FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1043-1049 | e-ISSN: 2347-470X

Certain Investigation on Improved Cluster Protocol with Trust security for Wireless Sensor Networks

Ramesh K[1]*, Renjith P N[2], M. AntoBennet[3] and S. Balasubramani[4]

[1]Professor, Department of Computer Science, Sri Krishna College of Engineering and Technology, Coimbatore, India, rameshk@skcet.ac.in

[2]Asst. Prof., Department of Computer Science, Vellore Institute of Technology, Chennai, India, renjith.pn@vit.ac.in

[3]Professor, Department of ECE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, drmantobenet@veltech.edu.in

[4]Asst. Prof., Department of Computer Science, Hindustan Institute of Technology and Science, Chennai, India, sbala@hindustanuniv.ac.in

***Correspondence:** Ramesh K; rameshk@skcet.ac.in

ABSTRACT- Immense development of Micro Electro Mechanical Systems (MEMS) made an incredible advancement in wireless technology. The Wireless Sensor Network (WSN) has created many opportunities for the development of various applications in the fields of military, research, medical, engineering, etc. In this research article, a novel trust-based energy-aware clustering protocol is proposed. The clustering algorithm concentrates on reducing the time spent on cluster formation, controlling redundant data forwarding, and prolonging the network's lifespan. In this model, clustered nodes are classified into three levels like Cluster heads (CH), secondary CHs, and sensor nodes (SN) are used to sense the environmental changes and report to the Base Station (BS). An extension of the lifetime of a WSN is possible by the use of secure multi-hop routing with an aggregation technique to forward data from a cluster to the BS. Compared to relevant works on clustering with the routing protocol, the simulation result showed improved energy efficiency and network lifetime.

Keywords: Confidential Data Forwarding, Clustering, WSN, Trust Evaluation.

ARTICLE INFORMATION

Author(s): Ramesh K, Renjith P N, M. AntoBennet and S. Balasubramani;
Received: 28/08/2022; **Accepted**: 09/11/2022; **Published**: 20/11/2022;
e-ISSN: 2347-470X;
Paper Id: IJEER 2808-39;
Citation: 10.37391/ijeer.100447
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100447.html

crossref member
CROSSREF.ORG THE CITATION LINKING BACKBONE

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

An exponential development in wireless technologies has raised an innovative technology called Wireless Sensor Networks (WSNs) consisting of relatively inexpensive, tiny shaped sensing units that can monitor environmental changes. The WSN operates by collaboration and coordination of numerous SNs placed in a targeted geographic area. In many fields, such as military, medical, logistics, and robotics, wireless networks are used. Due to the small size of WSNs, they have several limitations such as limited battery capacity, low computational power, and short communication ranges. The lifespan of the SN is being enhanced by a variety of WSN research. Due to the fact that WSNs are dependent on the coordination of numerous SNs, routing protocol is an essential component of data transfer in WSNs. Routing protocol determines the shortest route path with minimum re-transmission to improve the lifetime of the SN. Several studies have demonstrated a direct correlation between the lifetime of the network and the lifespan of the SNs. When the network is loaded with a potentially greater number of SNs, communications networks will be challenging. [1,2,3].

We present trust-based secure data forwarding under preserved energy utilization in WSNs using clustering techniques. WSN featuring a variety of battery-efficient SNs that uses little power. Collaboration of SNs that can collect trustworthy and precise information in any hazardous environment [1]. The time frame of the network's SNs affects the WSN's lifespan. The three major components that are delivered to SN are sensors, processors, and transceivers [2]. The processor evaluates the sensed information. Network management will be tough when the network is populated with a potentially higher number of SNs [3]. Additionally, adjacent SNs or SNs at specific geographical locations sense similar information. The same data is sensed by each SN and transmitted all through the network. Thus, redundant data keeps on being replicated and forwarded through the entire network. This method increases communication overhead and depletes network lifetime [5]. The lifetime of the network is prolonged and excessive data flooding is prevented by clustering SNs. An arrangement of sensors according to distance is referred to as the clustering approach. The SNs are divided into distinct groups named clusters, in which a group member is chosen to serve as the CH [6]. Clustering is a WSN energy-saving strategy that groups the SNs based on the distance apart they are from one other and the BS [7]. In clustering, a powerful solution that works effectively for higher scalable networks like WSN. Clustering is an efficient mechanism for extending the lifespan of a network and protecting the SNs' energy resources by operating at a minimum distance. This reduces energy wastage, retransmission and communication overhead [8]. The aim of this paper is to propose conserved energy with the clustering routing protocol with trust assessment for confidential data forwarding that can improve network lifetime and reduce retransmissions within the network. This will help to minimize energy consumption by the SN for data forwarding.

The reminder of this paper is organized as follows. Interrelated studies on current systems are briefly mentioned in *Section 2*. We cover clustering design challenges in *Section 3*. The problem definition is explained in *Section 4*. The suggested Trust-based Energy-aware clustering mechanism is described in *Section 5*. *Section 6* discusses the simulation environment and performance assessment. *Section 7* concludes with the facts and importance of the clustering algorithm.

2. RELATED WORKS

In WSN, routing protocol depends on the SN location and distance between the SNs. In this section, different types of routing protocols like hierarchical-based routing protocol, data-centric routing protocol and QoS-based routing protocol used in WSN are discussed in detail.

2.1 Hierarchical-Based (HB)

SNs used in the field of interest range in scalability from a few hundreds to thousands. A huge amount of SNs are grouped into clusters in the HB routing protocol, and each cluster is controlled by the group head. The CH will be in charge of maintaining intra-group communication. The sensed information will be forwarded to the CH by the cluster's member nodes. The received data will be transmitted to the BS by the CH. Data confidentiality is maintained by the CH. The hierarchical routing protocol minimizes transmissions and redundant data forwarding. The HB routing protocol Low Energy Adaptive Clustering Hierarchy (LEACH) is an example [14,16]. Leach is an adaptive, reactive, and self-organizing HB routing protocol. LEACH operates in two distinct modes: setup phase and constant phase.

2.2 Data Centric

The sink node communicates with the SN based on the availability of data in DC routing. A CH forwards the query to a specific network region and waits for the data. Each CH sends all the necessary data. DC Routing protocol receive information from queries by using attribute-based naming. The DC Routing protocol is the foundation of the Sensor Protocol for Information via Negotiation (SPIN) routing protocol [13,16]. SPIN employs a flat architectural style. The SPIN algorithm is based on SN that are close to the BS. The nodes that are closest to each other will sense and collect the same data. An algorithm like SPIN uses all SNs as BSs. SPIN, on the other hand, uses statistics negotiation and resource-aware algorithms to address the shortcomings of traditional methods. To gather sensed data, the end-user can send the query to any node. Meta-data is the data transmitted by SNs. There is the possibility of passing meta-data across all SNs prior to transmission. The protocol sends the query to a specific network region and retrieves the information based on the query. SPIN employs data negotiation as well as a resource-adaptive algorithm. SPIN does not store the node id or location.

2.3 QoS Aware

When implementing QoS-aware routing, quality-of-service parameters such as end-to-end delay, transmission overhead distance, residual energy remaining, transmission power, bandwidth, hop counts, packet service time, and throughput are taken into account. Several QoS-based routing protocols exist, including sequential assignment route [10], geographic routing in random duty-cycled wireless multimedia sensor networks [11], SPEED: a stateless protocol for real-time communication in sensor networks [11], and RAP: a real-time communication architecture for large-scale wireless sensor networks [12]. Contracts like these calculate QoS and route traffic. Such routing protocols will have a higher computational complexity than standard routing protocols.

2.4 Research Gap

The clustering algorithm is the process for identify groups of similar data points. There are many clustering algorithms discussed above, with many different methods of creating clusters in a dataset. This article focuses on the study of how to cluster entities of IoT data into meaningful segments based on common features such as location or topology. Clustering protocols for WSN have been extensively researched in the past decade. However, there is still a lack of understanding of how these protocols work in terms of their feasibility and effectiveness. There is a lack of research on clustering protocols for wireless sensor networks (WSNs). This is due to the difficulty in designing and implementing these protocols, as well as the lack of understanding of their potential benefits. Clustering can potentially improve the performance of WSNs by reducing communication overhead and increasing the data rate. However, there is a lack of understanding of how to design and implement clustering algorithms that are effective in WSNs. As a result, there is a need for more research on clustering protocols for WSNs. In this paper, an improved clustering protocol with trust security for WSN has been presented.

3. DESIGN ISSUES OF CLUSTERING

In the field of data collection using sensors, clustering plays a vital role. Such an unsupervised learning approach saves the maximum energy of the node while transmitting valuable data to the BS [14]. There are still a few issues with cluster formation and the security of data and cluster networks [17]. The following subsections deal with some major issues of clustering.

3.1 Node Mobility

Based on the application, the type of node in the sensing area may vary. As a result, it can be difficult to handle the framework architecture and packet delivery issues [15] if the node is not steady or is moving from one location to another. So, the threshold (based on time slot) is activated when there is a migration of SNs from cluster to cluster [18,19]. CH updates the member node count and connection establishment between those nodes by which routing and handover issues are to be minimized [16].

3.2 Cluster Count and Framework

In order to sense and transmit data with high efficiency, clustering plays a critical role. Among the tasks that have to be accomplished within the shortest possible amount of time are the broadcasting of the activity structure and the number of clusters, the selection of cluster members, and the range of nodes within each group. [8,20, 21].

3.3 Scalability

Scalability is one of the major issues when it comes to clustering. The sensor network itself must be capable of handling the variation in cluster formation [6, 22, 23]. The CH also must be capable of handling variation in its member nodes due to various factors like new node deployment, in a deployed area, actual node loss due to inclement weather, *etc.* [24, 25].

4. PROBLEM DEFINITION

The clustering protocol controls the energy consumption and transmission rate of SNs [2]. This section explains the objectives of clustering protocols such as controlling the data transmission rate, inter-cluster routing, and improving quality of service.

4.1 Control Data Transmission Rate

With the integration of cluster technique into WSN, SNs are programmed to serve as a member node in the cluster. The member nodes detect geographic changes and report them to the CH [3]. The CH checks for the availability of adjacent CHs via inter-CH communication, aggregates the sensed packets received from the member nodes, and forwards the cumulative packet to the BS. [5, 26] This method prolongs the life of a network and prevents SNs from running out of battery.

4.2 Inter Cluster Routing

There is a term referred to as inter-cluster routing that refers to communication between SNs and CHs. To control SN transmission, the CHs employ a method known as Time Division Multiple Access (TDMA). SNs within a cluster are assigned a specific time to send the sensed data to the CH, based on the time they are assigned. In addition to increasing network efficiency, this practice also reduces the likelihood of bottlenecks in the network. [6, 27].

4.3 Improve Quality of Service

In the context of network QoS, a process-based quality parameter ensures that the network has a long life, with minimal packet loss, less delay, high accuracy, and fast sensing capabilities [30]. QoS is improved with the utilization of clustering in WSN where retransmission and packet loss will be reduced considerably [5]. This increases the lifespan of the network. Clustering involves creating sub-networks within the main network. Each such sub-network is monitored with the help of the CH [31]. The CH controls the traffic within the network. As a result, WSNs can reduce network traffic and channel contention.

5. METHODOLOGY

The Trust-based Energy-Aware Clustering Routing Protocol (TEC primary) was designed with the goal of maximizing energy efficiency in WSNs by making efficient use of limited energy resources on nodes, and to improve clustering and routing techniques as well. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol uses a random selection of nodes, and as a result, the nodes' well-ordered functioning is able to get around many of the problems that the stochastic threshold approach runs into. By altering the CH and cluster node selection procedures in the LEACH protocol, the TEC framework implements the process of selecting nodes for the cluster. A clustering algorithm called LEACH [15] concentrates on the distributed energy utilization in WSN that use clusters. Choosing an SN with a high battery energy as the CH, which combines sensed data and transfers it to the BS, is the fundamental tenet of LEACH. LEACH establishes grouping of nodes and data forwarding in two stages: format and sturdy state. The format phase is concerned with the formation of a cluster. In *equation (1)* CH, the threshold T(n) is selected during setup. A chosen SN becomes the cluster's CH if its battery energy exceeds or equals T(n); otherwise, it continues to function as an ordinary SN. The sturdy state phase is concerned with data forwarding in a cluster. During this phase, each SN forwards its sensed data to the CH through unicast transmission and relay nodes (RNs). the setup phase. LEACH is based on the idea that a CH should be selected from the most energy-efficient nodes in each cluster, *i.e.*, those with more available battery energy than other nodes in the same cluster. The steady state phase is concerned with the operation of the cluster, which is achieved when all nodes are connected to a single CH. Once the cluster has been established, data can be forwarded from any node to the BS.

$$T(i) = \begin{cases} \frac{p}{1-p^*\left(rmod\frac{1}{p}\right)}, i \in G \\ 0 \qquad ,otherwise \end{cases} \qquad (1)$$

Where
P – Ration of a CH
G – Set of nodes that were not a CH 1/p round
r – Current round
T(i) – Threshold value

After SNs are deployed in a specific region, the SNs calculate the trust value (TEV) of their neighbour nodes and store the information in the trusted node and untrusted node tables in the BS's trust database. WSN has distinct characteristics that set it apart from other networks. Wireless sensor networks are self-starting, ad hoc networks in which SNs collaborate to send sensed data to a BS. The battery life of a node is a critical resource. A wireless SN's life is determined by its battery backup. The power consumption of the SN is also well known. Each SN is programmed to work for months or years due to the preinstalled battery capability. Complex algorithms and frequent long-distance communications will deplete the battery and shorten the node's lifespan. Trust-based routing employs a lightweight algorithm that consumes fewer battery resources while improving network performance.

5.1 Improve Quality of Service

Upon establishing communication with a neighboring SN, the node broadcasts a 'hello message'. In generic trust evaluation, these 'hello messages' are appended to the self-addressed trust packets in order to establish trust. It is common for a neighbor node to send an acknowledgement and trust packet when it receives a hello message and a trust packet from a neighbor. In a generic trust evaluation, the number of packets that are sent and received is recorded. The equation (2) is used to calculate a generic trust value that can be used in various situations. A network can be monitored that can be used to evaluate trustworthiness of other nodes in order to build reliable networks. The protocol would look at the number of packets received, the number of packets sent, and the amount of time between sending hello messages and receiving hello messages.

It would then use these metrics to create a trust value based on a different formula that the formula above.

$$\text{ß}\mathbf{T}_{EV_{i\rightarrow j}} = \int_0^t \frac{\sum_{T=1}^{n} N_{RP_{j\rightarrow i}}^{(A+T_{1\rightarrow n})}}{\sum_{T=1}^{n} N_{RQ_{i\rightarrow j}}^{(H+T_{1\rightarrow n})} + \sum_{T=1}^{n} N_{RE_{j-i}}} \qquad (2)$$

5.2 Evaluation of Node's Trust

The SNs trust is calculated using the *equation (3).*

$$T_{EV}(x) = a_0 + \sum_{n=1}^{\infty} (a_n\, \text{ßT}_{\text{EV}} + b_n\, T_{mV}) + PfaT_{EV_x})(3)$$

Where:

$$mT_{EV} = \sum(\text{ßT}_{\text{EV}} + T_{mV}) \qquad (4)$$

$$T_{mv} = \frac{1}{6}\sum(p_{wi} * T_{PD_\alpha} + p_{wj} * T_{RTT_t} + p_{wk} * \text{T}_{\text{TP}} + p_{wl} * T_{ED} + pw_{wm} * BP_{rem} + p_{wn} * T_{DT_t}) \qquad (5)$$

5.3 In-direct Trust Evaluation

'In-direct trust' refers to recommendations from neighbors about a particular SN. The indirect trust value varies from application to application. For mission-critical applications like health monitoring systems, indirect trust is kept to a minimum. The indirect trust is calculated using the *equation (6).*

$$aT_{EV_x} = \frac{1}{n}\sum(mT_{EV\,(a)} + mT_{EV\,(b)} + \ldots + mT_{EV\,(n)}) \quad (6)$$

5.4 Trust Evaluation

The trust evaluation value is calculated after the SN has been initialised. The trust evaluation threshold TH is set to 0.60. When a node's trust evaluation values fall below 0.60, it is labelled as untrusted and disconnected from the network. In addition to being sent to the neighbour node, the data is also saved in the BS database as well. If the SN's TH is higher than '0.74', the BS database will be updated and the node will be assigned to a highly reputable SN table. In the event that a node's TH exceeds 0.60, then it is added to the average trusted SN table and saved into the database. This is because it has a TH greater than 0.60. This database is regularly updated by the BS and the information is sent out to all SNs on a regular basis. The trust evaluation is performed on a regular basis and updates the information between the SNs and the BS. Every transaction is scrutinised. In the event that the neighbour node exhibits malicious behaviour, an immediate alert is sent to the neighbour node. A trust assessment is carried out. The overall trust evaluation method is represented by *eq.7.*

$$T_{EV}(x) = a_0 + \sum_{n=1}^{\infty} (a_n\, \text{ßT}_{\text{EV}} + b_n\, T_{mV}) + PfaT_{EV_x}) \quad (7)$$

ßT_{EV} -generic trust evaluation
T_{mV} -Main trust evaluation
aT_{EV_x} - In-direct trust evaluation
a_n, b_n - Metric weighting varies based on application
Pf - Primacy factor

Table 1: Representation of trust database

Node_id	BPrem	TEV	x	y
N_1	92%	0.75	14.623	38.78
N_2	96%	0.62	32.58	71.41
…				

The BS collects a concise view of SN position, current battery level, and node deployed in the specific geographical area of interest A BS divides an entire network area into equal grids. CHs are chosen in each grid based on the SN's battery power and trust value. The BS informs the CH about the sub-nodes that will be attached to it. When the information reaches the CH, the CH instructs the SNs to report to it. CHs are BS-selected nodes with high trust values and battery power. The BS uses a MySQL query to fetch several nodes and their locations within the specific grid. The trusted table in the trust database is used to determine the coordinates and node id.

5.5 Algorithm

Input: Trust Database
Output: CH and backup cluster selection

```
1: Locate the cluster using the coordinates ($x_1$, $y_1$) and ($x_2$, $y_2$)
2: Sort the Trusted table based on location of SNs in cluster
3: Sort Nodes with $BP_{rem}$ and Trust value
4: Count (Number of nodes = Max $BP_{rem}$ && $T_{EV}$ > 0.60)
5: If number of nodes >1{
6: Find the distance between midpoint nodes ($x_m$,$y_m$) and node coordinate
7: D (node, midpoint) =$\sqrt{(x_B - x_m)^2 - (y_B - y_m)^2}$
8: Compare distance of nodes and find shortest distance node
9: Ni = CH when [ $BP_{rem}$ > member nodes & $T_{EV}$ >0.6]
10: Sort Second highest $BP_{rem}$ of the Cluster
11: Make $N_j$ as Secondary CH
12: Advertise Member nodes of the cluster with CH and SCH node ids & location.
}
```

6. PERFORMANCE EVALUATION

A Trusted Energy-aware Clustering Protocol (TEC) is embedded in the SNs and deployed in a 100 x 100 m2 area. CBR is a source traffic generator that uses the common bit rate as a source of traffic. The experiment is conducted using Network Simulator 2.35. Simulations are run with ten different topologies, and the aggregate results are presented for discussion. This section discusses further detail about the number of active nodes, total packets received by the BS, packet transmission ratio, average end-to-end delay, and the average lifetime of the WSN.

6.1 SN Lifetime

The total number of SNs alive at each time interval is calculated in this performance evaluation. The experiment is done on a sensor network with 100 SNs and each is supplied with 2 joules of initial energy.

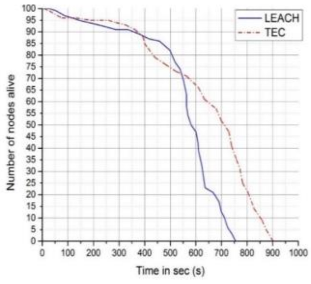

Figure 1: Represents Lifetime of the sensor nodes

The BS is programmed to query continuously in order to obtain data from each coordinate. According to the results, LEACH outperforms TEC in the initial stage and the number of nodes drops faster. The probabilistic method is used to form clusters. The SN's lifetime is much shorter than TEC's. *Figure 1* depicts several nodes that are alive at a given time interval in seconds. After 600 seconds of simulation, the performance of TEC and LEACH is nearly equal. By using the LEACH protocol, CHs forward packets directly to the BS as part of the LEACH communications protocol. Communication directly from the CH to the BS consumes more battery resources, as a result, battery life may be significantly reduced as a result. Each time the battery is used for transmission, 80mW is used. Inverse square law dictates that when the transmission distance increases, the amount of power used multiplies multiple times. TEC utilizes CH multi-hop communication which saves a lot of energy when compared with direct communication with the CH.

6.2 Cumulative Packets

This simulation finds the total amount of packets that reached the BS from the network at the given time interval. The measurement time, aggregation time, forwarding time, packet loss time, and received time at the BS comprise the time. Protocols ZRP, LEACH, and TEC are examined with continuous transmission of packets for up to 1000 seconds. The results showed that the TEC protocol transferred 30% more data to the BS than the LEACH protocol. In *figure (2)*, the total number of packets received by the BS at a given time interval is shown in seconds.

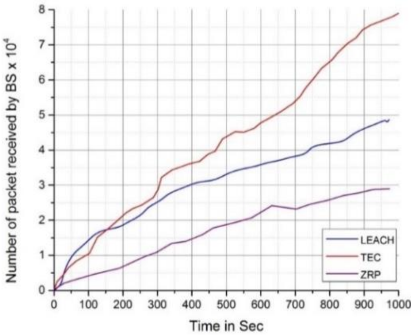

Figure 2: Represents cumulative packet transmission

This is accomplished through energy and power savings in CH selection and forwarding. Data are sensed by the cluster's member SNs, and the messages are transmitted to the cluster's head node. The CH compares the acknowledged packet data to data received from the cluster's other member nodes. Upon receiving packets from the CH, they are combined into a single packet, which is then routed to the BS for further processing. The LEACH protocol necessitates calculating some rounds and the battery power of each SN in a given round before selecting the highest-powered node as the CH. The network's performance will be low during this setup phase when compared to steady-state. A BS controls the TEC protocol to determine the cluster position, distance of each SN, and CH distances between each SN. The effective sorting method is followed to create clusters with CH, secondary CH, and cluster members.

6.3 Average Packet Delivery Ratio

The packet delivery ratio can be defined as the percentage of packets that are successfully delivered into the destination node from the source node. With the intensification in node density, total amount of packets sent and received is decreased due to transmission delay, handoff, and packet loss. When the SN count is increased, the total number of clusters also increases, and packet transmission will be affected due to the delay in transmission. *Figure 3* represents the packet delivery ratio with increasing number of SNs. Based on a comparison of the simulation results between the TEC protocol and the LEACH protocol, it can be concluded that the TEC protocol shows an improved PDR of 16% than the LEACH protocol.

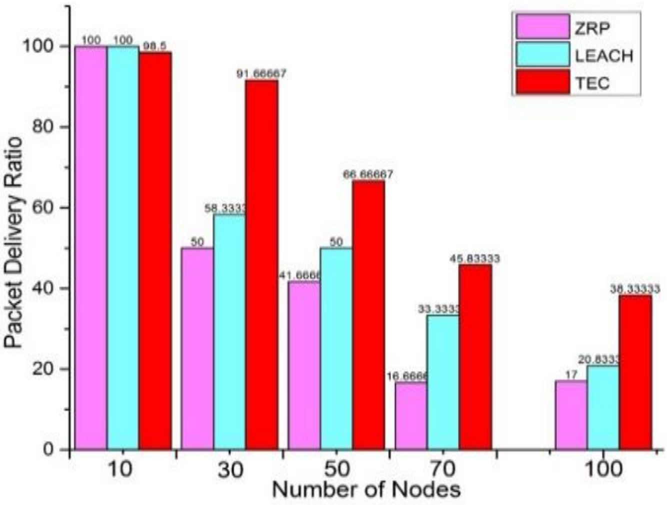

Figure 3: Represents Packet Delivery Ratio of the network

6.4 End-to-End Delay

Using the time, it takes packets to travel from the source to the BS, the average end-to-end delay is calculated. In addition to propagation and queueing, there are also retransmission delays. The simulation scenarios are altered by 10, 30, 50, 70, and 100 nodes, and results are produced. This simulation aims at comparing the end-to-end delay of the LEACH, ZRP, and TEC protocols in terms of their average end-to-end delay. The time it takes packets to travel from the source to the BS is used to calculate the average end-to-end delay. This includes propagation, queue, and retransmission delays, among other things. The simulation scenarios are altered by 10, 30, 50, 70, and 100 nodes, and results are produced. The average of the results from repeated simulations with increasing node density is used. *Figure 4* depicts the average retransmission rate as node density varies. In simulations, the ZRP routing protocol performs best with a small number of SNs; however, the packet delay increases as the number of sensors increases. Within the group of sensor nodes, ZRP uses a table-driven approach to maintain the route information of the cluster members. As the number of SNs increases, the size of the cluster also expands, which makes it more difficult to communicate between clusters as the number of SNs increases. Depending on the battery power of the SNs, the information may change dynamically depending on how much battery power they have.

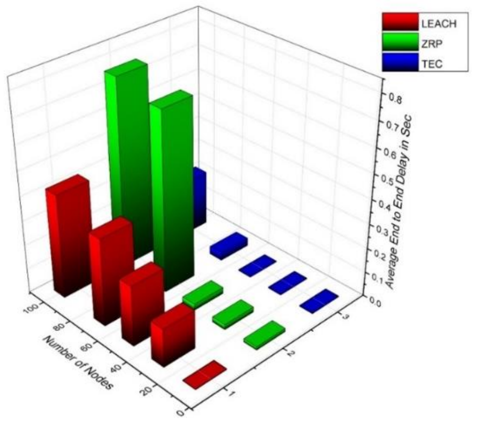

Figure 4: Represents Packet Transmission Rate

TEC handles the reactive type table-driven approach which utilizes BS support to maintain the entire cluster information. Hence CH reselection, filtering malicious nodes and computing distance will be done by the BS. The CHs are appointed based on distance, battery power, and trust value. This method will ensure limited packet loss and reduce delay in electing a CH.

7. CONCLUSION

The development of WSN applications provides a wide range of possibilities in a variety of fields. In WSN, the major problem is insufficient battery capacity and excessive energy usage. In this proposal, an improved Cluster Protocol with Trust security for Wireless Sensor Networks has been proposed. The SNs are grouped based on distance, battery power, and trust values. In designing any protocol for WSN, feasibility and extended network lifetime are the major issues to be considered. Due to the architecture of WSNs, it is known that a protocol with a high computational complexity will require a higher battery resource from the SN to perform the computation and to control computation complexity and communication overhead. The computations are done in the BS, and only queries are processed at the SNs. SN's parameters like node id, location, trust values and battery power remaining are updated in the trust database of the BS by the CH. The trust database will have the entire network status. The BS utilizes the trust database to examine the node performance and selecting a node as CH. When major computation like node selection, node member recommendation, aggregation query processing is performed in the BS, and SNs are given minimum strain in computation. Thus, with the help of computation performed in the base situation, a large amount of energy is conserved in the SNs. The study indicates that the more energy conserved for transmitting or receiving data per smart sensor, the longer the network can last, and thus, the longer the lifetime of the network as per simulation result, TEC outperforms LEACH and ZRP protocols in various performance metrics.

REFERENCES

[1] G. C. Jagan and P. Jesu Jayarin, "Wireless Sensor Network CH Selection and Short Routing Using Energy Efficient ElectroStatic Discharge Algorithm", Journal of Engineering, Volume 2022, Article ID 8429285, 10 pages, 2022.

[2] M. A. Alanezi, H. R. Bouchekara, M. Javaid, and M. S. Shahriar, “A fully connected cluster with minimal transmission power for IoT using electrostatic discharge algorithm,” Applied Computational Electromagnetics Society Journal, vol. 36, no. 3, 2021.

[3] Renjith P N, “Towards Secure Data Forwarding With Anfis And Trust Evaluation In Wireless Sensor Networks”, Wireless Personal Communication, Springer, 2020.

[4] A. Jari and A. Avokh, “PSO-based sink placement and load-balanced anycast routing in multi-sink WSNs considering compressive sensing theory,” Engineering Applications of Artificial Intelligence, vol. 100, Article ID 104164, 2021.

[5] K. Karunanithy and B. Velusamy, “Cluster-tree based energy efficient data gathering protocol for industrial automation using WSNs and IoT,” Journal of Industrial Information Integration, vol. 19, no. 19, Article ID 100156, 2020.

[6] V. S. Devi, T. Ravi, and S. B. Priya, “Cluster based data aggregation scheme for latency and packet loss reduction in WSN,” Computer Communications, vol. 149, pp. 36–43, 2020.

[7] T. Sood and K. Sharma, “LUET: a novel lines-of-uniformity based clustering protocol for heterogeneous-WSN for multiple-applications,” Journal of King Saud University-Computer and Information Sciences, 2020.

[8] Yan Qiang, Bo Pei, Wei Wei & Yue Li, 2015 ‘An Efficient CH Selection Approach for Collaborative Data Processing in Wireless Sensor Networks’, International Journal of Distributed Sensor Networks vol. 11, no. 6.

[9] Huang, H & Wu, J, 2005 ‘A probabilistic clustering algorithm in wireless sensor networks’, in Proceedings of IEEE 62nd VTC Conference, Dallas, TX.

[10] Prasad Rajendra, D, Naganjaneyulu, PV & Prasad, K, Satya, 2016 ‘Energy Efficient Clustering in Multi-hop Wireless Sensor Networks Using Differential Evolutionary’ MOPSO. Braz. arch. biol. technol. [online]. 2016, vol.59, n.spe2, e16161011. Epub Jan 23, 2017. ISSN 1678-4324. http://dx.doi.org/10.1590/1678-4324-2016161011.

[11] He,T, Stankovic, J A, Lu, C & Abdelzaher, T, 2003, ‘SPEED: a stateless protocol for real-time communication in sensor networks’, proceedings of the 23th IEEE International Conference on Distributed Computing Systems, pp. 46–55.

[12] Lu,C, Blum, B M, Abdelzaher, T F, Stankovic, J A & He, T, 2002, ‘RAP: a real-time communication architecture for large-scale wireless sensor networks’ in Proceedings of the 8th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2002), pp. 55–66, San Jose, Calif, USA.

[13] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks. 2005; 3(3):325–49.

[14] Wang Xiao-yun, Yang Li-zhen & Chen Ke-fei 2005 ‘SLEACH Secure Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks’ Vol.10 No. 1 2005 127-131.Wuhan University Journal of Natural Sciences, Article ID:1007 1202-01-0127-05.

[15] Edward Woodrow, Wendi Rabiner Heinzelman, SPIN-IT: a data centric routing protocol for image retrieval in wireless networks., Proc. 5th ACM/IEEE Mobicom, Seattle, WA, Aug. 1999. pp. 17485.ICIP (3) 2002: 913-916.

[16] Heinzelman WR, Kulik J, Balakrishnan H. Adaptive protocols for information dissemination in wireless sensor networks. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking; 1999 Aug. p. 174–85.

[17] Renjith, P. N., and E. Baburaj. "An analysis on data aggregation in Wireless Sensor Networks", 2012 International Conference on Radar Communication and Computing (ICRCC), 2012.

[18] Raed Alsaqour, Elmustafa Sayed Ali, Rania Abdelhameed Mokhtar, Rashid A. Saeed, Hesham Alhumyani, Maha Abdelhaq."Efficient Energy Mechanism in Heterogeneous WSNs for Underground Mining Monitoring Applications", IEEE Access,2022.

[19] K. Seelam, M. Sailaja, and T. Madhu, “An improved BAT-optimized cluster-based routing for wireless sensor networks,” in Intelligent Computing and Applications, pp. 115–126, Springer, Berlin, Germany, 2015.

[20] Senchun Chai, Zhaoyang Wang, Baihai Zhang, Lingguo Cui, Runqi Chai. "Wireless Sensor Networks", Springer Science and Business Media LLC, 2020.

[21] Renjith, P N, Ramesh K, Sasi Kumar S 2021, “An Improved trust-based Security framework for Internet of Things”, BJIT-D-19-00742R1, International Journal of Information Technology, Springer.

[22] Upasna Joshi, Rajiv Kumar. "Reinforcement learning based energy efficient protocol for wireless multimedia sensor networks", Multimedia Tools and Applications, 2021.

[23] Choonsung Nam, Dongryeol Shi. "Chapter 10 A CH Election Method for Equal Cluster Size in Wireless Sensor Network", IntechOpen, 2010.

[24] Harshavardhan Sabbineni. "An Energy- Efficient Data Delivery Scheme for Delay- Sensitive Traffic in Wireless Sensor Networks",International Journal of Distributed Sensor Networks, 2010.

[25] P. Jayalakshmi, S. Sridevi, Sengathir Janakiraman. "A Hybrid Artificial Bee Colony and Harmony Search Algorithm-Based Metahueristic Approach for Efficient Routing in WSNs", Wireless Personal Communications, 2021.

[26] Chun-Jung Hsu, Hung-Chi Chu, Jiun-Jian Liaw. "Connectivity and energy-aware clustering approach for wireless sensor networks", 2014.

[27] Jangseong Kim, Kwangjo Kim. "A scalable and robust hierarchical key establishment for mission-critical applications over sensor networks", Telecommunication Systems, 2011.

[28] Huabiao Qin, Xiaodong Zhong, Zhiyong Xiao."Balanced energy consumption and clusterbased routing protocol", 2011 9th IEEE International Conference on Control and Automation (ICCA), 2011.

[29] R. Ramya, Dr. T. Brindha. "A Comprehensive Review on Optimal CH Selection in WSN-IoT", Advances in Engineering Software,2022.

[30] Radhika Kavra, Anjana Gupta, Sangita Kansal. "Systematic study of topology control methods and routing techniques in wireless sensor networks", Peer-to-Peer Networking and Applications, 2022

[31] Sankar S., Ramasubbareddy Somula, Balakesavareddy Parvathala, Srinivas Kolli, Srilatha Pulipati, Aditya Sai Srinivas T. "SOAEACR: Seagull optimization algorithm-based energy aware cluster routing protocol for wireless sensor networks in the livestock industry", Sustainable Computing: Informatics and Systems, 2021.