International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp.765-773

ENERGY EFFICIENT FOR WIRELESS SENSOR NETWORK USING ENHANCED OMRA ALGORITHM

Dr. Dhaigude Tanaji Anandrao[1]
[1]*Department of Computer Engineering, Someshwar Engineering College, Pune, India*
Dr. Shertambari A. Chiwhane[2]
[2]*Department of Computer Engineering, NBNSSoE, Pune*

Abstract

Wireless sensor network (WSN) is made up of tiny sensor nodes which are autonomous and are connected to base stations. WSN is deployed in many applications where security is an important aspect. Energy is limited in WSN, so to solve energy limitation problem, OMRA algorithm was developed. For implementation of suitable cryptography in WSN, energy and storage resources are limiting factor. To solve all these problems in WSN, secure WSN model with enhanced OMRA algorithm is demonstrated in this paper.

Keywords: *Wireless Sensor Network, Security, Energy Efficiency, Bandwidth efficiency, Compression, Bandwidth, OMRA.*

1 Introduction

A Wireless Sensor Network (WSN) is a collection of tiny sensor nodes which are equipped with sensor, radio transceiver and tiny processor. A WSN has been deployed in many different areas like battlefield situation data, etc.

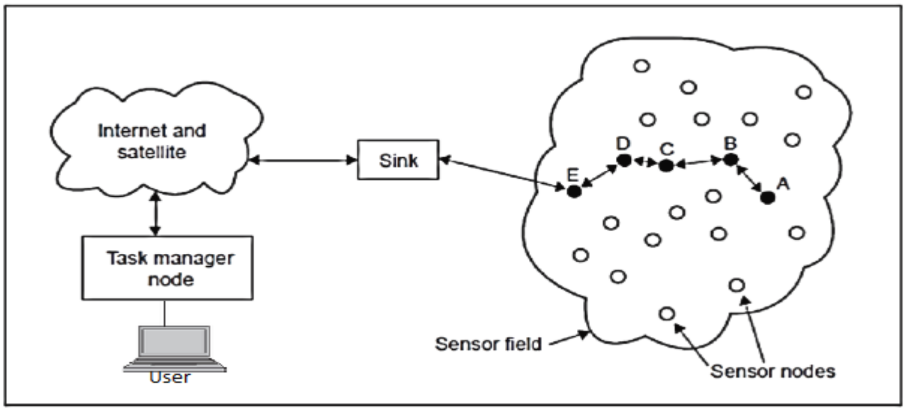

Fig 1: Wireless Sensor Network

In such WSN application, security is very important aspect. Data preservation is very important in such WSN applications [1]. Adding security layer for WSN is not easy because of energy and storage resource limitation. To solve energy limitation problem, enhanced OMRA is proposed in another paper [1]. In this, OMRA algorithm, intermediate nodes for communication are chosen by considering different factors such as communication radius, node failure, node to node distance and airtime cost for each available path. Effectiveness of OMRA algorithm is already presented in paper [1].To solve security problem, encryption and compression is added in this proposed scheme.

1.1 WSN Security Requirement

WSN security requirement is to protect the information from different attacks in WSN. Attacks can be one of the wormhole attacks, sinkhole attacks, Subversion of a Node, Physical attack, Passive information gathering, false node and malicious data, Acknowledgement spoofing [2].

WSN Security requirement include:

Authentication: Authentication is necessary to verify that received data is from valid source. In WSN, node should have ability to identify communicating node which is transmitting data. For authentication, secret key is required[18 19]. This secret key will be shared between sink and source nodes. The sink node will ensure reliability of incoming messages by using secret key.
Confidentiality: WSN is deployed in many applications where data is very sensitive e.g. military applications. In such applications, protecting the information from false nodes is very important. Data can be protected by using encryption secret key.
Integrity: Data integrity is to protect the information from any unauthorized modification. Data integrity can be achieved using data authentication.
Availability: Due to attack's, required data might not be available when it is required. So in WSN, there is risk of data loss.

2 Enhanced OMRA

To target security problem in WSN, energy limitation problem needs to solve first. To solve energy limitation problem, enhanced OMRA algorithm is used in secured WSN model. Flowchart in figure 2 explains the enhanced OMRA algorithm. In enhanced OMRA algorithm, nodes can be moved to new location which helps in energy saving and also, this keeps nodes within WSN communication range [1].

The various steps in the algorithm are given below:

- *Define a system:*
- *Let OM be OMRA protocol, OM = {}*
- ***Identifying the input:***

  Let, OM1 = {NO,Pkr,Pks,t,Rt,OMi}
  OM = {OM1,.....}
  NO = {NOj |j=1,2,...} where N is nodes
  Pktr = Packets received
  Pkts = Packet sent
  Rrt = Data transfer rate from node to sink OM1
  NOj = {Iml,Pml,Fm,Ri,LEn,Rcm},
  where,
  Iml = Node m to node n information flow rate
  Pml = Link m to n transmission power
  Fm = Node m's faireness index
  Ri = Max source rate for given node
  LEn = All node's limited energy
  Rcm = Max communication radius

- ***Identify the Weights:***

  Wml = Fml + Pml (1)
  Pml is Tx power

Fml is normalized min valu of flow rate

Fml = fmaxi- Iml (2)

where, fmaxi = Max information extracted from WSN.

In terms of all functions,

1) Weight Function:

Wml = Fml + Pml (3)

Pml in Tx power

2) Least weight function:

Node_PHx = min(Wml), path from source to sink

3) Fast re-route function:

If Node_PHx = TRUE then select Node_PHx else find next least weight Node_PHx

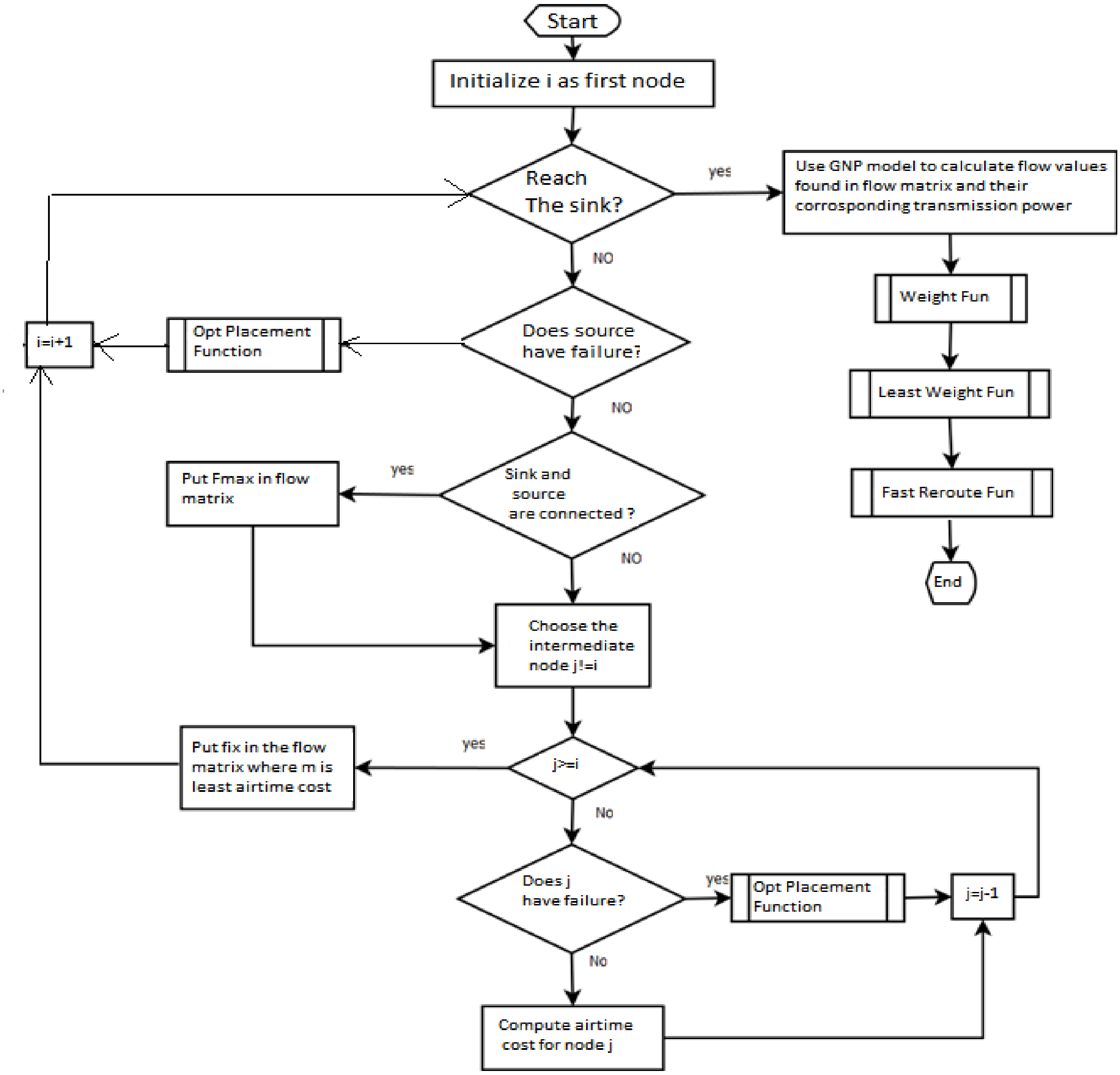
Start
Initialize i as first node
Reach The sink?
yes
Use GNP model to calculate flow values found in flow matrix and their corresponding transmission power
NO
Weight Fun
i=i+1
Opt Placement Function
Does source have failure?
Least Weight Fun
NO
Put Fmax in flow matrix
yes
Sink and source are connected ?
Fast Reroute Fun
NO
End
Choose the intermediate node j!=i
Put fix in the flow matrix where m is least airtime cost
yes
j>=i
No
Does j have failure?
yes
Opt Placement Function
j=j-1
No
Compute airtime cost for node j

Fig 2: Enhanced OMRA Algorithm

3 Encryption and compression

3.1 Encryption:

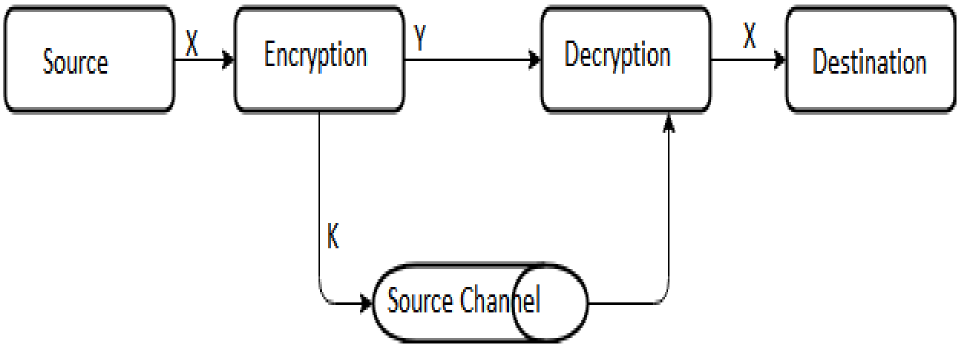

Fig 3: Encryption Algorithm

Figure 3 shows a communication in WSN using encryption. The input message X is encrypted, and its output is message Y with secret key K. Output message Y is sent to sink node. Sink node uses secret key K to decrypt message Y. Sink node using K, get back X from message Y. As shown in figure 3, key K is sent by secure channel[16 17]. Instead of sending this key over channel, it can be fixed and shared between source and sink nodes.

Encryption Algorithm:

```
Input: Secret key (k,e), Message m ∈ [0, k-1]
Output: Encrypted message yo
begin
        1.  Get yo = mge mod k 2.
        2.   Return yo.

End
```

Decryption Algorithm:

```
 Input: Secret key (k,e),Private key p, Cipher text yo
Output: message mg
begin
        1. Get mg = cp mod k
        2. Return mg.
End
```

Encoding:

Encoding is used to recover data at receiver if there is any loss of data due to noise in medium or channel. Here, in this WSN model, LDPC encoder is considered. Fig 4 shows LCPD block diagram. LDPC consists of iterative encoder and decoder. Because of iterative nature of LDPC, it gives better result as compared to other encoder. This LDPC encoder adds 120 bytes per 2 KB input message packet.

Using this 120 parity bytes, data can be recovered at sink node even if there is message loss during transmission.

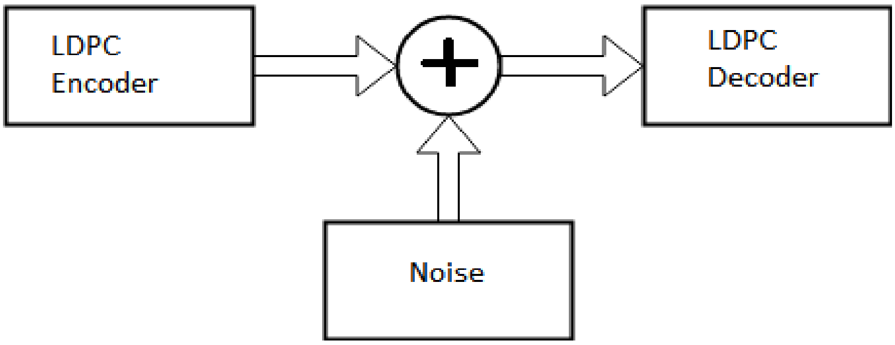

Fig.4: LDPC Encoder-Decoder

Compression:

Data compression represents the information in compact form which in turn reduces the size of input data [20 21]. Due to encoding, encoded bits will be added to input data as an overhead. As data increases, energy required for transmission increases. To reduce this problem, compression is used this mode. Lossless compression with compression capability of 30% is considered for this WSN model.

4 Proposed Algorithm:

Fig 5 shows proposed algorithm. In this proposed algorithm, in additional to enhanced OMRA algorithm, 3 more techniques are added. Additional 3 techniques are compression, encoding and encryption. These 3 techniques are added to provide better security to WSN data as for some applications, security of data is more crucial. In addition to security, this proposed algorithm also provides bandwidth saving by reducing number of bits in data.

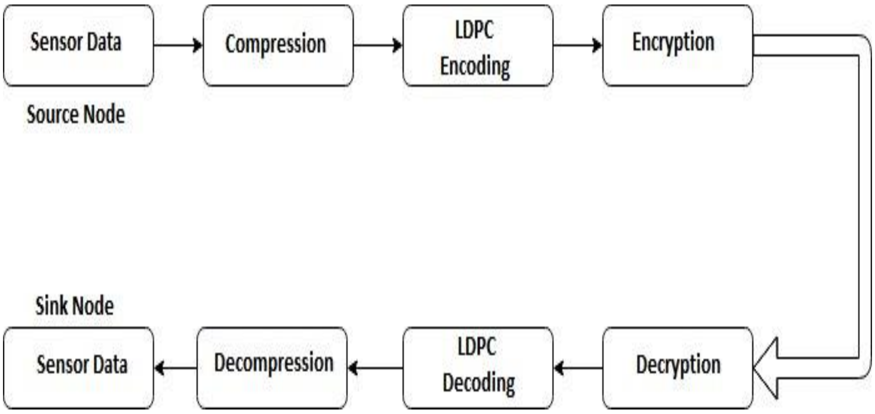

Fig 5: Proposed WSN Algorithm

An enhanced OMRA algorithm is used at sensor node. Then sensor data is compressed to reduce number of bits in data. This step helps in bandwidth utilization. After compression, to void data loss over noisy channel, ldpc encoding technique is added. Once encoded data is ready, then data is processed by encryption technique. Encryption step is added to provide data security

5 Results and Discussion

Proposed WSN model is simulated in NS2. Simulation parameters are described in table I. Total nodes selected for simulation are 200 in 1000 x 1000 area of simulation with receiving power of each node set to 0.01

Table I. Simulation Parameters

Area of WSN	1000 x 1000
Total nodes in WSN	200
Initial Energy in WSN	20Jl
Noise level in WSN	0.0341
Cost per bit (CPB)	0.00435
Data Reduction Ratio(Delta)	0.48
Aggregation cost in WSN	1
Receiving Power of nodes in WSN	0.01
Transmission Power of nodes in WSN	0.02
Total simulation Time of WSN	250

Simulation results are described in table II. From simulation results, it can be seen that packet delivery ratio is very high with this scheme.

Table II. Simulation Results

Parameter	Enhanced OMRA Algo-	Traditional OMRA algo-
Number of packets sent in WSN	620	620
Number of packets received in WSN	590	501
Packets delivery ratio in WSN (%)	95	81
WSN Control overhead	9554	9840
WSN Normalized overheads : rout-	16.274	18.75
Total delay in WSN	0.044023	0.669021
Total throughput	14641.2	23464.9
WSN: Jitter	0.282275	0.44343
Number of dropped packets	29	119
Dropping ratio in WSN (%)	4.67	19.19
Total Energy Consumption of WSN	4.82498	6.66532
Average Energy Consumption per	0.00797433	0.010439
Overall Energy in WSN: Residual	956.072	1001.435
Average Energy in WSN: Residual	9.65025	10.63430

As mentioned in above obtained result, it is observed that the proposed system is superior to existing techniques. With this scheme, energy conservation is improved, average energy per node gives 15%-25% improvement compared to existing methods.

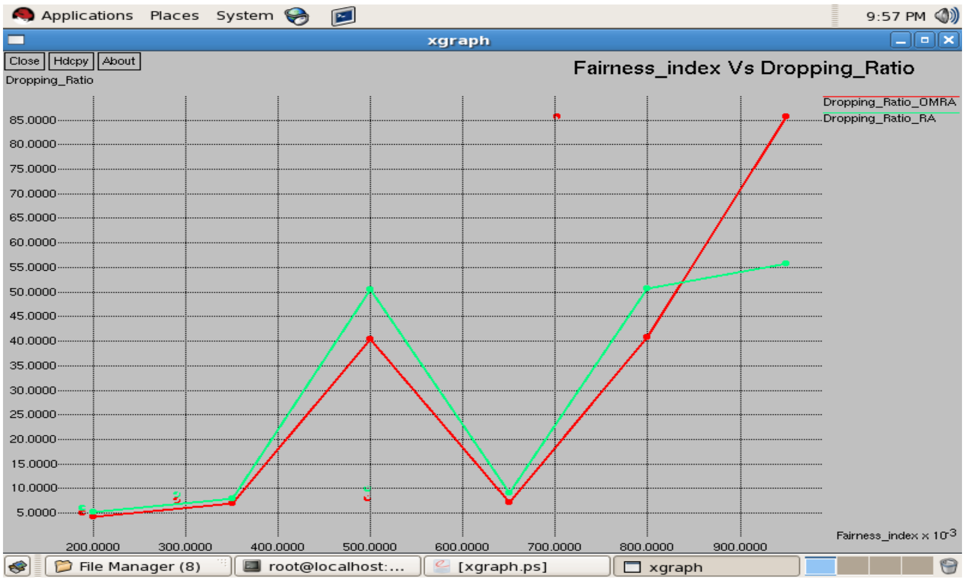

Fig.4. Fairness Index vs. Dropping Ratio

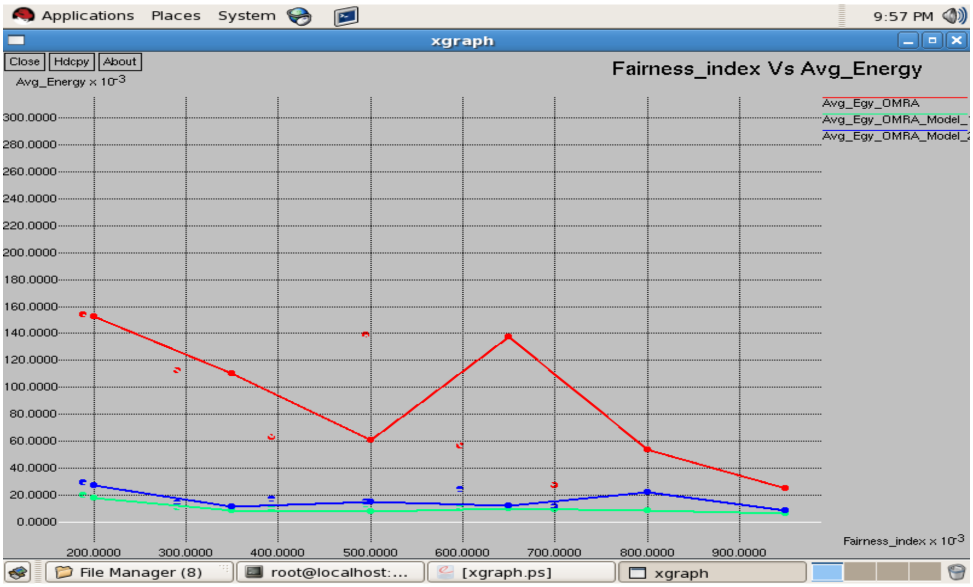

Fig.5. Average Energy vs. Fairness Index

Fairness index is the terminology used in WSN to determine whether applications or users are getting fair share of resources available. Figure 4 shows fairness index vs. dropping ratio. From figure 4, it can be seen that dropping ratio in WSN (with OMRA algorithm) is less compared to dropping ratio in WSN (with existing RA algorithm). Figure 5, Average Energy vs. Fairness Index.

This proves the effectiveness of OMRA algorithm in terms of drooping ratio.

Table III. Bandwidth Saving

Input data size MB	Compressed data size (compression ratio of 30 %)	Encoded size (120 bytes per 2048 bytes)	Encryption size	Output data size	% saving in bandwidth
10	7	7.4	7.4	7.4	26

Table III shows effectiveness of compression and encryption method in this scheme. Encryption, encoding and compression provide security to WSN data. In addition to security, it provides saving in bandwidth also. From bandwidth saving results, it can be seen that this proposed scheme provides ~26% saving in bandwidth.

Table II and III collectively shows the performance of proposed algorithm. From these tables, it can be seen that the proposed algorithm provides energy and bandwidth efficiency.

6 Conclusion:

This paper proposed a scheme for WSN which is robust and reliable. The proposed scheme tries to solve all problems in WSN end to end communication. Usefulness of this proposed scheme in end to end WSN communication can be seen by results. By using this scheme, 26% bandwidth saving is achieved with additional reduction of $10 - 20\%$ in energy consumption. In addition to these saving, it provides better data recovery using LDPC encoders.

References:

[1] R. Rizk, H. Elhadidy, H. Nassa :Optimised mobile radio aware routing algorithm for wireless sensor networks. IET Wireless Sensor System, 011,Vol.1,Iss.4, pp.206

[2] H. Hayouni, M. Hamdi and T. H. Kim :A Survey on Encryption Schemes in Wireless Sensor Networks. 2014 7th International Conference on Advanced Software Engineering and Its Applications, Haikou, 2014, pp. 39-43.

[3] Avinash J. Kokare, Manik K. Chavan Energy efficient routing protocols for wireless sensor network: A Survey, TEICC, Bikaner, Rajstan, 2012. ISBN : 978-81-923777-0-4.

[4] F. Al-Turjman, "Energy-Aware Data Delivery Framework for Safety-Oriented Mobile IoT," in IEEE Sensors Journal, vol. 18, no. 1, pp. 470-478, Jan.1, 1 2018. doi: 10.1109/JSEN.2017.2761396

[5] Handziski V, Kopke A, Karl H, Frank C, DrytkiewiczW : Improving the energy efficiency of directed diffusion using passive clustering. In Proceedings of the first European workshop on wireless sensor networks, EWSN , Berlin, Germany; LNCS 2920.

[6] Kulkarni, R., Fo´lrster, A., Venayagamoorthy, G.: Computational intelligence in wireless sensor networks: asurvey, IEEE Commun. SurveysTutor., 2010, 12, (3), pp. 1-29

[7] Chiara Buratti ,Andrea Conti, Davide Dardariand Roberto Verdone: An Overview on Wireless Sensor Networks Technology and Evolution. Sensors 2009, 9, 6869-6896; doi:10.3390/s90906869

[8] Anand M: Reconstruction of Path using Compressive Sensing in Dynamic Wireless Sensor Network. DOI 10.17148/IJIREEICE.2017.5429

[9] S. Sushmitha , V. Devi: Securable Identity Based Encryption Technique by Generating Key in Wireless Sensor Network. International Research Journal of Advanced Engineering and Science, Volume 2, Issue 1, pp. 198-199, 2017.

[10] S. C. Mukhopadhyay, "Wearable Sensors for Human Activity Monitoring: A Review," in *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1321-1330, March 2015. doi: 10.1109/JSEN.2014.2370945

[11] F. Al-Turjman, "Energy-Aware Data Delivery Framework for Safety-Oriented Mobile IoT," in *IEEE Sensors Journal*, vol. 18, no. 1, pp. 470-478, Jan.1, 1 2018.doi: 10.1109/JSEN.2017.2761396

[12] Deepak Sharma, Amol P Bhondekar, AmriteshOjha, A K Shukla, CGhanshyam: A traffic aware cluster head selection mechanism for hierarchical wireless sensor networks routing. 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)

[13] Junling Li, Danpu Liu: An energy aware distributed clustering routing protocol for energy harvesting wireless sensor networks. Communications in China (ICCC), 2016 IEEE/CIC International Conference on Communications in China (ICCC)

[14] D. R. Sarvamangala, Raghavendra V. Kulkarni: Multistage localization in wireless sensor networks using artificial bee colony algorithm. Communications in Computer and Information Science, vol. 776, pp. 451, 2017, ISSN 1865-0929, ISBN 978-981-10-6429

[15] Chetna Mudgule, Pramod Ganjewar Uma Nagaraj: Data Compression in Wireless Sensor Network: A Survey. IJIRCC- International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11, November 2014.

[16] Shwetambari Kharabe, C. Nalini," Robust ROI Localization Based Finger Vein Authentication Using Adaptive Thresholding Extraction with Deep Learning Technique", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018.

[17] Shwetambari Kharabe, C. Nalini," Using Adaptive Thresholding Extraction - Robust ROI Localization Based Finger Vein Authentication", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 13-Special Issue, 2018.

[18] Shwetambari Kharabe, C. Nalini," Evaluation of Finger vein Identification Process", International Journal of Engineering and Advanced Technology (IJEAT), International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S, August 2019.

[19] Udayan Birajdar, Sanket Gadhave, Shreyas Chikodikar, Shubham Dadhich, Shwetambari Chiwhane, "Detection and Classification of Diabetic Retinopathy Using AlexNet Architecture of Convolutional Neural Networks", Proceeding of International Conference on Computational Science and Application, online 05 January 2020, pp 245-253.

[20] Dr. C. Nalini, Shwetambari Kharabe, Sangeetha S," Efficient Notes Generation through Information Extraction", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S2, August 2019.

[21] Shwetambari Kharabe, C. Nalini , R. Velvizhi," Application for 3D Interface using Augmented Reality", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S2,August 2019.