ISSN 2723-6471

Trust Aware Congestion Control Mechanism for Wireless Sensor Network

G. Maria Priscilla[1,*], B.L. Shiva Kumar[2], Siti Sarah Maidin[3], Zainab S. Attarbashi[4]

[1,2]*Department of Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, India*

[3]*Centre for Data Science and Sustainable Technologies, Faculty of Data Science and Information Technology, INTI International University,71800 Nilai, Negeri Sembilan, Malaysia*

[4]*Kulliyyah of Information and Communication Technology (KICT), Malaysia*

(Received: November 18, 2024; Revised: December 15, 2024; Accepted: January 19, 2025; Available online: February 21, 2025)

Abstract

Congestion in wireless sensor networks (WSNs) can occur from various factors, including resource limitations and the transmission of packets surpassing the capacity of receiving nodes. This congestion may arise from natural causes or be exacerbated by self-serving nodes. Furthermore, malicious sensor nodes within WSNs have the capability to instigate congestion-like scenarios by either flooding the network with redundant fake packets or maliciously discarding genuine data packets. Relying solely on conventional congestion control techniques proves inadequate for ensuring fair delivery, necessitating a proactive approach to prevent such adversities by segregating these nodes from the network. Existing congestion control strategies often make the unrealistic assumption that all nodes are authentic and behave appropriately. To address these challenges, a proposed Genetic Algorithm based Trust-Aware Congestion Control (GA-TACC) not only manages congestion under natural circumstances but also considers scenarios where hostile nodes deliberately improve packet delivery. The GA evaluates the credibility score (CS), contributing to enhanced performance, and GA-TACC demonstrates superiority over existing state-of-the-art techniques for wireless sensor network.

Keywords: Blockchain Technology, Real Estate Transaction, Process Innovation

1. Introduction

The contemporary landscape of real estate transactions, despite the remarkable strides made in technology, remains plagued by sluggishness attributed primarily to the validation process. A key bottleneck in this system is the reliance on traditional paper-based documentation, wherein validation unfolds through manual procedures. The sheer volume of paper documents contributes to a high occurrence of errors that necessitate correction during the real estate registration process, rendering the entire transaction system slow and inefficient [1].

In response to the challenges posed by the existing real estate transaction system, blockchain technology has garnered increasing interest across various sectors [2]. Blockchain applications have permeated diverse domains, including digital payments, commercial registries, social media, insurances, public administration, and healthcare. Notably, the Government of Estonia has leveraged blockchain to secure health records, while the Singapore has launched a multi-year project named Project Ubin exploring the use of blockchain and its associated technology Distributed Ledger technology for payments and securities [3], [4].

The application of blockchain in real estate transactions has gained prominence due to its efficacy in addressing challenges associated with multiple stages and involving numerous participants, especially in processes like land registration [5]. Blockchain is recognized as a transformative solution capable of streamlining complex transactions and enhancing the overall efficiency of processes such as land registration.

Amidst the rise of cities and the bustling activities of buying and selling, commonly referred to as "real estate," this market has evolved into one of the most significant economic indicators in various countries [6]. The pivotal role

***Corresponding author: G. Maria Priscilla (mariapriscilla@srcas.ac.in)**
DOI: https://doi.org/10.47738/jads.v6i2.564

 ISSN 2723-6471

played by the real estate market highlights the urgency and importance of introducing innovations that can propel the industry into a new era of efficiency and transparency.

In alignment with the Sustainable Development Goals (SDGs) set forth by the United Nations, the incorporation of blockchain technology into real estate transactions offers potential for bolstering initiatives aimed at creating sustainable cities and communities (SDG 11) [7]. By promoting transparency, efficiency, and fair access to property rights, blockchain has the capacity to contribute significantly to these objectives. As the call for sustainable urban development intensifies, blockchain emerges as a powerful catalyst for driving positive transformations in the real estate sector, thereby advancing progress towards overarching global sustainability targets.

The congestion in Wireless Sensor Networks (WSN) is a significant obstacle that arises due to the limited resources and changing operating conditions of these networks. Congestion, which is marked by a substantial amount of data traffic, results in a decline in performance, heightened delay, and the loss of data packets. The restricted bandwidth of Wireless Sensor Networks (WSNs), combined with the energy limitations of sensor nodes powered by batteries, intensifies the influence of congestion on the effectiveness of the network. The difficulty of congestion management is influenced by factors like as the density of nodes, variations in data flow, and the presence of malfunctioning nodes [4]. Consequences of congestion encompass diminished capacity for data transmission, loss of energy, and degraded reliability. In order to tackle these difficulties, mitigating solutions such as adaptive routing protocols, data aggregation techniques, priority-based scheduling, traffic engineering, and energy-efficient protocols are utilized. The ongoing research in this topic seeks to create novel methods to efficiently control congestion in Wireless Sensor Networks (WSNs), guaranteeing their sustained dependability and efficiency across various applications.

Efficiently controlling data traffic and guaranteeing the smooth operation of the network are crucial aspects of congestion control in WSN. Effective congestion control is crucial in WSNs due to their limited resources, such as energy and bandwidth, which the sensor nodes run on. This entails the implementation of adaptive algorithms and protocols that dynamically regulate the data flow to avert network overload and mitigate performance degradation. Dynamic routing systems, which adapt data pathways according to real-time network conditions, aid in the equitable distribution of traffic and the mitigation of congestion hotspots [5]. Furthermore, data aggregation procedures are utilized to decrease the amount of data being transmitted, hence lowering the likelihood of congestion. WSNs commonly utilize priority-based scheduling to prioritize vital data or tasks, hence optimizing the utilization of resources [6]. The primary objective of congestion control in WSNs is to optimize network dependability, minimize latency, and prolong the operational longevity of sensor nodes by effectively managing the available resources within the network's limitations. Current research in this field is focused on developing new methods to tackle congestion issues that are specific to the distinct features of Wireless Sensor Networks [7], [8], [9], [10].

The introduction of WSNs has drastically transformed the process of collecting data in various fields, including environmental monitoring and industrial automation [11]. Nevertheless, the effective functioning of WSNs is sometimes hindered by problems like congestion, which can greatly affect the performance and dependability of the network [12]. To address these difficulties, researchers have investigated novel congestion control strategies to maximize data transmission in WSNs. An example of a promising strategy is the creation of a Trust Aware Congestion Control Mechanism [13]. This mechanism incorporates the notion of reliability into congestion control algorithms, with the goal of improving the overall efficiency and robustness of the network. This approach aims to dynamically regulate data flow, reduce congestion, and guarantee the secure and dependable functioning of wireless sensor networks in various application scenarios by incorporating trust metrics into the decision-making process [14]. This introduction provides a foundation for a more thorough examination of the Trust Aware Congestion Control Mechanism, emphasizing its ability to tackle significant obstacles and contribute to the progress of reliable and dependable wireless sensor networks [15], [16].

WSNs are important for areas such as environment monitoring and smart city, where the importance of effective data transmission cannot be underestimated. However, congestion can be caused by resource constraint, high packet transmission rate, and existence of malicious node. Traditional flow control processes usually always presume cooperation, which is seldom the case. This gap means that there is a need for new approaches to solving congestion problems whether they are natural or adversarial. To address this need, the new congestion control design, known as

ISSN 2723-6471

the Genetic Algorithm-based Trust-Aware Congestion Control (GA-TACC), includes trust evaluation mechanisms in its congestion management design. Due to the credibility assessment of the sensor nodes, GA-TACC is capable of recognizing and excluding the miscreants thus facilitating fair data transmission. It also helps to improve the performance of the whole network and contribute to the development of the more reliable system of communication. Lastly, GA-TACC aims at enhancing the performance of WSN which is a problem that requires efficient congestion control mechanism that can work effectively in different environment in real world.

2. Literature Review

In the study by Reddy et al. [15], the authors introduced a novel approach called Glowworm Swarm Optimization integrated with Ant Colony Optimization (GSO-ACO) to address the optimization of Cluster Head (CH) nodes in WSNs. The primary objective was to reduce the distance between CH nodes. The proposed algorithm incorporates multiple objectives, including distance, delay, and energy, to formulate a comprehensive fitness function. Through performance evaluation, the researchers observed an improvement in efficiency, indicating the effectiveness of the GSO-ACO approach in optimizing CH nodes within WSNs.

In a related work by Devershi Pallavi Bhatt et al. [17], the authors presented an optimized route selection technique utilizing the Cuckoo Search Algorithm (CSA) for wireless sensor networks. Recognizing the critical need for energy conservation in WSNs, the study aimed to contribute a cluster-based routing mechanism focused on preserving energy. The proposed technique relies on a clustering methodology and an optimized route selection process. Sensor nodes are organized into clusters, and the Cluster Head (CH) is strategically chosen based on the nodes' level of trust. The overall goal is to enhance energy efficiency in WSNs through intelligent route selection, contributing to the advancement of energy-preserving mechanisms in the context of wireless sensor networks.

Motivation is the underlying drive that propels us towards \ goals and promotes personal and professional development. The inner drive motivates individuals to conquer obstacles, strive for greatness, and welcome fresh possibilities. The presence of motivation is of utmost importance in both personal and professional domains, as it significantly impacts ability to persist, generate innovative ideas, and bounce back from setbacks. Highly motivated workers in the workplace exhibit increased productivity, innovation, and dedication towards accomplishing corporate goals. At an individual level, motivation enables people to establish and achieve significant objectives, encompassing areas such as health, education, relationships, and personal growth. It supplies the necessary energy to confront challenges, derive lessons from failures, and consistently pursue enhancement. Gaining insight into and effectively utilizing motivation not only improves personal satisfaction but also fosters a favorable and energetic atmosphere across multiple domains of life.

3. Proposed Methodology

3.1. Genetic Algorithm based Trust-Aware Congestion Control (GA-TACC)

In the area of WSNs three major concerns are Security, Energy Efficiency and, Congestion free packet delivery. In the proposed technique efforts has been made to incorporate above mentioned three major research issues conjointly in order to ensure reliable packet delivery. The security aspect has been addressed by implementing a trust-based method for credibility score (CS) calculation of each node in the network. Credibility score degree of trustworthiness of one node on another with respect to packet transmission. In this way, CS value serves as a determining factor between legitimate and malicious nodes. As a result, spiteful nodes will never get a chance to participate in the communication process and would not affect the system negatively. For minimizing the energy consumption clustering method has been applied. The value of clustering lies in the fact that it allows network traffic to be localized and long-distance transmissions are avoided. Thus, the clustering method is being used to reduce energy consumption during communication.

It is possible for internal attacks to cause congestion on sensor nodes or it can occur naturally, and the consequences can be severe. Therefore, instead of using a reactive method to prevent congestion, applied the proactive approach. In reactive method it is assumed that congestion is obvious and its occurrence cannot be omitted. So, method is applied to reduce its consequences. Whereas, proactive method tries to preclude any misfortune beforehand. In the literature researchers have used probability-based cluster head selection or they have considered remaining energy of nodes as a

 ISSN 2723-6471

criterion to select cluster head in each round of communication. That means node having maximum remaining energy is most suitable for transmission. It is a logical approach because ultimately main motive is energy efficient transmission and network lifetime enhancement. But they have not focused on their congestion status which tells whether the node is in state to receive packets or not. It is believed that it is an important factor that should be taken care of while electing cluster heads because even if a node has sufficient energy but it has not enough room to receive upcoming packets then it has no other option than dropping it. So, for this purpose along with energy factor buffer occupancy is incorporated of the node for measuring congestion status. The packet delivery ratio (PDR) is considered as a trust metric because there can be a case where malicious nodes whose only motive is to drop the packets so these types of nodes will have very low PDR and this low value will also be reflected in respective credibility score calculation.

3.2. Credibility Score (CS) Evaluation

In the realm of genetic algorithms, the integration of a CS introduces a novel dimension to the assessment of individuals within the evolving population. This score serves as a measure of trustworthiness, gauging the reliability of potential solutions based on various performance metrics. Factors such as fitness value, convergence stability, diversity maintenance, historical performance, and adaptability contribute to the calculation of the Credibility Score. Individuals exhibiting superior fitness, stability in convergence, and a capacity to maintain genetic diversity receive higher credibility scores, reflecting their reliability in addressing the optimization problem. As the genetic algorithm progresses through successive generations, individuals with elevated credibility scores are prioritized for reproduction, mimicking the principles of natural selection. The introduction of a Credibility Score aims to enhance the overall quality and trustworthiness of the evolving population, fostering the emergence of robust and dependable solutions to complex optimization challenges. Customization of the scoring mechanism ensures alignment with specific application requirements, making this integration a valuable tool for optimizing genetic algorithm performance.

The network status in WSNs varies dynamically. A genuine node can be compromised at any time, and the quality of a link varies due to the occurrence of events. As a result, the credibility score of sensor nodes must alter dynamically in order to accurately reflect the network's condition. In this section credibility of the nodes is calculated and parameters are been considered. The justification is also given for the chosen network parameter. The proposed method uses buffer occupancy, residual energy, and packet delivery ratio as metrics for calculating congestion status bit, energy trust, and communication trust respectively, which are combined to yield a credibility score. Congestion status bit is taken because most of the security attacks directly impacts network congestion which adversely affect network. So, objective is to select cluster head which is least congested. Residual energy of the node has been considered because cluster head is responsible for successful packet delivery to the base station that is why it requires significant energy for this role. Therefore, node with maximum remaining energy should be selected as a cluster head otherwise due to lack of energy the whole cluster will be paralyzed. Packet delivery ratio (PDR) gives insight about packet receiving and transmitting behavior of nodes [19]. So, this parameter is also taken for evaluation of CS. So, function of credibility score depends upon three following parameters.

$$f(CS(n_j, t) = w_b * f\left(CSB(n_j, t)\right) + w_b * f\left(ET(n_j, t)\right) + w_b * f\left(CT(n_j, t)\right) \quad (1)$$

$f(CS(n_j, t)$ represents credibility score of a node nj at time t. CSB refers to congestion status bit, ET is energy trust and CT is communication trust. The detailed description of above-mentioned metrics is given in the following subsection. wb, we, wc are the weight coefficients where wb + we + wc = 1. How to select and prioritize the weights has also been elaborated in subsequent section.

3.3. Congestion Status bit (CSB)

The susceptibility of WSNs to network congestion due to their characteristics, such as numerous-to-one transmission, multi-hop forwarding, and centralized data acquisition. These features make WSNs prone to congestion, which can be exacerbated by intentional actions of malicious nodes. The consequences of network congestion include a higher likelihood of packet drops and increased data transmission delays, both of which can significantly impact the overall performance of the network. To address the challenge of network congestion in WSNs, the text proposes the use of a queueing model to accurately assess the congestion level of individual nodes. Given that sensor nodes typically employ

 ISSN 2723-6471

microcontrollers with limited storage capacity as processing units, packets are processed sequentially. This sequential processing means that a node's acquisition data, as well as packets forwarded by its neighboring nodes, enter the node's queue.

In essence, the proposed solution involves employing a queueing model to manage and assess the congestion level of sensor nodes in wireless sensor networks. By addressing congestion, the aim is to mitigate issues related to packet drops and transmission delays, ultimately enhancing the overall performance and reliability of the network. The text highlights the unique challenges posed by the characteristics of WSNs and emphasizes the importance of managing congestion to ensure efficient data transmission in such networks [20]. The packet generating rate of node j is μ_j^{α} . The packet forwarding rate of node j's neighbor node n is μ_{nj}^{β} . The packet arrival rate of node j can then be expressed as:

$$\mu_j = \mu_j^a + \sum_{i=1} \quad \mu_{i,j}^{\beta} \tag{2}$$

Whenever packets arrive at a node's forwarding capacity, the node buffer space will be nearly full. There is a possibility of packets getting lost if other nodes are simultaneously forwarding data to it as there is no space left to accommodate them. In this case, the node gets congested. Thus, the implementation of the congestion status bit is used to evaluate the node's ability to route data packets. A congestion status bit simply indicates how much buffer space the node has to store incoming packets or, in simpler terms, how ready it is to receive upcoming packets. To standardize the buffer space measurement, the employed min-max normalization, ensuring that the Computed Buffer Space (CSB) value ranges between 0 and 1. A CSB value of 1 or close to 1 signifies that a node possesses sufficient buffer capacity to accommodate incoming packets. Conversely, a CSB value of 0 indicates that the buffer is entirely full, leaving no space for additional packets. Nodes with a CSB of 0 are deemed unsuitable for further packet transmission.

All nodes start with an initial buffer capacity of 50 packets. Additionally, the established two threshold values, q_min and q_max, representing the lower and upper limits of buffer space, respectively, within the overall buffer size range. If current buffer space of a node is greater than or equal to the q max threshold value, it is considered as ideal load state, and this node would have high CSB value. Whereas a node having buffer space less than the q min value, it is the case of heavy load state indicating this node is not suitable for transmission for this round of communication. And a node with buffer space lying between the q max and q min are considered as safe load state. CSB has been calculated by the following equation

$$f\left(CSB(n_j,t)\right) = \begin{cases} \in, if\ buffer \leq q\_min \\ 1, elsif\ buffer\ \geq q\_max \\ (1-\in) * \left[\frac{(Buffer-q_{\min})}{(q_{max}-q\_min}\right] + \in\ otherwise \end{cases} \tag{3}$$

3.4. Energy Trust

The node's energy consumption is proportional to the quantity of data to be transferred and the distance to be travelled. In a network, with all the genuine nodes, under normal operation the energy consumption rate is always steady. Malicious nodes engaging in DoS attacks exhibit higher energy expenditure compared to regular nodes. Consequently, the energy consumption rate (ECR) is incorporated as a parameter to calculate the energy trust. This is accomplished using the following equation:

$$\mathrm{E_{consumption}}(\mathrm{n_i},\mathrm{t}) = \mathrm{E_{trans}^{n_j}} + \mathrm{E_{recep}^{n_j}} + \mathrm{E_{dataaggr}^{n_j}} + \sum_{i=1}^{adjnodes} \left[\mathrm{E_{overhearing}^{n_i}}\right] \tag{4}$$

$$\mathrm{E_{residualenergy}}(\mathrm{n_i},\mathrm{t}) = \mathrm{E_0} - \mathrm{E_{consumption}}(\mathrm{n_i},\mathrm{t}) \tag{5}$$

$$\mathrm{ECR} = \frac{\mathrm{E_{residualenergy}}(\mathrm{n_i},\mathrm{t}) - \mathrm{E_{residualenergy}}(\mathrm{n_i}(,\mathrm{t}-\delta\mathrm{t}))}{(\delta\mathrm{t})} \tag{6}$$

here Eresidualenergy($n_i(,t-\delta t)$)represents residual energy of a particular node nj at $(,t-\delta t)$ time and $E_{residualenergy}(n_i,t)$ indicates residual energy of the same node at time t. To analyse the behaviour of a node in terms of energy consumption, two threshold values E min and E max have been taken. When malicious nodes carry out attacks such as flooding and denial of service, or a node purposefully remains idle for a long period of time, the ECR value will behave abnormally. Such nodes will have ECR value greater than the E max threshold and less than the E

min threshold respectively. Nodes that have ECR values that fall between the two threshold values are considered to be in the safe zone means they behave normally. So, with the help of ECR, energy trust has been calculated by the following equation

$$f\left(ET(n_j,t)\right)=\begin{cases}\zeta, \\ (1-\zeta)*\left[\frac{(ECR-E\_min}{(E_{max}-E\_min)}\right]+\zeta\end{cases} \quad (7)$$
$$else\ if\ ECR\ \leq E\_\min\ ||ECR\geq E\_max$$

3.5. Communication Trust

The assessment of communication trust is contingent upon the packet delivery ratio (PDR) metric, which is a crucial aspect in appraising the efficacy of network communication. This parameter has a dual purpose: evaluating the network's communication mechanism and detecting rogue nodes. A PDR value close to 1 implies successful transmission of all sent packets, whereas a PDR of zero indicates a total failure to transfer any packets. This statistic is extremely important for detecting various types of assaults, including blackhole and greyhole attacks.

$$\mathrm{PDR}_{\mathrm{n_i}}^{\mathrm{n_j}}(\mathrm{t1},\mathrm{t2})=\frac{\mathrm{Trans}_{\mathrm{pkt}_{\mathrm{ni}}^{\mathrm{nj}}(\mathrm{t1},\mathrm{t2})}}{\mathrm{Rec}_{\mathrm{pkt}_{\mathrm{ni}}^{\mathrm{nj}}(\mathrm{t1},\mathrm{t2})}} \quad (8)$$

Trans_$pkt_{ni}^{nj}(t1,t2)$ = Total number of packets delivered successfully from node i to node j in time interval t1 and t2. Rec_$pkt_{ni}^{nj}(t1,t2)$= Total number of packets received from node ni to node nj in time interval t1 and t2. Expected behaviour of the node or PDR can be calculated using beta distribution function. So, the computed Communication Trust of node i to j at time interval (t1, t2) CTj i (t1, t2) is as follows

$$\mathrm{f}\left(\mathrm{CT}(\mathrm{n_j},\mathrm{n_i},\mathrm{t})\right)=\mathrm{E}\left(\mathrm{Beta}\left(\mathrm{cint}_{\mathrm{n_i}}^{\mathrm{n_j}},\mathrm{nint}_{\mathrm{n_i}}^{\mathrm{n_j}}\right)\right)=\frac{\mathrm{cint}_{\mathrm{n_i}}^{\mathrm{n_j}}+1}{\mathrm{cint}_{\mathrm{n_i}}^{\mathrm{n_j}}+\alpha\mathrm{nint}_{\mathrm{n_i}}^{\mathrm{n_j}}+2} \quad (9)$$

where $cint_{n_i}^{n_j}$, $nint_{n_i}^{n_j}$ denotes number of cooperative interaction and non-cooperative interaction between node ni and nj. Cooperation is measured by the proportion of successfully received packets out of the total communicated packets, and non-cooperation is indicated by the proportion of dropped packets out of the transmitted packets. On the other hand, the original trust evaluation model based on Beta does not take into account external factors that influence node interactions, such as packet loss caused by network congestion. This work improves upon the previous model by incorporating an external attenuation factor α to specifically address this concern. The variable α denotes the ratio of non-cooperation caused by malicious nodes to the total non-cooperative interactions. By introducing this attenuation factor, the observed non-cooperation can be reduced from node i to j and lessen the impact of external influences on the evaluation of credibility scores. As a result, the trust evaluation accuracy is improved compared to the original model.

3.6. Recommendation Score

In calculating the trust score, it is not restricted merely to ourselves seeing direct interactions between nodes. In addition, the recommendation score is integrated. The complete credibility score, which is the final score used in the process of isolating malicious nodes and selecting cluster heads, is derived from the combination of these two ratings. In this proposed technique once the cluster heads (CHs) are selected, remaining nodes of clusters are known as its members. CH give recommendation score to its members based on their communication behavior with the help of common neighbors. In the literature authors have named this value as indirect trust or recommendation trust. The calculation of direct trust of node i to j they calculated their indirect trust from the common neighbors (B1, B2, B3, B4 and B5) of node i and j as shown in figure 1b. In this technique cluster head will do the same calculations as it is common neighbor of all its member nodes since they can directly forward their data to corresponding CH. This scenario has been shown in figure 1a. Thus, this technique reduces the overhead of indirect trust calculations for the node with less energy left over. 0.5 is taken as the initial recommendation score in the simulation. Cluster head derives recommendation score by averaging the assessment of credibility score given to a particular node by the nodes that share common neighbors by following equation.

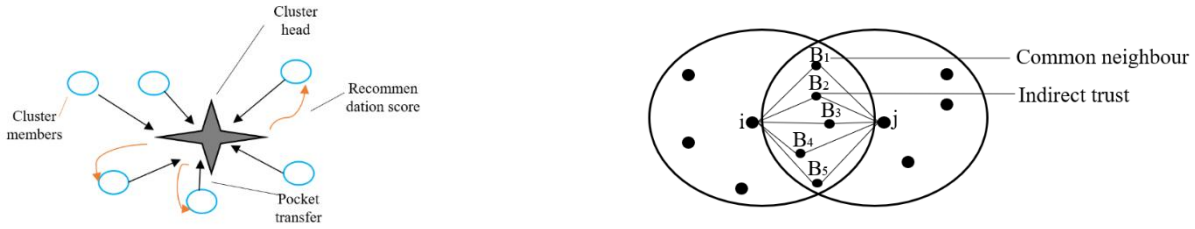
 ISSN 2723-6471

$$RS(n_j, t) = \frac{\sum_{i=1}^{k} CS(n_b \backslash n_j)}{K} \quad (10)$$

Here $RS(n_j, t)$ represents recommendation score for node nj by neighbor nodes nb and K represents the total number of recommendations made to the node nj . After determining the recommendation score, the cluster head also ensures that the value obtained is consistent. This is accomplished by calculating the deviation between the recommendation score and the corresponding credibility score using the equation below.

$$\sigma(CS\ RS)^{n_j} = \sqrt{\frac{1}{K-1}\sum_{i=1}^{k} RS(n_b \backslash n_j) - CS(n_j))^2} \quad (11)$$

High deviation indicates that there is a lot of variances in the observed data. This may happen because of opportunistic behavior of malicious nodes which perform well for some specific nodes and shows their selfish behavior on some sorts of nodes and there can be badmouthing attack also that intend to give wrong information about neighbor nodes. So, deviation value $\sigma(CS\ RS)^{n_j}$ helps to find out these cases. In this technique, deviation threshold (DEV T H) variable has been set in order to check the variations between credibility score and recommendation score of a particular node. This assumption is that a higher value of sigma is due to the malicious events. Therefore, as seen in figure 1, Cluster head sends the recommendation score table containing RS value of its member nodes along with its deviation threshold and deviation value to the base station as a ⟨ RECOMMEND SCORE ⟩ message.



(a) RS calculation in this technique (b) RS calculation in previous techniques

Figure 1. Recommendation Trust Calculation

Format of recommendation score table (RS table). Sink will nullify the recommendation score of a node whose deviation value exceeds the deviation threshold and penalizes the node by reducing its credibility score. If the deviation value is less than the threshold value, it means that the data observed is clustered tightly around the mean and recommendation score is consistent and can be considered for comprehensive credibility score calculation and node is rewarded by increasing its credibility score.

3.7. Comprehensive Credibility Score

To get more authentic results relying only on credibility score calculated by two peer to peer communicating node is not sufficient. So, in order to get CCS, recommendation score computed by cluster head for its cluster members has also been considered. Once the sink node receives recommendation score information through RS table shared by the cluster head, it checks for its consistency. If it finds out that deviation value is higher than the threshold, then recommendation score parameter gets nullified by assigning zero weight to it so that comprehensive credibility score of a node won't be affected. Sink node also penalizes this node by reducing its credibility score by following equation:

$$CS(n_j) = CS + (1 - CS) * \rho_+ \quad (12)$$

whereas, when deviation value is low and less than the threshold, it is assumed that node is genuine and it gets rewarded by increasing its credibility score as shown in equation below:

$$CS(n_j) = CS - CS * \rho_- \quad (13)$$

In the above equation ρ+ and ρ− refers to positive update and negative update parameter respectively. past credibility score has also been taken into account as it gives idea about how the node has performed previously. So, this aspect helps to counter on-off attacks. In this way, CCS value of a node nj is calculated as follows by combining the present and past credibility score along with recommendation score.

 ISSN 2723-6471

$$f(CCS\left(\left(n_j,t\right)\right)=\lambda f(CS\left(\left(n_j,t-\delta t\right)\right)+\lambda f(CS\left(\left(n_j,t\right)\right)+\psi f(RS\left(n_j,t\right) \quad (14)$$

λ, γ and ψ are weight coefficients and $\lambda + \gamma + \psi = 1$. The entire mechanism is given in Algorithm 1.

Algorithm 1. Genetic Algorithm based Trust-Aware Congestion Control (GA-TACC)

Initialize network parameters (buffer capacity, energy thresholds, initial node energy, buffer).
FOR each communication round:
  FOR each node n:
    Calculate Congestion Status Bit (CSB):
      IF buffer >= q_max THEN CSB = 1
      ELSE IF buffer < q_min THEN CSB = 0
      ELSE normalize CSB.
    Calculate Energy Trust (ET):
      Compute residual energy (E_residualenergy) and energy consumption rate (ECR).
      IF E_min ≤ ECR ≤ E_max THEN ET = 1 ELSE ET = 0.
    Calculate Communication Trust (CT):
      Calculate Packet Delivery Ratio (PDR).
      IF PDR = 1 THEN CT = 1 ELSE normalize CT.
    Calculate Credibility Score (CS) = f(CSB, ET, CT).
  Select cluster heads based on highest CS and form clusters.
  FOR each cluster head:
    Update CS and buffer for congestion detection.
    IF congestion is detected THEN mark node as unsuitable ELSE forward packets.
    Calculate Recommendation Score (RS) using neighbor recommendations.
    Compute deviation between CS and RS.
    IF deviation > threshold THEN penalize node ELSE reward node.
    Send RS to sink node.
    *Calculate Comprehensive Credibility Score (CCS) = λ * past CS + γ * current CS + ψ * RS.*
Repeat until network operation ends.

4. Results and Discussion

In this section, the simulation of the GA-TACC (Genetic Algorithm based Trust-Aware Clustering and Communication) approach is examined using Network Simulator 2 (NS2). The evaluation of GA-TACC involves assessing its performance using key metrics, including Packet Delivery Ratio (PDR), throughput, and delay. To establish the effectiveness of GA-TACC, a comparative analysis is conducted against state-of-the-art techniques, specifically GSO-ACO, and CSA. The simulation setup details are provided in table 1, outlining the parameters and configurations used in the experiments. The ensuing sub-section presents a thorough comparative analysis, allowing for the identification of the superior performance of the proposed GA-TACC approach in relation to the existing techniques, thereby contributing insights into its potential advantages and advancements in the field of clustering and communication in wireless networks.

Table 1. Simulation Setup

Parameter	Description
Sensor Node Count	500
Simulation Area Size	100*100 m2
Packet Size	512 bytes
Time Slot	2000 s
Range of Communication	20m
Initial Energy	1J

 ISSN 2723-6471

4.1. End to End Delay

Even when there are "N" automobiles in the area (i.e., a lane with sample count "C"), sampling determines the likelihood of detection. Therefore, the estimated count, E(C), equals Np, where Np is the total number of cars and the corresponding probability. The evaluation and decision-making process for the vehicles and persons in the various lanes varies and is based on probability. Table 2 show the comparison between each vehicle node.

$$DE(end-end) = N[DE(tr) + DE(prop) + DE(process) + DE(qu)] \quad (15)$$

DE (end - end) = end-to-end delay, DE (tr) = Vehicle transmission delay, DE (prop) = Vehicle propagation delay in particular platoon, DE (process) = Vehicle feedback processing delay, DE (qu) = Queuing delay.

Table 2. Comparison of end-to-end delay

Algorithm/ Vehicle Node	Existing Technique		Proposed Technique
	GSO-ACO	CSA	GA-TACC
200	654	718	556
300	687	734	562
400	726	756	571
500	751	779	591
600	783	812	693

The end-to-end delay (DE) is a crucial measurement in vehicular networks, comprising many elements such as the delay in transmitting data between vehicles, the delay caused by the signal propagating through a specific group of vehicles, the delay in processing feedback from vehicles, and the delay caused by queuing. The assessment takes into account a situation involving "N" vehicles in the vicinity, and the estimated count E(C) is calculated by multiplying the total number of cars (N) with the associated probability (p). The text gives a comprehensive analysis of the many factors contributing to the end-to-end delay. It includes a comparison table (Table 2) and a graph (Figure 2) that display the end-to-end delay values for different algorithms and vehicle nodes.

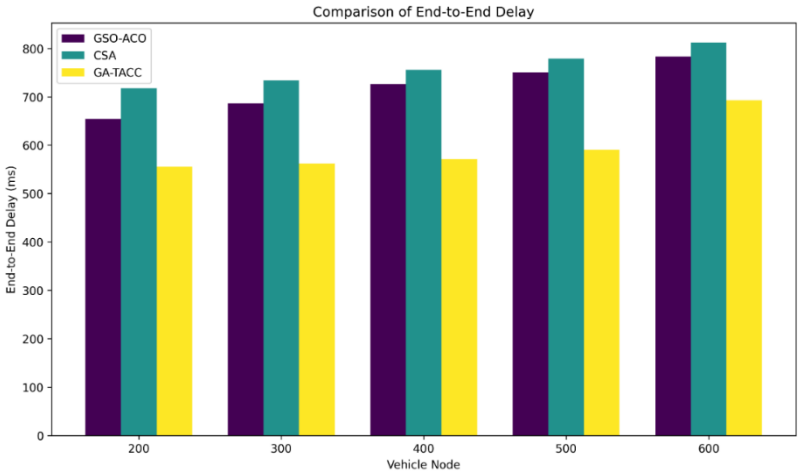


Figure 2. Comparison of end-to-end delay

4.2. Throughput

By adding up all the data that is being sent to the platoon leaders in a certain platoon, the throughput is determined. It uses the data arrival rate and exit rate to quantitatively determine the bandwidth use. The term "throughput" referred to the quantity of packets carried by the vehicles via the network for a specific period of time. To determine the amount of effort required for a link between two nodes, the total number of packets that have been successfully delivered to the desired nodes is determined. Throughput, which measures the number of packets transported by vehicles throughout the network over a certain time frame, is evaluated by considering the rates at which data arrives and leaves.

 ISSN 2723-6471

The throughput computation takes into account the aggregate number of packets that have been successfully transmitted to the intended nodes. The article contains a comparison table (Table 3) and a graph (Figure 3) that demonstrate the throughput values of various algorithms and vehicle nodes. These visual aids emphasize the higher performance of the proposed GA-TACC method.

Table 3. Comparison of Throughput

Algorithm/ Vehicle Node	Existing Technique		Proposed Technique
	GSO-ACO	CSA	GA-TACC
200	659	556	769
300	697	567	739
400	716	576	756
500	756	596	779
600	793	693	967

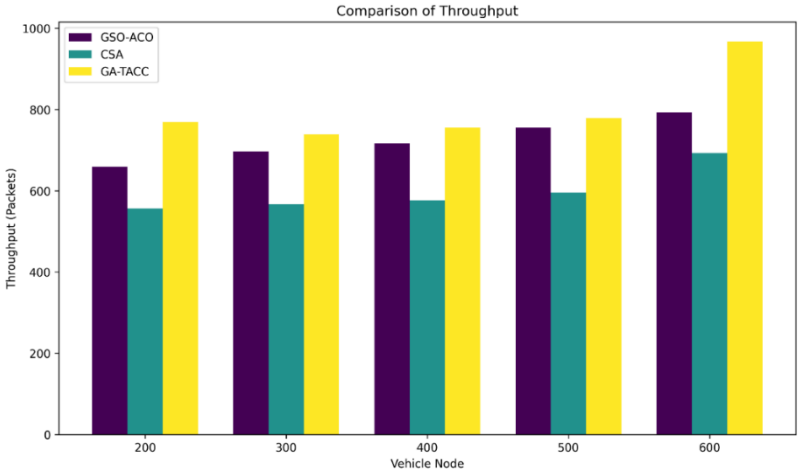


Figure 3. Comparison of Throughput

4.3. Packet Delivery Ratio

The ratio of data arriving at sink nodes to all data forwarded by sensor nodes is known as PDR. PDR is used to calculate the data drop rate. A network with a higher PDR is referred to as the best transmission network. The PDR calculation is as follows:

$$\text{PDR} = \frac{\text{Recd}_\text{p}}{\text{Snd}_\text{p}} \tag{16}$$

Recdp is Received Packets by sink node and Sndp is Sent Packets by vehicle nodes.

The PDR, or Packet Delivery Ratio, is a quantitative measure that represents the proportion of data received by sink nodes compared to the total amount of data transmitted by sensor nodes. The Packet Delivery Ratio (PDR) is a critical metric for assessing network efficiency, where a higher PDR signifies a more efficient transmission network. The text includes a formula for calculating PDR and shows a comparison table (Table 4) and a graph (Figure 4) showing PDR values for various algorithms and vehicle nodes. The suggested Genetic Algorithm-based Traffic-Aware Congestion Control regularly exhibits higher Packet Delivery Ratio (PDR) values in comparison to existing strategies, hence suggesting enhanced efficiency in data delivery.

Table 4. Comparison of PDR

Algorithm/ Vehicle Node	Existing Technique		Proposed Technique
	GSO-ACO	CSA	GA-TACC
200	89	87	91
300	91	87.5	93

ISSN 2723-6471

400	92	90	95
500	92.5	91	96
600	93	92	97

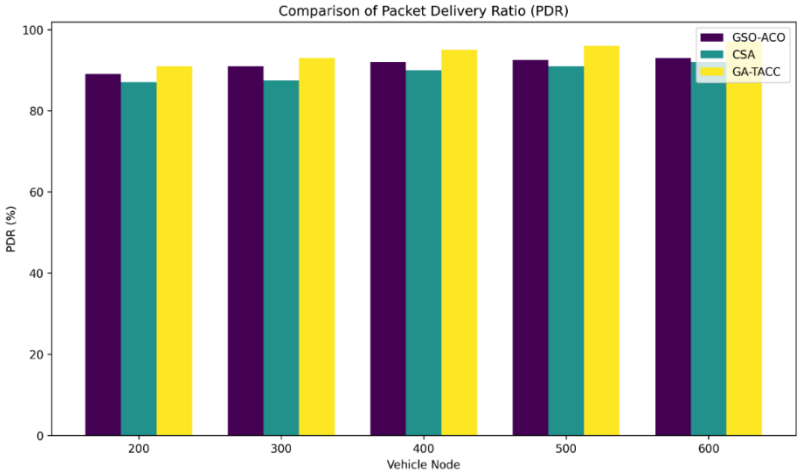


Figure 4. Comparison of PDR

The End-to-End Delay (DE) gives the overall time taken by a packet to travel from a source vehicle node to destination node in VANET. Some of these are the transmission delay (DE (tr), propagation delay (DE (prop)), feedback processing delay (DE (process)) and queuing delay (DE (qu)). These components are utilized jointly for computing the end-to-end delay for various congestion control algorithms such as GSO-ACO, CSA, GA-TACC as shown in table 2. For instance, with 200 vehicles the GA-TACC algorism has 556 ms of delay while 654 of delay were obtained by GSO-ACO, and 718 by CSA. This trend goes on as the number of vehicles in the transport system continues to rise. When there are 600 vehicles GA-TACC has the end-to-end delay of 693ms which is much less than 783ms of GSO-ACO and 812ms of CSA. This steady decrease in delay with the GA-TACC model indicates that the proposed model can better cope with higher density of vehicles and resulting congestion delay.

Lower end-to-end delay is possible in GA-TACC than in other conventional TACC techniques because GA-TACC involves trust-awareness for node selection that results to optimum periodic vehicle communication and thereby reduces chances of retransmission. This minimizes the queue approvals and processing which increases the efficiency of packet delivery and the networks performance in general. The fact that congestion control incorporates the use of a Genetic Algorithm (GA) in congestion control enables the reduction of delay since the load in the network is well distributed. Analyzing the numerical data presented in the Table 2, we can conclude that GA-TACC has a slightly better performance than CSA and significantly better than GSO-ACO in terms of delay for approximately 10-15% which make GA-TACC the best algorithm to reduce the end-to-end delay especially with the increase of traffic.

The metrics mentioned contribute to evaluating the proposed GA-TACC approach in automotive networks. These metrics demonstrate the potential advantages of this approach compared to existing techniques, including reduced end-to-end delay, increased throughput, and improved packet delivery ratio. The comparison research yields useful data regarding the efficiency and performance of these algorithms across different scenarios and node configurations.

5. Conclusion

The Trust-Aware Congestion Control Mechanism presented for WSNs offers an advanced solution to the complex issues of congestion, security, and energy efficiency. Within the domain of WSNs, where ensuring dependable data transmission is of utmost importance, the mechanism utilizes a strategy based on Genetic Algorithms. This technique considers the CSB, Energy Trust (ET), and Communication Trust (CT) as crucial metrics for evaluating trust. The technique assesses credibility scores in real-time to effectively manage congestion and security issues. These ratings consider aspects such as buffer occupancy, residual energy, and packet delivery ratio. By implementing a Recommendation Score (RS), cluster chiefs can evaluate member nodes indirectly, hence minimizing computing burden. The comprehensive credibility score (CCS) combines both direct and indirect evaluations of trust, providing a

complex measure of a node's dependability. Deviation thresholds improve the resilience of the process by detecting discrepancies in trust evaluations resulting from malevolent nodes. The use of dynamically given weight factors for trust measures ensures a fair and equitable evaluation, enhancing the adaptability and efficacy of the mechanism in different circumstances of WSN. To summarize, the Trust-Aware Congestion Control Mechanism is a comprehensive, adaptable, and proactive approach that holds great potential for improving congestion, security, and energy efficiency in WSNs.

6. Declarations

6.1. Author Contributions

Conceptualization: G.M.P., B.L.S.K., S.S.M., and Z.S.A.; Methodology: B.L.S.K.; Software: G.M.P.; Validation: G.M.P., B.L.S.K., S.S.M., and Z.S.A.; Formal Analysis: G.M.P., B.L.S.K., S.S.M., and Z.S.A.; Investigation: G.M.P.; Resources: B.L.S.K.; Data Curation: B.L.S.K.; Writing – Original Draft Preparation: G.M.P., B.L.S.K., S.S.M., and Z.S.A.; Writing – Review & Editing: B.L.S.K., G.M.P., S.S.M., and Z.S.A.; Visualization: G.M.P.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] F. Alawad and F. A. Kraemer, "Value of information in wireless sensor network applications and IoT: A review," *IEEE Sensors J.*, vol. 22, no. 10, pp. 9228-9245, 2022.

[2] O. Singh, V. Rishiwal, R. Chaudhry, and M. Yadav, "Multi-objective optimization in WSN: Opportunities and challenges," *Wireless Pers. Commun.*, vol. 121, no. Jun., pp. 127-152, 2021.

[3] H. Zhang, S. Xu, and J. Wang, "Security and application of wireless sensor network," *Procedia Comput. Sci.*, vol. 183, no. 1, pp. 486-492, 2021.

[4] A. Srivastava and P. K. Mishra, "A survey on WSN issues with its heuristics and meta-heuristics solutions," *Wireless Pers. Commun.*, vol. 121, no. 1, pp. 745-814, 2021.

[5] S. T. Abbas, H. J. Mohammed, J. S. Ahmed, A. S. Rashid, B. Alhayani, and A. Alkhayyat, "The optimization efficient energy cooperative communication image transmission over WSN," *Appl. Nanosci.*, vol. 13, no. Sep., pp. 1665–1677, 2021.

[6] S. Verma, S. Zeadally, S. Kaur, and A. K. Sharma, "Intelligent and secure clustering in wireless sensor network (WSN)-based intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 13473-13481, 2021.

[7] M. S. Sumalatha and V. Nandalal, "An intelligent cross layer security-based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN)," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. Feb., pp. 4559-4573, 2021.

[8] A. Rahim, "Cross layer design and energy efficient protocol for wireless sensor network," *Appl. Sci. Eng. J. Adv. Res.*, vol. 2, no. 1, pp. 8-12, 2023.

[9] N. Merabtine, D. Djenouri, and D. E. Zegour, "Towards energy efficient clustering in wireless sensor networks: A comprehensive review," *IEEE Access*, vol. 9, no. Jun., pp. 92688-92705, 2021.

 ISSN 2723-6471

[10] Daanoune, B. Abdennaceur, and A. Ballouk, "A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks," *Ad Hoc Netw.*, vol. 114, no. Apr., pp. 1-14, 2021.

[11] Amutha, S. Sharma, and S. K. Sharma, "Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions," *Comput. Sci. Rev.*, vol. 40, no. may, pp. 1-16, 2021.

[12] A. Srivastava, A. Singh, S. G. Joseph, M. Rajkumar, Y. D. Borole, and H. K. Singh, "WSN-IoT clustering for secure data transmission in E-health sector using green computing strategy," in *Proc. 2021 9th Int. Conf. Cyber IT Service Manag. (CITSM)*, vol. 9, no. Sep., pp. 1-8, Sep. 2021.

[13] V. Narayan and A. K. Daniel, "A novel approach for cluster head selection using trust function in WSN," *Scalable Comput. Pract. Exp.*, vol. 22, no. 1, pp. 1-13, 2021.

[14] S. T. Sheriba and D. H. Rajesh, "Energy-efficient clustering protocol for WSN based on improved black widow optimization and fuzzy logic," *Telecommun. Syst.*, vol. 77, no. 1, pp. 213-230, 2021.

[15] A. Grover, R. M. Kumar, M. Angurala, and M. Singh, "Rate aware congestion control mechanism for wireless sensor networks," *Alexandria Eng. J.*, vol. 61, no. 6, pp. 4765-4777, Oct. 2021. doi: 10.1016/j.aej.2021.10.032.

[16] D. L. Reddy, P. C., and H. N. Suresh, "Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in Wireless Sensor Network," *Pervasive Mobile Comput.*, vol. 71, no. Feb., pp. 1-18, Feb. 2021.

[17] D. P. Bhatt, Y. K. Sharma, and A. Sharma, "Energy efficient WSN clustering using cuckoo search," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1099, no. 1, pp. 1-7, Mar. 2021. doi: 10.1088/1757-899X/1099/1/012048.

[18] R. Srinivasan, R. Kavitha, V. Murugananthan, and T. Mylsami, "A process of analyzing soil moisture with the integration of Internet of Things and Wireless Sensor Network," in Intelligent and Soft Computing Systems for Green Energy, A. Chitra, V. Indragandhi, and W. R. Sultana, Eds. Wiley, 2023. doi: 10.1002/9781394167524.ch13.

[19] B. H. Hayadi and T. Hariguna, "Determinants of student engagement and behavioral intention towards mobile learning platforms," *Contemp. Educ. Technol.*, vol. 17, no. 1, pp. 1-25, 2025. doi: 10.30935/cedtech/15774.

[20] T. Hariguna and A. Ruangkanjanases, "Assessing the impact of social media interaction in s-commerce strategies mediated by relationship quality," *J. Infrastruct. Policy Dev.*, vol. 8, no. 2, pp. 1-20, 2023. doi: 10.24294/jipd.v8i2.2807.