussion

In this section, we will test the performance of our proposed technique to minimize data loss and its time efficiency. According to the assessment platform section, capacity of data loss can be justified by analyzing the *SNR* value produced by the output file after applying any error control technique. The capacity of minimizing data loss can be further analyzed by calculating percentage of *Information Loss (IL)*. *SNR* and percentage of *Information Loss* produced at the receiving end after applying proposed dual round of error control operations and some current corresponding techniques have been calculated with the help of Equation (1) and Equation (2). The results of these tests have been plotted in Fig. 2 to compare the performances of proposed error control technique in the context of minimizing transmission

errors. From the assessment platform section, it can be seen that *SNR* is one of the important parameter which can examine the efficiencies of any error control technique to remove the data errors after applying it. As per the definition, if any error control technique offers higher *SNR* then the used error correction technique is said to be efficient to remove data errors. Henceforth, to justify the performances of the proposed error correction technique in terms of its capacity of removing errors has been calculated and compared with corresponding error control techniques with respect to *SNR* in the following Fig. 2.

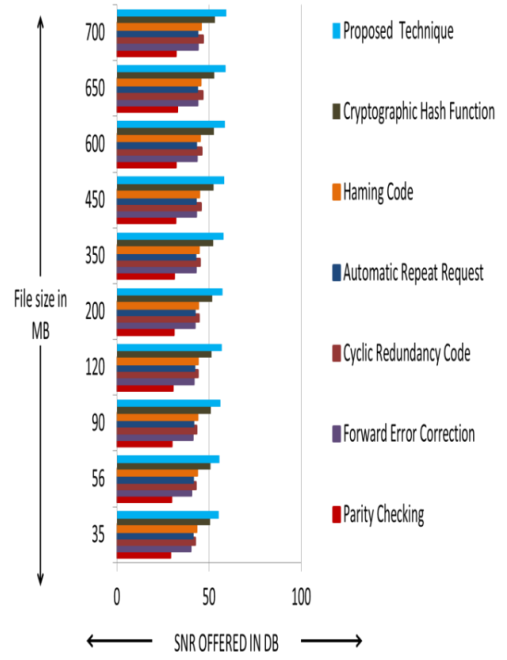

Fig.2. SNR Produced by Applying Distinct Error Control Techniques

As the proposed technique can address each and every error bits and remove them efficiently after detection. Henceforth, Fig. 2 shows that the proposed error control technique produces better *SNR* after removing maximum numbers of transmission errors than the other corresponding error control techniques. According to definition of assessment platform section, if any error control technique offers higher *SNR*, then the applied error control technique is said to be efficient to minimize the bit errors. Henceforth, according to the definition, our proposed error control technique is more efficient to minimize data errors, caused by dusting transmission limitations than other correspondents. The efficiencies of the proposed error control technique and other existing error control techniques for minimizing data loss as well as data errors are further investigated in terms of percentage of *Information Loss* (*IL*) and plotted in the following Fig. 3.

In Fig. 3, we have compared the efficiency of proposed technique to reduce data loss during the transmission process with few well known existing error control techniques.

From the definition of assessment platform section, it can be seen that if the percentage of *Information Loss* (*IL*) is low after applying any error control technique then the applied technique is considered as efficient to protect data loss during the transmission. Henceforth, from the Fig. 3, it can be seen that proposed error control technique offers minimum percentage of *Information Loss* (*IL*) rather than the other existing techniques. Henceforth, the proposed error control technique is efficient to protect data loss among the rest techniques.

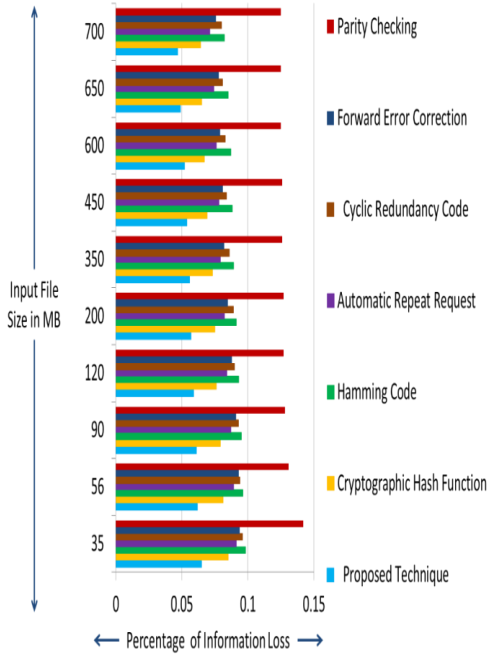

Fig.3. Percentage of Information Loss Offered by Distinct Error Control Techniques

Therefore, from Fig. 2 and Fig. 3, we can see that the proposed technique is efficient to reduce the distinct transmission errors and data loss during the transmission rather than the other existing error control techniques as proposed error control technique can address each and every error bits whether they are discrete or continuous. Even proposed error control technique can control any number of errors during its dual rounds of error control operations. Fig. 2 and Fig. 3 also show that Parity Checking offer very poor performance in controlling distinct transmission errors as well as the data loss during the data transmission in wireless sensor network environment. Henceforth, we will not further compare the performances of Parity Checking with our proposed error control technique in our discussion.

Another important aspect in wireless sensor network for secure data transmission is processing time. If any error control technique takes higher time during generation, incorporation of error control bits or during the detecting as well as correcting error at the receiving end, it may cause data loss. Henceforth, from the definition of assessment platform section, we have compared the time efficiency offered by the proposed technique with other existing techniques in terms of their capacities to offer *Throughput* with the help of Equation

(3). The results of such calculation and comparison have been plotted in Table 2.

Table 2. Throughputs Offered by Distinct Error Control Techniques

Error control techniques for data bits	Generation and Incorporation (MB/Sec)	Detection and/or Correction (MB/Sec)
Forward Error Correction	1.59	1.57
Cyclic Redundancy Code	1.24	1.22
Automatic Repeat Request	1.21	1.20
Hamming Code	1.21	1.23
Cryptographic Hash Function	0.91	0.93
Proposed Technique	1.75	1.73

The proposed error control technique performs both error control bit generation and incorporation at the sending end and dual round of error control operations at the receiving end in single iteration. Henceforth, it involves low time requirements rather than the other corresponding error control techniques. Therefore, the proposed error control technique offers higher *Throughputs* for both generating as well as incorporating error control bits at the sending end and error control operation at the receiving end. In Table 2, we can see that the proposed technique offers higher *Throughput* than the other existing techniques. Henceforth, according to the definition, data processing speed of the proposed error control technique is faster than the other existing techniques.Table 2 also shows that Cryptographic hash function offer lower time efficiency than others though it offers better result in controlling bit errors and protecting data loss during transmission (refer Fig. 2 and Fig. 3). The complexity of the proposed and other existing error control techniques have been further investigated by calculating the *Cyclomatic Complexity* with the help of equation (4). The results of such calculations have been plotted in the Table 3.

Table 3. Cyclomatic Complexities of Distinct Error Control Techniques

Error control techniques for data bits	Cyclomatic Complexities during generation and incorporation of error control bits	Cyclomatic Complexities during detection and correction of bit errors
Forward Error Correction	4	3
Cyclic Redundancy Code	4	3
Automatic Repeat Request	4	3
Hamming Code	3	3
Cryptographic Hash Function	4	4
Proposed Technique	2	2

In Table 3, we can see that proposed technique offers lowest *Cyclomatic Complexity* among the rest techniques. The proposed error control technique involves only dual rounds during both generation and incorporation of error control bits as well as during detection and correction of error control bits. On the other hand, the existing repetitive code transmission processes like cyclic redundancy code, forward error correction and automatic repeat request uses multiple iterations to replace all error bits during their execution. Consequently, Hamming code technique can only detect and correct single bit with in the eight bits. Hence, it requires large time to detect and correct large number of errors during its execution. In the Cryptographic hash function, complex encrypted text as well as hash values are generated during the execution in both error control bit generation as well as detection and correction process. Hence, cryptographic hash function involves high execution time and complexity. Conversely, Table 3 also justifies that proposed technique offers low execution complexity rather than other existing error control techniques. Hence, according to the definition, it is time and space efficient.

Henceforth, Fig. 2 and Fig. 3 show that the proposed technique is efficient to reduce transmission errors and data loss during the transmission process which satisfies our first and second objective. Consequently, Table 2 and Table 3 shows that our proposed technique offers better time and space efficiencies rather than the other existing error control techniques which satisfy our third objective as well.

VI. Conclusions and Future Work

Transmission errors are a big issue for any data communication system. In wireless sensor network, data loss may occur and data errors can be incorporated for diverse limitations of transmission system. Generally, these kinds of incorporated bits errors are multiple bits or single bit and incorporated in continuous or discrete form within the transmitted data. Mostly data link layer is responsible for controlling distinct error during the transmission process (Hong et al. (2010)[24] and Mancheno et al. (2015)[3]). In these layers, a number of error controls have been deployed. On the other hand, over the time of period, distinct error control techniques have been applied on the application layer too. However, these techniques are not capable of controlling large number of data errors whether they are discrete or continuous. Few of them can only detect the single bit error. The existing literature review shows that among distinct existing techniques, only cryptographic hash function can only detect as well as correct 8-bit discrete or continuous errors. Henceforth, to address as well as control any number of bit errors whether they are discrete or continuous, we have proposed an error control technique for wireless sensor network. The proposed error control technique involves dual round operations to control each individual error bit. Apart from it, the proposed technique offers a backup system for an accidental data loss. Result analysis section also justify that proposed technique is efficient to reduce data errors as well as data loss rather than other existing techniques. Result analysis also shows that proposed technique is time and space efficient rather than other correspondent. Thus, the dual objectives of this research work have been achieved.

However, the proposed error control technique cannot

control complete data loss. Henceforth, there is further future scope to improve it. Apart from it, time efficiency of the proposed technique can be improved by enhancing processing speed. Therefore, upgrading of processing speed and reducing the data loss are the future scope of this research.

REFERENCES

[1] R. Yin, B. Liu, H. Liu, Y. Li, and M. Dong, "A quantitative fault tolerance evaluation model for topology in wireless sensor networks based on the semi-Markov process," Neuro computing, vol. 149, no. PB, pp. 1014-1020,2015."doi:https://doi.org/10.1016/j.neucom.2014.07.032"

[2] H. W. Ferng, J. Nurhakim, and S. J. Horng, "Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network," *Wirel. Networks*, vol. 20, no. 4, pp. 625–637, 2014. "doi: https://doi.org/10.1007/s11276-013-0627-4"

[3] S. Mancheno and A. Sanchez, "Power Calculation Error Propagation Correction using Linear Regression Factors in a Distributed WSN for Household Devices," IEEE International Autumn Meeting on Power, Electronics and Computing(ROPEC),2015."doi:10.1109/ROPEC.2015.7395514"

[4] A. Karthikeyan, "A Novel approach for Simultaneous Compression and Encryption of Image in Wireless Media Sensor Network," *IEEE InternationalConference on Applied and Theoretical Computing and Communication Technology (iCATccT)*,pp. 364–369, 2015. "doi: 10.1109/ICATCCT.2015.7456911"

[5] H. Kesuma, A. Ahmed, S. Paul, and J. Sebald, "Bit-Error-Rate measurement of infrared physical channel using reflection via Multi Layer Insulation inside in ARIANE 5 Vehicle Equipment Bay for wireless sensor network communication," 2015 IEEE Int. Conf. Wirel. Sp. Extrem. Environ.,pp.1–6,2015."doi:10.1109/WiSEE.2015.7393099 "

[6] H. Cui, S. Zhang, X. Gan, M. Shen, X. Wang, X. Tian, and N. Mobile, "Information Recovery via Block Compressed Sensing in Wireless Sensor Networks,"*IEEE International Conference onCommunications(ICC)*, 2016." *doi:10.1109/ICC.2016.7510980* "

[7] S. K. Udgata, A. Mubeen, J. Chen, and W. Peng, "Wireless sensor network security model using zero knowledge protocol," *2011 IEEE Int. Conf. Commun. ICC 2011*, pp. 1–5, 2011."doi: *10.1109/icc.2011.5963368*"

[8] A. Miyaji and K. Omote, "Efficient and optimally secure in-network aggregation in wireless sensor networks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6513 LNCS, no. 22700066, pp. 135–149, 2011. "doi:https://doi.org/10.1007/978-3-642-17955-6_10"

[9] X. Liu, Y. Shen, S. Li, and F. Chen, "A fingerprint-based user authentication protocol with one-time password for wireless sensor networks," *Proc. 2013 Int. Conf. Sens. Netw. Secur. Technol. Priv. Commun. Syst. SNS PCS 2013*, pp. 9–12, 2013."doi: 10.1109/SNS-PCS.2013.6553825"

[10] A. Asaduzzaman, K. K. Chidella, and F. N. Sibai, "A smart data logger for enhancing data communication in Wi-Fi based mobile systems," *SoutheastCon 2015*, pp. 1–6, 2015. "doi: 10.1109/SECON.2015.7132925"

[11] M. M. Nisar and A. Chatterjee, "Guided Probabilistic Checksums for Error Control in Low Power Digital-Filters," *2008 14th IEEE Int. On-Line Test. Symp.*, pp. 239–244, 2008. "doi: 10.1109/IOLTS.2008.50"

[12] A. Berger, M. Pichler, D. Ciccarello, P. Priller and A. Springer, "Characterization and adaptive selection of radio channels for reliable and energy-efficient WSN," 2016 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Doha, Qatar, 2016, pp. 443-448."doi: 10.1109/WCNCW.2016.7552740"

[13] T. A. Alvar and R. Atan, "Algorithm analyzer to check the efficiency of codes," 2011 Int. Conf. Inf. Technol. Multimed. "Ubiquitous ICT Sustain. Green Living", ICIM 2011, no. November, 2011. "doi: 10.1109/ICIMU.2011.6122740"

[14] Y. Lim, H.M. Kim, and S. Kang, "A Reliable Data Delivery Mechanism for Grid Power Quality Using Neural Networks in Wireless Sensor Networks," *Sensors*, vol. 10, no. 10, pp. 9349–9358, 2010."doi: 10.3390/s101009349"

[15] T. Csóka and J. Polec, "Analysis of Additive Noise Characteristics in Indoor Wireless Sensor Networks," IEEE International Conference on Computer as a Tool (EUROCON),2015."doi:10.1109/EUROCON.2015.7313779"

[16] A. Al-riyami, N. Zhang, and J. Keane, "An Adaptive Early Node Compromise Detection Scheme for Hierarchical WSNs," *IEEE Access*, vol. 4, pp.4183-4206, 2016. "doi: 10.1109/ACCESS.2016.2594478"

[17] A. Sanchez-Macian, P. Reviriego, and J. A. Maestro, "Enhanced detection of double and triple adjacent errors in hamming codes through selective bit placement," *IEEE Trans. Device Mater. Reliab.*, vol. 12, no. 2, pp. 357–362, 2012. "doi: 10.1109/TDMR.2012.2186965"

[18] B. Cui and S. J. Yang, "NRE: Suppress Selective Forwarding attacks in Wireless Sensor Networks," *2014 IEEE Conf. Commun. Netw. Secur. CNS 2014*, pp. 229–237, 2014. "doi: 10.1109/CNS.2014.6997490"

[19] M. Jamalabdollahi and S. A. R. Zekavat, "Joint Neighbor Discovery and Time of Arrival Estimation in Wireless Sensor Networks via OFDMA," IEEE Sens. J., vol. 15, no. 10, pp. 5821–5833, 2015."doi: 10.1109/JSEN.2015.2449079"

[20] J. W. Wells, J. Natarajan, and A. Chatterjee, "Error resilient video encoding using Block-Frame Checksums," Proc. 2010 IEEE 16th Int. On-Line Test. Symp. IOLTS 2010, pp. 289–294, 2010."doi:10.1109/IOLTS.2010.5560186"

[21] P. Reviriego, M. F. Flanagan, S. F. Liu, and J. A. Maestro, "Error-detection enhanced decoding of difference set codes for memory applications," *IEEE Trans. Device Mater. Reliab.*, vol. 12, no. 2, pp. 335–340, 2012. "doi: 10.1109/TDMR.2012.2183873"

[22] T. Csóka, J. Polec, I. Il, and J. Doboš, "Binary error models for Wireless Sensor Networks," IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2016. "doi:10.1109/IWSSIP.2016.7502750"

[23] M. P. Singh and P. Kumar, "An Efficient Forward Error Correction Scheme for Wireless Sensor Network," *Procedia Technol.*, vol. 4, pp. 737–742, 2012."doi:https://doi.org/10.1016/j.protcy.2012.05.120"

[24] T. Hong, Y. Li, D. Mui, D. Lin, Z. A. Kaleq, and S. Mitra, "Quick Error Detection for Effective Post-Silicon Validation," IEEE InternationalTest Conference (ITC), pp. 1–10, 2010."doi: 10.1109/TEST.2010.5699215"

[25] B. Nkom, "Concise schemes for realizing 1-Wire cyclic redundancy checks," *3rd IEEE Int. Conf. Adapt. Sci. Technol. ICAST 2011, Proc.*, no. Icast, pp. 70–79, 2011. "doi: 10.1109/ICASTech.2011.6145157"

[26] S. Kaur and R. N. Mir,"Clustering in Wireless Sensor

Networks- A Survey", *International Journal of Computer Network and Information Security(IJCNIS)*, Vol.8, No.6, pp.38-51, 2016. "doi: 10.5815/ijcnis.2016.06.05"

[27] S. I.Ibrahim, H. Abuhaiba and B. Hubboub,"Swarm Flooding Attack against Directed Diffusion in Wireless Sensor Networks", IJCNIS, vol.4, no.12, pp.18-30, 2012."doi: 10.5815/ijcnis.2012.12.02"

[28] S. Mittal, A. Aggarwal, and S.L. Maskara, "Contemporary Developments in Wireless Sensor Networks",IJMECS, vol.4, no.3, pp.1-13, 2012. "doi:10.5815/ijmecs. 2012.03.01"

[29] Y. Mohd Yussoff and H. Hashim,"Analysis of Trusted Identity Based Encryption (IBE-Trust) Protocol for Wireless Sensor Networks", IJWMT, vol.1, no.6, pp.52-58, 2011. "doi:10.1109/ICSGRC.2012.6287183"

Authors' Profiles

Sunil Kumar received the B.Tech. degree in Computer Science & Engineering from Bundelkhand University, Jhansi, India, in 2001 and the M.Tech. degree in Computer Engineering from the Maharshi Dayanand University, Rohtak, India, in 2007. His research interests lie in the area of Computer Networks, Wireless Networks and Cryptography & Network Security. He is currently pursuing Ph.D in Computer Science & Engineering from I. K. Gujral Punjab Technical University, Kapurthala (Punjab), India.

Dr. C. Rama Krishna received B.Tech. from JNTU, Hyderabad (1992) with Distinction, M.Tech. from Cochin University of Science & Technology (1995) with First Division, Cochin, and Ph.D from IIT, Kharagpur (2010) in the area of Mobile Adhoc Networks, and he is Senior Member IEEE. Since 1996, he is working with Department of Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh and currently holding the position of Professor and Head of Department (with 20+ years of teaching & research experience). He conducted more than 125 training programmes (Online and Contact mode) of 1 and 2 weeks duration in the upcoming areas of CSE/IT for the faculty of Engineering Colleges and Polytechnics to improve quality of technical education. He is Professor In-charge for Campus-wide Internet Administration, Institute Web Portal and Hardware Maintenance, NCTEL Web Portal for Video Lectures, Go-Green Initiative (paperless office). He is also Liaison Officer for Delhi to finalize training needs and to mobilize teachers to attend various training programmes of NITTTR Chandigarh. His research interests include Computer Networks, Wireless Networks, Cryptography & Cyber Security, and Cloud Computing. He published more than 90 research publications in referred International and National Journals and Conferences. He guided more than 62 Master of Engineering theses in Computer Science and Engineering and he is guiding 8 Ph.D students in the area of wireless networks and cloud computing.

Dr. A. K. Solanki Prof. & Head Information Technology Deptt in Bundelkhand Institute of Engineering & Technology, Jhansi [U.P], India, has obtained his Ph.D degree in Computer Science & Engineering from Bundelkhand University, Jhansi. He has more than 28 years teaching Experience. Prof. Solanki has also appointed as an Executive Committee Member of National Executive Council of Indian Society of Technical Education (ISTE) for three years 2009-2012 for Utter Pradesh and Uttrakhand region. Now currently he is the Section Chairman of Utter Pradesh and Uttrakhand region of Indian Society of Technical Education (ISTE) for three years 2012-2017. He is a member of BOS/RDC in many Universities and also member of Selection & Inspection Committee of AICTE/UPTU and other Universities. He has published a good numbers of International & National research papers in area of Data warehousing, web Mining, Wireless Communication.

How to cite this paper: Sunil Kumar, C. Rama Krishna, A. K. Solanki,"Error Prone Transmission System to Resist Data Loss in a Wireless Sensor Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.11, pp.17-26, 2017.DOI: 10.5815/ijcnis.2017.11.02

