Energy-Efficient Robust Data Communication in WSNS (Wireless Sensor Networks)

[1]Joong-Ho Lee

Background/Objectives: *Wireless sensor networks (WSNs) with thousands of sensor nodes are deployed under hostile environments and battery constraints. Sensors have to operate for as long as possible in a WSN because of power constraints.*

Methods/Statistical analysis: *The LEACH (Low-energy adaptive clustering hierarchy) scheme is a clustering algorithm to help increase energy efficiency in WSNs. As the semiconductor technology develops, the feature size of sensor nodes also decrease, which is one of the main factors that deteriorates the reliability of the network. Therefore, a fault detection method is adopted among the sensor nodes in WSNs. Previous studies to reduce the power consumption of WSN nodes and increase the reliability of the network have been inherently conflicted because of the fact that increasing the network reliability leads to more power consumption.Findings: In order to guarantee reliable operation of the sensor nodes, the sensor node or the data transmission between the channels must have error recovery capability to compensate for any failure that may occur in a large network. In addition, these sensor nodes have to operate for as long as possible under power constraints. Error detection and correction methods are applied to WSNs even though they consume more power due to redundant parity bits. This study proposed an error-correcting code (ECC) scheme for use in WSNs and for reducing power consumption. This is rendered possible by simplifying the error detection and correction process in the ECC. In this paper, we analyze the efficiency relationship between a power-efficient clustering algorithm and WSN reliability improvement. We also analyze and model the types of errors that may occur in the links between sensor nodes and nodes in the network. Based on this analysis, we propose an ECC scheme with improved power consumption efficiency. Improvements /Applications: This proposed code is called a cross diagonal parity check code. It has the same parity check overhead as the Hamming code but reduced error-check complexity. The error correcting processing time is reduced from 6-XOR stages to 4-XOR stages (~33%) when compared to the ATM-8 HEC code for 64 bit data.*

Keywords: *Wireless sensor networks, Energy efficiency, LEACH scheme, clustering, reliability, ECC*

I. INTRODUCTION

Significant progress has been made in the wireless sensor network (WSN) field over the last few decades, which have led to the development of a wide range of applications. Owing to advances in semiconductor technology, micro electro mechanical system (MEMS)-based sensor technology--which involves low-power RF design--has facilitated the development of relatively low-cost wireless micro-sensors.[1,2] These tiny low-cost sensors can be used in applications requiring hundreds or even thousands of sensors to form a high-quality networks.[3] Paradoxically, as wireless sensor networks become smaller and cheaper, robust data collection and transmission become more difficult. Therefore, higher reliability is required in data collection and transmission.[4]

Sensors monitor a wide range of natural environments under harsh natural and limited power conditions. Under these conditions, the sensors must be able to reliably collect and transmit data.[5] Sensors are randomly deployed in a large area where people are not involved. Therefore, a sensor node must have self-recovery capability in case of hardware failure. Applying error recovery technology can help detect errors in sensor nodes and correct error bits. WSNs consist of a base station and hundreds-to-thousands of sensor nodes. Applying a sensor node grouping methodology within the communication area can reduce power consumption. Energy-efficient routings for WSNs have been researched previously.[6] LEACH(low-energy adaptive clustering hierarchy) uses a single-hop clustering algorithm in which the cluster head communicates with the sink node directly.

The ARQ(automatic repeat request) and FEC(forward error correction) schemes are typical methods for increasing network reliability. In ARQ, the transmitter retransmits if it does not receive a complete packet flag signal or receives a retransmission signal. FEC implementation is based on an error-correction code (ECC), which allows the addition of redundancy into packets to detect and correct specific bit errors. Therefore, FEC can improve reliability and is suitable for low-power operation compared to ARQ since there is no need to retransmit error packets.[7]

In this study, we examine the energy consumption model in the channel for improving of the reliability of a network, and propose an ECC based on this. We also simulate the search for alternate paths in case of a faulty node. We report the results of these simulations.

II. MATERIALS AND METHODS

Energy-efficient operation in WSNs is an important factor in system configuration. In particular, when data transmission errors occur due to system malfunction, it is necessary to perform additional operations to detect an error--a factor that lowers the energy efficiency. To build fault-tolerant WSNs, we need to examine analytical data on the energy efficiency between the data transmission packet length and the method for fault tolerance. The ARQ scheme, a typical method for controlling errors in a WSN, adopts a CRC(cyclic redundancy check) code scheme. However,

Revised Manuscript Received on January 03, 2019.

Joong-Ho Lee, Department of Computer Science, Yongin University, Korea.

the start node must retransmit data packets to the sink node if an error that cannot be corrected by the CRC code occurs.[8] The so-called ATM-8 HEC code is commonly used in the CRC to detect data bit errors within 64 bits. A total of 7 parity bits are added, the ECC code is generated from the polynomial x^8+x^2+x+1. The ATM-8 HEC code is made up of 6 XOR logic stages, with an overhead of ~700 XOR gates.[9] FEC is another error control strategy in WSNs. As an error-correcting strategy, it is more efficient in terms of power consumption because there is no need of retransmitting error packets.[10]

The Hamming code is a typical code system for ECCs and block codes such as Reed-Solomon. Likewise, BCH codes are efficient for larger data packets. The ECC block codes are represented as ***(n, k, p)*** and the code rate is defined as ***Rc = k/n***. Assume that the data consist of a certain number of information bits denoted by ***k***. A number of check bits ***p*** identifies the error from the check bits. A number of check bits ***p*** can identify a total of 2^p cases. Therefore, the check bits check for errors in the number of bits for the range of information bits from ***0*** to ***p*** + ***k***.

$$2^p \geq p + k + 1 \quad (1)$$

2.1. *Related Work*

The ATM-8 HEC code can be implemented in two ways: serial and parallel. A serial implementation base on the polynomial divisor $g(x) = x^8+x^2+x+1$ is simple, but it takes a lot of time to generate the codeword.[11] A parallel implementation is suitable for systems that require high-speed computation, although it is an expensive solution. However, it is not suitable for a system that operates beyond 3.2 Gbps clock speed. For example, the ATM-8 HEC code needs 6 stages of 2-input XOR gates for a data length of 64 bits. The CRC calculation time must be satisfied within a < tCCD = 5nCK.[12] The square code can improve the calculation speed and overhead compared to the ATM-8 HEC code. This coding scheme has row- and column-direction parity check bits for detecting bit errors. This row- and column-direction parity check bits can check crossly for each data bit. A parity bit is calculated along each row and column when the number of data "1" is odd. Table 1 shows the configuration of the code word. It represents a 24-bit code word(=n), with 16-bit information length(=k) and 6 parity bits(=p).[13] The parity bit p0 checks the odd bits of "1" from the sum of all the data bits d0-d3 in the first row. Parity bits p0-p3 check the odd bits with "1" in the row direction, and parity bits p4-p7 check the data bits in the column direction in the same manner. For the odd-parity check system, if the sum of the data bit is "1", the parity bit will be "1". Otherwise, the parity bit will be a "0". Finally, syndrome bit s0 must be "0", which is the sum of all the first row data bits and parity bits. The syndrome bits s1-s3 are calculated in the same manner. The generated codeword satisfies the minimum distance (d_{min} = 3), so that the error bit can be detected and corrected. Codewords are organized in the following sequence:

$$\text{codeword}(n) = d0\ d1\ d2\ d3\ p0\ d4\ d5\ d6\ d7\ p1\ d8\ d9\ d10\ d11\ p2\ d12\ d13\ d14\ d15\ p3\ p4\ p5\ p6\ p7 \quad (2)$$

Table 1: Configuration of 16 bits information

	16 bits				
	data	Data	data	data	parity
data	d0	d1	d2	d3	p0
data	d4	d5	d6	d7	p1
data	d8	d9	d10	d11	p2
data	d12	d13	d14	d15	p3
parity	p4	p5	p6	p7	

2.2. Radio Channel Modeling

The LEACH algorithm uses a simplified radio model E_{device} = 50 nJ/bit to operate transmitter/receiver devices, with ϵ_{amp} = 100 pJ/bit/m^2.[14,15] Figure 1 shows the radio model.

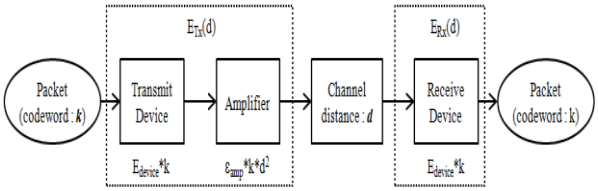

Figure 1. radio energy model between transmit and receive node

To transmit a k-bit message at distance d, the radio model expends is as follows:

$$E_{Tx}(k,d) = E_{Tx-device}(k) + E_{Tx-amp}(k,d)$$
$$E_{Tx}(k,d) = E_{device} * k + \epsilon_{amp} * k * d^2 \quad (3)$$

To receive a k-bit message from the transmit node, the radio model expends is as follows [14] :

$$E_{Rx}(k,d) = E_{Rx-device}(k)$$
$$E_{Rx}(k,d) = E_{device} * k \quad (4)$$

Based on previous assumptions, the ARQ scheme needs twice as much as radio energy than the FEC scheme. The total energy consumption is as follows:

$$2 * (E_{Tx}(k,d) + E_{Rx}(k,d)) =$$
$$2 * (E_{device} * k + \epsilon_{amp} * k * d^2 + E_{device} * k) \quad (5)$$

However, the FEC-based wireless energy consumption increases only in proportion to the number of parity bits ***p***. In the FEC scheme, radio energy for transmission and reception is expended as follows:

$$E_{Tx}(k+p,d) = E_{device} * (k+p) + \epsilon_{amp} * (k+p) * d^2 \quad (6)$$
$$E_{Rx}(k+p,d) = E_{device} * (k+p) \quad (7)$$

Eventually, the FEC outperforms ARQ in terms of energy efficiency in large-scale WSNs.

2.3. Odd-weight Cross Diagonal Parity Code

Data packets in a transmitting node encode a codeword, including parity. They are transmitted through the channel to the receiving node. The codeword is then decoded back to the original data. Figure 2 shows the basic schematics of the encoding, transmission, and decoding processes.

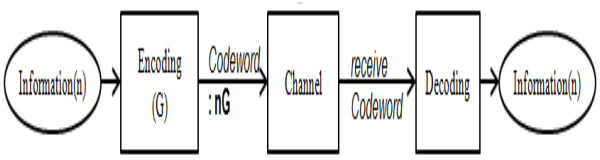

Figure 2. Encoding & Decoding in the transmission channel

The codeword of information ***n*** containing parity ***p*** may be generated by multiplication with generator ***G***. For ***n***-bit data length, ***G*** has a form $[I_n : C]$, where I_n is the $n \times n$ identity matrix and ***C*** is the $n \times p$ binary matrix where ***p*** denotes the number of parity bits. At the receiving node, the syndrome ***s*** is calculated when decoding the codeword. The parity matrix ***H*** is constructed from the generator matrix ***G***. It has the form $\mathbf{H} = [C^T : I_p]$. Syndrome **s** decodes the error vector ***e*** and is represented as follows:

$$s = nG^{H^T} + e^{H^T} \quad (8)$$

2.3.1. Odd-weight Cross Diagonal Parity Code Generation

For the 8-bit data in the proposed odd-weight cross parity (12, 8, 4) code, Table 2-a shows the mapping relationship between the data bits and the parity bits in the codeword generation. For a codeword with a data length greater than 8 bits, the table can be extended as in Table 2-b.

Table 2: Configuration of 8 bits, 9bits information

(a)8 bits Configuration

	8 bits			
	data	data	data	parity
data	d0	d1	d2	p0
data	d3	d4	d5	p1
data	d6	d7	-	p2
parity	p0	p1	p2	p3

(b) 9 bits Configuration

	9 bits			
	data	data	data	parity
data	d0	d1	d2	p0
data	d3	d4	d5	p1
data	d6	d7	-	p2
parity	p0	p1	p2	p3

From Table 2-a, the codeword generator G and the parity H are

$$G = \begin{bmatrix} 1&0&0&0&0&0&0&0&1&0&0&1 \\ 0&1&0&0&0&0&0&0&1&1&0&0 \\ 0&0&1&0&0&0&0&0&1&0&1&0 \\ 0&0&0&1&0&0&0&0&1&1&0&1 \\ 0&0&0&0&1&0&0&0&0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&0&1&0&1&1 \\ 0&0&0&0&0&0&0&1&0&1&1&1 \end{bmatrix}$$

$$H = \begin{bmatrix} 1&1&1&1&0&0&1&0&1&0&0&0 \\ 0&1&0&1&1&1&0&1&0&1&0&0 \\ 0&0&1&0&0&1&1&1&0&0&1&0 \\ 1&0&0&1&1&0&1&1&0&0&0&1 \end{bmatrix}$$

The syndrome equation is

S0 = d0 ⊕ d1 ⊕ d2 ⊕ d3 ⊕ d6 ⊕ p0
S1 = d1 ⊕ d3 ⊕ d4 ⊕ d5 ⊕ d7 ⊕ p1
S2 = d2 ⊕ d5 ⊕ d6 ⊕ d7 ⊕ p2
S3 = d0 ⊕ d4 ⊕ d3 ⊕ d6 ⊕ d7 ⊕ p3

The generated codeword satisfies the minimum distance 3, so that a single error bit can be detected and corrected. Let us consider an example of generating a codeword from a data bit to be transmitted. When the message is transmitted as ***n*** = [0000 0110], the codeword ***nG*** is generated as [0000 0110 0110]. If a 1-bit error occurs at the second bit in the message and ***n'*** = [0000 0100 0110], the data are received, and the syndrome value is ***s*** = [0110]. The data bits can be decoded into the original message since the generator ***G*** is a systematic code.

III. RESULTS AND DISCUSSION

3.1. Simulation of Faulty Node Bypassing

Figure 3 shows the simulated results of setting the bypass path, assuming the fault node shown in the figure, for about 1000 random nodes. As shown in the figures, the path bypassing the fault sensor node has the same or great number of nodes than the original path. This means that the bypass path requires more power to transmit packets by equations 3, 4. Therefore, correcting the error rather than bypassing the avoidance path can reduce the power consumption of the sensor node. Figure 4 shows a data comparison of the avoidance node and the error node in 100 accumulations.

3.2. Cross-Diagonal Parity Check Code Comparison

Figure 5 shows the minimum number of parity bits of a SEC (single error correcting) code for a range of values of n information bits. The proposed (12, 8, 4) code is a systematic, quasi-cyclic code that can correct and detect 1-bit errors.

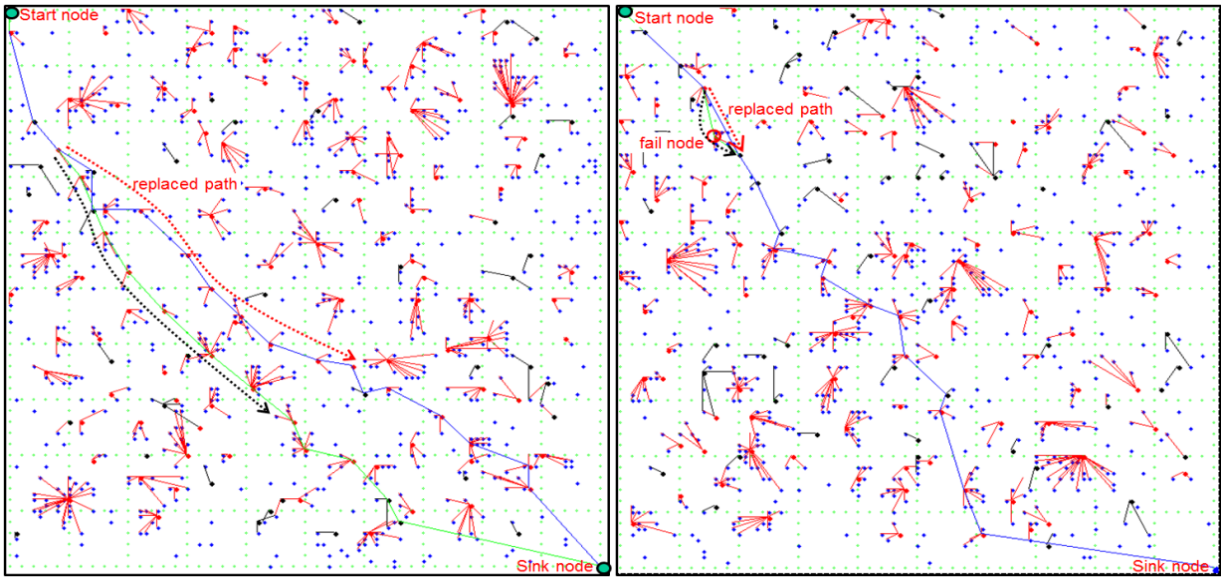

Figure 3. Simulation results showing example of faulty node bypassing

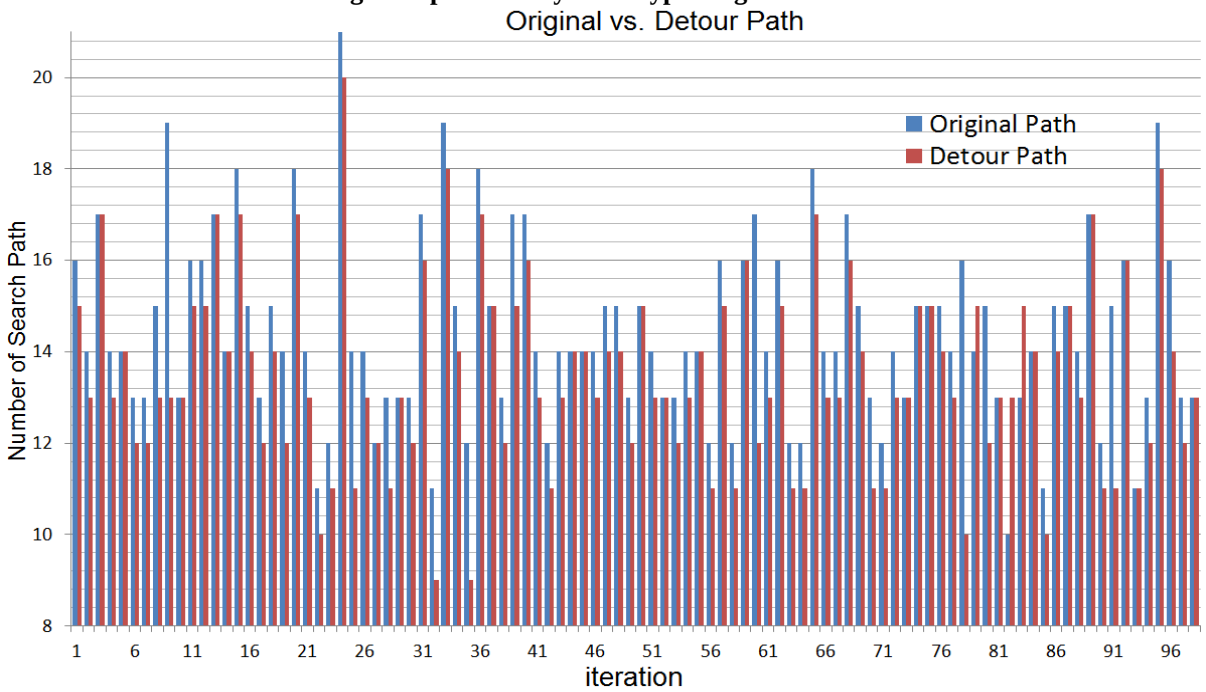

Figure 4. Simulation results showing 100 times accumulation between original and avoidance node

Number of Information Bits	Number of Parity Bits for SEC	
	Hamming Code	Cross-Diagonal Code
1	2	2
2	3	3
3~4	3	3
5	4	4
6	4	4
7~9	4	4
10~11	4	5
12	5	5
13~16	5	5
17~20	5	6
21~25	5	6
26	5	7
27~30	6	7
31~36	6	7
37~42	6	8
43~49	6	8
50~56	6	9
57~57	6	9
58~64	7	9

Figure 5. Parity bits for Error Correction

IV. CONCLUSION

This paper demonstrates the advantages of the cross diagonal parity check code in WSNs. Through radio channel modeling(equations 6,7), we showed that the application of the ECC technique based on the FEC scheme to faulty nodes in a WSN is advantageous over the ARQ scheme in terms of power consumption. In this paper, we assume that a sensor node failure occurs during data transmission in the WSN, and the simulation results showed that it consumes more power because it the bypass path required is longer than the original path.

The proposed scheme was compared to both the Hamming code and a previous square code. The proposed code scheme reduced the power consumption by ~30% when compared to the Hamming code because it can reduce the number of XOR stages from 6 to 4 to generate the codeword. Figure 6 shows the graph of differences between the parity length of the cross diagonal parity check code and that of the conventional code for the same information length. This shows that the proposed scheme has the same parity length as the Hamming code, except for the specific length.

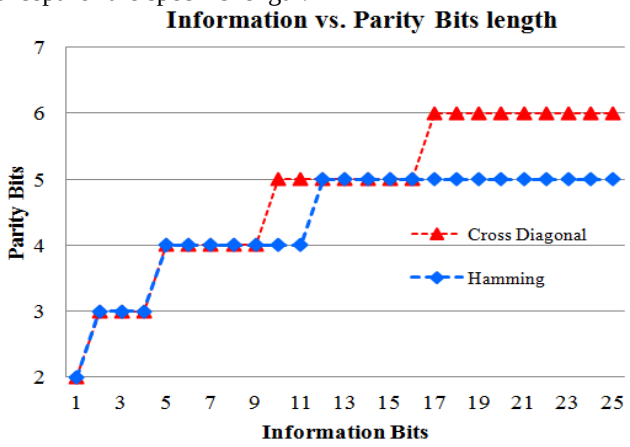

Figure 6. Parity bits comparison graph between Cross Diagonal Parity Check Code and Conventional Code

ACKNOWLEDGMENT

This work was supported by YongIn University.

REFERENCES

1. J. Hill et al., System Architecture Directions for Networked Sensors. Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS '00), 2000: 93-104,.
2. Chandrakasan, Amirtharajah, Cho, Goodman, Konduri, et al. Design Considerations for Distributed Microsensor Systems. In IEEE 1999 Custom Integrated Circuits Conference (CICC), 1999 May: 279–86.
3. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient routing protocols for wireless microsensor networks. Proc. 33rd Hawaii Int. Conf. System Sciences (HICSS), Maui, HI, 2000 Jan.
4. S. Mukhopadhyay, C. Schurgers, D. Panigrahi, S. Dey. Model-Based Techniques for Data Reliability in Wireless Sensor Networks. IEEE Transactions on mobile computing. 2009 April:8(4): 528-43.
5. S. Mukhopadhyay et al., Model Based Error Correction for Wireless Sensor Networks, Sensor and Ad Hoc Communications and Networks. IEEE SECON. 2004 Oct: 4-7.
6. Md. Zair Hussain, et al. Analysis of Lifetime of Wireless Sensor Network. International Journal of Advanced Science and Technology. 2013 April:53: 117~26.
7. Oskar Eriksson, Error Control in Wireless Sensor Networks: A Process Control Perspective. ISSN: 1401-5757, UPTEC F11 030, 2011:1-32.
8. M. Roshanzadeh. Error Detection & Correction in Wireless Sensor Networks By Using Residue Number Systems. I. J. Computer Network and Information Security, 2012 Feb: 29-5.
9. Kibong Koo, et al. A 1.2V 38nm 2.4Gb/s/pin 2Gb DDR4 SDRAM with Bank Group and x4 Half-Page Architecture. IEEE International Solid State Circuits Conference, 2012 Feb: 40-1.
10. R. Logapriya, et al. Efficient Methods in Wireless Sensor Network for Error Detection, Correction and Recovery of Data, International Journal of Novel Research in Computer Science and Software Engineering. 2016 May-Aug:3: 47-54.
11. F. Monteiro, A. Dandache, A. M'sir, B. Lepley. A Fast CRC Implementation on FPGA Using a Pipelined Architecture for the Polynomial Division. The 8th IEEE International Conference on Electronics, Circuits and Systems, ICECS, St Julian, Malta.2001 Sep:1231-1234.
12. J. Moon. Fast Parallel CRC & DBI Calculation for High-speed Memories:GDDR5 and DDR4, IEEE International symposium, Circuits and Systems (ISCAS), 2011 May15-19:317–20.
13. Joongho Lee. Square Code in WSN(Wireless Sensor Network). International Journal of Future Generation Communication and Networking, 2017 Jun:10(6): 55-4.
14. W. R. Heinzelman, A. P. Chandrakasan and H. Balakrishnan. An Application-Specific Protocol Architecture for Wireless Microsensor Networks. Transactions on Wireless Communications. 2002 October:1(4):660-70.
15. S.K.Bisoy, Pradeep Kumar Mallick, Anjana Mishra, "Fairness Analysis of TCP Variants in Asymmetric Network", International Journal of Engineering & Technology, Vol: 7 (2.12) , pp:231-233, 2018, ISSN: 2227-524X.