Energy Efficient Transmission in Wireless Sensor Networks

Shilpy Ghai[1], Prof. V.K.Katiyar[2]

[1]M.M.Engineering College, Maharishi Markandeshwar University, Mullana, Haryana, India (Research Scholar) [2]M.M.Engineering College, Maharishi Markandeshwar University, Mullana, Haryana, India (Professor, CSE Department)

Abstract- In both academia and industry field, Wireless Sensor Networks (WSNs) is an emerging and promising field. The use of such kind of networks is extended due to their unique properties, such as self-organization and ease of deployment. A wireless sensor network consists of a large number of sensor nodes which communicates wirelessly with other sensors. But as the technology is becoming advanced these days, the breaching into these technologies also increases. However, there are still some technical challenges, such as energy efficiency which depend on the number of packet loss, throughput of the network, delay time and so on. In this paper, we will design an energy efficient sensor network which will provide us a secure data transmission. For energy efficiency, we will use data aggregation. Data aggregation reduces the transmission cost and network overloading because we remove duplicate data in it. Various attacks targets the wireless sensor network through which the Wireless Sensor Topology can easily be accessed via third party. We will show the effect of sybil attack on the network and how we resolve this issue. Sybil attack targets the nodes of original path. Then we will optimize our result with ant colony optimization.

Keywords: *sensor nodes, wireless sensor network, data aggregation, energy efficiency, attacks.*

I. INTRODUCTION

With a large number of sensors of physically small devices, a Wireless Sensor Network is made, and is equipped with the capability of data processing, sensing the physical environment, and communicating wirelessly with other sensors. Commonly, we assume that there have certain constraints in each sensor in a wireless sensor network. These constraints are with respect to its energy source, power, memory, and computational capabilities [1].

A typical wireless sensor network [2], consisting of a collection of sensor nodes (also called "motes") and a base-station. Some of current deployments range from ten to hundreds of sensor nodes, although WSNs are expected for heavy distribution of thousands of nodes. Generally, the events of interest occur rarely and suddenly in sensor networks for environmental monitoring and surveillance applications. Therefore, the traffic of network is very low. When event of interest occurs, the traffic flow increases abruptly and leading to large amounts of sensory data from various sensor nodes being conveyed to the base-station in the event of a phenomenon of interest, leading to abrupt increase in traffic. Sensor nodes are deployed densely to ensure that the event of phenomenon of interest is captured properly and accurately. The densely deployed nodes not only ensure coverage and communication but also tolerate node failures.

A. Data Aggregation

In terms of computation capability, communication bandwidth and energy reserves a sensor node is extremely restricted. Actual method to collect the information sensed from the network is to allow each sensor node's reading to be forwarded to the base station, possibly through other intermediate nodes, before the base station processes the received data. However, this method is extremely expensive in terms of communication overhead which make researcher to designed and work on an energy efficient mechanism. In large WSNs, computing aggregates in-network (i.e., combining partial results at intermediate nodes during message routing) will reduces the amount of communication and hence the energy consumed by them. Sensor nodes process the raw data into a digest by using a data aggregation mechanism and only that digest will be send to the sink. Data aggregation reduces the transmission cost and network overloading because of reduced in amount of the digest.

Security is broadly used term including the characteristics of authentication, integrity, privacy and non repudiation. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the network has increased. Several cryptographic, steganographic and other techniques are used for the secure transmission of various types of information over networks. The main aim of third objective is to provide security to the data from different attacks in WSNs. Main focus of third objective is on studies the different attacks in WSNs and than briefly study the sybil attack, its affect on WSN and how we can prevent data from sybil attack.

To design an energy efficient protocol that provides extensible network support on Wireless Sensor Networks a new protocol will be made based on MAC protocol which should be able to modify the traffic and topology dynamics. In addition

requiring a reliable communication protocol, it is unreliable to the efficiency and effectiveness of data gathering. We are using algorithm to achieve the required energy efficiency and along with that taking care of security in WSNs, which will be achieved by Ant colony optimization.

In data Aggregation technique firstly the data is aggregated in an efficient manner after it has been gathered. By this redundancy of data have been reduced which will enhanced the network lifetime. Over a sensing area by adjustment of large number of sensors the data accuracy will increase. The same phenomena are sense by sensors used in the neighbouring region due to this lot of duplicate data is produce. Because of this redundancy of data will be there which will lead to more bandwidths requirement and more consumption of energy. Data De- distribution means removing duplicate data to reduce the redundancy. To perform De-duplication data aggregation techniques are used [3]. By sensor nodes data aggregation sensor data is collected which is further aggregated by using some data aggregation algorithms and then forwarded that aggregated data towards base station

For data aggregations strategies number of approaches are available. These approaches are In-network aggregation, with size reduction, without size reduction, Tree-based approach, and cluster-Based approach.

We will use the hybrid techniques (combinations of DBST and REDD) for data aggregations.

To solve hotspot problem and to improve energy conservation Dynamically Balanced Spanning Tree (DBST) [4] has been used which provides dynamic structure of tree.

To eliminate redundancy from valid data Redundancy Eliminated Data Dissemination (REDD) [5] algorithm use the context aware system for validation and correlation coefficient.

Dynamic balanced spanning tree (DBST)

To improve lifetime of network this algorithm some parameters are considers which are distance, residual energy and node weight. For all rounds number of researches has used a fixed routing tree. A time is needed for collection of one data unit from every node in the network and delivering the aggregated data to sink. But the hotspot problem occurs in this because the nodes are fixed. The drawback of hosspot is that it will drains the battery quickly. To solve this problem DBST is used. It balance the traffic load along with minimizes and maximum energy consumption between the sensor nodes. By using kruskals algorithm Tree can be formed in case of this smallest possible weight spanning [6] as DBST is a tree based approach.

In root node selection residual energy is used as a parameter in DBST. The highest residual energy will be selected as a root after each round of the node. Because of which the responsibility of getting root is delivered adequately between all nodes and by this the problem of hotspot will get solved. The hotspot problem will get solved by forming spanning tree for each round though DBST. To form spanning tree number of parameters have to be considered such as node weight and link weight. To find node weight in DBST we need to considered energy required for communication, residual energy and heterogeneity of network as main principle. By using node weight of all nodes link weight is determined as:

$$F_{i,j} = F_{j,i=WiWj}\frac{Ei,j}{Eo+\beta(\sqrt{Eri^2+Erj^2})}\,i,j=1,2\ldots n$$

DBST performs data gathering and aggregation after tree formation and root node selection. The root will forwards the aggregated data which is sent towards the root towards the sink.

The traffic load is balanced and energy consumption will be reduced by using dynamic routing tree in DBST. This will reduce the bandwidth overhead. As in this there is need to create new tree for each round which result in little bit increase in delay by using this algorithm.

Redundancy Eliminated Data Dissemination (REDD)

In this approach we divide the total geographical area into clusters which are based on grid. One header node which is called as representative node is selected in each cluster. Than further this header node is elected which is based upon battery power. There might be a chance that node may go in other cluster as the nodes of WSN are moving. Dynamic topology management module of REDD is used to handle this issue [7].

Whenever sink node queries for data of interest from source nodes, that query is forwarded by header to header forwarding into source [8]. This forwarding is done through shortest path founded by sink.

B. Attacks in Wireless Sensor Networks

Denial of service (DoS): DoS is produced by not planned failure of nodes or malicious action. It tries to disable the resources available to the victim node by sending extra unnecessary packets. At different layers, the DoS attacks could be Jamming, tampering, collision, misdirection, flooding etc.

Attacks on information in transit: Sensors monitor the changes of specific parameters in case of a sensor network, and address about it to the sink according to the requirement. During transmission the report can be changed or disappeared.

*Sybil attack***:** Sybil attack is that in which a node produces the identities of more than one node.

Blackhole/sinkhole Attack: In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Attacker tries to insert the malicious node into the network to do anything with the packets passing between them.

*Hello Flood Attack***:** In this attack, **Hello** packets are used to assure the sensors in WSN. Within the WSN these packets are delivered in a large area. The sensors are thus convinced that the attacker is their neighbour.

*Wormhole Attack***:** In this attack, at one location in the network attacker records the packets and tunnels those to another location. We can do bits tunnelling or its retransmission could be done selectively.

C. Ant Colony Optimization

The ant colony optimization algorithm (ACO) is used for solving computational problems. It is a technique which comes under probabilistic techniques this can be reduced to finding good paths through graphs. This algorithm come under a member of the ant colony algorithms family, in swarm intelligence methods, and it constitutes some meta-heuristic optimizations [9], Mauro Bimttari. Initially proposed by Marco Dorigo in 1992 in his PhD thesis, the first algorithm was aiming to search for an optimal path in a graph, based on the behaviour of ants seeking a path between their colony and a source of food. Original idea has been made to solve a wider class of numerical problems, and because of this several problems have appeared, depict on various aspects of the behaviour of ants.

In ACO through states of the problem a set of computational concurrent and asynchronous agents (a colony of ants) moves in corresponding to partial solutions of the problem to solve. Then by applying a stochastic local decision policy which is based on two parameters and they move which is called trails and attractiveness. A solution is constructed for the problem by incremented each ant by moving. The solution is evaluated by ant and during the construction phase or the completion of a solution modifies the trail value on the components which is used in its solution. This pheromone information will direct the search of future ants is directed by that pheromone information. Furthermore, two more mechanisms are including by an ACO which are trail evaporation and optionally, daemon actions.

From number of papers in Literature survey it has been analyzed and concluded that WSNs suffer from many security attacks when use either in remote or hostile environments. Have seen in previous papers that the Sybil attack is one of the severe attacks in which malicious nodes report false identities and location information such that the remaining nodes believe that many nodes exist in their vicinity. In paper [10] they have proposed a method for detecting Sybil attack using sequential analysis. This method works in two stages. First, by observing neighbouring node activities it collects the evidences than that collected evidences are combined to provide input to the second stage. In this stage, to decide whether the neighbour node is Sybil or benign that collected evidences are confirmed using the sequential probability ratio test. By using the network simulator ns-2, the proposed method has been evaluated. This paper simulation results show that the proposed method is very powerful in detecting Sybil attacks with very low false positive and false negative rates.

II. RELATED WORK

In 2011 Shahriar Mohammadi, et al. [11] focused on security of Wireless sensor networks (WSNs), divided it into four categories and considered them and then compared them. It including an overview of WSNs, WSNs security, the threat model on WSNs, a wide variety of routing attacks in WSNs. Hundreds or thousands small sensor nodes in WSNs usually consist of MICA2, which operate individually, there are some conditions such as cost, invisible deployment and many application domains, lead to small size and limited resources sensors which have many potential applications and unique challenges. There are number of routing attacks in WSNs and most of the existing traditional networks security techniques are useless on WSNs. Due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources. So, security is a very important requirement for these networks; but we have to design a proper security mechanism that attends to WSN's constraints and requirements.

In 2011 Christian Dominguez Medina, et al. [12] has proposed a meta-heuristic Ant Colony Optimization (ACO) to solve the issues in WSNs such as data routing problem. This problem becomes more complex by the increase in size of the sensor nodes in the network. The network lifetime can be maximized and latency in data transmission can be reduced by using ACO based routing algorithms , but this is only possible by means of an adaptable and balanced algorithm that takes into account the WSN main restrictions, for example, memory and power supply. In this paper the author presented the comparison of two ACO based routing algorithms for WSN by taking into account current amounts of energy consumption under a WSN scenario proposed.

In 2012 V. Kumar, et al. [13] analyzed and presented the performance of the secure hierarchical data aggregation algorithm. In this to achieve end to end security an efficient public key cryptosystem has been used.

In 2012 Madhu Dahiya, et al. [14] used a Flooding algorithm and limitations of this algorithm are also removed using grid network. Then, a horizontal-vertical method for load balancing of this grid network is proposed. In this method, first move one step horizontally and one step node vertically. Due to which the load on centralized

node increased. Then shift the load on neighbour node based on minimum load and then remove the centre node. Now energy consumption on central node will be minimum so that network can be used more efficiently.

In 2012 Chi Lin, et al. [15] proposed DAACA algorithm for data aggregation. DAACA is a family of ant colony algorithm which consist of three phases such as initialization, packets transmission in which to compute the probabilities for dynamically selecting the next hop and operations on pheromones each node estimates the amount of pheromones and the remaining energy of neighbour nodes. After number of rounds of transmission the pheromones adjustment have been performed. For prolonging the network lifetime in energy-constrained wireless sensor networks, energy efficiency is critical. To prolong the network life, four different pheromones adjustment strategies have been described and the experimental results proved that the data aggregation algorithms, DAACA shows higher superiority on average degree of nodes, energy efficiency, prolonging the network lifetime, computation complexity and success ratio of one hop transmission.

In 2013 A. Diop, et al. [16] discusses that the complex security algorithms cannot be used in sensor networks due to the limited memory resources and energy constraints. Therefore, to reduce the risks of security it is necessary the security level and the associated energy consumption overhead will balance. In WSNs hierarchical routing protocol is more energy-efficient than other routing protocols. So, to overcome these constraints number of secure cluster-based routing protocols has been proposed. In this paper, the author has discussed the secure Energy-Efficient Hierarchical Routing Protocols in WSNs and compares them in terms of security, performance and efficiency. Security issues for WSNs and their solutions are also discussed.

In 2014 Sweety Saxena, et al. [17] have proposed an algorithm for Sybil attack detection which is based on Time difference of Arrival (TDOA) localized method. It detects the malicious behaviour of the head node and member nodes in a cluster network method to detect head node and member node of cluster in WSN as Sybil. In the review of this paper various other algorithms are presented to detect Sybil attack. Their method has achieved a detection rate of 96% and very low false positive rate of 4% and below. The results show that the approach is effective in detecting Sybil attack in WSN.

In 2014 Samarth Anavatti, et al. [18] in order to improve life time of sensor nodes the author have explained many data aggregation techniques that perform data redundancy removal. The redundant data come because to endure the reliability, many sensor nodes are deployed in the monitoring environment and they forward it to the sink node after sensing the same kind of data. By this reduntant information we have achieved the reliability but at the same time the sink node energy get wasted in processing that redundant data. So in order to maintain the trade off between energy conservation and reliability there is a need to eliminate the redundancy in sensed data up to adequate level. By using different data aggregation techniques which perform data redundancy removal so that the life time of sensor nodes get improved. Further in this paper the author have discussed the advantages and limitations of data aggregation techniques.

In [19] Bhaskar Krishnamachari, et al. has modelled data-centric routing and its performance is compared end to end with traditional routing schemes. They have checked energy costs impact of source destination placement and communication network density and delay associated with data aggregation. Over a wide range of operational schemes the author has showed that significant performance gain is offered by data centric. The complexity of optimal data aggregation have also being examined by author, showing that there exist useful polynomial time special cases even though in general it is an NP-hard problem. An event-based system is distributed by sensor networks that differ from traditional communication networks in several ways: sensor networks have uncompromising energy constraints, redundant low-rate data, and many-to-one flows. For energy-efficient information flow data centric mechanisms that perform in-network aggregation of data are needed in this setting.

In 2016 Namrata, et al. [20] have purposed an routing protocol which is energy efficient so that the network lifetime get increased and in order to secure the network they have purposed zone intrusion detection system for MANETs for randomly deployed mobile nodes. Mobile Ad-hoc Networks (MANETs) are wireless networks consisting entirely of mobile nodes (without base stations) that communicate with each other. As there is no fixed infrastructure in Ad-hoc networks, therefore there are no routers or separate network elements and therefore the mobile nodes themselves act as the routers.

III. PROPOSED WORK

ALGORITHM

This work deals with the hybridization of the DBST and REDD algorithms for the data aggregation in Wireless sensor networks [21].

1. First, we have implemented DBST technique, in which cluster formation takes place and this deals with the hierarchical manner in which we will get an ordered manner of our network.

2.Each cluster is having number of nodes and each node will have different energies.

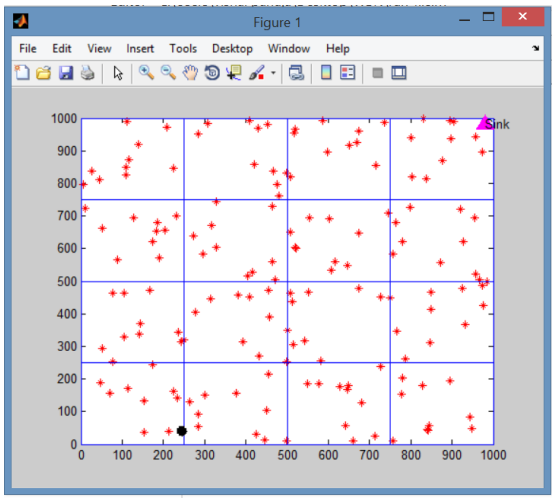

Fig.3.1 cluster formation

3. Each cluster will have one cluster head because instead of harvesting all energies of the node, Cluster head will communicate on behalf of each cluster for the conservation of energy and it will communicate with the sink node.

4. Then those cluster heads will be having tree structure as mentioned in the REDD structure which deals with the tree data structure.

5. In tree data structure, there is root node and leaf node and route will be performed from leaf node to root node and the root node is that cluster node which is having high residual energy than other cluster head nodes and those contains data in the form of packets which will be transferred to the root node.

6. The route will be performed with the use of the link weight[22].

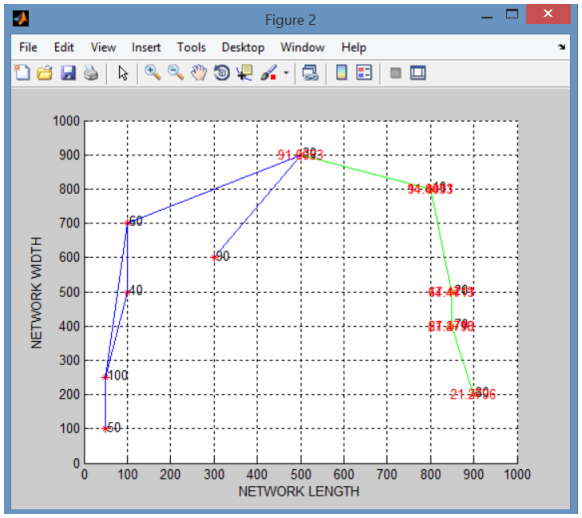

Fig.3.2 Selected route

7. The nodes are showing the selected route through which the packets are sending to the root nodes which is performing routing.

8. The below figure shows the Sybil attack which shows the multiple copies of the original node in the yellow color which will increase the load in the network. This will decrease the lifespan of the network. The Sybil attack is the routing attack due to which the packets will be dropped and it will increase the energy consumption of the network.

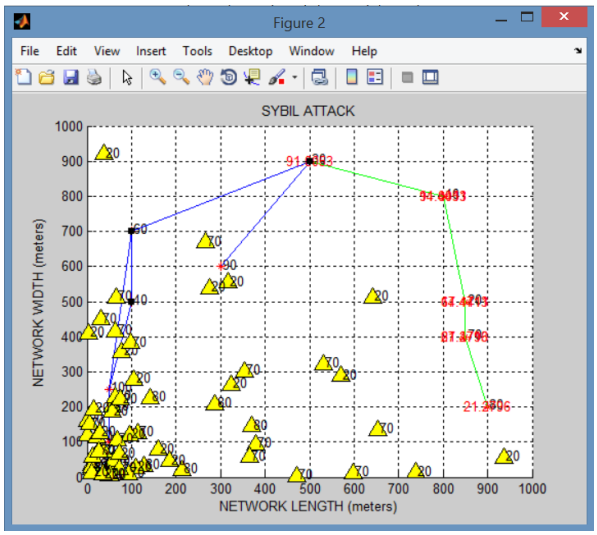

Fig.3.3 Sybil Attack

9. This figure shows that after applying the ACO optimization techniques on the network which is suffering from the Sybil attack. We have find the shortest path in the network by applying the Sybil attack

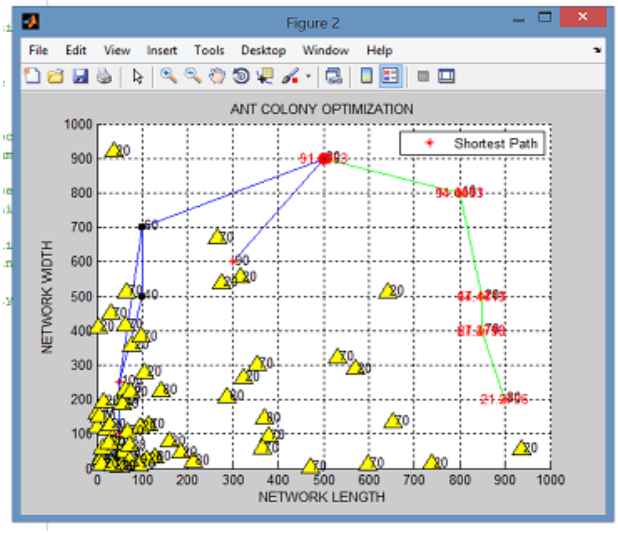

Fig.3.4 ACO Technique

10. This figure shows the optimization process using ant colony optimization in terms of the end delay. End delay is the end to end delay of transferring packets from leaf node to the root node and shows that the time delay is coming 25 ms for each particular 10 seconds which will iterative to the completion of the length of the data. The delay is coming less which is the desired output of the proposed approach.

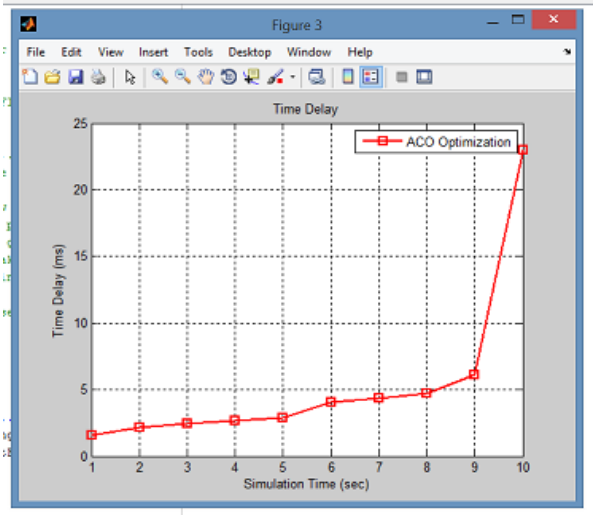

Fig.3. 5 ACO result in terms of the end delay.

11. The loss of number of packets is vary by the simulation time. At some point it will be maximum and on the another time it will be minimum. The result have shown that the simulation time is minimum when the simulation time is 2 sec which is the best time and on the other hand the results also shown that the loss of packet will be maximum when the simulation time will be 7.

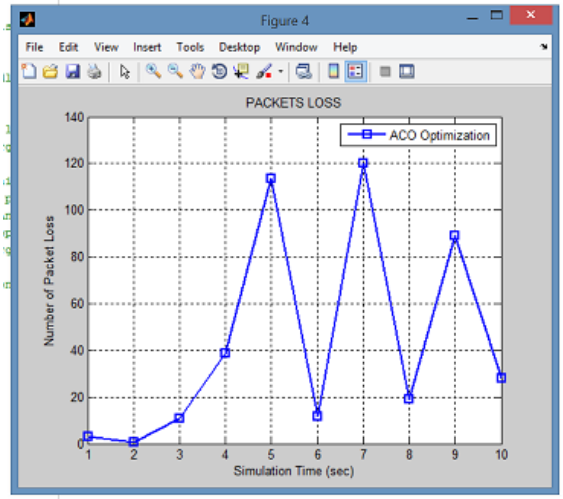

Fig.3. 6 ACO result in term of loss of packets

12. The figure of simulation result shows the energy consumption of the network which must be less and out proposed approach is able to achieve less energy consumption for the loss of the packets.

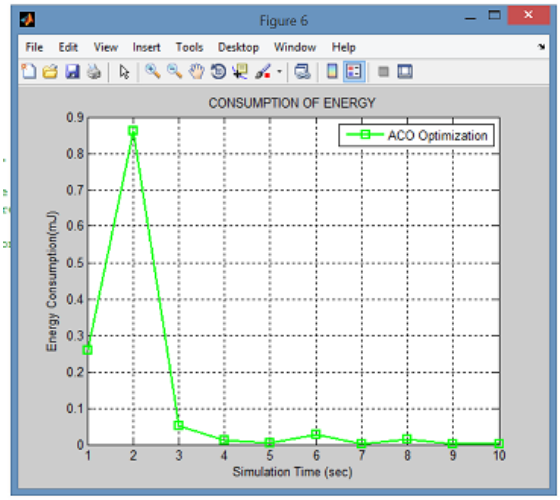

Fig.3.7 ACO results in terms of energy consumption

Through the above parameters we can say that our proposed approach is able to achieve less end delay, Less packet loss and less energy consumption to increase the lifetime of the network.

IV.CONCLUSION

In this paper, we have designed an energy efficient and secure approach for data transmission in wireless sensor networks. We have used data aggregation to reduce redundancy in wireless sensor networks to make energy efficient network. We have used a hybrid technique using DBST and REDD techniques. As a result, we get a hierarchical structure of the

nodes in which the root node has high energy value. We obtain a path in which the nodes travel from the source to the destination. Then we have applied sybil attack on it. Sybil attack targets the original node which is participating in the path from source to sink. Then for the optimized results we are using Ant Colony Optimization technique. We have applied our approach on some parameters like end delay, packet loss, energy consumption .

V. REFERENCES

[1]. Neha, Dua; R & Mathur, V. Wireless Sensor Networks: Architecture, Protocols, Simulator Tool. International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vol 2, Issue 5, pp. 229-233.

[2]. Guo, B.; Zhang. D. and Imai, M. Toward a cooperative programming framework for context-aware applications. Personal and Ubiquitous Computing, 2011, pp. 221-233.

[3]. Avokh, Avid ; Patil, Ghasem Mirjalily. Dynamic Balanced Spanning Tree (DBST) for Data Aggregation in Wireless Sensor Networks. 5th International Symposium on Telecommunications, IST2010, 978-1-4244-8185-9/10 , 2010 IEEE.

[4]. Ramachandran, Sumalatha; Gopi, Aswin Kumar; Elumalai, Giridara Varma ; Chellapa, Murugesan. REDD: Redundancy Eliminated Data Dissemination in Cluster Based Mobile Sinks. ICRTIT 2011, 978-1-4577-0590-8/11, 2011 IEEE.

[5]. Gagarin, A.; Hussain, S. and Yang, L.T. Distributed hierarchical search for balanced energy consumption routing spanning trees in Wireless Sensor Networks. J. Parallel Distrib. Comput, 2010, Vol. 70, no. 9, pp. 975-982.

[6]. Viana, A.C.; Ziviani, A. and Friedman, R. Decoupling Data Dissemination from Mobile Sink's Trajectory in Wireless Sensor Networks. IEEECommunication Letters, Mar. 2009, Vol. 13, no. 3.

[7]. Shehnaz T. Patel, Nital H. Mistry. A Review: Sybil attack detection technique in WSN. IEEE 4th international conference on Electronics and Communication, 2017, Vol. 21, pp. 184-188.

[8]. Pravin Khandare, Yogesh Sharma, S. R. Sakhare. Countermeasures for Selective Forwarding and Wormhole Attack in WSN. International Conference on Inventive Systems and Control (ICISC-2017), vol. 12, pp. 181-189.

[9]. Dorigo, Marco; Bimttari, Mauro. Ant Colony Optimization Artificial Ants as a Computational Intelligence Technique", IRIDIA – TECHNICAL REPORT SERIES, 2006.

[10]. Levine, Brian Neil; Shields, Clay; Boris Margolin, N. A Survey of Solutions to the Sybil Attack.

[11]. Mohammadi, Shahriar; Atani, Reza Ebrahimi and Jadidoleslamy, Hossein. A Comparison of Routing Attacks on Wireless Sensor Networks, Journal of Information Assurance and Security, 2011, Vol. 6, pp. 195-215.

[12]. Medina, Christian Dominguez and Cruz Cortes, Nareli. Energy-Efficient and Location-Aware Ant Colony Based Routing Algorithms for Wireless Sensor Networks. 2011, pp.117-124.

[13]. Kumar, V & Madria, S. Secure hierarchical data aggregation in wireless sensor networks: performance evaluation and analysis. International Conference on Mobile Data Management, 2012, pp. 196-201.

[14]. Madhu; Dahiya, A & Dahiya, B. Energy Efficient Data Transfer in Secure Wireless Sensor Networks. Advanced Computing and Communication Technologies (ACCT), 2012, pp. 495-499.

[15]. Lin, Chi; Wu, Guowei; Xia, Feng; Li, Mingchu; Yao, Lin; Pei, Zhongyi.. Energy efficient ant colony algorithms for data aggregation in wireless sensor networks. Journal of Computer and System Sciences, 2011, pp. 1686-1702.

[16]. Diop, A; Qi, Y; Wang, Q; hussain, S. An Advanced Survey on Secure Energy-Efficient Hierarchical Routing Protocols in Wireless Sensor Networks .IJCSI, 2013, Vol 10, pp. 1-11.

[17]. Manju, v c. Sybil attack prevention in wireless sensor network. International journal of computer networking, Wireless and mobile communications, 2014, vol. 4, pp. 125-132.

[18]. Sharma, Priyanka; Inderjeet Kaur. A Comparative Study on Energy Efficient Routing Protocols in Wireless Sensor Networks. International Journal of Computer Science Issues, 2015, Vol. 12, pp.98-106.

[19]. Avokh, Avid ; Patil, Ghasem Mirjalily. Dynamic Balanced Spanning Tree (DBST) for Data Aggregation in Wireless Sensor Networks. 5th International Symposium on Telecommunications, IST2010, 978-1-4244-8185-9/10 , 2010 IEEE.

[20]. Ramachandran, Sumalatha; Gopi, Aswin Kumar; Elumalai, Giridara Varma ; Chellapa, Murugesan. REDD: Redundancy Eliminated Data Dissemination in Cluster Based Mobile Sinks. ICRTIT 2011, 978-1-4577-0590-8/11, 2011 IEEE.

[21]. Bashyal, S. and G.K. Venayagamoorthy. Collaborative routing algorithm for wireless sensor network longevity IEEE, 2007.

[22]. Narasimhan, R. and Cox D.C. A handoff algorithm for wireless systems using pattern recognition, IEEE, 1998.