JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Hierarchical Clustering based Secured Routing Approach by Efficient Energy Utilization in Wireless Sensor Network

[1]Saziya Tabbassum, [2]Sanjeev Bangarh
[1]Research Scholar, [2]Associate Professor
Department of Computer Science,
OPJS University Churu, Rajasthan, India

Abstract: In wireless sensor networks (WSNs) for getting the information about the environment various sensor nodes are distributed in the region. Utilization of minimum energy and secured data transmission are the most challenging issues in WSN. In this work, we are going to use a hierarchical clustering protocol LEACH where for efficiently utilization of energy the remaining energy of each node in every round is considered so that early death of some nodes does not affect network lifetime. This paper also presents a solution for secured data transmission either inside the network or to the base station since. To deal with such kind of threats we have considered different security methods like authentication, encryption, decryption and intruder detection. Analysis and simulation result shows efficiency of proposed protocol in terms of network lifetime, throughput, number of packets to the base station, packet delivery ratio and packet drop ratio.

Index Terms: Wireless Sensor Network, Sensor, Nodes, Routing, LEACH, Energy Utilization, Secured Transmission, Security, Threats, Encryption, Decryption, Intrusion Detection.

I INTRODUCTION

With recent technological advances in micro-electro mechanical systems (MEMS), wireless communication and digital electronics have proved low-cost, low-power, multi-functional sensors with capabilities of sensing, data processing and wireless communication within short range. The intrinsic properties of individual sensor nodes pose additional challenges to the communication protocols in terms of energy consumption as well as security. The sensor nodes are spatially distributed autonomous devices using sensors to monitor the physical or environmental condition in a wireless network, which is known as Wireless Sensor Network (WSN). These sensor nodes consist of a sensing, communication, processing, power which helps to execute all the functionality of the sensor nodes. Each sensor node measures conditions in the environment surrounding them and then transform these measurements into signals which can be processed to find out characteristics of the phenomenon located in the area around these sensors. Then the signal is transferred from these sensor nodes to the base station through the gateway where the distance between the place where sensor nodes are deployed and base station depends on application of the network. Environmental monitoring, military, health care, home intelligence, industrial process control is some of the applications of WSNs (Zheng and Jamalipour, 2009; Trossen and Pavel, 2007; Koushanfar et al., 2002; Akyildiz and Vuran 2010). All of these applications have their specific functions in which sensor nodes have duties to monitor the environment, collect related data, and finally transmit those collected data to the base station (BS) where these data are used to decide the condition of the environment. In WSNs, routing strategies and security issues are great research challenges now a day where, a number of routing protocols have been proposed but the most well-known are hierarchical protocols like LEACH by (Heinzelman et al., 2000) and PEGASIS by (Lmdsey and Raghavendra, 2001). In hierarchical protocols energy consumption is reduced because of the data aggregation and reduction in transmission to the base station. In this paper we are going to use LEACH protocol as it uses cluster-based routing in order to minimize energy consumption.

With all these advancements there comes some security related threats which may compromise the privacy of data, resources, network structure, and many more. There exist various kinds of threats which can modify or drop the information that is being transmitted to the BS from sensor nodes. Security in WSNs mainly deals with data confidentiality, data integrity,

authentication, non-repudiation, data freshness and availability. Before designing an effective solution for network security, identification of attackers and their impact on clustering process should be done.

In this work we focus on one of the hierarchical routing protocols, LEACH and some of the security threats in this protocol along with solution to prevent such threats. This paper is structured as follows: section II specifies the basic security requirements in WSNs along with various related threats and some of the solutions to deal with such threats. Section III deals with LEACH protocols, their vulnerability, solution for system designing using the secure LEACH mechanism. Section IV gives the detailed analysis of our proposed work on the basis of effective energy utilization and securely routing. At last, in section V we will see the conclusion of our work.

II RELATED WORK

In WSN numerous studies have been done in recent years on LEACH protocol for clustering and routing. The overall energy efficiency, life and system scalability is contributed by cluster creation and assignment of CHs. A communication protocol has been developed by (Heinzelman et al., 2002), which can have a significant impact on the overall energy dissipation of the networks. In this work, the author describes LEACH as a clustering-based routing protocol where the whole load of the network is distributed to all nodes at a different point in time resulting in minimization of global energy usage. However, the performance in heterogeneous networks is not very well because it selects CH without considering residual energy of the nodes. To solve this problem, researchers improved LEACH and proposed many algorithms like Advanced LEACH given by (Ali et al., 2008), Centralized LEACH given by (Muruganathan et al., 2005), Energy LEACH given by (Manjeshwar and Agrawal, 2001), etc. Due to the advancement in communication, there are certain kinds of threats in the network related to data as well as resources too. So, with threats there comes solutions to prevent such threats and also overcome those attacks. Authors (Haseeb et al, 2019), presents a secret sharing-based energy aware and multi-hop routing algorithm for IoT based WSNs. In this work authors uses a secret sharing scheme to increase the performance of energy efficiency with multi-hop data security against malicious actions. They used three main aspects: firstly, based on the nodes location whole network is segmented into inner and outer zone and in each zone, on the basis of node neighborhood vicinity numerous clusters are generated. Secondly, the data transmission from cluster heads in each zone towards the sink node is secured using the proposed efficient secret sharing scheme. Lastly, the proposed solution evaluates the quantitative analysis of data links to minimize the routing disturbance.

Investigation is done by (Ferreira and et al, 2005) in the problem of adding security to cluster-based communication protocols for homogeneous WSNs, and propose a security solution for LEACH. In their solution they use building blocks from SPINS, which is a suite of highly optimized security building blocks that rely solely on symmetric- key methods. This solution is lightweight and preserves the core of LEACH protocol. Authors (Alshowkan et al., 2013), aim to provide an improved secure and more energy efficient routing protocol called Light-weight Secure LEACH (LS-LEACH). In this paper authentication algorithm is integrated to assure data integrity, authenticity and availability. Because of the added security measures the overhead of energy consumption is also taken care of, hence making this protocol an improvement over LEACH protocol. The authors (Sundararajan and Arumugam, 2015) propose an Intrusion Detection System (IDS) mechanism to detect the intruders in the network which uses LEACH protocol for its routing operation. To compute the intrusion ratio (IR) by the IDS agent, authors use the detection metrics such as number of packets transmitted or received. The computed value shows the normal or malicious activity. Whenever the sinkhole attack is captured, the IDS agent alerts the network to stop the data transmission. Thus, it can be a resilient to the vulnerable attack of sinkhole.

Whereas, authors (Kumar et al., 2017), presented a hierarchical, robust and well adapted intrusion detection system named THIDS (Threshold Hierarchical Intrusion Detection System) which is integrated into the secure hierarchical cluster based hierarchical routing protocol. Here, they have used RLEACH to be equipped with proposed IDS. In THIDS, it is required that each sensor node including monitoring nodes (MNs) has a local list called the isolation list (or blacklist). Selective forwarding and black hole attacks are detected after that member nodes relay their data messages. MNs in each cluster start monitoring their CH, by hearing exchanged messages, during a period of time. If the MN finds that there is no data message sent by its CH, this last is henceforth considered as attacker. Consequently, the MN puts CH's identifier in its blacklist, and diffuses a local alert message, containing the related ID to the neighboring nodes which may be part of adjacent clusters. On the reception of the alert message, nodes update their blacklists by adding attacker ID. A secure and low-energy zone-based routing protocol (SLeZoR) is presented by (Mehmood and et al., 2016), where the nodes of WSN are split into zones and each zone is separated into clusters. Each cluster is controlled by a CH. Initially, a secret key is used for sending the information to the zone head later the zone head sends the data to base station using the secure and energy efficient mechanism.

III METHOLOLOGIES

3.1. Basic Idea

Hierarchical routing also known as cluster-based routing methods is utilized to perform energy-efficient routing in WSNs. In a hierarchical architecture, higher-energy nodes can be used to process and send the information, while low-energy nodes can be used to perform the sensing in the proximity of the target. The creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency. Hierarchical routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order to decrease the number of transmitted messages to the BS.

Authors (Tabbassum and Bangarh, 2020) used a genetic algorithm on cluster-based approach on one of the hierarchical routing algorithm LEACH where, randomized rotation of local cluster base stations is used to evenly distribute load among the sensor nodes. In this work we are going to incorporate a clustering protocol LEACH, review some of the attacks on this protocol and method to resolve such threats. With all methods of deployment, environment monitoring and data collection various levels of security threats can cause a number of damages to the network resources as well as data resources. In clustering protocols CHs communicate directly or indirectly with the base station which are particularly attractive for compromise. After a certain number of

these nodes are compromised the whole network, its collected information and communication is compromised. Due to vigorous research going on in WSNs, it is found out that like many protocols for WSNs LEACH is vulnerable to various security attacks including jamming, spoofing, replay. As we know that LEACH is a cluster-based protocol, it relies on their CHs for routing and most damaging part is attacks involving CHs. If an intruder manages to become a CH, it can stage attacks such as sinkhole and selective forwarding, thus disrupting the network. The intruder may also leave the routing alone, and try to inject bogus sensor data into the network, one way or another. In WSNs attacks may come from outsiders or insiders. If a network is cryptographically protected, outsiders do not have any credentials like keys or certificate to show that they are a member of the network, but insiders do have those credentials. Insiders may have been compromised or have stolen their credentials from some legitimate nodes in the network, therefore it may not always be trustworthy. One assumption we have to make that the base stations are trusted. In this work we are going to propose a secure solution against node compromise and various attacks in hierarchical clustering protocol.

3.2. Low Energy Adaptive Clustering Hierarchy (LEACH)

LEACH is a clustering-based protocol in which randomized rotation of local cluster base station used to evenly distribute load among the sensor nodes in the WSNs. It uses localized coordination to enable scalability and robustness for dynamic networks and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station. LEACH is self-organizing in which all the sensor nodes in the network are deployed on the basis of application requirement. The operations of LEACH are divided into a number of rounds and each round consists of two phases: set-up phase, in which clustering is done and the steady state phase, in which data is being sent to the base station from all the sensors. Initially, when the clusters are formed in the set-up phase all sensor nodes decide to become a cluster head (CH) or not in the current round. This decision is made by node *n*, choosing a random number between 0 and 1. If the number is less than threshold value *T(n)*, then it becomes a cluster head (CH) for the current round where *T(n)* is given by

$$T(n) = \begin{cases} \frac{P}{1-P*(r \bmod \frac{1}{P})}, & if\ n \in G \\ 0, & otherwise \end{cases} \quad (1)$$

Where, *P* is the desired percentage of cluster head, *r* is the current round and *G* is the set of nodes that have not been cluster head in the last $\frac{1}{P}$ round.

Once the CHs are elected then the remaining nodes join the CH to form clusters. The nodes in each cluster then transmit data to the CH of that cluster in the allocated time slot. Now CH has lots of similar types of data collected from many nodes in the cluster then, it performs signal processing function to compress the data into a single signal. This signal is then sent to the base station which is far away and requires a high energy transmission. Randomized rotation being as a cluster head increases the lifetime of the network. Nodes die randomly and dynamic clustering enhance network lifetime. It allows member nodes to remain in sleeping mode except for specific time duration.

3.3. Energy Consumption Model

Sensing, communication and data processing are three main operations on which the energy consumption always depends. During sensing and data processing operation the energy consumption basically depends upon the type of sensors used in the application. Whereas, in this work the energy consumption during communication between sensors is considered. The radio model discussed by (Heinzelman et al., 2000) is incorporated in the proposed model while transmitting the data for energy consumption by sensor nodes. Here, a threshold value is defined and if distance is less than that threshold value then a free space (fs) model is used otherwise multi-path (mp) model is used.

The energy consumed by the sensor node to transmit a k-bit data over a distance *d* is given as follows:

$$E_{Tx}(k,d) = \begin{cases} \left(E_{elec} + \varepsilon_{fs} \times d^2\right) \times k, & d < d_0 \\ \left(E_{elec} + \varepsilon_{mp} \times d^4\right) \times k, & d \geq d_0 \end{cases} \quad (2)$$

Where, E_{elec} , ε_{fs} and ε_{mp} be the energy required by the electronics circuit and by the amplifier in free space and multipath respectively.

The energy required by the radio to receive a k-bit message is given by

$$E_{Rx}(k, d) = E_{elec} \times k \quad (3)$$

Various factors like digital encoding, modulation, filtering, and spreading of signal affects the energy consumed in generation of k-bit messages which is given by E_{elec}. The amplifier energy d_0 depends on the distance between the transmitter and the receiver and also on acceptable bit error is given by

$$d_0 = \frac{\varepsilon_{fs}\, d^2}{\varepsilon_{mp} d^4} \quad (4)$$

3.4. Algorithm Description

The implementation of our proposed approach is divided into four phases: cluster set-up phase, steady state phase, encryption & decryption phase and lastly intrusion detection phase. In this work, before the first phase begins, we assume a wireless sensor

network model in which sensor nodes are randomly deployed in the region with base station at the center. All sensor nodes and base station are stationary after deployment and assigned unique id to each sensor nodes. All sensor nodes are having similar functionalities and at the time of deployment they have same initial energy depending on the batteries they are equipped but base station is not limited by power source. Each node knows its own location by using efficient localization techniques or GPS like device equipped with them. The location information of base station is known by all sensor nodes. All communications are over a wireless link which is established between two nodes only if they are within communication range of each other. The sensor nodes sense data and send it to the base station located at the center of the region.

3.4.1. Cluster Set-Up Phase

In this phase, the network is divided into clusters very similar like LEACH protocol discussed in (Heinzelman et al, 2002). The whole operation is divided into number of rounds. At first the network is partitioned into clusters for that there is competition between all sensor nodes to become CH, i.e., all sensor nodes want to become CH. So, to solve this problem a threshold value *T(n)* is used from equation (1) to elect CH. Once CHs are elected for the current round, they broadcast advertisement message using CSMA-MAC protocol. Non-CH nodes receive this broadcast message and then they decide to which CH they want to join. Based on the communication range between CH and non-CH nodes they join the CH forming clusters. Once this cluster is formed then CH got the information of its cluster members, the CH broadcast TDMA schedule back to its member nodes informing them when it can transmit data.

Our first goal of this work is to efficiently utilizing energy of the network which can be achieved by efficiently utilizing energy cluster wise for that some of the parameters optimizing energy of clusters are as follows:

- *AVERAGE CLUSTER DISTANCE:*

There are some sensor nodes in a cluster which are forced to join the CH which are far from them as compared to other nodes. These sensor nodes consume extra energy for transmitting data to CH resulting faster death of the nodes. To solve this problem, we should minimize the average cluster distance. Thus, average cluster distance is given by

$$AvgDist = \sqrt{\frac{1}{m}\sum_{j=1}^{m}\{\mu_D - AvgClusDist(c_i)\}^2} \quad (5)$$

Where, m is the number of CH.

$$\text{and } \mu_D = \frac{1}{m}\sum_{j=1}^{m} AvgClusDist(c_i) \quad (6)$$

$$AvgClusDist(c_i) = \frac{1}{n_j}\sum_{i=1}^{n}\{dist(s_i, c_j) * \alpha_{i,j}\} \quad (7)$$

Where, $\alpha_{i,j}$ gives value 1 if sensor node s_i is assigned to CH c_j otherwise, it gives value 0.
For overall energy of network to be maximized the average cluster distance should be minimized.

$$\text{Therefore, } MaxLife \propto \frac{1}{AvgDist} \quad (8)$$

- *CLUSTER HEAD LIFETIME:*

In our work, we have also considered that those CH which have lower residual energy should have lower rate of energy consumption per round as compared with CHs which have higher residual energy. Therefore, energy consumption of CH c_i with n_i number of member sensor node due to inter cluster activity in a single round is given as:

$$E_{CH}(c_i) = n_i * E_R + n_i * E_{DA} + E_T(c_i, BS) \quad (9)$$

Where, CH c_i has n_i number of sensor nodes assigned. E_R is the energy consumption due to data receiving from another sensor node. E_{DA} is the energy consumption due to data aggregation of data collected from different sensor nodes. E_T is the energy consumption due to data transmission to the base station, dist (c_i, BS) is the Euclidean distance between the CH and the BS. Let E_{res} be the residual energy of CH c_i, or remaining energy of that node. Therefore, lifetime of the CH c_i can be defined as

$$L_{CH}(i) = \frac{E_{res}(c_i)}{E_{CH}(c_i)} \quad (10)$$

For maximizing the lifetime of overall network, the lifetime of CH should be maximized. Therefore,

$$MaxLife \propto L_{CH} \quad (11)$$

Equation (8) and (11) combined imply that

$$MaxLife \propto \frac{L_{CH}}{AvgDist}$$

$$MaxLife = K * \frac{L_{CH}}{AvgDist}$$

Where, K is a proportionality constant and, in our case, we assumed K = 1.

Therefore, $MaxLife = \frac{L_{CH}}{AvgDist}$ (12)

3.4.2. Data Transmission Phase:

The data transmission phase is the steady state phase of LEACH protocol where in each round monitored data is first of all collected in the cluster by sensor nodes. Based on the TDMA schedule of each sensor node in the cluster sensed data is send from sensor node to its CH. The CH collects all those monitored data and aggregate it. Lastly, CH send the aggregated data to the BS based on the energy model given in equation (2). If the distance between two nodes is less than the threshold value d_0 then free space model is used i.e., data will be directly sent from CH to BS otherwise multipath model is used i.e., data will be sent from one CH to another CH acting as a relay node to the BS.

3.4.3. Encryption & Decryption Phase:

Wireless sensor networks are deployed in hostile environment most of the time based on the application requirement. Such networks are always prone to security threats which can tamper physical resources as well as data resources. Even there exists attackers who can get location information of sensor node, listen the communication between nodes in clusters, insert bogus data and corrupt original information, etc. to solve such problem we have to use authentication and encryption & decryption. For authenticating the sensor nodes, we have already used unique id for each of them and later advertised its location information to its neighboring node while deploying the sensor nodes in the network. Therefore, our network is authenticated.

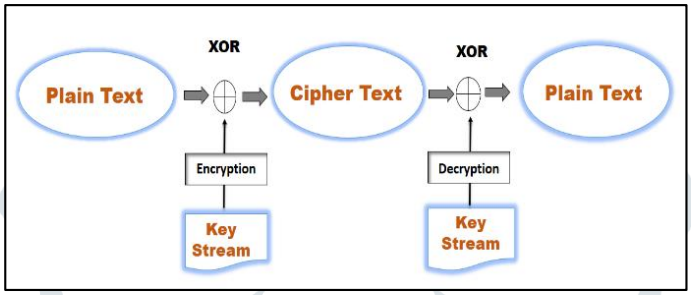

Figure 1. XOR Cipher

Whereas, there is chance that somehow attacker got information about sensor node or any other network related information and it inserts malicious node in the network. In such situation Sybil Attack or HELLO Flood attack can occur due to which whole network is lost. For such issue in our work, we have used encryption and decryption. While transmitting or receiving either within intra cluster, inter cluster or cluster to BS all the data are encrypted and decrypted by using XOR Cipher technique. XOR encryption and decryption is explained in figure (1). In XOR encryption a key is used to encrypt the message while transmitting converting it into cipher text. At the receiving end for XOR decryption key is used to decrypt the message from cipher text. For encryption and decryption, the key stream used is always same and they are pseudo random stream.

3.4.4. INTRUSION DETECTION PHASE:

In the intrusion detection phase analysis of data packets are done at the BS to identify any kind of malicious activity in the network. Suppose in the network attackers try to add malicious node at the time of deployment and that malicious node become a part of network or somehow got the information about any node in the network. In such situation the attacker can insert bogus data, control the CH, corrupt data, etc. Therefore, to find out about such malicious node we need an intrusion detection system. Here the BS monitor the packet ratio (P_i) of packets transmitted by the CH c_i to the packet received by the CH c_i.

Once, this packet ratio is calculated by the BS, it can identify that the node is malicious node or a normal node. If the value of P_i is numeric value ($P_i \geq 1$) then it denotes that the node is normal node not a malicious node, the data is not fully dropped. Otherwise, the value of P_i is infinite ($P_i = \infty$) then it denotes that the node is a sinkhole node which had dropped the data packet completely. There exist one more possibility of selective forwarding attack if the value of packet transmitted and packet received has huge difference. By using the value of packet ratio P_i we can find whether that node is a normal node or a malicious node and further we restrict that malicious node to participate in the CH selection process and routing.

IV SIMULATION & ANALYSIS

In this section, we evaluate the efficiency of proposed work in MATLAB. We performed an extensive experiment on our proposed work and it was taken on a diverse number of sensor nodes between 100 and 500 and CH ranging between 15 and 50 in an area of 300m × 300m. We compare the performance of our proposed work with different routing protocols like LEACH and DEEC. Simulation results show that the proposed work performs better than as compared to above work in terms of Energy Consumption, Average Residual Energy and Throughput. We also evaluate the proposed work in terms of Packets to BS, Delay, Packet Drop Ratio and Packet Delivery Ratio.

For simulation we have considered that the base station which is not battery limited is located at the center. All sensor nodes are assigned initial energy 2J. For the energy model, the parameters are set as follows: E_{elec}= 50nJ/bit, ε_{fs} = 10pJ/bit/m^2, ε_{mp} 0.0013pJ/bit/m^4. Energy consumption is calculated while data transmission from sensor nodes to CH within clusters and from CH to the BS either directly or via relay nodes based on equation (2) & (3). The sensor node deployment, cluster set-up, and communication within network is shown in figure 2. Here, we can see that monitored data is being transferred from sensor node from one cluster to another via relay node to the base station.

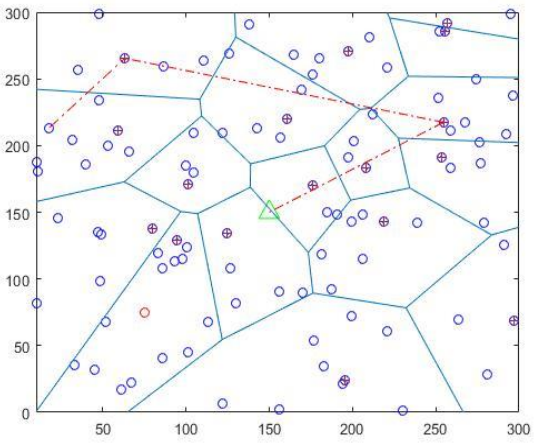

Figure 2: Sensor node deployment in an area of $300m \times 300m$ and data transmission.

Our proposed work is hierarchical clustering based secured routing approach using efficient energy utilization in wireless sensor network. Therefore, our proposed work consists of two parts: efficient energy utilization in WSN and secured routing approach in WSN. Firstly, we will consider the energy efficiency part for which we use the following metrics to evaluate the performance of our proposed work at each round and compare it with other protocols: Energy Consumption, Average Residual Energy, Throughput while routing data.

Energy Consumption: it is defined as the energy utilization of CHs during data receiving from other sensor nodes in the network, while data aggregation at the CH and while transmitting the data to the base station. Figure 3 shows the comparison between our proposed work and other routing protocols in terms of energy consumption with respect to number of nodes in the network. In figure 3 we can see that our proposed work consumes less energy when number of sensor nodes are either 50 or 100 or 250 as compared to other protocols LEACH and DEEC.

Average Residual Energy: it is defined as the amount of energy remaining after utilization in sensor node due to data transmission, data receiving, data aggregation, cluster formation in each round. Figure 4 shows the comparison between our proposed work and other routing protocol. In figure 4 it is illustrated that our proposed work has higher average residual energy as compared to LEACH protocol and DEEC protocol.

Throughput: it is defined as the actual amount of data that is successfully sent or received over communication link. Figure 5 shows the comparison between proposed work and other routing protocol. In figure 5 it is illustrated that our proposed work has better throughput as compared with LEACH and DEEC in terms of number of nodes. When throughput of our proposed work is nearly 0.9 Kbps if number of nodes is 150 whereas, at the same time LEACH and DEEC have throughput nearly 0.5 Kbps.

Furthermore, in our proposed work we have considered secured routing part. For securely transmission of data to the base station, protecting the network, and data from intruders we have incorporated authentication, encryption, decryption and intrusion detection system in our proposed work. Therefore, we use here following metrics to evaluate the performance of our proposed work in our proposed work at each round and compare it with other protocol: Packets to Base Station, Delay, Packet Delivery Ratio and Packet Drop Ratio. In figure 6 there is comparison between number of packets delivered to the base station with respect to number of rounds in our proposed work and other routing protocol. Figure 6 illustrate that our proposed work can send nearly 2000 packets to the base station in 100 rounds whereas, LEACH and DEEC can send around 1400 and 1200 packets to the base station respectively.

Whereas, figure 7 illustrates the packet delivery ratio in which it is the ratio of total number of packets delivered to the destination node and total number of packets sent from the source node. From figure 7 we can depict that the packet delivery ratio is lower of LEACH protocol than DEEC and our proposed work has the highest ratio. Figure 8 depicts the packet drop ratio which gives the number of packets dropped while transmitting data from source to destination. From our result we can see that our proposed work has minimum packet drop ratio as compared with other protocols with respect to number of rounds.

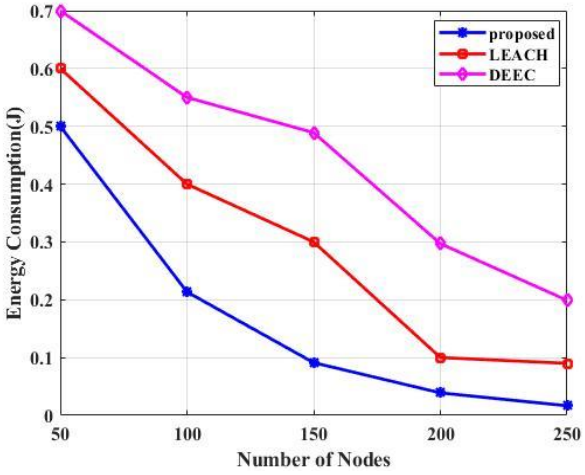

Figure 3: Energy Consumption in the network

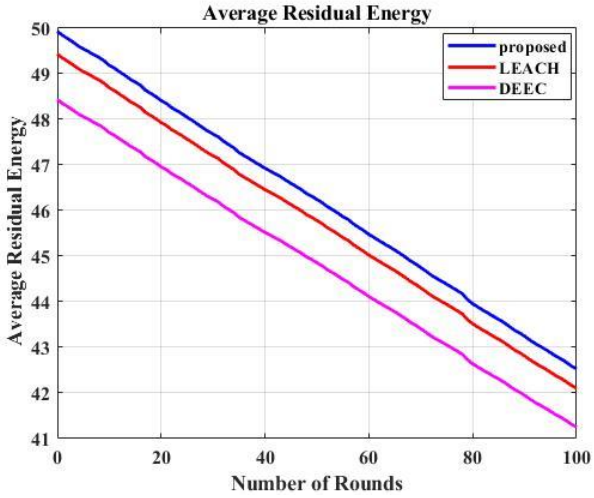

Figure 4: Average Residual Energy

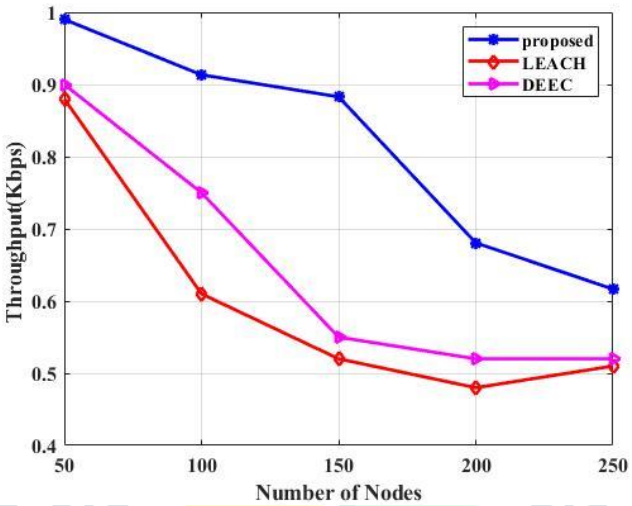

Figure 5: Throughput

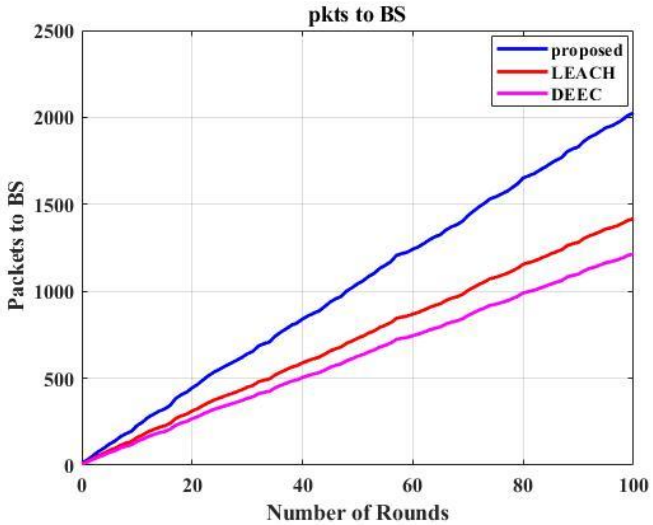

Figure 6: Packets to Base Station

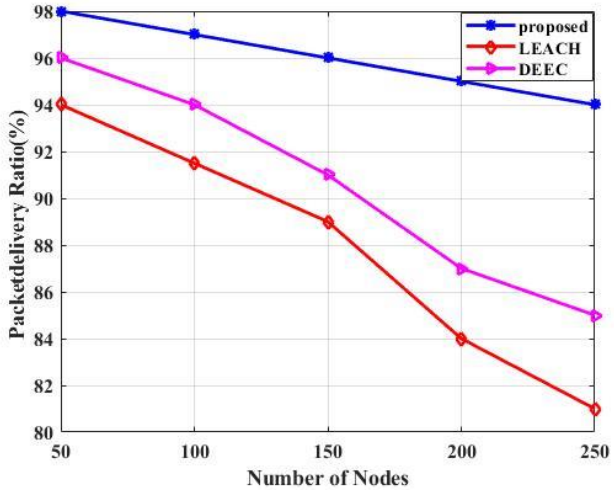

Figure 7: Packet Delivery Ratio

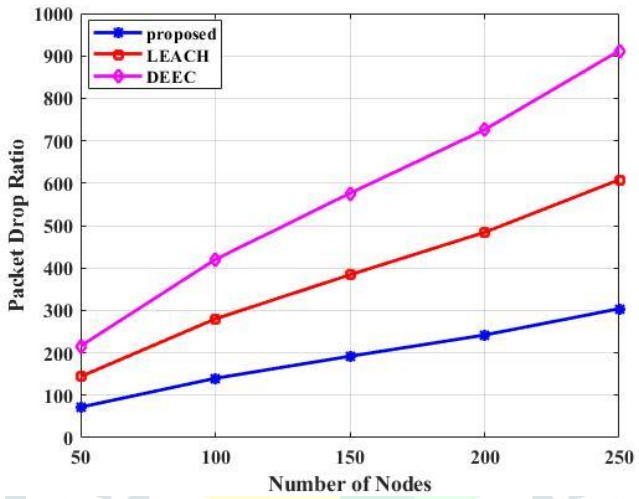

Figure 8: Packet Drop Ratio

V CONCLUSION

In this work, we propose a secured routing approach for a hierarchical clustering-based environment by utilizing energy efficiently in wireless sensor network. The main objective of our proposed work is to utilize the energy of each node efficiently so that network lifetime is maximized and it is protected from intruders resulting in secured communication. We can see that our proposed work outperforms other protocols like LEACH and DEEC in terms of energy consumption, average residual energy, throughput. For achieving it we have considered the residual energy of each and every node in a cluster. We have also considered the problem of distance between various nodes and solved it by calculating average cluster distance before the setup phase. Overall early death of node is minimized and lifetime of network is extended. Our work also outperforms LEACH and DEEC in terms of packets to base station, packet delivery ratio and packet drop ratio. It is achieved by efficient energy utilization as well as securing the network from intruders which can cause several damages as we have discussed earlier. We have authenticated our network by assigning a unique id to each and every node in the network before cluster setup phase through which we can keep track on the malicious nodes if they are found in the network. We have also considered here XOR encryption and decryption while transmitting and receiving data respectively. If somehow intruder managed to get inside the network or mimic itself as one of the nodes in network then to find and eliminate it, we have intrusion detection system as the final phase of our work. Hence, resulting in a secured approach for the network from various attacks with enhanced network lifetime.

REFERENCES

[1]. Akyildiz, I.F. and Vuran, M.C. (2010), Wireless Sensor Networks, John Wiley & Sons, Ltd.

[2]. Ali, S., Dey, T., and Biswas, R. (2008), "Advanced LEACH Routing Protocol for Wireless Microsensor Networks", Department of Computer Science & Engineering Khulna-9203, 5th International Conference on Electrical and Computer Engineering ICECE 20-22.

[3]. Alshowkan, M., Elleithy, K., AlHassan, H. (2013), "LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks", in 2013 IEEE: Proceedings of ACM 17th International Symposium on Distributed Simulation and Real Time Applications, 1550-6525.

[4]. Ferreira, A.C., Vila¸ca, M.A., Oliveira, L.B. (2005), "On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks", Springer-Verlag Berlin Heidelberg, pp. 449-458.

[5]. Haseeb, K., Islam, N., Almogren, A. (2019), "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs", IEEE, Mobile edge computing and mobile cloud computing: Addressing heterogeneity and energy issues of compute and network resources, pp. 2169-3536.
[6]. Heinzelman, W.R., Chandrakasan, A.P., and Balakrishnan, H. (2000), "Energy Efficient Communication Protocol for Wireless Micro-Sensor Networks", Proceedings of the 33rd Hawaii International Conference on System Sciences.
[7]. Heinzelman, W.R., Chandrakasan, A.P., Balakrishnan, H. (2002), "An application specific protocol architecture for wireless microsensor networks". IEEE Transactions on Wireless Communications, 1(4), 660.
[8]. Koushanfar, F., Potkonjak, M., and Sangiovanni, A.V. (2002), "Fault – tolerance techniques for ad hoc sensor networks", Proceedings of IEEE Sensors, vol. 2, pp. 1491 – 1496.
[9]. Kumar, B.A., Anuradha, N., Supriya, M. (2017), "Routing and securing the clustered step sized Wireless Sensor Networks", SSRG International Journal of Mobile Computing & Application, ISSN: 2393-9141.
[10]. Lmdsey, S. and Raghavendra, C.S. (2001), "Power-Efficient Gathering in Sensor Information Systems", Computer Systems Research Department, the Aerospace Corporation, CA 90009-2957.
[11]. Manjeshwar, A., and Agrawal, D.P. (2001), "A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks", Center for Distributed and Mobile Computing OH 45221- 0030, 0-7695-0990.
[12]. Mehmood, A., Lloret, J., and Sendra, S. (2016), "A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring", Wireless communication and mobile computing, pp. 2869-2883.
[13]. Muruganathan, S.D., Daniel, C.F.MA, Bhasin, R.I., and Fapojuwo, A.O. (2005), "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks", IEEE Radio Communications, 0163-6804.
[14]. Sundararajan, R.K., and Arumugam, U. (2015), "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks", Hindawi Publication Corporation: Journal of Sensors, pp. 203-814.
[15]. Tabbassum, S., and Bangarh, S. (2020), "Load Balanced Clustering Approach in Wireless Sensor Network using Genetic Algorithm", International Journal of Engineering Research and Applications, 2248-9622.
[16]. Trossen, D. and Pavel, D. (2007), "Sensor networks, wearable computing, and healthcare Applications", IEEE Pervasive Computing, vol. 6, no. 2, pp. 58 – 61.
[17]. Zheng, J., Jamalipour, A. (2009), Wireless sensor networks; a networking perspective, Wiley, Chichester.