International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-11 Issue-6, August 2022

Effective and Enhanced Congestion Control Technique using Adaptive Routing Protocol to Improve the Performance of Crammed WSN

S. Mohanarangan, D. Sivakumar

Abstract: ***Nowadays, congestion on the network becomes a usual fact which is to be focused and to be addressed appropriately especially in Wireless Sensor Networks (WSN) for crammed type networks. Limited capacity on channel and wastage of energy are the root cause of congestion in WSN. The effects of congestion implies on QoS parameters, queue length, data arrival rate etc. Furthermore, data packets should be transmitted energy-efficiently to the sink node. In this regard, an Energy-Efficient Routing Protocol is offered to efficiently transmit the nodes to their end node or destination. To control congestion, an Adaptive Buffer trade-off and Improved Trust-based Energy Efficient Routing protocol are first presented, this method identifies the congestion-free paths and the Buffer trade-off handles the buffer effectively. To route the protocol, a Cross-Layer Security-Based Fuzzy Logic Energy Efficient Packet Loss Preventive Routing Protocol has been developed. The proposed protocol routes the nodes and the protocol adopts a routing protocol that imparts security in terms of avoiding malicious nodes and preventing data loss. Consequently, to improve the lifetime of the network, a Density Aware Optimal Clustering Approach is presented. The proposed method is evaluated based on the Matlab software and the QoS performance metrics are Energy Consumption, Packet Delivery Ratio, Trust Value Computation, latency, reliability, energy efficiency, end-to-end delay, Average Throughput, accuracy and network lifetime. The effectiveness of the research is evaluated by comparing it with other existing techniques, including Trust Aware Secure Routing Protocol (TASRP), Artificial Flora Algorithm Based Support Vector Machine (SVM-AF), Well-Organized Trust Estimation-Based Routing Scheme (ETERS), LionFuzzyBee, and BatFuzzyBee Algorithm. Accordingly, the suggested method's performance is higher than the existing methods for Packet delivery ratio, throughput, network lifetime, energy efficiency, and reliability. Consequently, the proposed method improves the congestion control performance in an energy-efficient manner, in future; a recently advanced technique is proposed to effectively improve the network performance respectively.***

Keywords: Congestion Control, Cross-Layer Security, Network Performance and Network Lifetime, QoS Parameters, Trust Based Energy Efficient Routing Protocol

Manuscript received on 09 July 2022 | Revised Manuscript received on 18 July 2022 | Manuscript Accepted on 15 August 2022 | Manuscript published on 30 August 2022.

***** Correspondence Author

S. Mohanarangan*, Assistant Professor, Department of Computer Science and Engineering, Arunai Engineering College, Tiruvannamalai (Tamil Nadu), India E-mail: sramrangan@gmail.com

Dr. D. Sivakumar, Professor, Department of Electronics & Communication Engineering, Easwari Engineering College, Chennai (Tamil Nadu), India E-mail: dgsivakumar@gmail.com

I. INTRODUCTION

A wireless sensor network (WSN) contains a variety of sensors and has its transmitter, receiver, processor, memory, and power source. To gain relevant information, sensors gather data from their neighbours and transmit it to a central location. There are sensor networks that are limited by a variety of factors, including available memory, bandwidth, data rate, and battery power. The functions of sensors provide a variety of monitoring and sensing facilities, including safety, industry production, and traffic control [1]. A WSN is a collection of small sensors or actuators that can gather, compute, and broadcast sensory data to the Internet. The unsatisfactory situations like longer delay, lower throughput, and higher packet loss ratio because WSNs are particularly prone to congestion due to open characteristics such as self-organizing, battery-constrained, large-scale, and dynamic topology [2]. WSNs are simple computers with a variety of devices mounted on them that are used to configure environmentally as well as physical data such as pressure, sound, orientation, vibration, and temperature, amongst many other factors. The input attained from the sensors is redirected from one sensor to another via a multi-hop routing protocol to access the sink node. Then a secure protocol for routing is given to route the network from the base station. The base station has the results aggregation and analysis. The sensor nodes have low battery power and their physical area has no source to renew their power source. Subsequently, need an energy-efficient protocol design that increases the network's lifespan. In a variety of applications like industrial automation, environmental monitoring, and health monitoring, sensor networks have recently been used. From the source to the sink, a continuous flow of data has occurred and a significant amount of data transmission is required for Wireless Multimedia Sensor Network (WMSN) applications. A lot of information and continuous flows required more resources than the available hence congestion arises in the network [3].WSNs are divided into multi-sink WSNs and single sink WSNs depending on the number of sink nodes used in the network. Near the sink node, sensor nodes could experience the "hot spot" issue in single sink WSNs, and even in the sink node itself, fast failures may occur.

Into the destination application, the detected data from the environment cannot be routed in these situations.

Increased fault tolerance can be established by using several sink nodes, and even if one or more sink nodes fail, the essential services can still be provided by other sinks.

Furthermore, by lowering the distance or various hops between the sensor and the destination nodes, the deployment of many mobile sink nodes can reduce the sensor nodes' energy consumption [4]. In global and local networks, the quantity of packets is reduced by decreasing the sending rate of traffic control strategies which is classed as rate adjustment and an alternate path algorithm chooses the best path to send packets when network congestion is detected [5]. In terms of bandwidth, memory, processing capabilities, and power are the resource limitations of WSN technologies, if they are optimised appropriately, they can handle modern high-demand network computing applications provided. As a result, QoS algorithms should take sensor node restrictions into account. By assuring availability and resource control for various network services or applications, effective network operations are ensured for this the goal of QoS is to establish some level of network engineering priority [6].

A. Congestion in WSN

Congestion is the most common problem in WSNs, and it must be addressed effectively to avoid negative effects on network QoS metrics. To complete the task in a network, the data process before transferring it to its final destination to occupy the space, when it is occupied, congestion occurs. Software exploitation, hardware disaster, protocol in use, low signal amplitude at the terminus, overtaxed network nodes, human or normal intrusion, or unwarranted noise for this, the data loss is not limited [7].The data created at intermediary nodes rises when simultaneously sent the data by numerous sensor nodes. As a result, the quantity of data packets and generated data from the source nodes exceeds the underlying capacity of the network queue and at the same time makes the networks underperforming due to congestion. There are many reasons for congested networks in WSNs, including queue overloading, packet collisions, sharing the bandwidth by parallel transfers of the data packet, etc. In these situations, congestion can easily occur in the network, especially at the data collection and forwarding points in a many-to-one data forwarding network like WSN. Furthermore, wireless sensor network congestion is becoming more prevalent. The following factors caused this in WSNs: transmission rate, node buffer overflow, dynamic transmission channel with time fluctuation, transmission channel contention, packet collision, and many-to-one data transmission scheme. Packet congestion in routers' outgoing queues results in Performance degradation and low network reliability occurs when the congestion of packets at the outgoing queues in routers. To address the problem of traffic congestion control (CC), a large variety of systems have recently been proposed [8]. Energy consumption, end-to-end delay, and packet delivery ratio (PDR) are only a few of the QoS components that are strongly impacted by congestion in wireless nodes. As a result, to offer the required delivery ratio for WSN applications and to extend the network lifetime, it is vital to focus on the problem of sensor network congestion [9]. As a result, in recent years, WSN congestion control technology has become an important research topic and effective congestion prevention is a key performance measure for WSNs, and a hot topic in recent years [10].

B. Congestion Control Mechanism

Congestion control has an impact on a variety of applications, including event-based, query-driven, continuous sensing, and hybrid applications. Congestion control is used in several transport layer protocols, including the SCTP and Transmission Control Protocol (TCP). Congestion control is required for many conditions, such as buffer overflow, packet collisions, channel contention, and interference, whereas congestion control is not required for slow processors, buffer size shortage, and slow links [11]. A reliable and congestion-based protocol is suggested by (Sharma, *et al* [12]), that offers rate adjustment and bidirectional reliability-based congestion control. It determines the best path for data transfer using the TOPSIS technique because TOPSIS chooses an option that is the greatest distance from a negative ideal and the least deviation from the optimal solution. To determine the degree of congestion, the ratio of average packet service time to average inter-arrival time for packets is employed to detect the congestion. Congestion is not desirable and must be mitigated or controlled as it causes adverse effects on the network performance and the quality of service, mainly in terms of significant packet loss which leads to degraded throughput. In WSN, congestion may occur due to radio collisions and buffer overflow [13].Then (Lakshmi, *et al* [14]) demonstrated how to successfully manage congestion control and adaptive buffer switching. Congestion is detected simultaneously based on residual buffer space, residual energy, and the conviction level of sensor nodes. The methodology demonstrates the selection of adaptable main and spare buffers based on cost evaluation. Swapping and dynamic buffer switching are used to enhance congestion results. Nonetheless, congestion causes the node's energy dissipation, network performance deterioration, packet loss and time delay increases [15]. Subsequently, it is essential to design energy-efficient congestion control protocols to detect, mitigate and control congestion effectively. The remaining work is structured in the following sections: section 2, which exhibits the study's literature review, section 3, which depicts the problem definition and motivation, and section 4 depicts the proposed research methodology. Section 5 reveals the experimentation and result discussion, and section 6 discloses the conclusion part of the research.

II. LITERATURE SURVEY

The survey illustrates the investigation of mechanisms for congestion control. In this study, the network performance and the network lifetime are improved based on the optimization methods.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Prasanthi,*et al* [16] presented BatFuzzyBee as a biodiversity-based monitoring system. In order to manage congestion, WSN bio-definitions use location data. In this research, to reduce packet loss a new cluster-based WSN is also employed. When the network comprises nodes with varied transmission ranges and the least power consumption, BatFuzzyBee can determine the closest or best reliable path. Multiple variables, such as energy consumption, accuracy, and packet delivery ratio are used to compare the proposed BatFuzzyBee to alternative systems. Aimtongkham, P, *et al* [17] suggested a path determination architecture for WSNs that takes congestion into account.

The architecture is classified into three phases, excluding the path determination's final criteria: (1) in a top-down hierarchical structure, the path is constructed, (2) with energy-aware assisted routing, the path is constructed, and (3) exponential smoothing is utilized for congestion prediction. A bat algorithm is used to optimize the weight over the membership functions and the proper weights among numerous criteria including remaining energy, forwarding rate, buffer occupancy and hop count are determined by fuzzy logic systems. The results showed that the suggested technique performs better than state-of-the-art protocols in terms of reduced packet loss, balancing overall energy usage, high throughput, and extending network lifetime. To effectively address congestion while maintaining data accuracy, a CADC is presented by Zhuang, *et al* [18], and the impact of CC is examined based on data accuracy. While maintaining a certain overall data error estimation constraint in a distributed way, CADC uses adaptive lossy compression to reduce congestion. A weighted CADC scheme is suggested in this work so that higher priority data is less distorted because various data may have varying priorities in a CPS application.

To ensure the accuracy of certain aggregate computations, they modify CADC. The CADC's usefulness and efficiency are demonstrated through extensive simulations. The FCOABC protocol was presented by Kalaikumar, *et al* [19] regarding congestion control. To extend the network's lifespan and save energy, the concepts of media accessibility and energy-efficient hierarchical-based cluster routing are integrated into the proposed protocol. In this suggested FCOABC protocol, the OABC optimization method is used from CHs to the master station routed through inter-cluster multi-hop; as a result, the protocol was effective and reliable data transfer is achieved to the master station. In terms of evaluation parameters such as scalability, energy consumption, and network lifespan, the simulation results showed that the FCOABC protocol outperformed other clustering protocols.

Grover, A, *et al* [20] proposed a new rate-aware CC (RACC) mechanism that three stages of congestion are described depending on delay, overhead, throughput, and data rate. To test the optimum modulation strategy for this approach, the RACC has also been used in different modulation schemes such as QPSK (Quadrature Phase Shift Keying), BPSK (Binary Phase Shift Keying), and 16 QAM (Quadrature Amplitude Modulation).The NS2 tool's simulation results revealed that RACC outperforms previous strategies (Joint energy replenishment and load balancing (J-ERLB) and (Delay-aware congestion control protocol (DACC)) in WSNs. To increase network performance, an effective congestion avoidance method based on the Huffman coding algorithm and ant colony optimization (ECA-HA) was proposed by Yadav, S.L, *et al* [21]. Traffic- and resource-oriented optimization is incorporated in this study. To locate multiple congestion-free alternate routes, ant colony optimization has been used. To an ideal path, Huffman coding examines the packet loss rate on multiple alternate paths determined using ant colony optimization. In terms of latency, packet delivery ratio, throughput, and average energy consumption, this method outperforms other methods. To reduce or alleviate network congestion, a DRCDC approach is suggested by Tan, J, *et al* [22].

By intelligently decreasing data that includes less information while keeping a low rate of information distortion gathered by the network, the DRCDC technique can reduce congestion. (1) In terms of spatial congestion alleviation. Some missing data in space can be retrieved using matrix completeness theory from other spatially collected data because sensing data has a geographic correlation, in the case of obtaining a particular amount of data. (2) Temporal congestion reduction. Limiting the time slots' data collection containing tiny data minimises the flow rate that must be communicated when the network becomes congested while minimising the network's data distortion rate congestion is prevented.

The router buffer has a dual-threshold set to CC, a CC approach for WSNs was used by Li, S, *et al* [23] that uses a cache state. Moreover, the channel transmission status regulates the congestion that is monitored by the queuing variation tendency and the transmission rate. The active queue management method is the foundation for the DI-RED model-based dual-threshold, which is intended to improve network performance. Several channel indicators are derived by solving the DI-RED model, including throughput, average queue length, packet loss rate, and delay. The suggested DI-RED model exhibits greater control and is more stable, which may overcome the RED mechanism's parameter sensitivity, according to simulation results. Raman, *et al* [24] introduced a fast CC (FCC) technique based on routing with a hybrid optimization algorithm.

Two processing steps are considered in this proposed scheme. First, we propose a multi-input time on task optimization algorithm for selecting the proper next hop with minimal unwanted queuing delay. Then, we propose an altered gravitational search algorithm for making an energy-efficient route between sources to destination. The suggested FCC solution reduces congestion by enhancing routing to select the optimum next node during data forwarding. The experimental findings demonstrate that The FCC scheme effectively minimises energy consumption, and data loss, and maximises network lifetime and average hop counts. For CC in large-scale WSNs, a hybrid bio-inspired algorithm is suggested by Royyan, *et al* [25].

First, to prevent congestion while maintaining fairness across sensor nodes, a C-LV model is used. Toenhance C-LV, PSO is used to optimise the parameter for minimising end-to-end delay. This system is adaptive to change by utilizing PSO. The suggested technique, which is indicated in the simulation results, enhances the QoS in WSNs.

III. RESEARCH PROBLEM STATEMENT AND MOTIVATION

Congestion is a major challenge in WSN and it increases the load in the transmitting channel. Consequently, detecting and reducing WSN congestion requires an effective approach. It leads to congestion in the network when the incoming packets do not increase beyond the actual ability of the network. Congestion on a network can cause sensor power loss and packet loss, increase network delay, and limit bandwidth. As a result, better ways of dealing with traffic congestion are required. To increase network performance, it is necessary to analyse and supervise congested resources in the wireless network. The sensor node loaded a large amount of data, and the data can lead to a variety of difficult problems that are required to be processed for wireless communication. Moreover, one of the main restrictions for WSN is energy consumption. Various approaches for energy consumption enhancement are introduced to avoid data losses during the transmission with improvement in network lifetime.

It is nature of application such as many to one data flow, data-centric and infrastructure of sensors offers solutions can be different some applications like reprogramming nodes or sending commands to them necessary, the sink can send data to the sensors in the least possible time. In solving congestion in an upstream-like downstream, direction CC is needed. In this approach, congestion in sensor sink traffic but no protocol can be controlled bidirectional congestion. Optimization shows a crucial part in WSN. Optimization is a method for attaining the optimum outcomes under a certain condition. Subsequently, countless optimization methods are obtainable and are used to accomplish preferred objectives in networking. It is categorized into solitary and multi-objective optimization. However, in multi-objective optimization, various objectives are concurrently optimized. Real-world problems contain many purposes, where all objectives must be enhanced simultaneously which considerably improved the network performance, such as packet loss rate and throughput, alleviating network congestion and improving network QoS.

IV. PROPOSED RESEARCH METHODOLOGY

Networks consisting of large numbers of nodes are termed WSNs, which have characteristics of self-organizing, low cost, and random deployment. The establishment of secured data transmission and optimum routing is ensured. The suggested best solutions allow secure and dependable data transport while consuming less energy. Consequently, in practical applications, each node in the WSNs is required to consume energy as little as possible for data collection and transmission to increase network lifespan. To maximize network lifetime through energy conservation, routing protocols should be more energy efficient. Therefore, reducing node energy consumption has become the main aim of routing protocols.

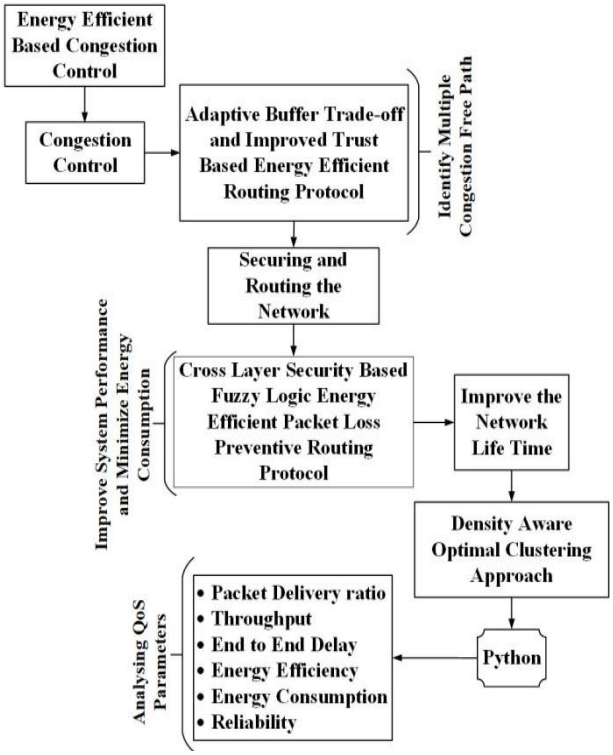

Fig. 1. Architecture Diagram of the Proposed Method

Figure 1 displays the research's workflow diagram. An energy efficiency-based congestion control system was provided in the research. The Adaptive Buffer trade-off and the Improved Trust-based Energy Efficient Routing Protocol (AB-ITEER) are used in this process' initial search for several congested-free paths. Using Cross-Layer Security-Based Fuzzy Logic Energy Efficient Packet Loss Preventive Routing Protocol (CLS-FEEPLPR), route the network and secure it. It improves the system performance and minimizes energy consumption. After that, a Density Aware Optimal Clustering Approach (DAOCA) is introduced to improve the network lifetime, respectively.

A. Multiple Congestion Free Paths Identification

The AB-ITEER Protocol for finding an optimal congestion-free path and handling buffers effectively. A congestion-free path is provided by this method to the node because the congestion is occurred due to the packet transfer from one node to another, to avoid the congestion, the congestion-free path is required. It ensures trust in routing with minimal delay as well as network energy efficiency. Using the cluster head and each sensor node's weighted trust value, the Trust-based energy-efficient routing protocol is utilised to discover the best-trusted path between the source and destination.

In WMSNs, for a continuous and broad data flow this protocol depends on the sensor node's remaining resources, buffer, and trust level. It is designed to handle buffers effectively in WSNs. Congestions are defined by different congestion indicators.

Retrieval Number: 100.1/ijeat.F37070811622
DOI: 10.35940/ijeat.F3707.0811622
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

For avoiding congestion and bottleneck nodes, each node dynamically adjusts for load balancing purposes; the transmitter offers each one-hop neighbour a different transmission rate and balance ratio. The spare buffer is triggered by alarm signals; the current buffer assumes responsibility. The main buffer is now going to sleep mode for energy conservation. The process is called buffer refinement from the primary buffer to the secondary buffer.

B. Adaptive Buffer and Trust-based EERP

The Buffer swapping technique has been introduced in the proposed system to show effective buffer management in WSN. Figure 2 represented that the data is transferred from the Cluster Heads (CH) to the relay node. From the Relay node (RN), the data is transferred to the base station. If the data received from CH is extensive and the RN does not have enough buffer space, then RN will send the signals to all the cluster heads to transfer the data to the Spare Node (SN). Formerly the CH will divert transmitting the data to the spare node. When the Buffer of RN gets empty, the SP swaps the data to RN Buffer.

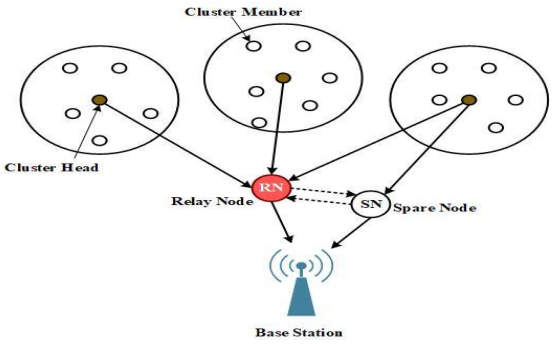

Fig. 2. Adaptive Buffer Trade-off Function

At that point, identifying the congestion-free paths using the trust-based energy-efficient routing protocol is depicted in the subsection that follows.

C. Trust-Based Energy-Efficient Routing Protocol

The most reliable route between the source and the destination is found using the proposed ITEERP. The cluster head and each sensor node's weighted trust value were used to identify these trusted pathways. A frequent peer-to-peer trust evaluation is carried out between two CHs and two SNs. At the SN level, each SN is responsible for submitting the results of its trust evaluation to its CH, which conducts CH-to-SN trust evaluations for all SNs in its cluster. A CH is also responsible for reporting its trust assessment of other CHs in the network to the base station, which conducts station-to-CH trust assessments of all CHs in the system. The ITEERP can more effectively prevent security breaches by calculating the trust weighted value between nodes and generating the overall trust metric by combining indirect and direct techniques.

This section labels the ITEERP's overall architecture. When a source node wants to get a destination node's trust value, utilize both the one-hop trust model and the multi-hop trust model. Either the indirect trust model or the direct trust model is used depending on whether the destination ID is located within the cluster. Trust can be represented as a confidence level that if a node can trust another node. The trust value is used in this case to determine if a node can function normally in WSNs. In this paper, the trust value is assumed to be in the range of 0 to 1. The node is completely trustworthy and considered if the trust value is between 0.6-0.9 or 1, and the node can be avoided if it is between 0.1-0.5 or 0. Direct trust can be calculated if a source node can communicate or transmit the data directly or without any intermediate nodes. Calculated the indirect trust value based on suggestions from nearby nodes. Informational and communication substance and residual energy are the three major characteristics of trust. To determine the path trust value, the probability of the trust value was estimated based on the aforementioned parameters. In this paper, the ITEERP technique is used to find the available trusted paths between the source and the destination node. To compute the nodes' trustworthiness, the combination of both direct and indirect trust is used in this paper.

D. Computation of Trust Value by Direct Trust

In Sensor Network, the nodes usually collaborate and communicate with sensor nodes and also with the cluster head to perform their tasks. Usually, all communications in the network will consume a certain amount of energy to transmit the information or the data packets. Subsequently, the trust value for data content, residual energy and communication are defined in ITEERP. To find whether the data transmitted have reached the destination without any alteration the data content is used. To measure if the node is proficient in performing its intended functions or not the residual energy is used and the communication is used to find whether the packets transmitted by a node have reached the destination correctly whether the node is a selfish node, or a replica node or malicious node. The trust values for the above properties using a direct trust are computed as follows.

Data Content: The data content is evaluated based on the packet drop ratio. Packet dropping is demonstrated as the ratio between the total packets lost to the total packets sent. This can be derived using the Gaussian probability as follows.

$$P_{dc} = \frac{1}{\sqrt{2\sigma^2 \pi}} e^{-\frac{(d_i - \mu)^2}{2\sigma^2}} \quad (1)$$

Where, P_{dc} denotes the data content probability, d_i indicates the PDR of i^{th} time and i varies between $1, 2, \ldots, n$. μ is mean (and also its median and mode). σ is standard deviation and σ^2 is variance.

For each node the probability value is calculated and if the probability value is high that particular node is chosen and used for the path selection to transmit the data. The packet dropping ratio is low if the packet sent by the source node is received correctly by the destination without any loss and has a high Packet dropping rate if the packet received by the destination is less.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Trust value for data content τ is computed as the probability of the difference in a number of the probability of packets dropped not occurring at the time t. Accordingly, the data trust is calculated by

$$\tau_{dc} = (1 - P_{dc}(t)) \quad (2)$$

Residual Energy: Whenever there is a data transmission takes place the residual energy of that particular node will be consumed. Then the probability value of the remaining energy is calculated and from that, the trust value is found which ranges between 0-1.

In general, an energy threshold T_e is predefined for a sensor node and it is compared with the probability of residual energy p_r. If the $p_r < T_e$, then due to insufficient energy the particular node is not considered for the path selection. A sensor node's residual energy p_r is thought to be between 0 and 1. The residual energy p_r is calculated based on the consumption energy rate E_c of a sensor node, where $E_c \in [0,1]$. It is defined as the difference between the total energy of the node to the energy used by the node. The probability of residual energy is calculated by:

$$p_r = \frac{1}{\sqrt{2\sigma^2 \pi}} e^{-\frac{(e_i - \mu)^2}{2\sigma^2}} \quad (3)$$

Where, e_i denotes the energy consumed over i^{th} time and i varies between $1, 2, \ldots n$. The trust value τ_{re} for residual energy can be computed as the probability of the difference in the probability of energy consumed not occurring at the time t. It is calculated by

$$\tau_{re} = (1 - p_r(t)) \quad (4)$$

Communication Trust: Communication trust C_t is a significant parameter to estimate the sensor node's trust value. Communication C_t is defined in a way such that if the number of packets sent by a source node has reached the destination correctly without any packet loss. PDR is distinct as the ratio between the total number of packets received to the total number of packets sent. Therefore, PDR is evaluated as

$$C_t = \frac{1}{\sqrt{2\sigma^2 \pi}} e \frac{-(d_{r_i} - \mu)^2}{2\sigma^2} \quad (5)$$

Where C_t denotes the communication trust based on the packet delivery ratio, d_{r_i} is the number of packets received in i^{th} a period and i ranges between $1, 2, \ldots n$. Consequently, the trust value for the communication is considered as the probability of the difference in the probability of the packet received not occurring at the time t. It is calculated by

$$\tau_{ct} = (1 - C_t(t)) \quad (6)$$

Table- I: Algorithm for Trust Value Calculation

Algorithm 1: Trust Calculation Algorithm
Input: Source node A, Dest Node B Output: Trust Value T ***Step 1:*** Source node A Find the List of Neighbours N_i . in the cluster ***Step 2:*** The Id of dest node B is checked in the List of Neighbours N_i in the cluster by A, ***Step 3:*** If the dest node B is in the list N_i , Source node A and dest B have direct communication. ***Step4:*** (a) Calculate Data trust using Packet Dropping Ratio by Gaussian probability as equation (1) and $\tau_{dc} = (1 - P_{dc}(t))$ is the evaluated trust value (b) Probability of Residual Energy is evaluated by equation (3) and the evaluated trust value as $\tau_{re} = (1 - P_r(t))$ (c) Communication trust probability is calculated using Packet Delivery Ratio as in equation (5) and the trust value is computed as $\tau_{ct} = (1 - C_t(t))$ ***Step 5:*** If the dest node B is not in the list N_i , it will check for the other clusters and the Source node A and dest B have indirect communication. ie. A should get the information from other cluster heads. ***Step 6:*** Tore the Trust Value T

E. Weighted Trust Value Calculation by Direct Trust

In order to find the trust value for every path, the weighted trust value for the individual sensor node is identified. The weighted value for each node using a direct trust T_{wd} is calculated by the summation of all the parameters like data content, residual energy and communication trust. The weighted trust value for the direct trust T_{wd} of a single node is derived as follows

$$T_{wd} = \sum P_{dc} + P_r + C_t \quad (7)$$

Where, T_{wd} is the weighted trust value for direct trust, P_{dc} denotes the probability of data content, p_r indicates the probability of residual energy, C_t and denotes the communication trust based on the packet delivery ratio.

F. Weighted Trust Value Calculation by Indirect Trust

In this paper, to calculate the probability trust value using an indirect trust, Dempster-Shafer's theory is used for each node. The belief function is the main part and is based on two fundamental ideas which include degrees of belief about a proposition. This can be obtained from subjective probabilities, and these degrees of belief can be combined on the condition that they are from independent evidence. The probability trust value for indirect trust is assessed utilizing this belief function and by combining the rule of belief; we can combine more results from neighbour nodes. Based on the Dempster Shafer theory K_{DS} is defined as:

$$K_{DS} = x_{n1}(T) + x_{n2}(T) + x_{n3}(T) + \ldots\ldots + x_{ni}(T) \quad (8)$$

Where, node $n1 \le x \le n$, is a one-hop neighbour of node S and node D. The same process is used for indirect trust I_t to find the weighted trust value. It can be demonstrated as follows

$$ID_t = KD_s \quad (9)$$

Where, ID_t is the weighted trust value for indirect trust and KD_s is the probability of summation of all the one-hop neighbour nodes. The process can be repeated for all each cluster's available sensor nodes in the network. After the evaluation of the individual nodes 'weighted trust value by both direct and indirect trust, the average weighted trust value can be calculated.

G. Average Weighted Value

Based on the node weighted trust value, the average weighted trust value for a single path for direct and indirect trust can be computed as follows

$$A_{wt} = \frac{1}{N}\sum_{i=1}^{N} T_{wd} + ID_t \quad (10)$$

Where, A_{wt} is the average weighted trust value for a single path, T_{wt} is the weighted trust value of direct trust for a single node, ID_t is the weighted trust value of indirect trust for a single node and N is the number of available paths. Subsequently, the average path trust value is identified using this equation and this technique is used to decide whether the particular path can be selected for data transmission or not.

H. Securing and Routing the Network

The CLS- FEEPLPR is proposed. The protocol adopts a routing protocol that imparts security in terms of avoiding malicious nodes and prevents data loss as well as constrains the utilization of excess energy. In order to provide an energy-efficient secure route to the destination, it makes use of the fuzzy decision-making model. Cross-layer security is implemented using a fuzzy logic calculation approach for a protocol called the cross-layer protocol. To lessen the impact of security concerns on the WSN, this protocol makes use of several factors that are retrieved from the inter-layer information exchange. An incredibly efficient way to guarantee the maximum level of safety in a WSN is to use the proposed CLS- FEEPLPR. It also improves the network performance and minimises energy consumption.

I. Cross-Layer Protocol Design

Cross-layer protocol is a security method that switches different parameters for the best results. The three main objectives that must be understood while developing cross-layer architecture are QoS, security, and mobility. Cross-layer design is designed to increase the exchange and control of two or more information layers and significant improvement of performance by enhancing the interaction between different protocol layers.

J. Unified Cross-Layer Design Approach

The network layer, transport layer, application layer, physical layer, and MAC layer functions are all included in the technique, which replaces all conventional layers. The methodology replaces all traditional layers and incorporates all layer functions (application layer, transport layer, MAC layer, network layer, and physical layer) to share the information. It is an energy-efficient approach and through cross-layer design, the strategy is designed to enhance service quality and performance within different operating conditions. The theory of design is a full seamless cross-layering so that conventional communication layers both inform and operate in one protocol. Here are some details on the cross-layer operation. Communication is based on a single layer and is based on an initiative notion. The principle helps each node to determine whether to participate in the communication. A fully distributed and adaptive operation is therefore implemented. The next hop is not decided in advance in each contact.

Additionally, the decision to participate in communication is based on an initial determination process for each node. The determination of initiative constitutes the basis of the unified cross-layer and implicitly integrates the inherent communication capabilities necessary for effective WSN communication. A node starts transmission by sending an RTS packet to alert its neighbours that it has transmitted a packet. Each node neighbour i agrees to take part in the communication or not after receiving an RTS packet. The decision is made by determining initiative. Determining the initiative is a binary system in which a node wants to interact when it takes its initiatives 1. Denoting the initiative I, it is determined as follows:

$$I = \begin{cases} 1, & if \begin{cases} \xi_{RTS} \ge \xi_{Th} \\ \lambda_{relay} \le \lambda_{relay}^{Th} \\ \beta \le \beta^{\max} \\ E_{rem} \ge E_{rem}^{\min} \end{cases} \\ 0, & otherwise \end{cases} \quad (11)$$

If the four conditions are satisfied in (11), then the initiative is set to 1. Each condition in (11) constitutes certain communication functionality. The reliable communication link is established by the first condition. For this reason, it specifies that an RTS packet's received signal-to-noise ratio (SNR) ξRTS is above a certain limit ξTh for a node to be active in communication. For local congestion control, the second and third conditions can be used. As shown in this component the second condition reduces congestion by restricting the traffic a node may relay. The third condition guarantees the node has no buffer overflow and thus avoids congestion as well.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The last condition guarantees the remainder of a node's energy E_{rem} stays above a minimum $E_{rem}^{\min}$. The restriction also guarantees energy consumption distribution. Such constraints are the cross-layer functions of the unified cross-layer which determines a node's initiative to engage in communication. Utilizing the initiative paradigm, a unified cross-layer performs reliability for hop-by-hop, local CC, and distributed operation.

K. Fuzzy Logic

The Fuzzy Logic concept centres around the idea of partial set membership, instead of crisp or discreet set membership. Initially, it was introduced as an alternative approach to processing data that has behaviour defined by a "fuzzy" set, which contains elements whose degree of membership varies in the set. The Fuzzifier, also known as the degree of membership, normalises the fuzzy variables in the range of 0 to 1 based on the crisp input. The inference system with a rule base is then given by the fuzzy input in which the fuzzy variables are mapped to a fuzzy output.

The mapping of the fuzzy variables to the inference system is not discrete and can be partial or overlapping. The set of fuzzy outputs is combined and applied to the Defuzzifier, which reverses the effect of fuzzification. Different techniques can be used to obtain the crisp output from the fuzzy output, after applying it to the membership function.

$$x^* = \left(\sum x.\mu(x)\right) / \sum \mu(x) \qquad (12)$$

In equation (12), 'x^*' represents crisp output after defuzzification, 'x' represents the centroid of the fuzzy variables calculated from the membership graph and '$\mu(x)$' represents the area calculated from the membership graph bounded by the membership degree and the abscissa for each fuzzy variable.

L. Fuzzy Logic Energy Based Packet Loss Preventive Protocol

FEEPRP offers fresh information by offering a suitable route and monitoring particular parameters whose present values are collected from the nodes, analysing them, and using fuzzy decision-making models to choose a path. The design of our proposed algorithm for FEEPRP consists of two phases: choice of route and route discovery as explained in detail in the next sub-sections.

Route Discovery: Whenever a source node seeks a route to any particular destination node, it sends a request packet to the network. A multicast of the request packet is done. The request packet holds the address of the sender and the destination address initially as it is dispersed. Consequently, this can be noted that a request packet is not the original message that is due to be transferred. The request packet is equipped with a sequence number, a source address, a destination address and a certain vacant space for holding values like the address of intermediary nodes, hop count, packets dropped and residual energy. Each request packet maintains a list of intermediary nodes as long as a route to a destination is discovered. Consequently, FEEPRP overlooks issues of scalability instead of its advantages over energy efficiency, shorter path discovery and security in terms of route. According to the algorithm, the request packet is the first multicast from the source node. According to the transmission range of the sensor node, the packet reaches some other node. The design of our algorithm is thus presented as follows.

Table- II: Algorithm for Route Discover

Algorithm 2: Route Discover

```
Input: destination address, request packet.
Output: 'Stack 2' – A stack of intermediary node addresses.
Initialize:
❖ hop count=0
❖ time-to-live=maximum
❖ packets dropped=0
❖ residual energy=0
 while (node address is not equal to destination address and time-to-live is not equal to zero)
 {
   if (the sequence number of the packet already entered in the node memory)
      Discard request packet;
    else
    {
❖ enter the node memory's sequence number
❖ decrement time-to-live
❖ add the intermediary node's address to the request packet's memory in stack 1
❖ increment hop count by one
❖ update: packets dropped=packets dropped + packets dropped at the node; store
❖ update: residual energy=residual energy + residual energy at the node
❖ forward request packet
}
if (node address=destination address)
{
   route _reply ();
   exit;
}
}
route _reply ()
 {
    while (source address is not reached)
    {
❖ pop address of intermediary nodes from stack 1
❖ traverse through the popped address
❖ push the address to stack 2
     }
}
```

It should be observed that keeping a note of the sequence number helps to successfully eliminate any loop formation. After all, routes have been developed from a specific source to the destination, and route selection is carried out. Keeping into consideration the memory constraint of sensor nodes, in FEEPRP, as soon as a route is availed, nodes erase from their memory the record of perceived packets. Route discovery is carried out each time demand is encountered.

Choice of Route: A route is decided upon using a fuzzy method, according to our design of FEEPRP, all paths from the source to the destination are available at the source. Therefore, for any outsider, there is an unpredictable probability of any route to be selected. Since the same route probability being selected is less and which route is selected is unpredictable, this adds a security aspect as attacks on the selected route become less probable.

Defuzzification of the values input would give a single route R as the output (equation 12) depending upon the conditions defined in terms of the membership graphs determined and the rule base established by the user for the fuzzy system.The fuzzy approach taken according to our proposed algorithm is outlined below.

M. Network Lifetime Improvement

The DAOCA is presented to improve the lifetime of the network. Considering the balanced use of energy, a network's longevity is depending. Consequently, the energy is uniformly distributed among cluster formation and nodes considers the density of the region because of the same.

The structural centres are measured using structural centrality. The factors considered here, are the density of the node and relative distance. These parameters are determined by the separation between two nodes.

Table- III: Algorithm for Choice of Route

Input: From Stack 2:
- The nodes' residual energy
- Route's hop count
- Net packets dropped in route

Output: route R: defuzzified crisp output
BEGIN
- Get the values of residual energy, packets dropped and hop count of each particular route reported at the source node by stack 2
- Fuzzify the crisp input parameters: packets dropped, residual energy, and hop count
- Apply the fuzzy rule to get a fuzzy output
- Defuzzify the fuzzy output using the centroid method of defuzzification to get a crisp output using equation (12)
- The defuzzified crisp output gives a specific optimum route concerning packet loss and minimal energy consumption in the network

END

N. Density Aware Optimal Clustering Approach

A network's lifespan is dependent on balanced energy usage. The structural centralities' formal definitions and explanations are provided as follows. The graph notation $G=(V,E)$ is used in the un-weighted and undirected network. Where the whole network is represented by G, the set of all nodes is given by V and the set of all edges is given by E. An adjacent matrix A can be used to represent the network's topological structure. The connectivity between nodes with 1 or 0 is characterized using its relation.

Node Density: Adjacency matrix of the network is taken as A. The node i 's density in a network is given by,

$$\rho_i = \sum_{j}^{i} \varphi\left(d_{ij} - d_c\right) \tag{13}$$

Where, $\psi(x)=1 \; if \; x \le 0$, and $\psi(x)=0$ otherwise; distance between a node i and j is given by d_{ij} in A and cut of distance is given by d_c, the number of neighbour nodes within distance d_c is represented by ρ_i. Distances between nodes are measured using Geodesic distance which is also used to measure distance metrics like information distance and common neighbours. These are used as an alternative measure. The change in the relative magnitude ρ_i affects the performance of an algorithm. It demonstrates that the outcomes are significantly influenced by the value d_c. The mean neighbour number is made 1 to 2% of total network nodes by automatically choosing the value of cut-off distance d_c as suggested. During experimentation, it is observed that the diameter of the network is superior to the value of d_c and most of the time it has the value of 1. Consistent results can be produced by changing cut-of distance d_c and results are strongly influenced by the same. In community detection, based on the thumb rule, the value d_c is set to 1. The degree of centrality equals the density of the node.

Relative Distance: By calculating the minimum distance between a node i and a node with high density, relative distance δ_i can be measured and it is given by,

$$\delta_i = \begin{cases} \min\left(d_{ij}\right) \\ j : p_j > p_i \end{cases} \tag{14}$$

Assume conventionally $\delta_i = \max\, j\left(d_{ij}\right)$, for the nodes having a high value of local density. The δ_i value is too large when compared to the distance of the nearest neighbour. It holds for nodes with a global or local density maximum value. The nodes are thus acknowledged as the communities' structural centres. In this instance, a node's value is excessively high.

Structural Centrality: The structural centres have a high-density value when compared to their neighbours. They maintain a large distance with nodes with high density. The node i 's structural centrality is given by

$$sc_i = p_i * \delta_i \tag{15}$$

The density of node and relative distance is proportional to the structural centrality as shown in equation (15). The computation involves normalising the structural centrality value using different computing techniques. Relative distance is used to compute the distance between the nodes with the highest density value. It prevents the selection of structural centres from the same high centrality community nodes. The nodes which are having a local maximum of structural centrality are recognized as a cluster's structural centre. In the relative distance plot, other nodes are separated from structural centres concerningthe density of the node.

V. EXPERIMENTATION AND RESULT DISCUSSION

The Matlab r2021a software is used to evaluate the results of the research. The operating system of the software is Windows 10 Home; its memory capacity is 6GB DDR3. It uses the Intel Core i5 @ 3.5GHz processor, and the time taken for simulation is 10.190 seconds, which is depicted in table 4.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table- IV: Simulation System Configuration

Simulation System Configuration	
MATLAB	Version R2021a
Operation System	Windows 10 Home
Memory Capacity	6GB DDR3
Processor	Intel Core i5 @ 3.5GHz
Simulation Time	10.190 seconds

In congestion control, there is approximately 50 to 100 are used and their communication range is 100 m. Several performance metrics are considered for analyzing the proposed method's performance such as Energy Consumption, Packet Delivery Ratio, Trust Value Computation, Average Throughput, latency, energy efficiency, end-to-end delay, reliability, and network lifetime.

The performance of these parameters is depicted as follows.

Packet Delivery Ratio (PDR): To analyze the performance of the network based on delivered packets Packet Delivery Ratio is an important metric. The relation between the numbers of correctly delivered packets from the total number of packets available is known as PDR.

$$PDR = \frac{N_{dp}}{N_{ap}} \tag{16}$$

The total number of packets available is indicated as N_{ap}, where N_{dp} is the total number of delivered packets.

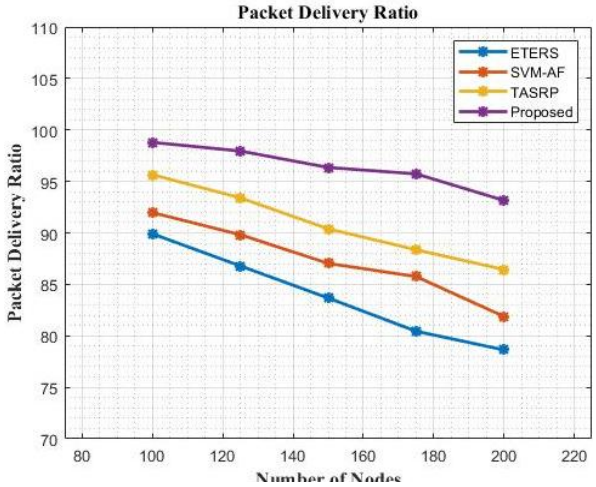

Fig. –3. Results of Packet Delivery Ratio

Figure 3 reveals the performance graph of the PDR, the PDR of the proposed method is 99%. The suggested model's PDR is compared with those of the existing ETERS [26], SVM-AF [27], and TASRP [28] techniques. While compared to these existing methods, the proposed method's performance is higher.

Energy Consumption: The energy effectiveness of the protocol is reflected by the average energy devoted per packet to reach the sink. The energy efficiency will be high if the energy consumed will be low.

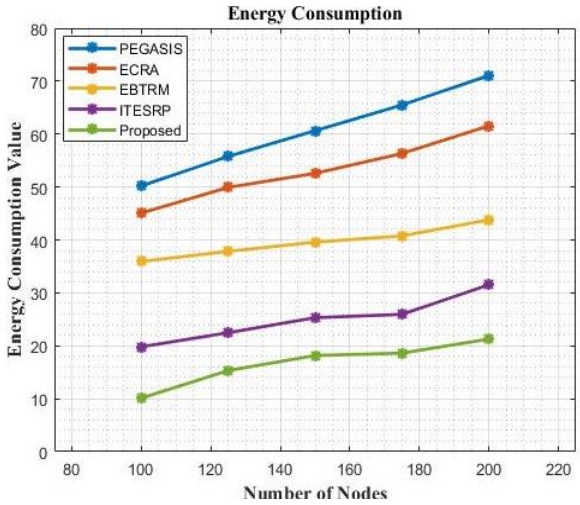

Fig. 4. Graph for Energy Consumption

Figure 4 portrays the energy consumption graph. The analysis shows that when the number of network nodes rises, energy consumption does as well. However, when it is compared with the existing protocol the energy consumption is less and it gives better results.

Computation of Trust Value: Total packets received can be used to calculate the trust value. It is simple to see the number of packets transmitted varies depending on many packets are received. These variations may be caused by alteration of packets, the addition of packets, and packet loss. The probability value of packets that have been altered, added and missed can be derived as

$$T_r = \frac{P_{rp}}{P_{tp}} \tag{17}$$

Where, P_{rp} is the remaining packets and is defined as $P_r = P_s - P_r\, P_s$ the number of packets sent, P_r is the number of received packets and P_{tp} the total packets.

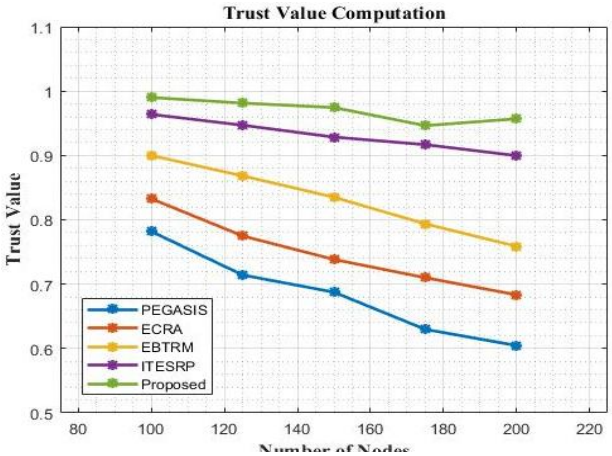

Fig. 6. Performance Graph of Trust Value

Figure 5 depicts the performance graph of computation trust value. It is observed that there is a progressive decrease in the trust value of the node when there is an increase in the number of nodes.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Consequently, the proposed system gives better results with high trust value when it is compared with the other existing protocols.

Average Throughput (AT): One of the main important performance metrics is Average throughput. AT is the average successful message delivery rate over a communication channel. The optimal system will typically have a high average throughput when the total nodes are increased. The metric is considered to analyze the performance of the research by increasing the number of nodes. Here the throughput is calculated by using the below formula.

$$T_{avg} = \frac{S_p}{T_p} \quad (18)$$

Where, S_p denotes the total number of successfully transmitted packets and T_p is the total number of packets. Figure 6 reveals the performance graph for the presented work, it is examined that the throughput value of the research is increased while there is an increase in the number of nodes compared to previous approaches. Similar to this, the proposed approach performs better when more network nodes are added

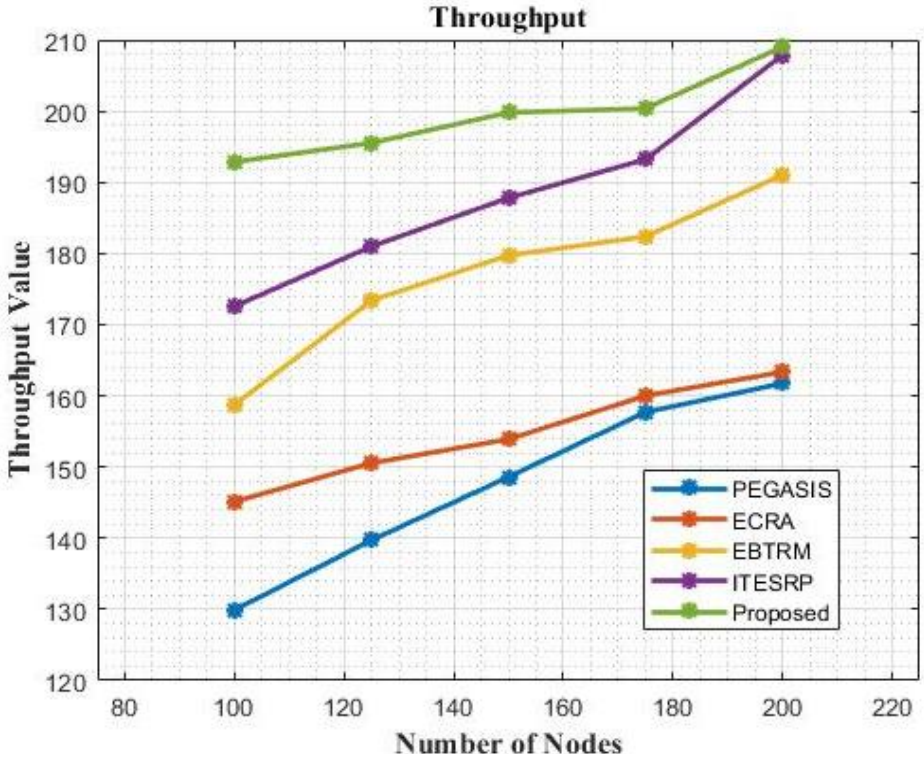

Fig. 7. Performance Graph for Throughput

Table- V: Comparison Table of Proposed Congestion Control Algorithm

	PDR%	Energy Consumption	Trust Value	Throughput	Energy Efficiency	Accuracy	End-to-End Delay	Reliability	Network Life Time
ETERS	84.32	-	-	-	-	96	-	-	-
SVM-AF	87.4	-	-	-	-	-	-	-	-
TASRP	90.9	-	-	-	-	-	-	-	-
PEGASIS	-	60.9	0.68	147.6	-	-	-	-	-
ECRA	-	53.06	0.75	154.1	-	-	-	-	-
EBTRM	-	39.9	0.84	177	-	-	-	-	-
ITESRP	-	25.16	0.93	188.4	-	-	-	-	-
FBCC	-	-	-	-	92.78	-	76.12	0.88	-
CDTMRLB	-	-	-	-	92.94	-	72.84	0.89	-
PPI	-	-	-	-	96.2	-	28.56	0.91	-
AWFCC	-	-	-	-	96.76	-	22.5	0.94	-
Lion Fuzzy Bee	-	-	-	-	-	94	-	-	99.51
Bat Fuzzy Bee	-	-	-	-	-	-	-	-	99.25
Proposed Method	96.48	16.9	0.97	199.7	97.52	97.2	16.7	0.95	99.65

Table 5 depicted the comparison table for a proposed method with the existing congestion control methods. The performance metrics are PDR, energy consumption, trust value, throughput, energy efficiency, accuracy, end-to-end delay, reliability, and network lifetime. Consequently, the results of this work is compared with the different existing methods, depicted in table 5, it demonstrates that the proposed method produces best values than the other methods, respectively.

The energy efficiency graph of the research is depicted in figure 7. It demonstrates that the energy efficiency of the proposed work is high, and it decreases when the time is increased. The suggested method outperforms other existing methods in terms of energy efficiency.

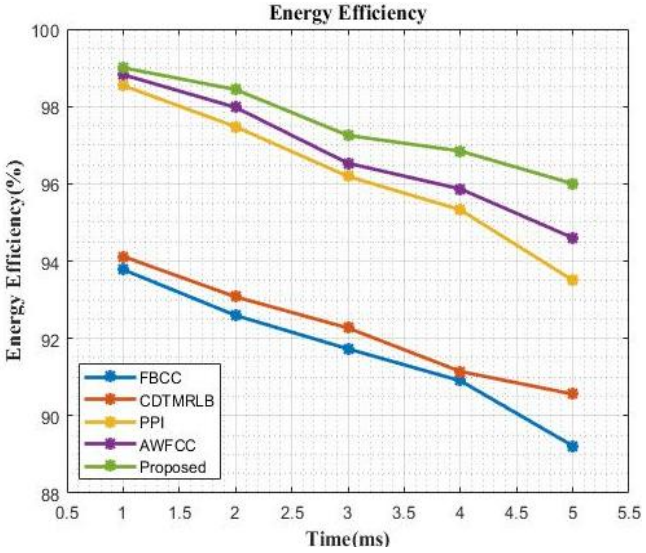

Fig. 7. Performance Graph of Energy Efficiency

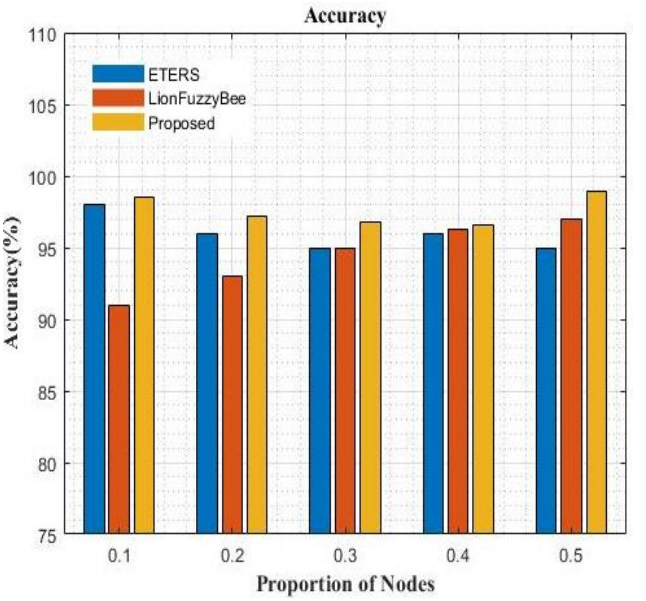

Fig. 8. Results for Accuracy

Figure 8 discloses the accuracy graph of the work. The presented work outperforms the other current methods, as shown in the above graph. ETERS and Lion Fuzzy Bee [29] are the compared methods. The proposed method's accuracy produces higher values than the other existing method. The end-to-end delay performance graph is shown in figure 9. It portrays that, the proposed method has a less delay value, and it increases the delay when the time (ms) increases. The performance of the proposed method is compared with the other existing methods, when compared to these; the proposed method has the best performance. The figure 10 illustrates the performance graph of reliability and it shows that the proposed method has a very high-reliability value. It depicted that the proposed method's reliability increases when time increases. The proposed approach is contrasted with the existing method, and when these two are compared, the proposed method performs at the highest level. The network lifetime performance graph is shown in figure 11. The new approach is contrasted with the existing Bat Fuzzy Bee [30] and Lion Fuzzy Bee approaches. The proposed method yields greater values when compared to the current method. Consequently, the proposed method gives the best performance than the other methods, respectively.

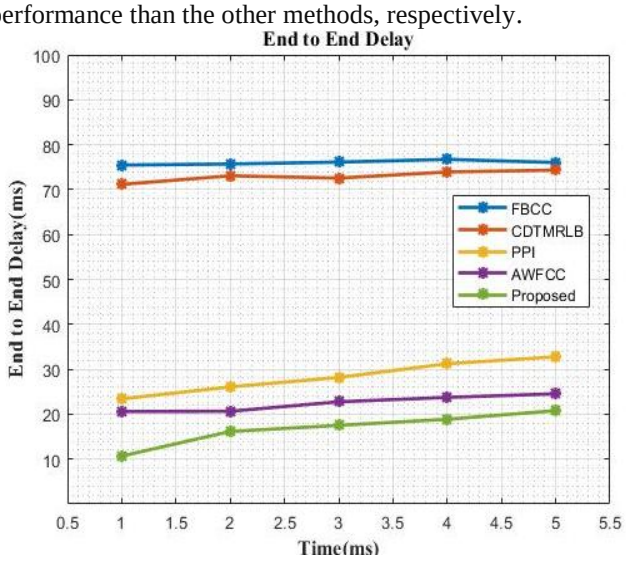

Fig. 9. End-to-End Delay Graph

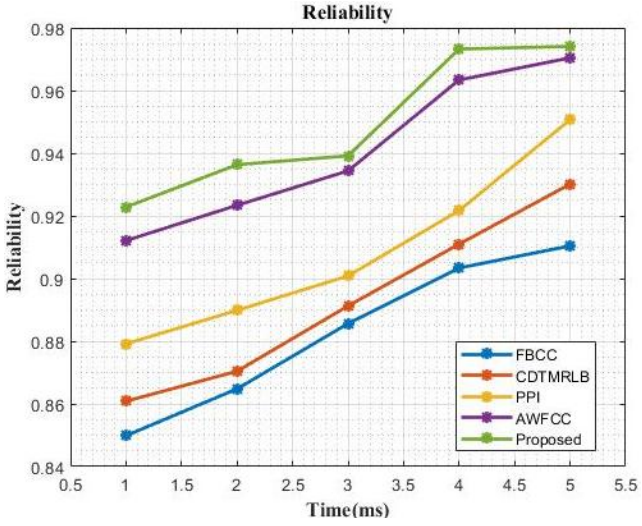

Fig. 10. Performance Graph for Reliability

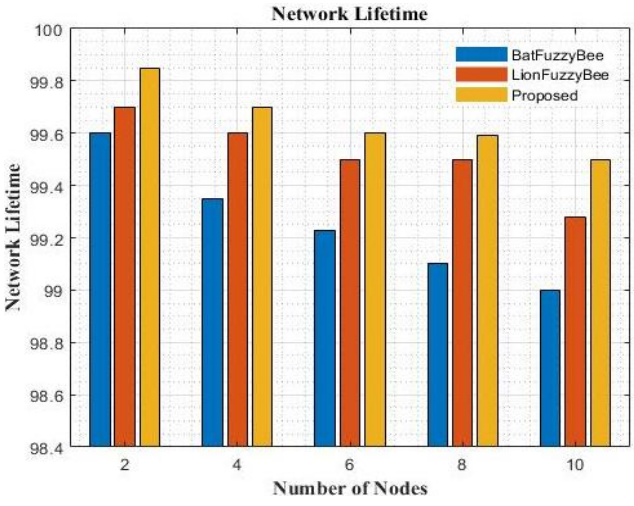

Fig. 11. Performance Graph for Network Life Time

VI. CONCLUSION

Congestion control is a crucial area of concern in WSNs. When the packets that are coming get increased then the actual capacity of the network or nodes results in congestion in the network. Congestion in the network can cause a reduction in throughput, an increase in network delay, and an increase in packet loss and sensor energy waste. As a result, an energy-efficient routing strategy is suggested in this study to reduce network congestion. An Adaptive Buffer trade-off and Improved Trust-based Protocol are introduced to identify several congestion-free paths and handle the buffer effectively. The network is then routed using a Cross-Layer Security-Based Fuzzy Logic Energy Efficient Packet Loss Preventive Routing Protocol. After routing the network, a DAOCA is introduced for network lifetime improvement. The proposed method is implemented using Matlab software.

- The performance metrics are Energy Consumption, Packet Delivery Ratio, Trust Value Computation, Average Throughput, latency, energy efficiency, end-to-end delay, reliability, accuracy and network lifetime.
- The results of the research work outperform the other existing methods, for PDR, the performance of the proposed method is nearly 3% higher.
- As a result, the suggested approach's end-to-end delay and energy consumption are respectively 5% and 8% greater than those of the existing methods. Accordingly, the proposed model produces less value than the other methods for delay and energy.
- The proposed method is 6%, 8%, 4%, 3%, 7%, and 2% higher than the existing methods for trust value, throughput, energy efficiency, accuracy, reliability, and network lifetime.

Therefore, this study showed that the suggested strategy outperforms the alternative methods and enhances congestion control and it also enhances the network performance and network lifetime. Subsequently, considering the Internet of Things environment, a recent advanced algorithm can be introduced in future, which will include more parameters like breakage or dynamic traffic load in the link to identify more optimal data routing path, it will avoid congestion in the network and it improves the network security, respectively.

REFERENCES

1. Srivastava, V., Tripathi, S., Singh, K. and Son, L.H., 2020. Energy efficient optimized rate-based congestion control routing in wireless sensor network. Journal of Ambient Intelligence and Humanized Computing, 11(3), pp.1325-1338. [CrossRef]
2. Qu, S., Zhao, L. and Xiong, Z., 2020. Cross-layer congestion control of wireless sensor networks based on fuzzy sliding mode control. Neural Computing and Applications, 32(17), pp.13505-13520. [CrossRef]
3. Sumathi, K. and Pandiaraja, P., 2020. Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks. Peer-to-Peer Networking and Applications, 13(6), pp.2001-2010. [CrossRef]
4. Masdari, M., 2020. Energy efficient clustering and congestion control in WSNs with mobile sinks. Wireless Personal Communications, 111(1), pp.611-642. [CrossRef]
5. Chappala, R.A.M.A.D.E.V.I., Anuradha, C. and Murthy, P.S., 2020. Adaptive alternative path and rate-based congestion control for 6LoWPAN, WSN towards internet of things. Indian Journal of Computer Science and Engineering, 11(5), pp.446-453. [CrossRef]
6. Letswamotse, B.B., Malekian, R., Chen, C.Y. and Modieginyane, K.M., 2018. Software defined wireless sensor networks and efficient congestion control. IET Networks, 7(6), pp.460-464. [CrossRef]
7. Osuo-Genseleke, M., Kabari, L. and Nathaniel, O., 2018. Performance measures for congestion control techniques in a wireless sensor network. International Journal of Scientific and Research Publications, 7, pp.1-5. [CrossRef]
8. Farahani, S.S.S. and Fakhimi Derakhshan, S., 2019. LMI-based congestion control algorithms for a delayed network. International Journal of Industrial Electronics Control and Optimization, 2(2), pp.91-98.
9. Singh, K., Singh, K. and Aziz, A., 2018. Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm. Computer Networks, 138, pp.90-107. [CrossRef]
10. Yang, X., Chen, X., Xia, R. and Qian, Z., 2018. Wireless sensor network congestion control based on standard particle swarm optimization and single neuron PID. Sensors, 18(4), p.1265. [CrossRef]
11. Najm, I.A., Hamoud, A.K., Lloret, J. and Bosch, I., 2019. Machine learning prediction approach to enhance congestion control in 5G IoT environment. Electronics, 8(6), p.607. [CrossRef]
12. Sharma, B., Srivastava, G. and Lin, J.C.W., 2020. A bidirectional congestion control transport protocol for the internet of drones. Computer Communications, 153, pp.102-116. [CrossRef]
13. Chowdhury, S. and Giri, C., 2018, December. Non-cooperative game theory-based congestion control in lossy WSN. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE. [CrossRef]
14. Lakshmi, M.S., 2021. An Adaptive Buffer tradeoff, energy-aware Congestion Control protocol in WSN. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), pp.4880-4891. [CrossRef]
15. Zhao, L., Qu, S., Huang, X. and Luo, J., 2019, June. Congestion control of wireless sensor networks using discrete sliding mode control. In 2019 Chinese Control and Decision Conference (CCDC) (pp. 2462-2466). IEEE. [CrossRef]
16. Prasanthi, B.G., 2021. Design of A Bio Based Approach for Congestion Control in Wireless Sensor Network.
17. Aimtongkham, P., Nguyen, T.G. and So-In, C., 2018. Congestion control and prediction schemes using Fuzzy logic system with adaptive membership function in wireless sensor networks. Wireless Communications and Mobile Computing, 2018. [CrossRef]
18. Zhuang, Y., Yu, L., Shen, H., Kolodzey, W., Iri, N., Caulfield, G. and He, S., 2018. Data collection with accuracy-aware congestion control in sensor networks. IEEE Transactions on Mobile Computing, 18(5), pp.1068-1082. [CrossRef]
19. Kalaikumar, K. and Baburaj, E., 2020. Fuzzy enabled congestion control by cross layer protocol utilizing OABC in WSN: Combining MAC, routing, non-similar clustering and efficient data delivery. Wireless Networks, 26(2), pp.1085-1103. [CrossRef]
20. Grover, A., Kumar, R.M., Angurala, M., Singh, M., Sheetal, A. and Maheswar, R., 2022. Rate aware congestion control mechanism for wireless sensor networks. Alexandria Engineering Journal, 61(6), pp.4765-4777. [CrossRef]
21. Yadav, S.L., Ujjwal, R.L., Kumar, S., Kaiwartya, O., Kumar, M. and Kashyap, P.K., 2021. Traffic and energy aware optimization for congestion control in next generation wireless sensor networks. Journal of Sensors, 2021. [CrossRef]
22. Tan, J., Liu, W., Wang, T., Zhang, S., Liu, A., Xie, M., Ma, M. and Zhao, M., 2019. An efficient information maximization based adaptive congestion control scheme in wireless sensor network. IEEE access, 7, pp.64878-64896. [CrossRef]
23. Li, S., Xu, Q., Gaber, J., Dou, Z. and Chen, J., 2020. Congestion control mechanism based on dual threshold DI-RED for WSNs. Wireless Personal Communications, 115(3), pp.2171-2195. [CrossRef]
24. Raman, C.J. and James, V., 2019. FCC: Fast congestion control scheme for wireless sensor networks using hybrid optimal routing algorithm. Cluster Computing, 22(5), pp.12701-12711. [CrossRef]
25. Royyan, M., Ramli, M.R., Lee, J.M. and Kim, D.S., 2018, June. Bio-inspired scheme for congestion control in wireless sensor networks. In 2018 14th IEEE international workshop on factory communication systems (WFCS) (pp. 1-4). IEEE. [CrossRef]

26. Khan, T., Singh, K., Hasan, M.H., Ahmad, K., Reddy, G.T., Mohan, S. and Ahmadian, A., 2021. ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. Future Generation Computer Systems, 125, pp.921-943. [CrossRef]
27. Kasthuribai, P.T., 2021. Optimized Support Vector Machine Based Congestion Control in Wireless Sensor Network Based Internet of Things. International Journal of Computer Networks and Applications, 8(4), pp.444-454. [CrossRef]
28. Khan, T. and Singh, K., 2021. TASRP: a trust aware secure routing protocol for wireless sensor networks. International Journal of Innovative Computing and Applications, 12(2-3), pp.108-122. [CrossRef]
29. Prasanthi, B.G., Energy Efficient Secure Hybrid Bio Inspired Congestion Control Mechanism in Wireless Sensor Network.
30. Prasanthi, B.G., Design of a Bio Based Approach for Congestion Control in Wireless Sensor Network.

AUTHORS PROFILE

Mr. S. Mohanarangan, obtained his fist post graduate M.S in Information Technology from Bharathidasan University and second post graduate M.Tech in Information Technology from Sathyabama University, Chennai. Currently pursuing his research studies at Anna University and his area of research interest is wireless networking. He is having 15 years of teaching experience in engineering field alone and presently working as Assistant Professor in the Department of Computer Science and Engineering at Arunai Engineering College, Tiruvannamalai.

Dr. D. Sivakumar, B.E., M.E., Ph.D., M.I.S.T.E., F.I.E.T.E., S.I.A.C.S.I.T completed his under graduation in Electronics and Communication from Madras University and Post graduation in Instrumentation from Annamalai University. He was awarded doctorate under the faculty of Information and Communication by Anna University, Chennai. He is having 20+ years of teaching and research experiences in various reputed engineering colleges in and around Tamil Nadu. Presently he is working as Professor in the Department of ECE at Easwari Engineering College, Chennai. He has guided more than 25 projects for UG and PG students.