Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Improved Cluster and Route Strategies in Wireless Sensor Networks: An Energy Efficient Approach with ANN-Based Intrusion Detection Systems

Saziya Tabbassum[1], Chandra Kumar Jha[2], Sneha Asopa[3]

[1]*Research Scholar, Department of Computer Science, Banasthali Vidyapith, India*
[2]*Professor & Head, Department of Computer Science, Banasthali Vidyapith, India*
[3]*Assistant Professor, Department of Computer Science, Banasthali Vidyapith, India*

Effective energy utilization and secured transmission of data is a major challenge while designing wireless sensor network. Resolving this challenge is addressed in this proposed work by applying clustering and routing approach an enhanced low energy adaptive clustering hierarchy for effective utilization of energy (LEACH). Whereas this method also integrates an intrusion detection system for finding the presence of intruders present in network. The intrusion detection system consists of a preliminary screening stage which is conducted by the base station my monitoring the behaviour of packets received from cluster head. Then a machine learning approach Artificial Neural Network (ANN) is incorporated which classifies that node is a legitimate or malicious node. Using performance metrics, the efficacy of the proposed methodology is accessed, the outcome of evaluation shows that the proposed methodology performs better when compared with some existing methodology.

Keywords: Wireless Sensor Network, Clustering, LEACH, Intrusion Detection System, Artificial Neural Network (ANN).

1. Introduction

Recently wireless sensor network (WSN) have been used in several applications of day to day life such as weather forecasting, defence, industry, logistics, healthcare, etc. for the sole purpose of gathering information related to the changes in its surrounding conditions [1]. The whole working of such monitoring is made possible in WSN with the help of heaps of sensor nodes that are scattered over the location of application. The sensor nodes are minuscule, cheap, and have small memory due to which it is compatible to be used in almost every application of WSN that can be handled far away from the monitoring location [2]. These

sensors gather information related to particular phenomena, then with the help of analog-to-digital converter it makes computation on that information and then communicate it to the base station which may be far from the region. The client can get access to the collected information by connecting with base station using the wireless broadband channels. The information received to the base station can be either raw reading that have been gathered while sensing or expected outcome. Sensor nodes are inbuilt with batteries for its operations where the power of battery is consumed at the time of information gathering along with transmission of data packet to the destination [3].

In WSN the process of gathering information and transmission of data from sensors to destination need proper planning. Numerous research is going on in this field for properly utilizing the network resources so that overall function of network should be enhanced. One such resource of WSN is the power with which sensor node operate. The remote location of network makes it almost impractical to recharge the batteries of deployed nodes, also if not utilized properly while sensing and data transmission it can get deplete soon. Hierarchical clustering is a technique in WSN that categorizes network into different layers and each layer is assigned different functions [4]. In hierarchical clustering complete network is partitioned into several clusters and every cluster has a cluster head that manages their cluster and member nodes in that cluster.

The communication of information from sensor node to the base station is carried out either directly or through intermediate nodes in the network using multi-hop. Recently various techniques are proposed by researchers which involve clustering and routing for energy efficient transmission. WSNs have open and broadcast nature which makes it exposed to security related threats. There are attackers lurking to get access of the network or resources of network and cause attacks such as wormhole, sinkhole, replication attacks, or denial-of-service (DoS) attacks [5]. These intruders if got access of network they can show itself as legitimate node of the network further controlling the network and inserting their bogus data for transmission. Such type of attack in WSN can tamper, alter, or drop the data packet which are being transmitted to the base station [6]. Therefore, there is need for resolving two challenges of WSN, utilizing energy efficiently and securing the network.

Several mechanisms have been proposed for preventing attackers to enter into the network such as establishing key and maintaining trust among sensor nodes, authentication, secure routing, privacy, resilience to node capture [7]. However, these mechanisms allow the network to prevent intruders entering into the network. Somehow these intruders get access to the node, or the shared key then it is possible for them to enter into the network and act as its part. Especially serious damage can be caused by intruders if they capture the cluster head or nodes that are nearer to the base station. Hence, there is requirement of designing a high level mechanism for dealing with such security threats. Intrusion Detection System (IDS) is one such high level mechanism which works for finding the presence of intruders by monitoring the behaviour of network along with data packet that are being communicated. Therefore, in this paper intrusion detection based on machine learning technique along with efficient energy utilization using enhanced low energy adaptive clustering hierarchy (LEACH) is presented.

Following are basic idea of the proposed work:

- In the beginning, sensor nodes are randomly placed in the required region, the details of nodes and its neighbour is gathered.
- Improved energy efficient clustering LEACH is employed on the sensor nodes so that utilization of energy is done efficiently.
- Monitoring the packets received at the base station malicious activity of sensor node and presence of intruders in the network be detected using the intrusion detection system.
- Artificial Neural Network is applied in intrusion detection system for finally finding the malicious node in the system among several doubtful activities of network.

Sections that remain in the paper are categorised into following sections: in section 2 the study related to the efficient energy utilization and security in WSN have been discussed. The proposed methodology and its framework is described in section 3. Section 4 contains the experimental result and discussion. Finally, section 5 concludes the work.

2. LITERATURE RIVEW

For efficient energy utilization and transmitting data safely to the destination several mechanisms have been presented. The following were some of the recently introduced ones that were discussed.

Sanapala and Duggirala [8] gives an enhanced LEACH approach for energy efficiency and increasing the stability of cluster heads. In this approach the choice of cluster head is made on the basis of nodes consumed energy ratio and random number generation. Here, transmission of packet is based on reputation which selects forwarder node. Nodes that has greater reputation score when compared to all nodes in a particular round are chosen a forwarder node through which data transmission takes place.

An energy efficient routing protocol was presented by Kalidoss et al [9] for solving the problems of secure data transmission by using authentication method for trust model. Here key based security mechanism is used for calculating trust scores. Later authors presents secured data transmission approach which works on clustering where, choice of cluster heads are done using metrics of QoS and trust scores are used for data transmission.

Sharma et al [10] have given a machine learning approach that works as an optimization tool for IoT nodes used in applications of smart city. When machine learning approach is employed in WSN it presents the learning about nodes along with networks from the experience from the past and predicting outcome on it. Here, authors have used 61% of supervised learning algorithms, reinforcement learning is used 27%, and unsupervised learning algorithms are used 12%. Machine learning algorithms are strong and versatile that can be employed for different WSN based IoT when designing applications such as smart cities.

Fawad et al [11] have presented Sectored-LEACH which is a solution to deal with few limitations of LEACH protocol. In this approach the area is restricted for sensing and transmitting by partitioning into different sectors using square symmetry theory resulting in reduced energy consumption. Nodes distribution is done randomly and location of node as

well as base station is used to get the knowledge of sector number related to nodes.

A defect tolerant estimator based on neuro-fuzzy optimization method is given by Rajan et al [12] in which estimator of failure detection is presented for clusters. In this approach intrusion detection is designed for situation where false positive is generated and attacks are unpredictable by using fuzzy and neural network. The behaviour of local node is categorised as trusted, untrusted, and enemy.

An energy efficient and secured routing protocol based on trust have been presented by Han et al [13] in which on the basis of direct and indirect trust value is employed. Extra energy utilization due to black hole, selective forwarding, sink hole, and hello flood attacks through which fast identification of malicious nodes are made possible. Based on the value of trust calculated the cluster head choose safest route among the multiple paths from cluster head to base station for data transmission.

Gebremariam et al [14] have presented a security mechanism against DoS attack for detecting and localizing multiple attacks. The approach consists of localization and machine learning methods as two parts. Here, gradient decent method is used for finding the attack really fast for which back propagation ANN was employed. Training and testing is done using multilayer perception.

Haseeb et al [15] have given a hybrid protocol secure and energy aware heuristic-based routing (SEHR) for finding and preventing the compromised nodes in the network. In this approach for secure data transmission graph heuristic protocol based on artificial intelligence is used. Maintenance of route is also taken care of in this method by analysing the traffic for reducing the failure of links and dis-connectivity in network.

Bala et al [16] have presented an intrusion detection system model using enhanced LEACH called as NI-LEACH in which replication attack is detected. Avoidance of miss detection in this approach is achieved by utilizing various monitoring nodes which are present in network and consumption of energy is monitored by each sensor nodes. Part of network which is contaminated is immediately isolated from other parts of the network.

Mohapatra et al [17] have designed an IDS based on man in the middle attack (MITM) in which intruders are found, it is isolated from rest of the network, and for such attacked nodes reconfiguration is done. Here, the attackers are monitored using the signature-ID templates. In this approach packet sniffer tools and network IDS (NIDS) are used for examining the traffic in network. The NIDS is mostly rule based so there is no need to store whole log file but instead update the rules based on conditions.

Arya et al [18] presented a routing approach based on deep belief network for energy efficiency in which by selecting proper path improved communication is achieved. Reinforcement learning is used for the formation of clusters along with reward is given to that node which belong to certain cluster. Cluster heads are selected in the next step which is used for data transmission efficiently with the help of deep learning approach.

The literature discussed here contains several methods and approaches to achieve energy efficient clustering and secure data transmission in WSN. These methods generate better results but still suffers from some drawbacks which reduces the accuracy of network.

The trust model used in [9] need extra load of maintaining key and id of sensor nodes since there are hundreds and thousands of sensor nodes present in the network. In [10] location of sensor nodes is required for knowing the sector number, [15] maintenance of paths is required, [16] computational overhead for monitoring node. In order to overcome such limitations, the proposed approach uses intrusion detection mechanism using ANN and enhanced LEACH.

3. PROPOSED METHODOLOGY

The use of wireless sensor networks has been increased nowadays due to its versatile and open nature. The nodes in WSNs are randomly deployed in the area without proper planning and structure of network is maintained based on the requirements of application. The sensor nodes positioned in the region of application have single aim to monitor the physical phenomena near them, gather information and finally transmit it to the base station either in one hop it base station is near or using multiple hop if base station is not within the communication range via other sensors. Therefore, successful data transmission becomes a serious matter of WSN. Also, the sensors are positioned in an environment which are prone to several security threats as attackers can get access of packets that are being transmitted. These attackers have tendency to alter the packet, insert their messages in packet, drop the packet, or they may capture a legitimate node and compromise it. Hence, WSN drastically suffers from security attacks by intruders which can damage the packet being transmitted, capture node, or destroy the links for transmission. In this paper, detection of intruders based on machine learning and energy efficient clustering for secure data transmission in WSNs is employed.

3.1 System model

In the presented method sensor nodes are positioned randomly and uniformly scattered in the required area for the purpose of gathering information from there surrounding. In this work for data transmission hierarchical framework clustering is applied in which gathered information is first collected by several heads of network at first layer then these heads transmit it to the sink in next layer. The network is homogeneous but energy depletion of nodes is different depending on the activities performed by node such as monitoring, processing, aggregation, receiving, and transmitting data. Applying security in the WSN is added in this proposed work an intrusion detection system (IDS) is designed for finding the presence of intruders in the network and deal with such node if found. The IDS integrates the machine learning approach Artificial Neural Network (ANN) for detecting the malicious node through monitoring the pattern of communication.

3.2 Enhanced energy efficient clustering

A hierarchical clustering low energy adaptive clustering hierarchy (LEACH) is employed in the proposed work for utilizing energy efficiently while gathering information and routing. In the traditional LEACH protocol an extra step is included for choosing the best cluster head in every round so that the hot spot issues of LEACH protocol are resolved. This method works on the basis of round and every round have two steps: cluster formation and routing.

Cluster Formation: after the sensor nodes are positioned in the network they are initialized. Then in the next step begins the round where in every round sensor are grouped together for forming several clusters in the network. Here, all the sensor node shows their interest to

become a cluster head. Selection of cluster head is done by using the ratio of energy consumed by a sensor node for a particular round. In this process initially an improved random number is generated by multiplying the random number with sensors initial energy to its remaining energy. Then in the next step ratio of energy consumed by a node is calculated by using its initial energy and remaining energy. A threshold function is modeled using the ratio of energy consumed along with value of nodes probability. Further a comparison is drawn between the improved random number and threshold function, if the value of improved random number is less than the threshold then that node is chosen as a cluster head for the current round. Once a cluster head is chosen then it sends the advertisement broadcast signal in the network informing that it has been selected as a cluster head. On the basis of signal received from the advertisement other sensors join the cluster head which are near to them thus forming a cluster.

Routing: when the formation of cluster is complete the whole network is partitioned into several clusters. Each cluster has a cluster head that manages the cluster as well as its member nodes. The cluster head gives a particular time slot to its cluster members for transmitting the gathered information. The cluster member node sends the gathered information to its cluster head. Then the cluster head collects all the information from its cluster member node, it aggregates the data for removing duplicated information, and then it finally transmits the information to the base station. The cluster head can send the data packet directly to base station if base station is within the communication range of cluster head otherwise, it sends the data packet through intermediary nodes.

3.3 Intrusion detection system

The presence of intruders which performs malicious activity in the network can be found with the intrusion detection system (IDS). In this work the IDS designed utilizes the artificial neural network (ANN) for detecting the intruder along with an initial behavioral examination of packets communicated by the cluster head to base station. In the examination of behavioral pattern of packets that are being transmitted to the base station a simple technique is applied which determines that the packet received at the base station is from a legitimate node or it is from a suspicious node. Further ANN is applied which classifies further that the suspicious node behaviour is due to some generous reason or due to malicious activity of node.

Pattern of Packets Being Transmitted by Cluster Head: the cluster member nodes gather information related to changes in physical phenomena of their surroundings. They transmit those collected data to their cluster head, then cluster head performs aggregation on those data after that it transmit it to the base station. A ratio of packet transmitted from a particular cluster head by packet received by a cluster head is calculated and base station analyze this packet ratio. With the result of the calculated ratio three scenario arises: if the final output is a simple numeric value like 1 then the node is considered as normal, if the output is infinite then the node is considered malicious node, and there is a big difference between packet that is transmitted and received from a node then also it is considered a malicious node. Therefore, the final output of the ratio decides whether the packet received at the base station is from a legitimate of malicious node.

Artificial Neural Network (ANN): it is a machine learning approach designed as the biological neural network or central neuron system of animal. Based on the several input parameters ANN can predict outcome with training such as unusual behaviour of network activities. ANN

is applied for identifying several denial of service (DoS) attack such as Sybil, sink hole, black hole, etc. present in network. Proper monitoring of important parameters like packet drop, received, transmitted are done for finding adversary node in the network. Once the sensor nodes are deployed in the region, and the transmission of information begins in the network then pattern of this transmitted packet is closely monitored for finding if the transmitting node is either normal or a harmful node. Then the supervised learning technique ANN is applied on it for further classifying if a nodes behaviour is suspicious then it is due to some technical fault or because of attacker present in network. In this approach for training NSL-KDD dataset is used in which features are selected in a feedforward mechanism for classifying whether a node is normal or malicious node. The node variable in the dataset are used as input in the given ANN classifier, the output of this classifier predicts if that node is malicious.

3.4 Description of proposed work

The proposed methodology of secure routing along with improved clustering energy efficiently incorporates LEACH protocol with an intrusion detection system. A few modifications have been done while choosing cluster head in a traditional LEACH approach. Here, a ratio of consumed energy is used along with an improved random number based on the nodes initial energy and its remaining energy. The ratio of consumed energy is considered to choose only those sensor nodes which have higher energy left as cluster head need extra energy for transmitting, receiving, and aggregating the data. This step resolves the issue of hotspot occurred in the traditional LEACH in which only probability aspect was considered for choosing a cluster head. A threshold function is defined using the probability and ratio of consumed energy and compared with the improved random number. If random number is less than the threshold value, then that node is selected as a cluster head thus forming a cluster. Once clusters are formed then it the transmission of data packet from sensor node to cluster head and from cluster head to the base station is carried out in the routing phase of this approach. Further in the IDS phase the base station then monitors closely the behaviour of packets received and transmitted from a cluster head and it gives outcome for that node as legitimate node or a distrusted node. Later, ANN is integrated in the IDS which takes predicts output for those distrusted node that it is either a node which has been doing such activity due to technical error or due to some attackers which have compromised the node. The ANN finally predicts based on training dataset that the node is a malicious node or a legitimate node. If a malicious node is found, then all communication from this node is disconnected. The workflow of proposed methodology is depicted in figure 1.

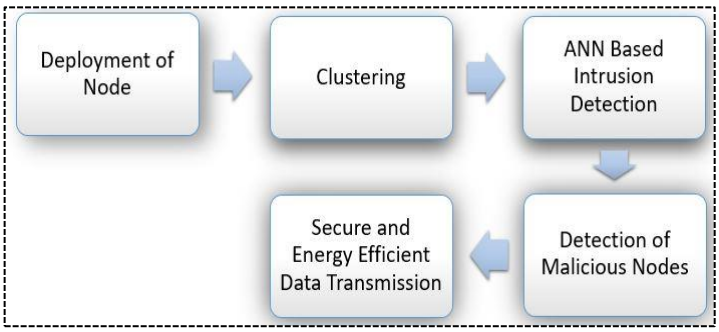

Figure 1. Workflow of Proposed Methodology

4 RESULT AND DISCUSSION

An intrusion detection system (IDS) integrated by machine learning approach artificial Neural Network (ANN) in an energy efficient environment have been presented in this work. Where the proposed methodology utilized an improved LEACH protocol for clustering and routing in the network energy efficiently. Further for IDS ANN is employed along with an initial scanning of the packets that are being transmitted from the cluster heads by base station. So, base station first depicts the behaviour of node as a trusted or distrusted node further the applied ANN scans the distrusted node using training data from dataset and predicts the outcome as normal node and malicious node. An Intel i5-3330s CPU, 64-bit operating system, x64 based processor, and 8GB memory were used to implement the proposed model using MATLAB R2020b. Also for intrusion detection system NSLKDD dataset is applied in the proposed methodology.

Around 100 number of sensor nodes are positioned in an area of 300m × 300m, and each node having initial energy of 10 joules. Figure 1 illustrates the deployment of sensor nodes in the region in which improved LEACH protocol is applied. In improved LEACH we can see from the figure that complete network is partitioned into several clusters having a cluster head for each of it. The transmission of data in routing phase of proposed work is also depicted in figure 1 in which it is clearly seen that the data from a sensor node is communicated to the base station through several cluster head as intermediary node.

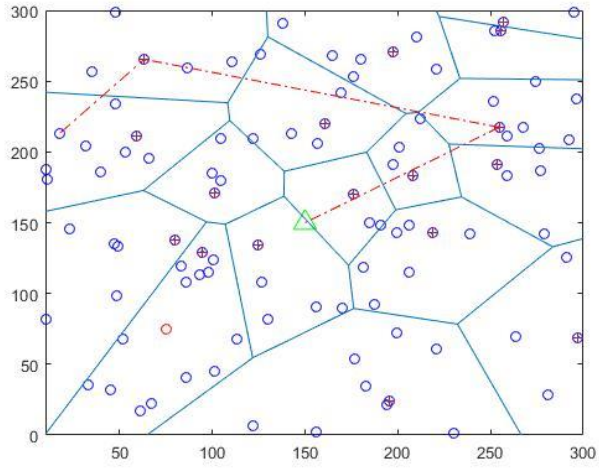

Figure 2: Deployment and Clustering in WSN

Then the proposed methodology is compared with existing protocols like LEACH and DEEC using several performance metrics of networking such as energy consumption, throughput, and packet delivery ratio. The analysis of proposed model is carried over varying number of sensor nodes. Figure 3 depicts the energy consumption in the network of proposed work compared with the existing models. The energy consumption is the amount of energy utilized by a sensor node for several tasks that it performs like monitoring, computation, transmission, receiving, etc. From figure it is clearly seen that our proposed work consumes minimum

energy as compared to the other approaches.

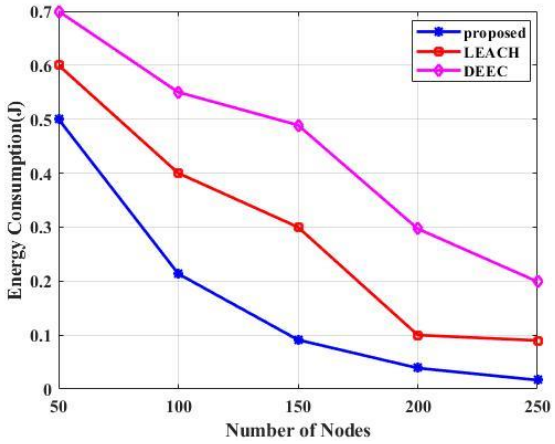

Figure 3: Comparison of Energy Consumption

Further figure 4. illustrates a graphical representation of the overall throughput of the proposed work when comparison is drawn between given and existing model. Throughput of a system is described as the amount of information which are transmitted or received on a particular communication channel. The graph in figure 4 have number of sensor nodes on the X-axis and throughput in Kbps on the Y-axis. When the number of sensor nodes are 100 then the throughput of proposed method is 0.92Kbps. Similarly, figure 5 illustrates a graphical representation of comparison of packet delivery ratio of the proposed work with existing methods. Packet delivery ratio is the total number of packets that are delivered to the base station to the total number of packets that are sent from the sensor node. The graph in figure 5 have number of sensor nodes on the X-axis and ratio of packet delivered on the Y-axis. When the number of nodes are 100 then the throughput of proposed model has 97%. Thus the proposed model performs better than the existing model.

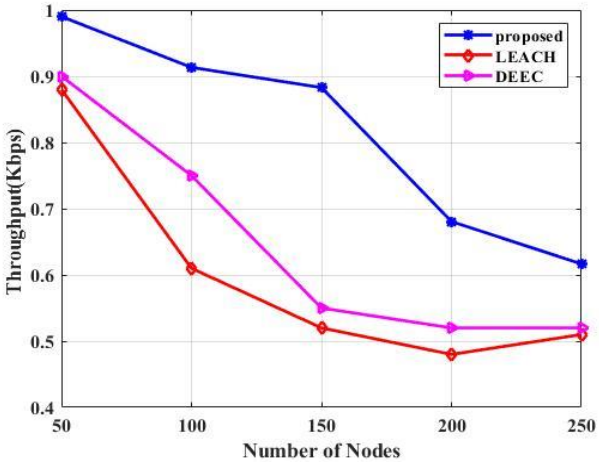

Figure 4: Comparison of Throughput

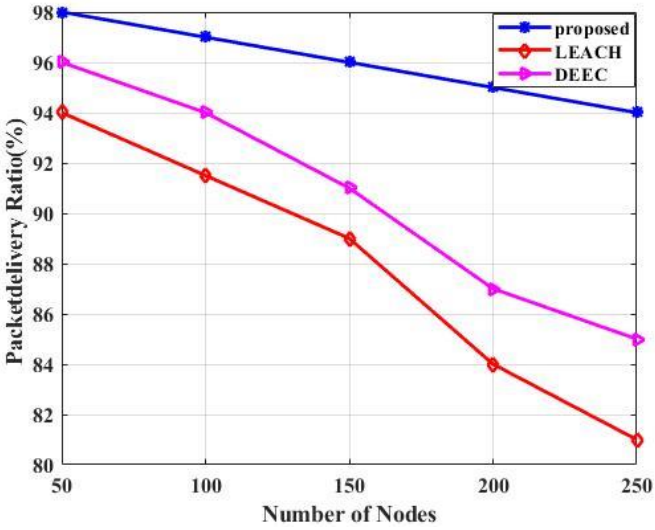

Figure 5: Comparison of Packet Delivery Ratio

Further, in the proposed methodology IDS is applied in which initially the base station monitors ratio of packets which are transmitted from the cluster head and packet received by the cluster head. The base station using this ratio depicts the behaviour of that node as trusted or distrusted. Next ANN is employed on this result of base station and finally predicts the outcome whether the distrusted node is either a normal or malicious node. the performance of proposed model is compared with existing methodologies in terms of several performance metrics like error, precision, false positive ratio (FPR). Figure 6 depicts the performance metrics error on the proposed model using ANN compared with different classifiers like SVM, KNN, and NB. The figure clearly illustrates that the proposed model has lower error value as compared with other classifiers.

Similarly, figure 7 illustrates comparison of precision of the proposed work ANN classifier towards other classifiers. The metrics precision calculates the machine learning models frequency of correctly predicting the positive class. The figure clearly illustrates that the proposed method has highest percentage of precision as compared to the other models. Similarly, figure 8 illustrates comparison of false positive ratio (FPR). In a FPR statistic evaluation the prediction is made positive but in reality it is false. From figure 8 it clearly depicts that the proposed method has minimum percentage of false positive rate when compared to other classifiers. Therefore, with all these analyses it has been proved that the proposed work of intrusion detection using ANN classifier outperforms when compared to other classifiers as depicted in performance comparison table.

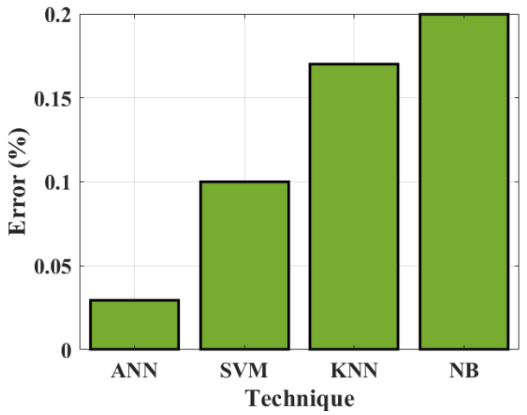

Figure 6: Comparison of Error

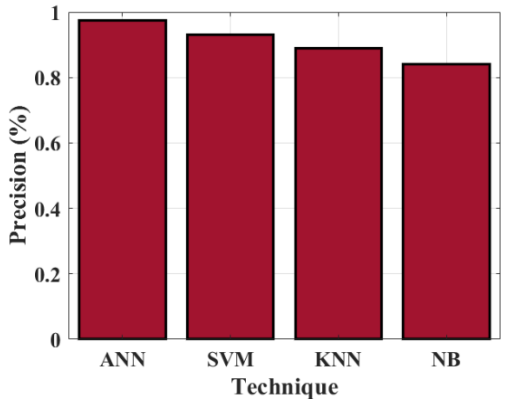

Figure 7: Comparison of Precision

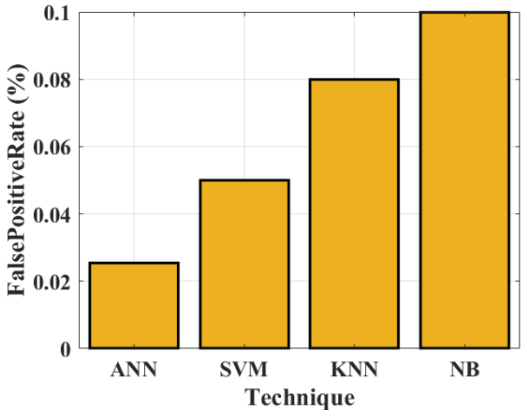

Figure 8: Comparison of False Positive Ratio

Table 1: Comparison of performance metrics of the proposed methodology

Technique / Metrics	ANN	SVM	KNN	NB
Error	0.03%	0.1%	0.17%	0.2%
Precision	97%	95%	90%	85%
FPR	0.032%	0.05%	0.09%	0.1%

5 CONCLUSION

The improvement on WSN have demonstrated several evolutions in the processing of information from the sensor node to the base station in network. The WSNs have limited resources such as energy, memory, computational capabilities, which must be utilized properly. Also, WSN suffers from several security attacks such as sinkhole, wormhole, selective forwarding, Hello flood attack. In this work a solution for effectively utilizing energy in WSN along with an intrusion detection system using ANN classifier for securing the network from intruders is presented. For effectively utilizing energy improved LEACH is employed using the ratio of energy consumed for choosing cluster head efficiently while forming clusters. The intrusion detection system first screens the network for malicious activity of node by monitoring the behaviour of packets received at base station. Then ANN classifier is used in the next step of IDS which predicts the outcome of node as either legitimate or malicious node present in network. Several performance analyses have been done on the proposed work and it shows that it has 0.03% error, 97% precision, and 0.032% false positive ratio. Therefore, the proposed methodology of effectively utilizing energy in LEACH and securing the network with an IDS based on ANN classifier is best as compared to other approach.

References

1. Aljehane, N. O., & Mansour, R. F (2022). Big data analytics with oppositional moth flame optimization based vehicular routing protocol for future smart cities. Expert Systems, 39(5), e12718.
2. Bhatti, S. A., Glover, I. A., Atkinson, R., Shan, Q., Yang, Y., and da Rocha Neto, J. S. (2010). Vulnerability of Bluetooth to impulsive noise in electricity transmission substations. IET International Conference on Wireless Sensor Network, 53– 58.
3. Maheshwari P, Sharma AK & Verma K. (2021). Energy efficient cluster-based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. Ad Hoc Networks, 110: 102317.
4. Ali, S., Fathima, S. J., Lalitha T., Ahmad F., Karthick S. U. (2022). design based location service for subterranean network using long range topology. Wireless Personal Communications, 124(2): 1815–1839
5. Culler, D. E and Hong, W. (2004). Wireless Sensor Networks. Communication of the ACM, Vol. 47(6), pp. 30-33.
6. Vinitha, A., & Rukmini, M. S. S. (2022). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5), 1857-1868.
7. Perrig, A., Stankovic, J., Wagner, D. (2004). Security in Wireless Sensor Networks.

Communications of the ACM, Page53-57.
8. Sanapala, R. K., & Duggirala, S. R. (2022). A Secure LEACH Protocol for Efficient CH Selection and Secure Data Communication in WSNs. International Journal of Computer Network and Information Security, 12(5), 82.
9. Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110, 1637-1658.
10. Sharma, H., Haque, A., and Blaabjerg, F. (2021). Machine Learning in Wireless Sensor Network for Smart Cities: A Survey. Electronics, 10, 1009-1012.
11. Fawad, M. A., Mekky, N., Suleiman, H. H., & Hikal, N. A. (2022) Sectored LEACH (S-LEACH): An enhanced LEACH for wireless sensor network. IET Wireless Sensor Systems, 12(2), 56-66.
12. Rajan, M. S., Dilip, G., Kannan, N., Namratha, M., Majji, S., Mohapatra, S. K., Karanam, S. R. (2021). Diagnosis of fault node in wireless sensor networks using adaptive neuro-fuzzy inference system. Applied Nanoscience, 1-9.
13. Hu, H., Han, Y., Yao, M., Song, X. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE Access, 10, 10585-10596.
14. Gebremariam, G. G., Panda, J., Indu, S. (2023). Localization and Detection of Multiple Attacks in Wireless Sensor Networks using Artificial Neural Network. Wireless Communication and Mobile Computing, Volume.
15. Haseeb, K., Almustafa, K. M., Jan, Z., Saba, T., & Tariq, U. (2020). Secure and energy- aware heuristic routing protocol for wireless sensor networks. IEEE Access, 8, 163962-163974.
16. Bala, P. M., Usharani, S., Abarna, V. (2021). Detect the Replication Attack on Wireless Sensor Network by Using Intrusion Detection System. Journal of Physics: Conference Series 1717.
17. Mohapatra, H., Rath, S., Panda, S., Kumar, R. (2020). Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System. International Journal of Emerging Trends in Engineering Research, 8(5), pp. 1503- 1510.
18. Arya, G., Bagwari, A., & Chauhan, D. S. (2022). Performance Analysis of Deep Learning Based Routing Protocol for an Efficient Data Transmission in 5G WSN Communication. IEEE Access. 10.1109, 3142082.