# An Energy-Efficient Data Gathering In WSN Using EE-Pegasis And BFOA Algorithm

Manpreet Kaur[1],Tanisha Saini[2]
[1]*M.tech (Scholar),* [2] *Assistant Professor*
*Chandigarh Group of College,Landran*

***Abstract-*** An assemble the data is an energy efficient and appropriate manner is the fundamental task of WSN. The limited energy is used for battery operated with sensor nodes and it required to preserve their power of battery to extend the lifetime of WSN. The routing protocols used in WSN such as LEACH, PEGASIS, EE_PEGASIS and TEEN etc; are no-longer suitable for WSN (Wireless Sensor Network) in EE-PEGASIS(Energy Efficient Power Efficient Gathering in Sesnor Information Systems). The wireless sensor network is less energy consumed based on a CHAIN based protocol which is EE-PEGASIS with GREEDY algorithm. This protocol work on the hierarchical environment to succeed their own methods and enhanced energy efficient. In this research work, we implement EE-PEGASIS protocol based on Chain based method used and Bacteria Forgaing Optimization Algorithms (BFOA) used to reduce the performance of the energy in the WSN. Here, added for four qualities of service performance parameters, namely as 'End-to-End Delay','Energy Consumption' and 'Throughput' which are developed and compared to their quality of service performance parameters.

***Keywords -*** *Wireless Sensor Network, EE-PEGASIS, chained based method, Greedy Algorithm and BFOA.*

## I. INTRODUCTION

The introduction to micro electro mechanical system, it becomes attainable to construct sensor nodes in huge scale at low cost. Sensor nodes consider the dissimilar natural phenomenon like temperature, humidity and pressure from a remote hazardous field such as dense forestry, deep sea floor etc [1]. Wireless Sensor Networks contain of a huge number of less cost, limited energy used to power intelligent sensor nodes with individual more sinks or main station. The major constraints of sensor nodes are their very few finite non-replaceable battery energy and power which is limitings the lifetime and quality of the sensor network. So implementing realistic network is a huge challenge for the investors. The recent days it has been identified that energy consumed is the main problem, when implementing WSN, because it is non-replaceable and non-chargeable once the SNs are plotted. In a wireless sensor network, a binary tier architecture is used with constrained energy, where SNs with limited power and energy constrained, reliability belong to low tier and abundant energy with unlimited questions powered base station in upper tier architecture [2].

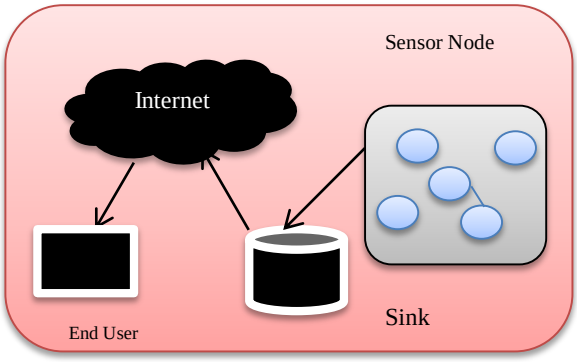


Fig 1.Wireless Sensor Network

The SNs have the abilities to grouped data and route data back to the destination and the end-users. Data is routed back to the end-user by numerous environment, architecture through the destination. The destination might communicate it the task manager node via internet/satellite[3]. In this protocol is based on the energy and power and energy efficient algorithm requires and environment of networking. On the other hand, various factors shall be taken into research consideration and when developing the protocol in wireless sensor networks. An energy efficient is a major part in the network security along with these factors. Power Efficient Gathering in Sesnor Information System protocol is an improved Energy Efficient-Power Efficient Gathering in Sesnor Information Systems[4]. The main focus in the clone attacker node, where attacker first actually detentions come of the authentic nodes from wireless sensor networks, assembles their re-commendation from individual remembrances, copy them on various nodes, i.e. how it creates clone nodes and lastly re-plot them in the sensor network. If adversary prospers, it is possible for him to create attacks such as, clone attack, selective forwarding attack and packet, changing attack, etc. Various attacks in WSNs are prohibited by creative use of out-dated cryptographic explanations [5]. For attacks like Clone node attack prohibited explanations are insufficient. As a consequence, various different techniques for detecting cloned attack in static as well moveable have been proposed. Although, mentioned methods except works to discover the replicas in wireless sensor networks, while the method discussed in prevents against clone attack node . The detection

methods define that, the clone node has been plotted in wireless sensor networks, and they use dissimilar methods to discover and mitigate clone nodes of the network, whereas the prevention methods objective to stop deployment of clone nodes at start node, they don't assume the adversary to plot illegal clones in the wireless sensor network. The method in avoiding clone node attacks in static WSNs; however, to the best of our knowledge based have proposed, i.e. method yet which avoids clone attack node in moveable WSNs[6,7].

## II. RELATED WORK

**Mr. Tushar Chauhan et a., 2016 [8]** experimental novel approach zig-zag enables client to interleave rule pole vigorous order of their physical deliver thus stray then considered to as a turning of lesser networks. The proposed work with clustering approach is worn for the grille grow not newer and it is unrestrained distinguished passage in Ad hoc networks. **Sanjoy Mondal et la., 2016 [9]** implemented energy efficiency and load balanced ant colony optimization based interconnected data gathered method. The designing area is of separated into optimize K-OPT number of clusters using k means clustering approach. The sensor nodes in a cluster form a chain method using ant colony optimization with the selection of cluster-head or leader. **Harsh Darji et al., 2016 [10]** designed machine learning algorithm could be used for reducing energy consumption. The main objective is progress machine learning based routing protocol, which having energy gathered from architecture instead of batteries. **Imane Boulhares et al., 2016 [11]** it consists of tiny SNs with sensing, consumed energy and wireless communication competencies. Routing protocols are individual of the novel key technology which has become a research in current days since the requests of WSNs are enhancing everywhere. **Debabrata Singh et al., 2016 [12]** In the homogeneous method initial energy is similar to each other, but it is dissimilar method used for different protocol that is LEACH, PEGASIS and lastly regenerated the previous protocol is called enhanced energy managed routing protocol. In this protocol is based on cluster format, Choosing the CH (Cluster Head), cluster routing and other features i.e destination node of LEACH protocol. The proposed technique is a set of tree hybrid protocols between division or grouped based LEACH – IR protocol and Chain base EE-PEGASIS protocol, where our main objective is to improve he lifetime of the network.

## III. RESEARCH METHODOLOY

We implement the hybrid approach with EE-PEGASIS and BFOA algorithm to increase the life span in the network. EE-PEGASIS routing protocol, individual node interconnects only with a adjacent neighbor node takes moves transmitting to the BS, thus optimizing the amount of energy occur per rounds. We implement the BFOA algorithm used to optimize the energy performance of the WSN. In BFOA algorithm is population size set and rotate the SNs in the network. In rotation process are two forms; tumbling and swimming. In tumbling process is a slow and swimming process is faster as compared to initial state. First, spread the packet information in the WSN and some data drop in the network cause of failure route and node in the network. In last phase, we reproduce of the failure route then recover the information from the failure route with the help of cost functions. The methodology of implementing the EE- PEGASIS PROTOCOL is quite simple. In this contrast, we would be defining with optimization techniques in case of any failure occurrence while the transmission of the data through a wireless sensor network. With optimization techniques would be calling the objective function first for the other optimal path which would list down all those possible paths which may be included to transmit the data with the most possible least energy and the maximum number of data packets transferred. There is a function name fitness function in with optimization techniques which would figure out the best optimal solution for the transmission of the data through the E- PEGASIS protocol. The ethical E- PEGASIS protocol would be configured as it is.

**Step 1:** Firstly node deployment takes place by entering the no. of node values, length of the network and width of the node in which implementation has been done. Calculate location of x-axis and y axis and time stamp of each node.

**Step 2:** Time stamp of the nodes has been chosen as a rule or protocol parameter by E-PEGASIS algorithm:

1. Starting of optimization
- Calculate time- stamp of nodes in the first block to select the cluster head.
- Measure X and Y distance of the network.Find the coverage set between the nodes.
- Checking of availability of destination.

**Step 3:** Sending of data packets from source to destination. The Selection of any node from coverage set for setting of the current node. Network checking of nodes till node9. Termination conditions will apply if node is not found between nodes 9. Plot final route between sources to destination. Plotting of remaining nodes in the network

**Step 4:** Randomly attacker will come in the WSN. The attack occurs in the network, then duplicate the nodes and delay, overhead occur and decrease the throughput.

**Step 5:** We implement the proposed algorithm using a Bacteria foraging optimization algorithm to prevent the attacker nodes. Then calculate performance parameters like throughput, delay and energy etc.

**Step 6:** Comparison between proposed performance parameters with existing performance parameters (Delay and energy consumption).

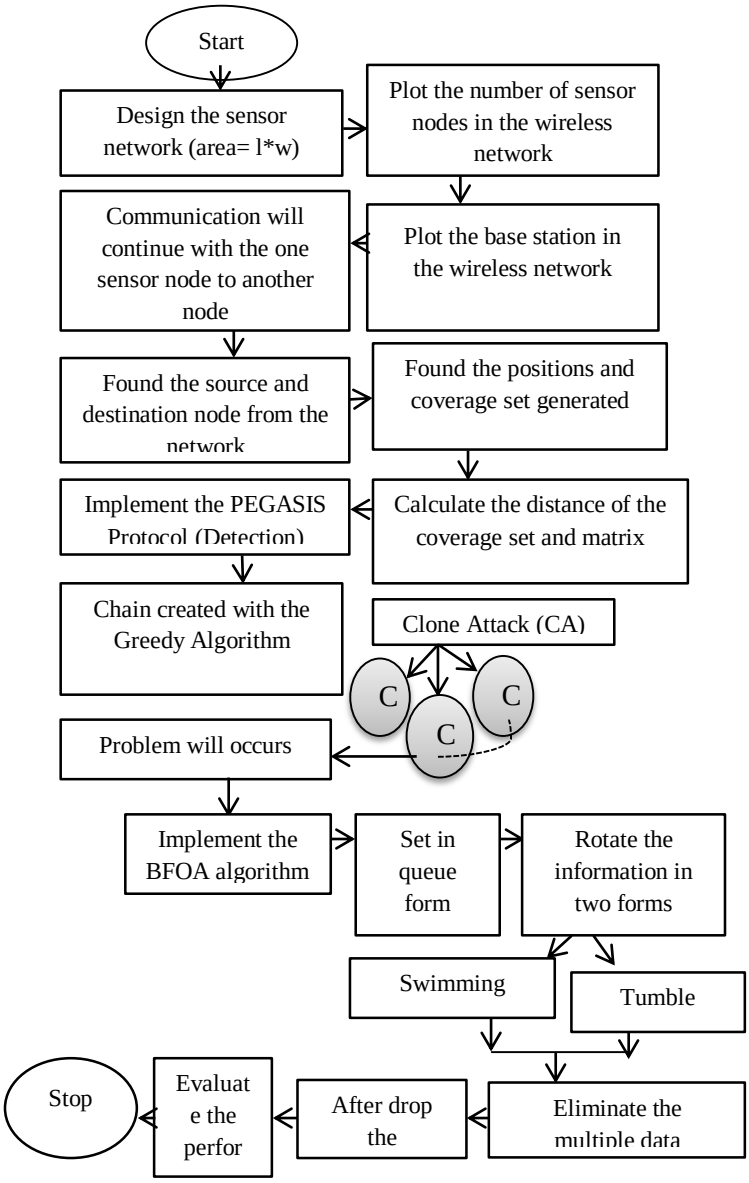


Fig 2. Proposed Flow chart

**Pseudo Code of Proposed EE-PEGASIS Protocol**

Step 1: Initialize the Wireless Sensor Network
- Destination broadcasts a low cost manage messages for header selection to all nodes.
- All sensors send positions and energy information to Destination.

Step 2: Cluster-Head - Set Selection.
- D (destination) selects a sensor with the greatest remaining energy becomes the first header for Cluster Head Set.
- Header transfer the information
- Other sensors reply to the header with Acknowledgement signal.
-Three Nodes with high Energy are choosing as a head set member.

Step 3: Path Chain Formation and Leader initialization.
- End Cluster active-head sends to next cluster.
-Leader sends the next cluster to Destination
- Destination broadcasts the 'chain completion' message.

Step 4: Data changing
- Associate nodes of each cluster send data to active cluster head.
- Active cluster heads collect the data.
- Active cluster heads send the composed data to the leader through the chain.
- Leader node sends the final collected data to the destination.

Step 5: Altering Active Header
- If E of active cluster head < eth, the Head set member with high energy becomes a new pass.
- If E of the three associates is less than eth, go to Step 2.

## IV. ANALYSIS

In this section, we analysis of the research work with energy consumption inter CCP (Cluster Coordinate Protocol) accept a layered method for clusters. It is a CB (cluster based) evaluation in which different levels of clusters are evaluated on the premise of received signal-quality to observe the distance of clusters from the Main station and depends the quality of cluster organizers to create levels for the cluster head to transmit the transformation.

### *A. Selection of the cluster head*

It's become a CH , sensor node has to evaluate residual energy as preferred:

$$Pi\ (tt) = CC * \frac{Residual\ Energy}{Average\ Energy} * \frac{BSmax}{Bs(i,S)} \quad \text{..... (i)}$$

Where the residual energy of node (i) ; BS(i,S) is speed from the node to the base station, BS max the factor value , which is used to calculated after sensor e plotting in the simulation and Average Energy defining the all energy of all live nodes in the wireless sensor network m is the overall number of nodes.

$$Pi\ (tt) = CC * \frac{Residual\ Energy}{Average\ Energy} * \frac{BSmax}{Bs(i,S)} \quad \text{..... (ii)}$$

*B. Formulate the cluster*

Selection of CH, then cluster head broadcast a message to its nearest nodes and other random node combine inside the CH by getting combine message from their respective Cluster Head.

$$BS(i,chjj) = Max\left(\frac{Residual\ Energy\ (chjj)}{rr(S,chjj) + rr(i,chjj)}\right) \quad \text{…….. (ii)}$$

Where rr(I,chjj) are the distance from node I to CH (jj) and BS(S,chjj) are the distance from the CH base station.

*C. Computation Model of Energy*

Communicating

ECx (mm,rr) = ECx –ele (mm) +ECx – amp (mm,rr) …… (iii)
Ecx(mm,rr) = Eele *mm +€amp *mm *rr2 …..(iv)
Achieving
EAx(mm) = Eax-ele (mm) EAx(mm) …….(v)

The elec energy , is depends in the digital coding ,filtering and alteration of defining signal, whereas the energy depends upon communication or receiver.Radio energy model is equal to
EAx (mm) = elec*mm …….. (iv)

The proposed security, network concept is implemented in MATLAB with Scripting Language. the display message in command window. Enter the wireless sensor nodes according to user choice; enter the network length and width. Calculate the area of wireless sensor network. It represents the cluster head node id in the wireless sensor network.

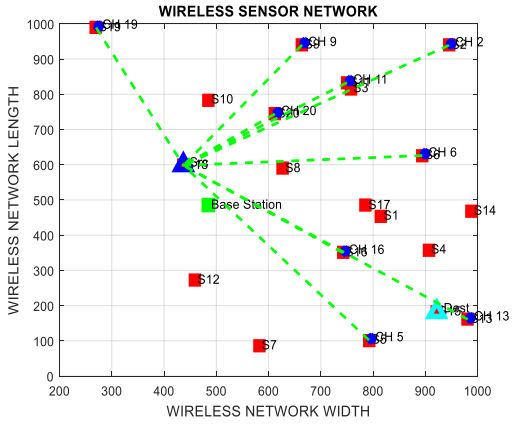


Fig 3. WSN with CH

The above figure defined that the cluster data mean EE-PEGASIS protocol design the user to communicate the sub-cluster and then packet transferring one node to another node. The line format continues communication in source to the destination node.

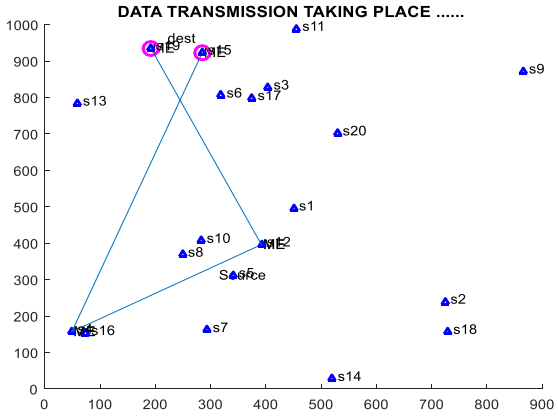


Fig 4. Data Transmission

Above figure defined that the numbers of nodes are implemented in the network randomly under the control of an administrator. These are well configured, energy efficient, and trust able nodes in the network. During node formation, each node will get a HELLO memo from the BS with a time stamp message representative the node creation time (birth time) in the network. The message verification source to other intermediate nodes. The E-PEGASIS algorithm is used during the discovery and data transmission in the network, where the node information is checked from the Base Station node information . After verification of EE-PEGASIS algorithm, the algorithm collects the ID, timestamp, and current location address of the nodes and compares with initial information when they are registered. The results of the EE-PEGASIS algorithm can provide only the trusted nodes in the route to ensure secure data transmission.

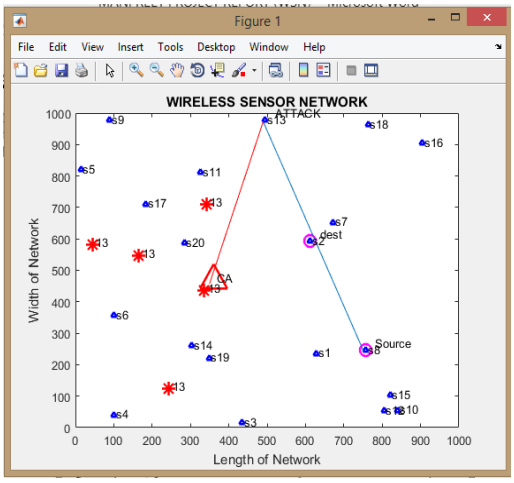


Fig 5 . Clone Attack Detect

The above figure shows the cloning attack, we assume that sensor node not tamper proof and deployed an unattended location. The adversary can capture the node collect all the secret keys, code stored on it. All the credentials are exposed to the attacker. The attacker can straightforwardly duplicate it in a large number of replicas and deploy them on the network.

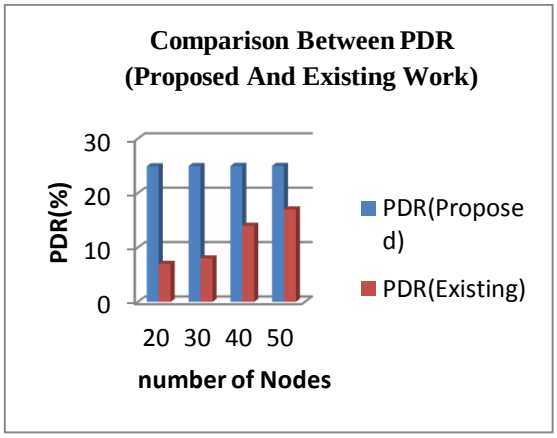


Fig 6: Comparison between PDR (Proposed and Existing work)

The above figure, we improve the PDR value with BFOA and compared the existing E-PEGASIS) protocol. The packet delivery rate with respect to wireless sensor network. The packet will drop when an attack will occurs. The packet delivery proportion is the part of packets successfully received to the total sent. Delivery is the rate at which information is sent through the network. If a network develops congested and there is good, correct, packets may column up at the source and never enter the network. Those packets will not contribute to throughput, but because they are never sent, won't affect the PDR at all. The packet delivery rate with Proposed approach. We improve the performance parameters i.e value is 24.84, 24.92,24.98 and 25.

Table no.1 Comparison between Packet Delivery Rate (Proposed and Existing Work)

| Number of Sensor Nodes | PDR(Proposed) | PDR(Existing) |
|---|---|---|
| 20 | 24.92 | 7 |
| 30 | 24.98 | 8 |
| 40 | 24.99 | 14 |
| 50 | 25 | 17 |

Table no. 2 Comparison between Delay (Proposed and Existing Work)

| Number of Sensor Nodes | Delay (Proposed) | Delay (Existing) |
|---|---|---|
| 20 | 2.4 | 17 |
| 30 | 1.5 | 11 |
| 40 | 2.2 | 12 |
| 50 | 2.8 | 7 |

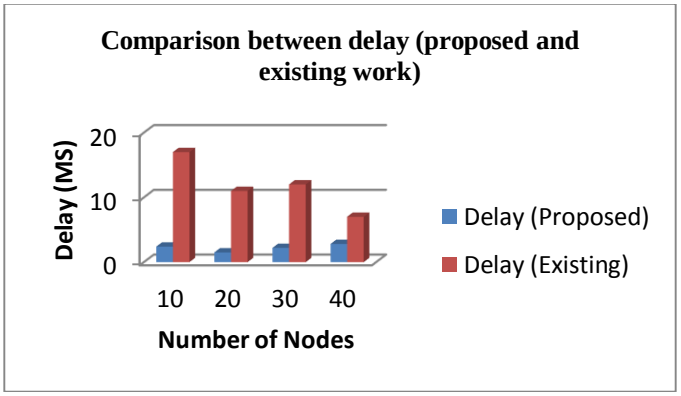


Fig 7: Comparison between delay (proposed and existing work)

The above figure represents that comparison between delay proposed and existing work. We decrease the delay with BFOA algorithm and increase the delay with E-PEGASIS protocol based. The end to end delay with CLONE attacks increase the delay and loss the packets in the network. Average end to end delay of load balanced is round about 17 milliseconds at the start of transmission and as the transmission goes on it becomes 12 millisecond but for Pegasis its minimum value is 7 milliseconds. It means averaged end to end delay is reduced with greater extend. This reduction in delay improves throughput that means now source node is sending packets more quickly to the destination then basic Message passing and verification method. The decrease the end to end delay performance parameters.The node delay in proposed scheme has been reduced significantly in the proposed scheme when system is operating for 25 ms node mobility.

Table 3: Proposed Based Detect Clone Node EE-PEGASIS and BFOA) Algorithm

| Number of Nodes | Detect Clone Node (EE-PEGASIS) | Detect Clone Node (P-BFOA) |
|---|---|---|
| 6 | 2 | 2 |
| 10 | 3 | 2 |
| 16 | 4 | 1 |
| 20 | 5 | 1 |

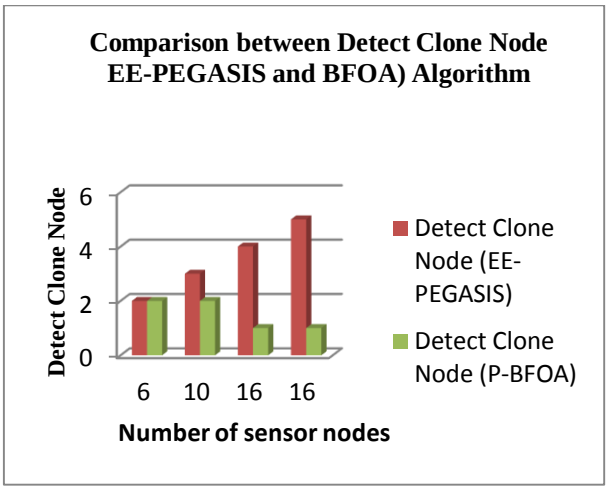


Fig 8: Comparison between detect clone node (EE-Pegasis and BFOA) algorithm

Above figure shows that the clone nodes identify and detection procedure is deployed during transmission, if it's detects the Cloned node and it automatically avoids that cloned node for transmitting the data. Data loss can prevent through detection. In this scenario the number of times for consumption should be considered for the improvement of the quality of service. The detection rate of the Replication attack is more accurate, but considering waste of time in such a kind of situation, prevention as a factor that directly eliminates the cloned node is the deciding factor in the place of detection. Subsequent elimination of the procedure message verification and passing method for prevention of the Clone attack is applicable, but the detection rate is smaller compared to E_PEGASIS and other existing methods. The detection rate of the Replication attack is more accurate, but considering waste of time in such a kind of situation, prevention as a factor that directly eliminates the cloned node is the deciding factor in the place of detection. Subsequent elimination of the procedure message verification and passing method for prevention of the Clone attack is applicable, but the detection rate is smaller compared to BFOA and other existing methods.

## V. CONCLUSION AND FUTURE SCOPE

In this conclusion the EE-PEGASIS and Optimize technique is applied for studying the trustworthiness / otherwise for a detection the clone node. The event of a sensor node as an attacker node with fake information could happen only when the nodes have final information regards other nodes. Create the route of the identification required the application of WSN protocols. Rather than spoil them for EE-PEGASIS to verify each and all nodes, the information identifies and transferring the GREEDY ALGORITHM which has created the chain and fuse data transfer source to the destination node. If a node does have authentication by the BS, it can communicate with any other sensor node in the WSN. The E-PEGASIS routing protocol in WSN is so effective for more-time saving than any other protocol. Optimized algorithm and EE-PEGASIS Protocol method needs modifications and optimization in time consuming and for cost effectiveness. The network size isn't limitations. The accuracy of the network shall be higher than the other security approach which is applied earlier in the network security. The data transfer the E-PEGASIS protocol based is applied for analyzing the trustworthiness, or otherwise for a detecting the Cloned node. The action of a node as a Cloned node with duplicate info can happen only when the node has wide-ranging information about other nodes. Confirmation of the node needs the application of BFOA and E-PEGASIS . Instead of wasting time for BFOA and E-PEGASIS to check each and every node, the communication verification and parsing process are applied for authentication prior to communication. If a node does not have any authorization by the base station, it cannot interconnect with any other node in the network.

Future researchers can even pick more refined optimization approaches for system enhancement. The future work, in this thesis can be done if this ABC Algorithm would be a half breed with the existing calculation, it may perform better than the current.

## VI. REFERENCES

[1]. Ghosh, Saurav, Sanjoy Mondal, and Utpal Biswas. "Fuzzy C Means based Hierarchical Routing Protocol in WSN with Ant Colony Optimization." In *Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on*, pp. 348-354. IEEE, 2016.

[2]. Lindsey, Stephanie, and Cauligi S. Raghavendra. "PEGASIS: Power-efficient gathering in sensor information systems." In *Aerospace conference proceedings, 2002. IEEE*, vol. 3, pp. 3-3. IEEE, 2002.

[3]. Muruganathan, Siva D., Daniel CF Ma, Rolly I. Bhasin, and Abraham O. Fapojuwo. "A centralized energy-efficient routing protocol for wireless sensor networks." *IEEE Communications Magazine* 43, no. 3 (2005): S8-13.

[4]. Jung, Sung-Min, Young-Ju Han, and Tai-Myoung Chung. "The concentric clustering scheme for efficient energy consumption in the PEGASIS." In *Advanced Communication Technology, The 9th International Conference on*, vol. 1, pp. 260-265. IEEE, 2007.

[5]. Chang, Ruay-Shiung, and Chia-Jou Kuo. "An energy efficient routing mechanism for wireless sensor networks." In *Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on*, vol. 2, pp. 5-pp. IEEE, 2006.

[6]. Maheswari, P. Uma, and P. Ganesh Kumar. "Dynamic Detection and Prevention of Clone Attack in Wireless Sensor Networks." *Wireless Personal Communications*: 1-12.

[7]. Mishra, Surabhi, and Parul Kansal. "Routing protocol based on sleep scheduling and tree cluster structure in wireless sensor network." In *Advances in Computing, Communication, &*

*Automation (ICACCA)(Fall), International Conference on*, pp. 1-4. IEEE, 2016.

[8]. Chauhan, Tushar, and Meenakshi Nayyer. "Review on energy efficient protocol based on LEACH, PEGASIS and TEEN." In *Emerging Trends in Communication Technologies (ETCT), International Conference on*, pp. 1-5. IEEE, 2016.

[9]. Mondal, Sanjoy, Saurav Ghosh, and Utpal Biswas. "ACOHC: Ant colony optimization based hierarchical clustering in wireless sensor network." In *Emerging Technological Trends (ICETT), International Conference on*, pp. 1-7. IEEE, 2016.

[10]. Darji, Harsh, and Hitesh B. Shah. "Genetic algorithm for energy harvesting-wireless sensor networks." In *Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on*, pp. 1398-1402. IEEE, 2016.

[11]. Boulhares, Imane, and Mohammed Omari. "Hybridizing PEGASIS with LEACH-1R protocols in wireless sensor networks." In *Modelling, Identification and Control (ICMIC), 2016 8th International Conference on*, pp. 1037-1042. IEEE, 2016.

[12]. Singh, Debabrata, Binod Kumar Pattanayak, and Chandan Kumar Panda. "Analysis of an improved energy balanced routing protocol for wireless sensor network." In *Communication and Signal Processing (ICCSP), 2016 International Conference on*, pp. 1807-1811. IEEE, 2016.