ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Cluster Based Congestion Avoidance and Security (CBCAS) Technique Using Wireless Sensor Network

V.Perumal[1], K.Meenakshi Sundaram[2]

Ph.D Research Scholar, Department of Computer Science, Erode Arts & Science College(Autonomous), Erode, Tamilnadu, India[1]

Associate Professor, Department of Computer Science, Erode Arts & Science College (Autonomous),Erode, Tamilnadu, India[2]

ABSTRACT: Wireless Sensor Network is one of the main features in physical environmental inquiry. Wireless Sensor Network (WSN) consists of many sensor nodes which are capable of Sensing, Computing and Providing Wireless Communication. Sensor nodes are deployed in a region of interest to be applied in many applications such as Smart Office Monitoring, Military Surveillance, Industry and other types of Monitoring Applications. Since wireless sensor nodes suffer from limited power, large scale network designing has posed many challenges. Clustering techniques is one of the most effective methods employed to conserve energy of the sensor node. It reduces the network traffic in the Base Station and also enables the routing of data to reduce the power consumption in WSN. The Congestion mechanism avoids packet loss and is mostly focused on traffic that affects the continuous flow of data and arrival of data from the source to destination delay time. Finally, Security is a technique that can be used today to hide confidential information from the attack of an intruder.

KEYWORDS: Sensor nodes, Clustering, congestion Avoidance, Cryptography, WSN.

I. INTRODUCTION

Wireless Sensor Network consists of many sensor nodes which are capable of Sensing, Computing and Wireless Communication. These nodes are deployed in a region of interest to be applied in many applications such as Smart Office Monitoring, Military Surveillance, Industry and other types of Monitoring Applications [1].

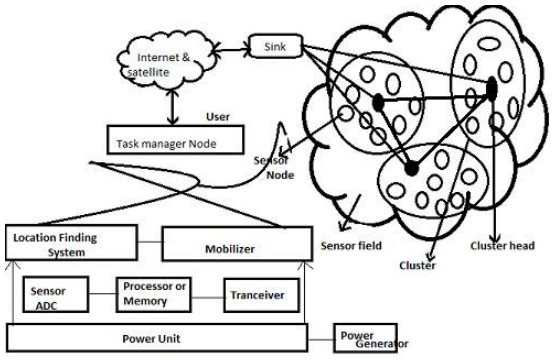


Fig 1.1 WSN Architecture

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

The major constraints of WSNs are the limited power sources of the sensor nodes. The battery operated sensors are often deployed in an unattended hostile environment, so replacement of their battery is almost impossible which make the sensor node energy constraint. Clustering sensor node is one of the most effective techniques which is employed to conserve energy of sensor node. In the process of clustering the network is divided into many groups, called Cluster Head (CH). CH responsible for collecting the data from their members sensor nodes within the clusters, aggregate them and send it to a remote base station (BS) directly or through other CHs. The base station is connected to a public network such as internet for public notification of the event [3,4].

Mainly congestion happens in the intra cluster to do the process of transmitting the destination of packets in many to one manner form sensor node to CH. The main reason for occurrence of congestion is communication path, node's energy level and node's buffer size. The congestion organizes technique in WSN are classified under two categories: Link level congestion and node level congestion. Node level congestion arises from buffer overflow in the node, which results in packet loss. The link level congestion is related to wireless channels shared by several nodes through competitive MAC layer protocol. Link level congestion control can achieve by using multiple access technique such as CSMA, FDMA, TDMA and CDMA to prevent congestion by exercising light degree buffer management. The most challenging congestion mechanisms are congestion Avoidance, detection and alleviation. The congestion avoidance is referring to as proactively routing protocol plays an important role to select best nodes and to route the data traffic from the source to destination. Congestion detection in a timely manner during data forwarding, sensor nodes monitor the buffer occupancy and the channel utilization [5,6,7].

Cryptography enables to store sensitive information or transmit it across insecure networks. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptology embraces both cryptography and cryptanalysis. A cryptographic algorithm or cipher is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key – a word, number, or phrase – to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. The cryptography can be classified into two categories: conventional cryptography and public-key cryptography. In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption [8,9,10].

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

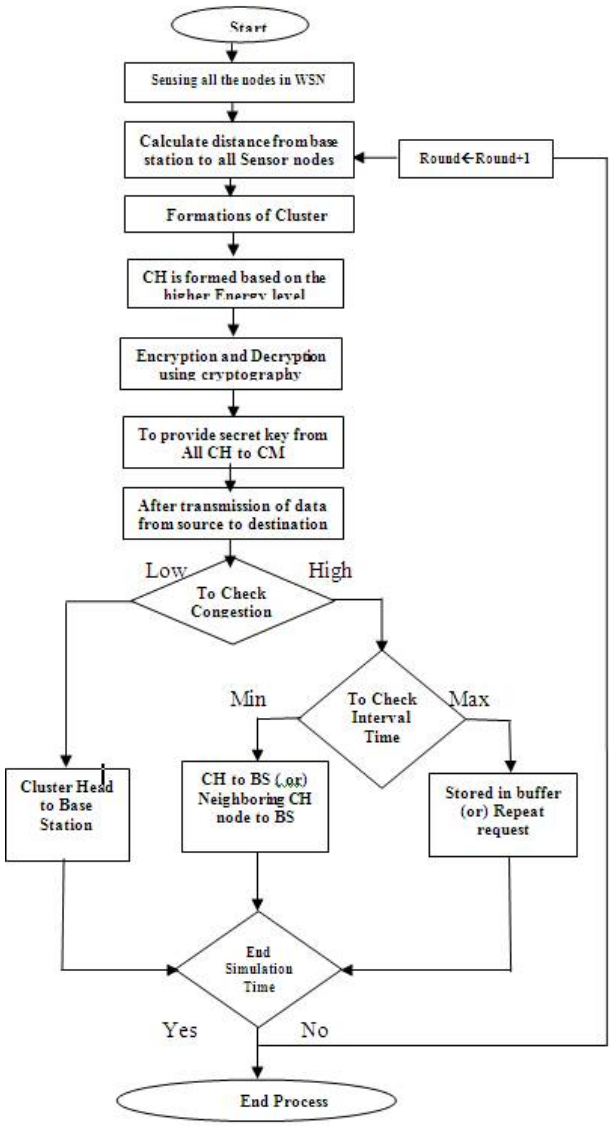


Fig: 3.1 Cluster Based Congestion Avoidance and Security

Our suggested method will choose the high energy level of the nodes and will appropriately spread the cluster heads in the cluster area. Through the cluster head, broadcasting of information takes place in two ways: 1st way from cluster head, sensor nodes have collected data and straight away transmit to the base station. 2nd way, from neighboring cluster head data will be transmitted through base station.

While data transmission time congestion is occur, this is right to check congestion level they are low and high. When the congestion level is low then the packets are directly sends to base station from CH. In order to describe that congestion level is high, and then condition occurs to check the interval time. In mean while condition falls in less than or equal position then the packets are transmitted from CH to BS or in another way it will transmit the data from neighboring CH node to BS. When the condition is greater than the maximum interval time, then the packets are stored

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

in the buffer or repeat request process will be active. At the last all these process will meet the end simulation time, while the simulation ends then the process will end or otherwise data transmission will repeat its process from the start to end.

WSN compute the radius of the cluster head through its distance from base station. CBCAS algorithm is classified into various rounds. In every round, every cluster node will decide whether they will become a cluster head according to the threshold value of the entire network.

$$T(n) = \frac{p}{1-p\left(r \bmod \frac{1}{p}\right)}, \quad n \epsilon G \qquad (1)$$

N denotes the no. of node; P is a priority for the probability of a node which being a chosen cluster. R indicates the current round and G is the set of node that has not yet become head set and Members for the last 1/p rounds. Every cluster head selection will produce a round between 0, 1. Each node's are compute its CH radius in terms of its distance from the BS using.

$$R_{size} = R_{min}\left[1 + \frac{dBS - dBSmin}{dBSmax - dBSmin}\right] * speed_{changr\_rate} \qquad (2)$$

R_{min} is the minimum cluster size and speed $_{change\ rate}$ differs the speed rate in radius they are protocol parameter .d_{BSmin} is the distance of a node which is nearer to the base station and d_{BSmax} is the distance of the farthest node to the BS.

The Energy information broadcasted and receiving is determined as transmission Energy which is represented by $E_{Telec\ and}$ receiving Energy represented by $E_{Rx.}$ Tobroadcast s bit packet length within distance d, a sensor node utilizes on Energy E_{Tx} provided by

$$ETx(s,d) = ETxelec(s) + ETxamp(s,d)$$

$$= Eelec * s + Eamp * s * d^2 \qquad (3)$$

To receive an s packet length within a distance d, a sensor node utilizes an Energy E_{Rxelec} provided by

$$ERx(s) = ERxelec(s) + Eelec * s \qquad (4)$$

The total energy consumption in each round is

$$E_{total} = \sum_{i=1}^{K} E_{CH}(i) + \sum_{j=1}^{N-K} E_{mem}(j) \qquad (5)$$

Where K is the number of cluster heads and N is the number of sensor in the network.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

The information is distinguished from the sender, the loss of time to go to the recipient and following the Queuing delay (d_Q), Propagation delay (d_P) and Transmission delay (d_T).

$$D(S,R) = dQ + dT + dP \quad (6)$$

The link delay D (Sender(S), Recipient (R) is a measure of the delay a packet experiences when traversing a link from node S to R node.

The Queue length Q_l is defined as the ratio of number of packets in the buffer to the maximum buffer size of node. It can be calculated as

$$QL(i) = \frac{NP}{BS(i)} \quad (7)$$

Where $Q_l(i)$ is the queue length of node i, N_P is number of packet in the buffer, S(i) is the maximum buffer size of the node i.

Contribution level P is calculated based on the total number of flows passing through a node as

$$P = (\text{Current number of flows/Number of sources}) \quad (8)$$

To minimize the network communication overload, the authentication process built upon the first part of the key. The key establishment between a sensor node and the base station is a two party authentication process. The cluster head send the secret key from the member nodes to the base station to initialize the transmission session. The proposed system has created a new hybrid cryptographic technique to combine Blowfish for symmetric and Elliptic Curve Diffie-Hellman for asymmetric named as Blowfish Elliptic Curve Diffie-Hellman Algorithm.

Figure 3.2 shows the encryption and decryption process of hybrid cryptographic Blowfish Elliptic Curve Diffie-Hellman Algorithm (BECDH). During the encryption process, the acknowledgment packets are input to the Blowfish encryption algorithm. The packets are encrypted with the sub keys of Blowfish and circularly swapped left or right. At last left and right jointly produces cipher text.

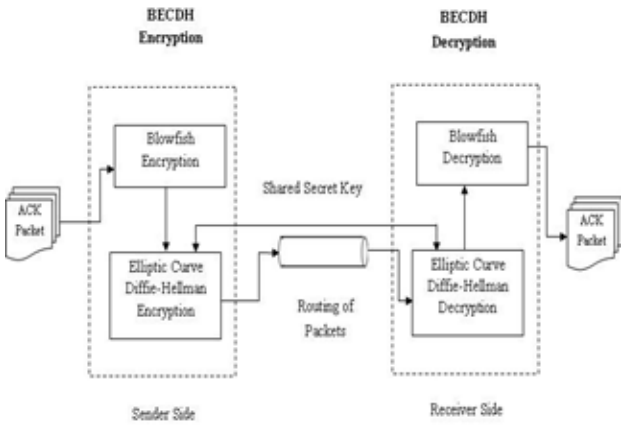


Figure 3.2: Process of BECDH

Then perform another encryption on cipher text using Elliptic Curve Diffie-Hellman asymmetric (public) key which produces the final cipher text. Thus the encryption algorithm ensures data security as well as authentication. In

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

decryption process, the asymmetric (private) key is generated to decrypt the received cipher text by the decryption algorithm Elliptic Curve Diffie-Hellman, produces the output.

IV. SIMULATION RESULTS

The suggested Cluster Based congestion avoidance Security methodology is improved by Network simulator ($NS_{2.34}$) Environments.

Parameters	Values
Number of Node	50
Area Dimension	400 * 400(Meter)
Routing Protocol	AODV
Total Energy	150 Joule
Initial Energy	0.5 Joule
Packet Size	4000 bits
Total packet size	5000 bytes
Type of the MAC	802.11
Simulation Tool	NS2.34

The proposed algorithm of some existing system is highlighting on the network energy with new developed method CBCAS is provide a good output with respect to the packet delivery ratio, End to End delay time, packet losses and Energy Savings.

Performance of packet delivery ratio

The representation of fig: 4.1 denote that the existing method was overcome by CBCAS. In this packet delivery ratio, the packets are transmitted from the sources to destination by proper routing path to evaluate the number of packets that are delivered in WSN like cluster head approaches in WSN.

Table 1: Packet delivery ratio

Packet Size (Bytes)	EEBHC	HCBCA	BECDH	CBCAS
500	83.143	96.846	97.176	99.176
1000	94.202	99.017	99.756	99.577
1500	82.738	97.614	97.900	98.900
2000	88.772	96.819	98.645	99.033
2500	89.383	98.208	98.821	99.932
3000	73.970	92.912	96.078	98.978
3500	93.151	96.104	99.427	99.732
4000	92.852	93.706	98.321	99.991
4500	86.141	99.575	99.411	99.664
5000	89.797	97.679	97.734	98.834

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

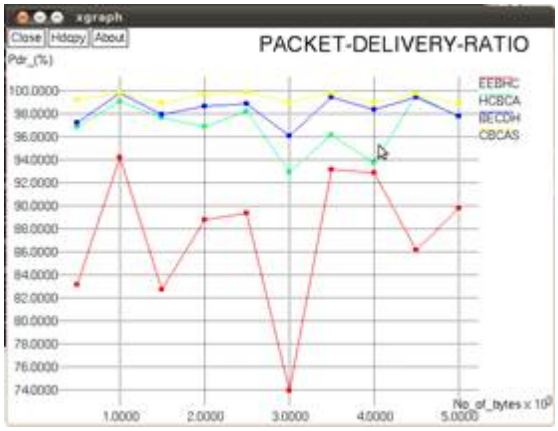


Fig: 4.1 Packet Delivery Ratio

While compared to the existing method, the proposed method gives better result.

Performance of End to End delay

The packet delay was average Maximum time to arrive in the destination. It take time maximum delay when congestion is occur for that time packets are stored in buffer or Repeat Request process is activated.

Table 2: End to End delay

Packet Size (Bytes)	EEBHC	HCBCA	BECDH	CBCAS
500	20.535	26.12	23.754	28.790
1000	11.741	15.808	18.368	21.345
1500	18.107	22.306	22.234	23.098
2000	14.812	18.754	20.354	19.890
2500	20.231	16.905	18.543	20.112
3000	27.907	30.213	27.003	25.432
3500	14.711	21.709	23.911	27.213
4000	17.113	25.318	26.309	24.091
4500	23.312	19.137	21.379	25.189
5000	19.380	18.515	19.016	22.894

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

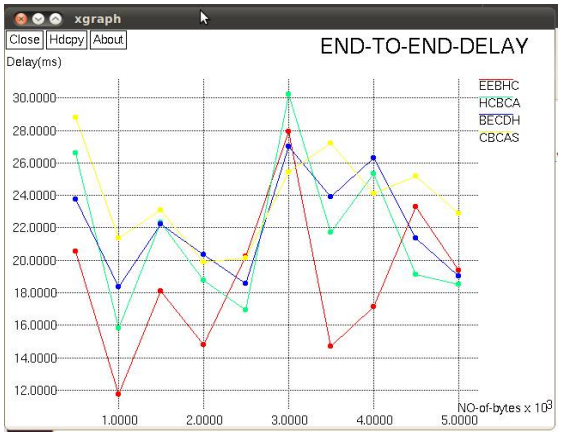
An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

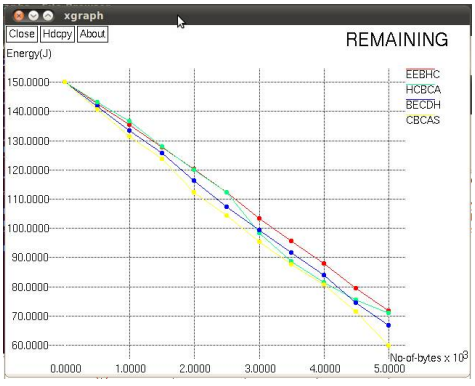


When comparing to the existing method, the proposed method gives better performance for transmit the packets.

Remaining Energy

Table 3: Remaining Energy

Packet Size (Bytes)	EEBHC	HCBCA	BECDH	CBCAS
0	150.000	150.000	150.000	150.000
500	142.496	142.964	141.496	140.496
1000	135.271	136.712	133.283	131.271
1500	127.581	127.815	125.581	123.581
2000	120.207	120.007	116.207	112.581
2500	112.233	112.241	107.324	104.233
3000	103.371	98.331	99.231	95.371
3500	95.537	88.375	91.503	87.818
4000	87.740	81.418	83.590	80.343
4500	79.357	75.309	74.545	71.658
5000	71.763	70.996	66.330	59.882



ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 8, September 2018

International Conference on Emerging Trends in Science, Technology and Mathematics (ICETSTM-2018)"

22nd August 2018

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

4.3: Remaining Energy

Initially, by comparing the remaining energy and joule by taking 100% and 150 joule as a sample for that, we get the following results the existing and proposed work.

V. CONCLUSION

In wireless sensor network, data transmission is done by cluster base and during that process of network routing path selection, congestion avoidance and security problems occur. To avoid this type of problem, three techniques have been used. The Energy Efficient Based Hybrid Clustering (EEBHC) is allowed to select the sensor node with high energy level and routing path based data transmission, which provides high force on Cluster Head (CH) selection and hence energy is saved effectively with respect to the network lifetime. Hybrid Cluster Based Congestion Avoidance (HCBCA) provides high transmission of packet delivery ratio to improve the network lifetime performance with respect to time, and at the same time, packet losses while packet retransmission. The hybrid cryptographic technique uses Blowfish Elliptic Curve Diffie-Hellman (BECDH) algorithm for detecting malicious nodes in the Wireless Sensor Network. The highest speed of encryption and decryption process of BECDH has not affected the speed of communication channel. Finally, the combination of above three techniques named Cluster Based Congestion Avoidance and Security (CBCAS) it gives better result.

REFERENCES

[1]. Perumal.V and Dr.K.Meenakshisundaram, "An Energy Efficient Based Hybrid Clustering (EEBHC)", International journal of Engineering & Technology (IJET), Vol.7 (2), pp.150-154, 2018.
[2]. Perumal.V and Dr.K.Meenakshisundaram, "Hybrid Cluster Based Congestion Aware (HCBCA) Approaches in Wireless Sensor Network", International Journal Of Computer Science and Information Security (IJCSIS), Vol.16 (4), pp202-208, 2018.
[3]. Chang J.Y & Ju P.H "An Efficient cluster based Power Saving Scheme for Wireless Sensor Networks" Journal on Wireless Communication and Networks, vol.1, pp.1-10, 2012.
[4]. Shideh Sadat Shirazi, Aboulfazl Torqi Haqiqat "Energy Efficient Hierarchical Cluster-Based Routing For Wireless Sensor Networks" CS & IT-CSCP, pp.61–69, 2015.
[5]. Mohadmed Eshaftri , Ahmed Y.A1- Dubai Imed Romdhani "A New Energy Efficient cluster based protocol for WirelessSensor Networks" Proceeding of the FEDCSIS , PP.1209-1214, IEEE-2015.
[6]. Rheleh Hashemzehi, Reza Nourmandipour, Farokh Koroupi "Congestion in Wireless Sensor Networks and Mechanisms for Controlling Congestion" Indian Journal of Computer Science and Engineering(IJCSE) vol.4, pp.204-207, 2013.
[7]. Chia-Hsu Kuo, Tzung-Shi Chen, Zheng-Xin Wu "Congestion Control under Traffic Awareness in Wireless Sensor Networks" International Computer Symposium, pp.429-434, IEEE-2016.
[8]. Mohamed Elhoseny , Hamdy Elminir , Alaa Riad Xiaohui Yuan "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption" Journal of King Saud University – Computer and Information Sciences, pp. 262–275, ELSEVIER-2016.
[9]. Preetika Joshi, Manju verma, Pushpendra R Verma "Secure Authentication Approach Using DiffieHellman Key Exchange Algorithm for WSN" International Conference on Control,Instrumentation, Communication and Computational Technologies (lCCICCT), IEEE-2015.
[10]. Chaitali Haldankar, Sonia Kuwelkar "Implementation of AES and Blowfish Algorithm" International Journal of Research in Engineering and Technology (IJRET), Volume.3(Special Issue), 2014.
[11]. Shamina Ross.B, Josephraj.V "Performance Enhancement of Blowfish Encryption Using RK-Blowfish Technique", International Journal of Applied Engineering Research IJAER) , Volume. 12, pp.9236-9244, 2017.
[12]. Omer Chghutai, Nasreen Badruddin, Azlan Awang, Maaz Rehan "congestion-aware and traffic load Balancing scheme for routing in WSNs" Telecommun Syst-Springer, 2016.
[13]. Asha Rani Mishra, Mahesh Singh "Elliptic Curve Cryptography (ECC) For Security in Wireless sensor Network" International Journal of Engineering Research and Technology (IJERT), Vol.1(3), 2012.
[14]. Abdullah Smadi, Hesham Enshasy, Qasem Abu Al-Haija "Estimating Energy Consumption of Diffie-Hellman Encrypted Key Exchange (DH-EKE) for Wireless Sensor Network" International Conference On Intelligent Techniques In Control, Optimization And Signal Processing, IEEE-2017.