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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Enhanced Cryptographic Mechanism with Data Recovery for Secure, Power Efficient and Reliable Routing in Mobile WSN

Poonam Kudale[1], Prof. M. D. Ingle[2]

P.G. Student, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India[1]

Associate Professor, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India[2]

ABSTRACT: WSNs are constrained in terms of assets. Energy is one of the biggest valuable resources in WSN. Hence excellent use of energy is important. An innovative energy-efficient routing protocol for WSNs is imported. The protocol is decent in terms of data delivery at the base station. The introduced protocol is hierarchical and cluster based. Each group of nodes contains one cluster head node and some normal sensor nodes. Also one data collection node is selected which performs data aggregation and handles mobility of nodes. The regrouping time and power requirements have been minimized by introducing the concept of CH panel. At the primary phase of the protocol, the BS chooses a chunk of apparent CH nodes and forms the CH panel. In consideration of the reliability characteristics of the protocol, it gives big attempts to guarantee a specified throughput level at the BS. The data transmission from the CH node to the DCN node and then to the BS is carried out either directly or in multihop fashion. Likewise, substitute paths are considered for data transportation among CH node and the BS. The data compression technique saves the power utilization at each node while transmitting data. The existing work doesn't focus on the issues such as confidentiality, mobility of nodes, recovery of lost data and attacks on sensor nodes. In proposed work we consider the prevention of attacks on nodes also by means of using data loss recovery model is introduced. This will produce an output in terms of increased energy efficiency, throughput and prolonged lifetime of the nodes.

KEYWORDS: Cryptographic technique, Energy Efficiency, Mobile Nodes, Data Recovery, Wireless Sensor Networks.

I. INTRODUCTION

A wireless sensor network typically includes a huge number of low-powered, less-cost sensing devices called as sensors with restricted computational, memory and communication assets. Remote sensor network contains a few number of sensor nodes which are dispersed over different areas with the objective of monitoring their physical or environmental conditions, gathers the information and processes it. These sensing devices are comprised of basic controller, application particular sensors, transceiver and battery. Data aggregation is utilized to decrease the transportation overhead because of finite amount of power in sensor nodes. In the data aggregation technique, the information of sensor nodes is merged at cluster head nodes and then transmitted that aggregated data to the base station. Data aggregation approach includes gathering of data and making information accessible to the base station in energy profitable manner. Fundamentally, based on topology, data aggregation protocols can be classified into tree based and cluster based protocols. In tree based data aggregation, data flows from leaf nodes (child nodes) to the upper level nodes (parent nodes) wherein aggregation is performed at the parent nodes. In case of cluster based aggregation, groups of nodes are formed which are called as clusters.

As the sensors are restricted in terms of estimation, saving capability, power, amount of transportation can be reduced by utilizing the concept of compression. Data transportation cost can be reduced by transmitting the compressed data from sensors to the base station. This will also save the power utilization at each node while transmitting data. With the issue of power profitability, there is a need to consider the issue of security also. Sensor nodes are vulnerable as a result of they are placed in neglected atmosphere. Hence they are easily prone to attacks by criminals. Cryptographic

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

techniques such as encryption decryptions can be used in order to deal with security issue. Data can be transported from sensor nodes to BS after performing compression and encryption. At arriving end i.e. at BS, data will get decompressed and decrypted for further processing. Using advanced cryptographic techniques, compromised nodes can be easily discovered by BS.

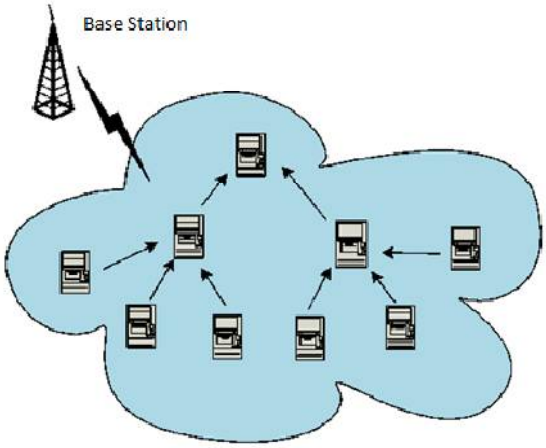

Figure1. Wireless sensor network

II. RELATED WORK

In this paper [1], authors have proposed a protocol named E2R2, which is hierarchical and cluster based protocol. In this, each cluster contains one CH node, and the CH node is assisted by two DCH nodes, which are also called cluster management nodes to handle the energy efficiency, reliability and mobility of the nodes and BS.

In this paper [2], authors have introduced LEACH protocol. LEACH selects the cluster head by random number generation. Cluster gets formed based on the nearest distance. LEACH uses one hop conversation.

S. Lindsey, C.S. Raghavendra, [3] have introduced the basic idea of chain based protocol titled PEGASIS is to increase the life of the network. This can be achieved by forming the chain of the nodes deployed in the network, from sending node to the Base Station.

A. Manjeshwar and D. P. Agarwal, [4] have introduced a protocol named TEEN. This technique uses the terms called hard threshold, soft threshold. Based on these values the clusters are formed and the time of transmission is decided

A. Manjeshwar and D. P. Agarwal [5], have introduced APTEEN protocol. APTEEN which is the advancement over TEEN is a hybrid protocol that modifies the threshold values utilized in the TEEN protocol as per the user's necessity and the type of the application.

O. Younis and S. Fahmy [6], have introduced another energy efficient protocol Hybrid Energy Efficient Distributed clustering Protocol (HEED) HEED protocol considers energy and network structure features such as sensor node degree, distances to acquaintance to form the clusters and to select the CH.

In this paper [7], authors have proposed Energy Efficient Clustering Scheme (EECS) protocol. EECS protocol is a clustering scheme which decides CH with maximum energy.

In this paper [8], authors have introduced a power efficient clustering algorithm for mobile sensor network on the basis of the LEACH protocol. The introduced protocol extends the features of LEACH to support for mobile or dynamic location changing nodes and also decreases the utilization of the network resource.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

III. PROBLEM DEFINITION

The problem definition of the system is to design a power profitable and reliable transmitting protocol for a mobile WSN that functions in a neglected style and, occasionally, in unfavourable atmosphere. As the sensor nodes are assets restrained (especially restrained power and restrained saving capability), the transmitting protocol should absorb less power and should not trouble the nodes with storage burden. Also to allow secure shipment of data packets in multihop fashion by discovering and avoiding attack on nodes.

IV. EXISTING SYSTEM

Figure 2 shows the extant system structure (E2R2). As shown in fig, in extant system, each group of sensor nodes subsist of one cluster head (CH) node, two deputy CH nodes, and some regular sensor nodes. Data transports from sensor nodes to base station via Cluster head and Deputy Cluster heads. Extant system considers the movability of both the sensor nodes as well as base station. But the enhancement over this is that, it does not consider the issue of security and attacks on sensor nodes. Discovery and avoidance of compromised nodes is not pointed in E2R2 system.

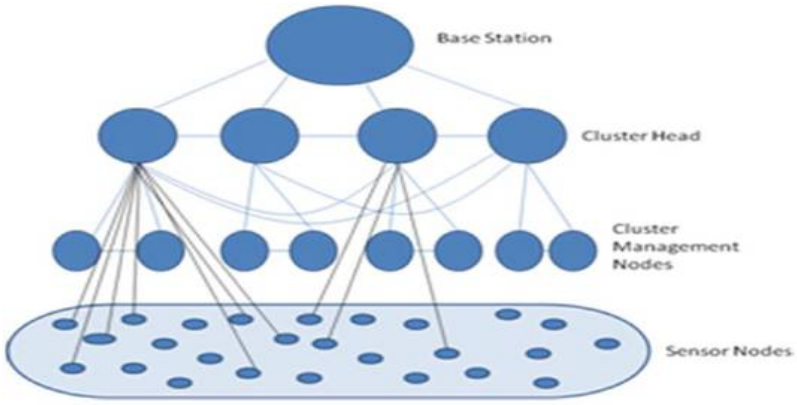

Figure2. Existing System Architecture

V. PROPOSED SYSTEM

Figure 3 characterizes the system structure and depicts the sensor nodes with distinct roles in the system. After the stationing of the sensor nodes, the BS constructs groups of various sensor nodes in order to configure clusters. Each group or cluster encloses a CH node and regular sensor nodes. And one Data collection node (DCN) is elected. The BS selects a set of relevant sensor nodes from each cluster, which can act as CH or DCN at a coming after stage. This bunch of nodes is called CH panel. The cluster members or sensor nodes, forward data to the corresponding CH node. The DCN node does the data aggregation to discard verbosity and then forward the aggregated data approaching the BS. The CH nodes do not transport data straight to the BS, unless it is the nearest one to the BS. The communication style or the route for the CH nodes is discovered by the BS and dispersed to the corresponding CH nodes. It is pretended that the BS has an idea about the expected number of data packets (i.e. the volume of data) to be arrived in it during a specified time interval. Therefore, the BS keeps on auditing the actual volume of data received from distinct groups in the network. If the BS recognises less arrival of data packets from some groups in contrasting with a pre-specified threshold level, then it instructs the corresponding CH nodes to check their relatedness with their cluster members. The CH considers this as response from the BS and accordingly verifies the current relatedness with its cluster members. If the relatedness status of the cluster members with the corresponding CH is very poor, the BS resolves this issue by shifting the charge of cluster headship to another suitable member from within the CH panel. On the basis of the relatedness scenario, the cluster headship may be given to the DCN node also. The transportation decisions are made at the BS and then broadcasted to the sensor nodes. Since the sensor nodes are assets restricted and,

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

moreover, the nodes are also devoted to data processing and communication apart from sensing activities, it is always fortunate to offload the transportation decision making process from the sensor nodes. Therefore, this protocol exploits the resourcefulness of the BS by shifting routing and some cluster management activities to the BS. As we are considering mobility of nodes, there may be loss of connectivity. Also in case of attack detection on DCN or CH node, charge is shifted to the other node. Data may get lost while shifting the charge from one node to another node. Hence the data recovery model is introduced which makes use of cache for storing data until the next iteration, which can be retransmitted in case of data loss. Figure 3 depicts the system structure.

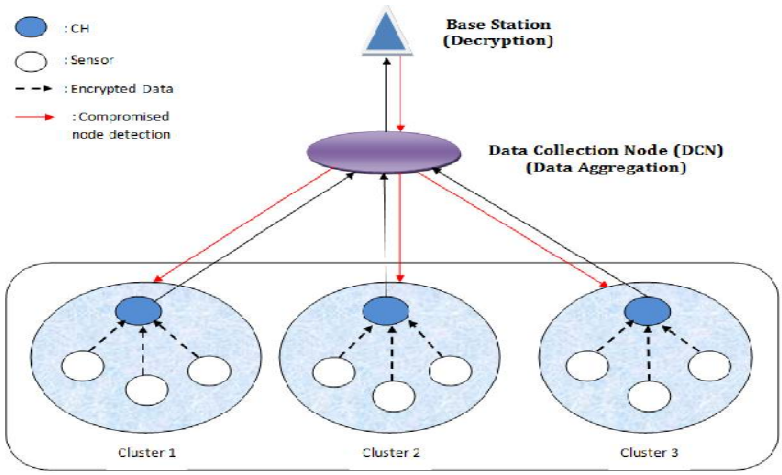

Figure3. Proposed System Architecture

The System is split into number of stages which are interpreted as follows:

- Network deployment- In this the input i.e. number of sensor nodes to be deploy is taken from user and the network of sensors is created.
- Clustering- In this module, all the sensor nodes are divided into number of clusters.
- Selection of cluster panel- Here, for each cluster, one node is selected as a cluster head (CH). Also one Data collection node (DCN) is selected which is common for all the clusters. This selection of CH and DCN is done on the basis of 3 parameters energy, distance to BS and density of neighbour at each node.
- Sending of data- In this module, the data will be generated. Then Compression and encryption process (encryption using ECC algorithm) will be done on the generated data. After that the data is further passed to DCN via CH node. At DCN, aggregation of data will be performed. And at last the aggregated data will be forwarded to the BS.
- Detection of compromised node- Here, Base station performs attack detection i.e. it detects the compromised nodes (the node under the control of attacker). On detection, it removes the compromised nodes immediately from the network.
- Data Recovery Model- In this, lost data can be recovered by using the concept of cache memory. Each node is provided with extra cache in order to store the transmitted data. This cached data can be retransmitted in case of data loss while shifting the charge from one node to another node.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

VI. MATHEMATICAL MODEL

A. Set Theory

Let, S be a system S = {N, C, CLH, DCN, AGR, CMN}, where,

1) Place Sensor nodes.
N= {N1, N2, ..., Nn},
N is set of all placed sensor nodes.

2) Cluster creation.
C = {C1, C 2,....,Cn},
C is a set of groups of sensor nodes/ clusters.

3) Select head of the cluster for each cluster.
CLH= {CLH1, CLH2, ..., CLHn},
CLH is a set of Cluster head.

4) Select Data Collection Node.
DCN= {DCN1, DCN2, ..., DCNn},
DCN is a set of Data Collection Node.

5) Aggregate data to be send to the BS.
AGR= {AGR1, AGR2, ..., AGRn},
AGR is a set of aggregated data.

6) Detection of compromised nodes.
CMN= {CMN1, CMN2, ..., CMNn},
CMN is a set of data compromised nodes.

B. Mathematical Model for Proposed Work

For ECC Algorithm:

- Key generation
  W = r * c
  Where,
  W= public key
  r = random number from (1 to n-1)
  c = point on curve

- Encryption
  C1 = K * p
  C2 = M + k * W
  C1 C2 = cipher text
  K= random number between 1- (n-1)
  c = point on curve
  M = original message
  W = public key

- Decryption
  M = C2 - r * C1

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

For Energy Calculation:
ETx (k, d) = Eelec * k+ amp * k * d
ERx(k) = Eelec * k
d: Distance for neighbouring sensor node.
amp: Energy required for the transmitter amplifier.
Eelec: Energy consumed for driving the transmitter or receiver circuitry.
k = bits per message.

For data loss recovery:
Data size = Number of aggregated packets at BS.
Data loss = Size of data received - No. of nodes in network.
After recovery:
Actual data size = previous data size + recovered data.

VII. ALGORITHM

Input: N (Number of nodes)
Output: Safely routed data at base station.
1. Start2. Put the number of nodes.
3. Deploy the sensor nodes in network.
4. Formation of clusters using clustering algorithm.
5. Calculate the energy, distance to BS and density of neighbours at each node.
6. Based on calculation in step 5, select proper cluster head (CH).
7. Select the Data Collection Node (DCN).
8. Generate data and accomplish compression and encryption of data.
9. Transmit data to cluster head (CH).
10. Transmit data from CH to DCN.
11. Accomplish data aggregation at DCN.
12. Convey aggregated data to the BS.
13. Discover Compromised Nodes.
14. Eliminate Compromised Nodes from network.
15. Safe Routing Of Data.
16. Stop

VIII. EXPERIMENTAL SETUP

The system developed in Netbeans (version 8.1) tool using Java framework (version jdk 8) on Windows platform. The network is generated using Jung tool in which contain sensor nodes. The system doesn't need any specific hardware to run, any standard machine is capable of running the application.

IX. SYSTEM ANALYSIS

A. Residual Energy Graph

Figure 4 shows the comparison graph for residual energy ratio of existing and proposed system. As per expectation, the residual energy in the proposed system is more as compared to existing system.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

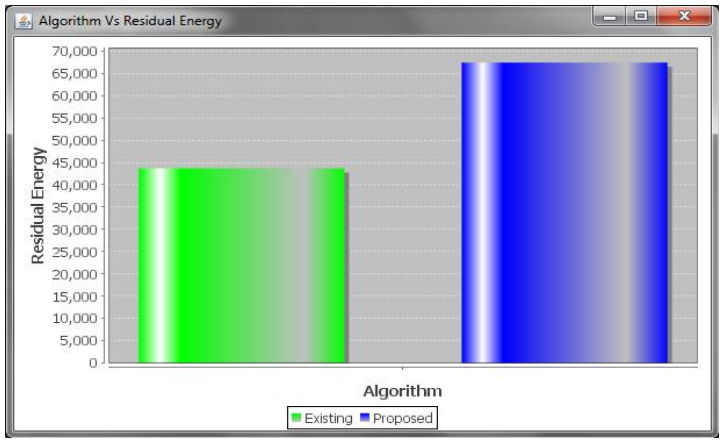

Figure4. Residual Energy Comparison between Existing and Proposed System

Table1. Residual Energy Comparison between Existing and Proposed system

Work Task	Existing System	Proposed System
Energy	44000	68000

B. Latency Graph

Figure 5 shows the comparison graph for required time ratio of existing and proposed system. As per expectations, proposed system is faster and more robust as compared to existing system.

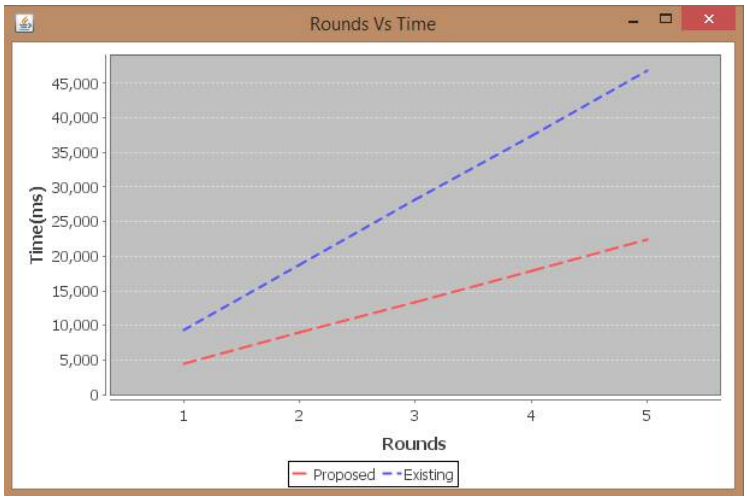

Figure5. Latency Comparison between Existing and Proposed System

C. Packet Delivery Ratio

Figure 6 shows the comparison graph for packet delivery ratio of existing and proposed system. As per expectation, the packet loss is less as compared to existing system as we have integrated our proposed system with data loss recovery model. From graph we can conclude that proposed system is efficient.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

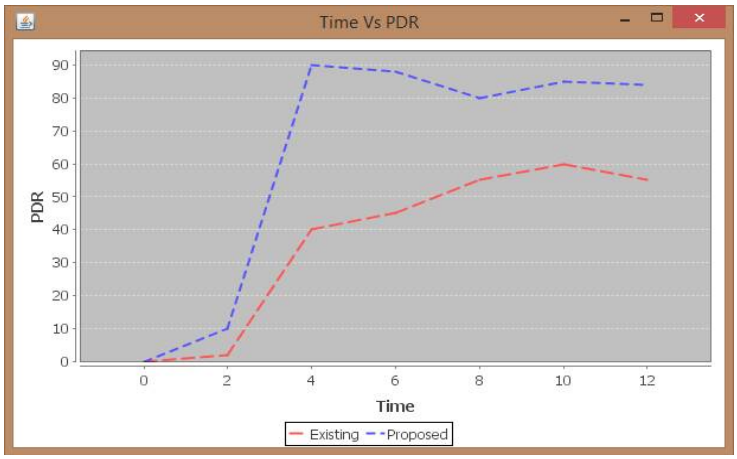

Figure6. Packet Delivery Ratio Comparison between Existing and Proposed System

X. CONCLUSION

Enhanced Cryptographic Mechanism with Data Recovery for Secure, Power Efficient and Reliable Routing protocol for mobile WSNs is introduced. The technique works in hierarchical and cluster manner. Every cluster subsists of one CH node, and the CH node is assisted by Data Collection Node (DCN), which are also named as cluster management nodes. This cluster panel enhances the lifespan of the network. We are electing power profitable and reliable route for transporting data. Such a routing protocol is useful when the sensor nodes are mobile. The protocol assures reliability in terms of data shipment at the BS; this is accomplished through the utilization of multiple paths and switching of the paths as decided by the BS. A probability-based mathematical model can be utilized for determining the most relevant path for data forwarding. Cryptographic techniques are used such as encryption decryption for maintaining the secrecy of the data. Also we are considering the issue of discovering an attack on sensor nodes and avoidance of such attacks to avoid loss of sensitive data. All this allows secured, power-profitable and reliable transportation of data in wireless sensor network. Also use of cache with each sensor node helps in recovery of lost data in case of loss of connectivity or shifting charge to another node. In future, we can work on the recovery of compromised node and redeploying it in the network.

REFERENCES

[1] Hiren Kumar Deva Sarma, Member, IEEE, RajibMall, Senior Member, IEEE, and Avijit Kar, "E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks," IEEE systems journal, vol. 10, no. 2, june 2016
[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. 33rd Annu. HICSS, 2000, pp. 1-10.
[3] S. Lindsey, C.S. Raghavendra, "PEGASIS: power efficient gathering in sensor information systems", in:Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002, pp. 1125-1130.
[4] A. Manjeshwar and D. P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks" in Proc. 15th IPDPS Workshops, 2000, pp. 2009-2015.
[5] A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in Proc. IPDPS, 2002.
[6] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366-379, Oct.-Dec. 2004.
[7] M. Ye, C. Li, F. Chen, and G. J.Wu, "EECS: An energy efficient clustering scheme in wireless sensor networks," Int. J. Ad Hoc Sens. Netw., vol. 3, no. 2/3, pp. 99-119, 2007.
[8] L. Tien Nguyen, X. Defago, R. Beuran, and Y. Shinoda, "An energy efficient routing scheme for mobile wireless sensor networks," in Proc. IEEE ISWCS, 2008, pp. 568-572.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

BIOGRAPHY

Ms. Poonam P. Kudale, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India 411007. She received her B.E (Computer) Degree from Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, Indi 411007. Her area of interest is Wireless Sensor Network and Network Security.

Prof. M. D. Ingle, is currently pursuing Ph.D in WSN. He earned his M.Tech (Computer) Degree from Dr. Babasaheb Ambedkar Technological University, Lonere, Dist. Raigad- 402103, Maharashtra, India. He earned his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India. He is currently working as M.E coordinator and Asso. Prof. (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India.