Data Aggregation and Energy Efficient Transmission in Wireless Sensor Networks

R.Venkadesh, M.Poovitha, R.Kuttimani
Department of Electronics and Communication Engineering
Dhanalakshmi Srinivasan Institute of Technology, Samayapuram, Tamil Nadu, India

Abstract - In each academia and enterprise field, Wireless Sensor Networks (WSNs) is an rising and promising field. The use of such variety of networks is extended due to their unique properties, such as self-organization and ease of deployment. A wi-fi sensor network consists of a giant quantity of sensor nodes which communicates wirelessly with other sensors. But as the science is becoming advanced these days, the breaching into these technologies also increases. However, there are still some technical challenges, such as energy effectivity which rely on the quantity of packet loss, throughput of the network, delay time and so on. In this paper, we will diagram an strength efficient sensor community which will supply us a impenetrable statistics transmission. For electricity efficiency, we will use records aggregation. Data aggregation reduces the transmission price and community overloading due to the fact we eliminate reproduction facts in it. Various assaults goal the wireless sensor community thru which the Wireless Sensor Topology can without difficulty be accessed through 1/3 party. We will show the effect of sybil assault on the network and how we get to the bottom of this issue. Sybil assault goals the nodes of authentic path. Then we will optimize our result with ant colony optimization. Keywords: sensor nodes, wireless sensor network, statistics aggregation, electricity efficiency, attacks.

I. INTRODUCTION

With a large wide variety of sensors of bodily small devices, a Wireless Sensor Network is made, and is outfitted with the capability of facts processing, sensing the physical environment, and speaking wirelessly with different sensors. Commonly, we expect that there have sure constraints in each sensor in a wireless sensor network. These constraints are with admire to its strength source, power, memory, and computational competencies [1].

An ordinary wireless sensor network [2], consisting of a collection of sensor nodes (also known as "motes") and a base-station. Some of current deployments range from ten to thousands of sensor nodes, even though WSNs are predicted for heavy distribution of thousands of nodes. Generally, the occasions of hobby happen not often and abruptly in sensor networks for environmental monitoring and surveillance applications. Therefore, the visitors of network is very low. When match of pastime occurs, the visitors flow will increase all at once and leading to large amounts of sensory information from a variety of sensor nodes being conveyed to the base-station in the tournament of a phenomenon of interest, leading to abrupt extend in traffic. Sensor nodes are deployed densely to make certain that the tournament of phenomenon of hobby is captured suitable and accurately. The densely deployed nodes not only make sure insurance and communication but additionally tolerate node failures. In the current years, Wireless Sensor

Networks (WSNs) have been considerably employed in more than a few functions such as industrial monitoring, far off controlling, military, medical, and auto-motive sensing [13].

WSNs are commonly battery-powered Ad-hoc networks which are in a position to sense and react to activities in a particular environment [14].The procedure of routing information from all the nodes to the sink is frequent as convergecast [14].Since energy consumption has direct relation with nodes distance [14], [15], multi-hop conversation and information aggregation could be regarded as appropriate solutions. Kruskal's Minimum Energy Spanning Tree (MEST) and Dijkstra's Shortest Path spanning Tree (SPT) are conventional examples of tree routing protocols [14].In [14], authors tackle the performing of more desirable Data Aggregation Converge cast (DAC) in an strength and latency environment friendly manner. The standard first order radio mannequin is used to account the amount of energy spent in at some stage in verbal exchange [14], [15]. Furthermore, in many techniques [2], [10], the fee of the hyperlinks and the strength for communicating between two nodes are used interchangeably. Since strength consumption has direct relation with nodes distance [2], [3], multi-hop conversation and information aggregation could be considered as suitable solutions. One of the most popular protocols is tree based totally routing algorithms which use only mum or dad and infant relationship [16]. One of the most popular protocols is tree based routing algorithms which use solely guardian and baby relationship [17]. Espan is an energy-aware and dispensed spanning tree algorithm which chooses the root node with respect to residual power [18]. In Espan algorithm [18], the node with best possible ultimate electricity is selected as root node. In [19], each node selects a node with most power within its neighbors as parent but it additionally considers the distance as 2d factor.

A. Data Aggregation

In phrases of computation capability, verbal exchange bandwidth and electricity reserves a sensor node is extremely restricted. Actual technique to accumulate the records sensed from the network is to permit every sensor node's analyzing to be forwarded to the base station, perchance thru different intermediate nodes, before the base station procedures the obtained data. However, this approach is extremely expensive in terms of conversation overhead which make researcher to designed and work on an electricity environment friendly mechanism. In giant WSNs, computing aggregates in-network (i.e., combining partial consequences at intermediate nodes in the course of message routing) will reduces the quantity of verbal exchange and hence the strength ate up via them. Sensor nodes technique the uncooked facts into a digest by means of the usage of a statistics aggregation mechanism and only that digest will be ship to the sink. Data aggregation reduces the transmission value and network overloading due to the fact of decreased in quantity of the digest. Security is extensively used term such as the traits of authentication, integrity, privacy and non repudiation. The greater the dependency on the information supplied by the networks has been increased, the extra the hazard of invulnerable transmission of facts over the network has increased. Several cryptographic, steganographic and different techniques are used for the invulnerable transmission of a number sorts of data over networks. The major intention of 0.33 objective is to grant safety to the information from exceptional assaults in WSNs. Main focus of 1/3 objective is on research the one of a kind attacks in WSNs and than quickly study the Sybil attack, its affect on WSN and how we can prevent data from Sybil attack. To sketch an strength environment friendly protocol that affords extensible community help on

Wireless Sensor Networks a new protocol will be made primarily based on MAC protocol which have to be in a position to adjust the visitors and topology dynamics. In addition requiring a reliable verbal exchange protocol, it is unreliable to the efficiency and effectiveness of data gathering. We are using algorithm to attain the required energy efficiency and along with that taking care of safety in WSNs, which will be executed by Ant colony optimization.

In facts Aggregation approach firstly the facts is aggregated in an efficient manner after it has been gathered. By this redundancy of information have been decreased which will enhance the network lifetime. Over a sensing place by using adjustment of a giant number of sensors, the records accuracy will increase. The equal phenomena are sensed by means of sensors used in the neighboring vicinity due to this lot of reproduction data is produced. Because of this redundancy of information will be there which will lead to greater bandwidths requirement and greater consumption of energy. Data De- distribution capacity eliminating duplicate data to reduce the redundancy. To operate De-duplication information aggregation methods are used [3]. By sensor nodes, data aggregation sensor records is collected which is further aggregated by the use of some records aggregation algorithms and then forwarded that aggregated information in the direction of the base station. For statistics aggregations techniques a variety of methods are available. These techniques are In-network aggregation, with size reduction, except size reduction, Tree-based approach, and cluster-Based approach. We will use the hybrid strategies (combinations of DBST and REDD) for statistics aggregations. To clear up the hotspot trouble and to improve energy conservation Dynamically Balanced Spanning Tree (DBST) [4] has been used which affords a dynamic structure of the tree. To put off redundancy from legitimate data Redundancy Eliminated Data Dissemination (REDD) [5] algorithm use the context-aware device for validation and correlation coefficient.

Dynamic balanced spanning tree (DBST)

To enhance the lifetime of the community this algorithm some parameters are considers which are distance, residual energy, and node weight. For all rounds variety of researches has used a constant routing tree. Time is wanted for the series of one records unit from every node in the network and turning in the aggregated information to sink. But the hotspot problem happens in this due to the fact the nodes are fixed. The drawback of the hotspot is that it will drain the battery quickly. To clear up this problem DBST is used. It balances the traffic load along with minimizes and most electricity consumption between the sensor nodes. By using Kruskal's algorithm Tree can be formed in case of this smallest possible weight spanning [6] as DBST is a tree-based approach. In root node determination residual energy is used as a parameter in DBST. The perfect residual strength will be chosen as root after every spherical of the node. Because of which the responsibility of getting root is delivered properly between all nodes and with the aid of this, the trouble of hotspot will get solved. The hotspot problem will get solved by way of forming spanning tree for each spherical although DBST. To structure spanning tree quantity of parameters have to be regarded such as node weight and link weight. To find node weight in DBST we need to viewed power required for communication, residual strength and heterogeneity of community as the most important principle. By the usage of node weight of all nodes hyperlink weight is determined as:

$$F_{i,j} = F_{j,i} = W_i W_j \frac{-E_{ij}}{E_0 + \beta\sqrt{Er_i^2 + Er_j^2}} \quad I,j = 1, 2 \ldots\ldots.. n$$

DBST performs records gathering and aggregation after tree formation and root node selection. The root will forwards the aggregated facts which is despatched towards the root towards the sink. The site visitors load is balanced and strength consumption will be decreased by using the use of dynamic routing tree in DBST. This will decrease the bandwidth overhead. As in this, there is a want to create a new tree for each spherical which outcomes in a little bit amplify in delay through using this algorithm.

Redundancy Eliminated Data Dissemination (REDD)

In this approach, we divide the whole geographical region into clusters which are based on a grid. One header node which is known as as the representative node is selected in each cluster. Than in addition this header node is elected which is based upon battery power. There may be a risk that node may go in any other cluster as the nodes of WSN are moving. Dynamic topology administration module of REDD is used to manage this difficulty [7]. Whenever sink node queries for information of hobby from supply nodes, that question is forwarded by means of the header to header forwarding into supply [8]. This forwarding is executed through shortest route centered through the sink.

B. Attacks in Wireless Sensor Networks

Denial of service (DoS): DoS is produced by using not deliberate failure of nodes or malicious action. It tries to disable the sources available to the victim node by sending extra pointless packets. At special layers, the DoS attacks should be Jamming, tampering, collision, misdirection, flooding etc. Attacks on records in transit: Sensors monitor the changes of specific parameters in case of a sensor network, and tackle 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 greater than one node. Blackhole/sinkhole Attack: In this attack, a malicious node acts as a black gap to appeal to all the visitors in the sensor network. The attacker tries to insert the malicious code into the network to do something with the packets passing between them.

Hello Flood Attack: In this attack, Hello packets are used to guarantee the sensors in WSN. Within the WSN these packets are delivered in a large area. The sensors are consequently satisfied that the attacker is their neighbor.

Wormhole Attack: In this attack, at one area in the network attacker records the packets and tunnels these to another location. We can do bits tunneling or its retransmission ought to be performed selectively.

C. Ant Colony Optimization

The ant colony optimization algorithm (ACO) is used for solving computational problems. It is a technique which comes underneath probabilistic methods this can be reduced to discovering suitable paths through graphs. This algorithm come under a member of the ant colony algorithms family, in swarm talent methods, and it constitutes some meta-heuristic optimizations [9], Mauro

Bimttari. Initially proposed by Marco Dorigo in 1992 in his Ph.D. thesis, the first algorithm was aiming to search for an gold standard route in a graph, primarily based on the behavior of ants searching for a course between their colony and a supply of food. The unique thought has been made to solve a wider classification of numerical problems, and due to the fact of this numerous troubles have appeared, depict on various elements of the conduct of ants. In ACO via states of the problem, a set of computational concurrent and asynchronous agents (a colony of ants) strikes in corresponding to partial options of the trouble to solve. Then through making use of a stochastic nearby choice coverage which is primarily based on two parameters and they pass which is known as trails and attractiveness. A solution is constructed for the trouble by way of incremented every ant by moving. The answer is evaluated by an ant and for the duration of the building section or the completion of a solution modifies the trail price on the factors which is used in its solution.

This pheromone data will direct the search for future ants is directed through that pheromone information. Furthermore, two extra mechanisms are which includes by way of an ACO which are path evaporation and optionally, daemon actions. From a number of papers in Literature survey, it has been analyzed and concluded that WSNs suffer from many protection attacks when the use of both in faraway or opposed environments. Have viewed in previous papers that the Sybil assault is one of the extreme assaults in which malicious nodes document false identities and vicinity facts such that the last nodes accept as true with that many nodes exist in their vicinity. In paper [10] they have proposed a technique for detecting Sybil attack the use of sequential analysis. This technique works in two stages. First, through observing neighboring node activities it collects the evidence than that accrued evidence are blended to provide enter to the second stage. In this stage, to determine whether the neighbor node is Sybil or benign that accumulated proof is proven the use of the sequential likelihood ratio test. By the use of the network simulator is-2, the proposed technique has been evaluated. These paper simulation consequences show that the proposed method is very powerful in detecting Sybil attacks with very low false wonderful and false terrible rates.

III. PROPOSED WORK

ALGORITHM
This work offers with the hybridization of the DBST and REDD algorithms for the statistics aggregation in Wireless sensor networks [11].
1. First, we have carried out the DBST technique, in which cluster formation takes region and this deals with the hierarchical manner in which we will get an ordered manner of our network.
2. Each cluster is having a wide variety of nodes and every node will have exclusive energies.
3. Each cluster will have one cluster head due to the fact alternatively of harvesting all energies of the node, Cluster head will talk on behalf of each cluster for the conservation of strength and it will communicate with the sink node.
4. Then those cluster heads will be having a tree shape as referred to in the REDD structure which offers with the tree facts structure.
5. In the tree data structure, there is the root node and leaf node and route will be performed from a leaf node to the root node and the root node is that cluster node which is having excessive residual power than different cluster head nodes and those incorporate facts in the shape of packets which will be transferred to the root node.

6. The route will be carried out with the use of the hyperlink weight[12].
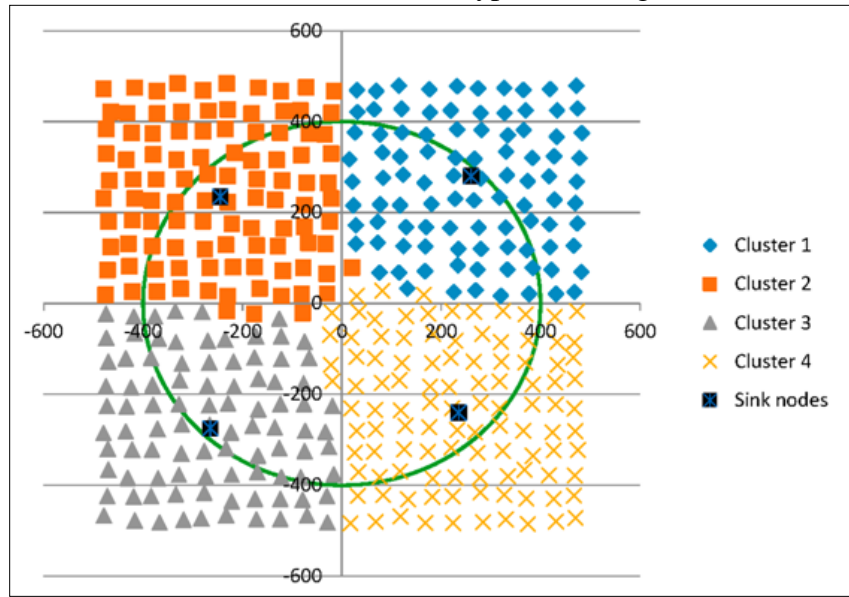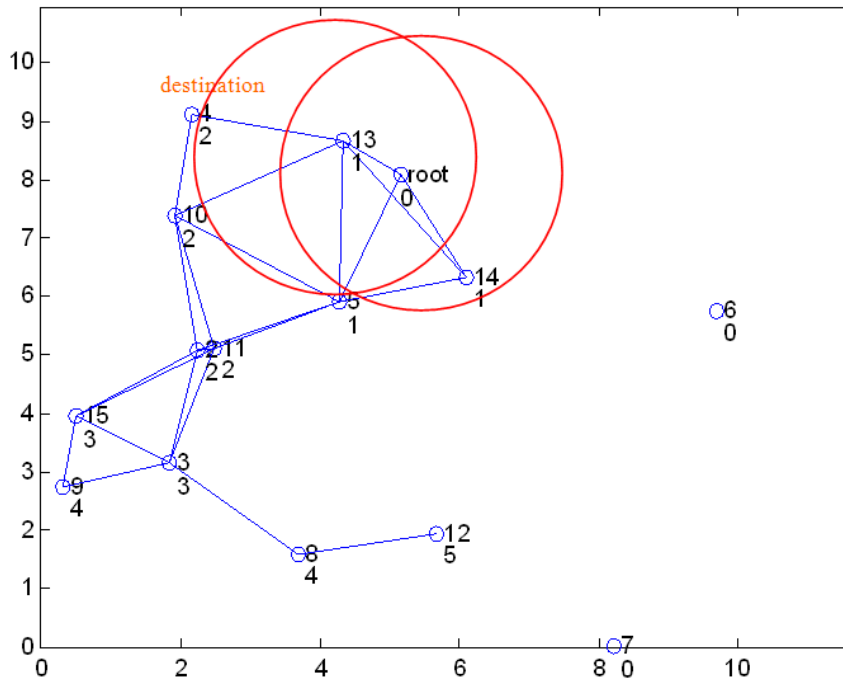

Fig. Cluster Formation

Fig. 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.
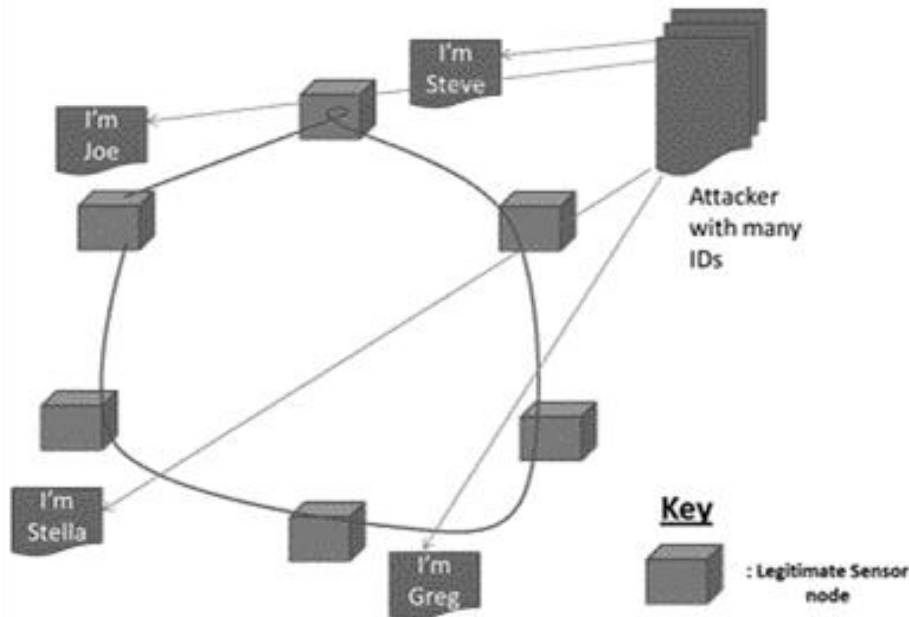
Fig. Sybil Attack

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

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.
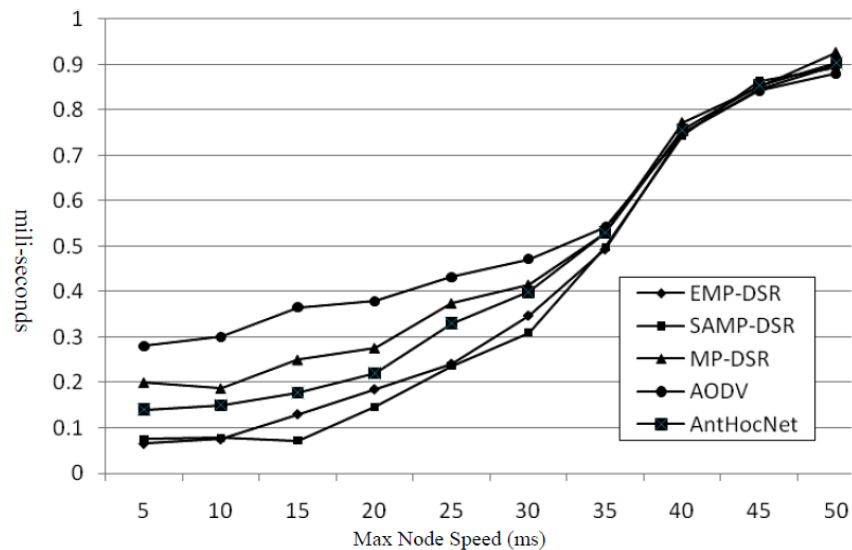

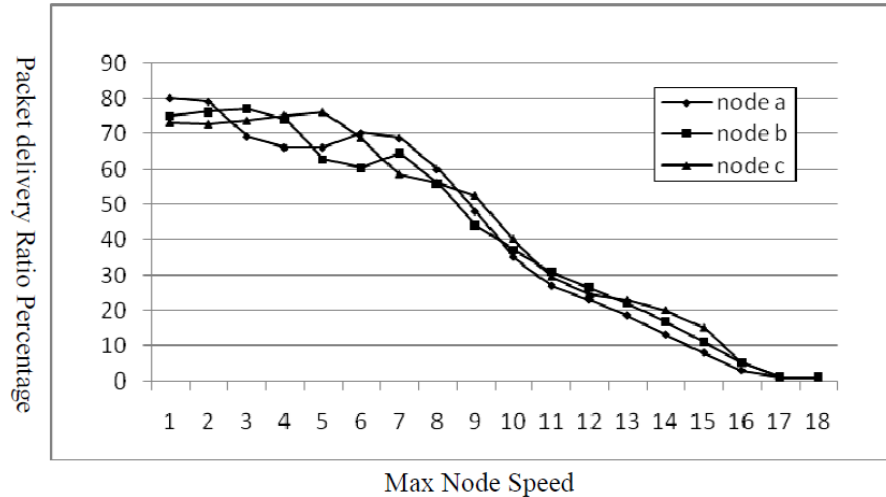Fig. ACO Results in terms of End Delay

Fig. Packet Delivery Speed & ACO Energy Consumption

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.

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. 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] Yadav, S.S.P. and Chitra, D.A., 2012. Wireless Sensor Networks-Architectures, Protocols, Simulators and Applications: a Survey. International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956), 1(04), pp.1941-1953.

[2] Guo, B., Zhang, D. and Imai, M., 2011. Toward a cooperative programming framework for context-aware applications. Personal and ubiquitous computing, 15(3), pp.221-233.

[3] Avokh, A. and Mirjalily, G., 2010, December. Dynamic balanced spanning tree (DBST) for data aggregation in wireless sensor networks. In Telecommunications (IST), 2010 5th International Symposium on (pp. 391-396). IEEE.

[4] Ramachandran, S., Gopi, A.K., Elumalai, G.V. and Chellapa, M., 2011, June. REDD: Redundancy eliminated data dissemination in cluster based mobile sinks. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on (pp. 330-335). IEEE.

[5] Gagarin, A., Hussain, S. and Yang, L.T., 2010. Distributed hierarchical search for balanced energy consumption routing spanning trees in wireless sensor networks. Journal of Parallel and Distributed Computing, 70(9), pp.975-982.

[6] Viana, A.C., Ziviani, A. and Friedman, R., 2009. Decoupling data dissemination from mobile Sink's trajectory in wireless sensor networks. IEEE Communications Letters, 13(3), pp.178-180.

[7] Patel, S.T. and Mistry, N.H., 2017, February. A review: Sybil attack detection techniques in WSN. In Electronics and Communication Systems (ICECS), 2017 4th International Conference on (pp. 184-188). IEEE.

[8] Khandare, P., Sharma, Y. and Sakhare, S.R., 2017, January. Countermeasures for selective forwarding and wormhole attack in WSN. In Inventive Systems and Control (ICISC), 2017 International Conference on (pp. 1-7). IEEE.

[9] Ali, Z. and Shahzad, W., 2011, July. Critical analysis of swarm intelligence based routing protocols in adhoc and sensor wireless networks. In Computer Networks and Information Technology (ICCNIT), 2011 International Conference on (pp. 287-292). IEEE.

[10] Levine, B.N., Shields, C. and Margolin, N.B., 2006. A survey of solutions to the sybil attack. University of Massachusetts Amherst, Amherst, MA, 7, p.224.

[11] Bashyal, S. and Venayagamoorthy, G.K., 2007, December. Collaborative routing algorithm for wireless sensor network longevity. In Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on (pp. 515-520). IEEE.

[12] Narasimhan, R. and Cox, D.C., 1998, September. A handoff algorithm for wireless systems using pattern recognition. In Personal, Indoor and Mobile Radio Communications, 1998. The Ninth IEEE International Symposium on (Vol. 1, pp. 335-339). IEEE.

[13] Upadhyayula, S. and Gupta, S.K., 2007. Spanning tree based algorithms for low latency and energy efficient data aggregation enhanced convergecast (dac) in wireless sensor networks. Ad Hoc Networks, 5(5), pp.626-648.

[14] Sohraby, K., Minoli, D. and Znati, T., 2007. Wireless sensor networks: technology, protocols, and applications. John Wiley & Sons.

[15] Avokh, A. and Mirjalily, G., 2010, December. Dynamic balanced spanning tree (DBST) for data aggregation in wireless sensor networks. In Telecommunications (IST), 2010 5th International Symposium on (pp. 391-396). IEEE.

[16] Krishnamachari, L., Estrin, D. and Wicker, S., 2002. The impact of data aggregation in wireless sensor networks. In Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on (pp. 575-578). IEEE.

[17]   Weng, C., Li, M. and Lu, X., 2008, July. Data aggregation with multiple spanning trees in wireless sensor networks. In The 2008 International Conference on Embedded Software and Systems (ICESS2008) (pp. 355-362). IEEE.

[18]   Lee, M. and Wong, V.W., 2005, August. An energy-aware spanning tree algorithm for data aggregation in wireless sensor networks. In Communications, Computers and signal Processing, 2005. PACRIM. 2005 IEEE Pacific Rim Conference on (pp. 300-303). IEEE.

[19]   Eskandari, Z., Yaghmaee, M.H. and Mohajerzadeh, A., 2008, August. Energy efficient spanning tree for data aggregation in wireless sensor networks. In Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th International Conference on (pp. 1-5). IEEE.