International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

A Behavioral Trust Using Gannet Optimization Algorithm to Improve Fault Tolerance in Wireless Sensor Network

R. Vinothani[1], Dr. P. Kanmani[2]

[1]Research Scholar, [2]Associate Professor, Department of Computer Science, Thiruvalluvar Government Arts College, Rasipuram, Namakkal, Affiliated to Periyar University, Salem – 636 011, Tamil Nadu, India.

***Abstract*-- Wireless Sensor Networks (WSNs) are more prone due tonode failures, link quality issues, communication errors, and malicious activities because of their restricted resource. So, the fault tolerance mechanism will be more essential to create a reliable network. This paper proposes a novel fault-tolerant framework based on behavioral trust for both cluster head (CH) and cluster member (CM) nodes. The behavioral trust model is calculated based on Packet Delivery Ratio, Packet Loss Rate and Communication reliability to identify faulty or malicious node. To enhance network performance, aGannet Optimization Algorithm is used to form clusters which selects two cluster heads for each cluster: a Primary Cluster Head (PCH) and a Vice Cluster Head (VCH) which reduce work load of cluster and if one cluster head dies, then other cluster play a vital role. The PCH is responsible to aggregate normal data and then the data will be transmit to base station, if PCH cause any fault in network mean the VCH is used to take backup the data. In addition, a threshold used to identify malfunctioning node, that node will be ignored and network dynamically choose other route for hop. The proposed approach reduces packet loss rate, improves network lifetime, and enhances fault recovery performance. According to the simulation resultit performs well compared to the standard clustering fault tolerance techniques in terms of network reliability and efficiency.**

***Keyword* - Wireless Sensor Networks, Fault Tolerance, Behavioral Trust, Gannet Optimization Algorithm, Cluster Head Selection, Packet Loss Rate.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have significant technology, now a days it played a vital role in day today life and it has various applications including environmental monitoring, healthcare systems, industrial automation, and military surveillance. A WSN consists of numerous sensor nodes which deployed randomly over a geographical area to sense, process, and transmit data to a central base station. These sensor nodes have limited resources like energy, computation capability and communication overhead, so it cause more prone to sensor nodes which act as faulty node in network. [1], [2].

In WSN, faults occurred in multi-way like packet dropping, hardware malfunction, energy depletion, environmental damages these factors are considered to be faulty nodes. Once the network contains faulty nodes then the network degrades its performance. It causes packet dropping, energy consumption, occur delay and reducing throughput. Finally, all the nodes dies quickly in short period of time.So, the fault tolerance techniques needed in WSN. The network will function more effectively whatever the fault may occur and easy to detect then recover from faults [3]. The conventionalfault tolerance techniques, such as redundancy and retransmission, improve reliability but it require more energy and communication cost [4].

Clustering is one of the significant technique it effectively improve energy efficiency in WSNs. In clustering protocol, group of nodes to form clusters, each cluster have Cluster Head (CH) and Cluster Member (CH). CH has responsible for data aggregation and send the data directly to the base station (BS). One of the initial and most popular cluster based protocol called Low-Energy Adaptive Clustering Hierarchy (LEACH) [5]. Moreover, LEACH struggle to select random CH selection and lack of fault tolerance, reduce its performance when CH fails.

To tackle these challenges, researchers have proposed many optimization-based clustering techniques. Meta-heuristic algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO) have been implemented to improve CH selection, the objective functions like energy and distance [6], [7].

These algorithms enhance the network performance, but still real-time fault tolerance techniques are needed to improve to recover overall network issues.

Recently, trust-based mechanisms haveinspired researchers to improving reliability and security in WSNs. Trust models examine the behavior of nodes based on parameters such as packet delivery ratio, packet loss rate, and communication efficiency. Behavioral trust easily find out faulty or malicious nodes in network based on their communication pattern [8]. Nodes with low trust values are not chosen for routing purpose and clustering processes, so they maximize network reliability.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

In addition, Packet Loss Rate (PLR) is an essentialperformance metric used to evaluate communication reliability in entire network. High PLR denotes poor link quality or misbehavior of the node. Several studies used PLR as a parameter to detecting faulty and attacking nodes such as black hole, warm hole attack [9]. Still, PLR with trust-based method stands as an open research challenge.

Other crucial issue in clustering-based protocols deal with single point of failure associated with cluster heads. If one CH fails, the entire cluster need to wait until a new CH is selected. To point this issue, backup mechanisms use secondary or vice cluster heads have been proposed to perform continuous process [10]. Here the most challenging issue to select vice CH.

To resolve these challenges, this paper proposed a novel fault-tolerant technique that combine behavioral trust with Gannet optimization algorithmwhich is used to select efficient cluster head. In this method, introduces a dual cluster head mechanism consisting of a Primary Cluster Head (PCH) and a Vice Cluster Head (VCH) in each clusters. Before selecting the CH multiple parameters are checked like trust threshold, communication reliability and residual energy.

In addition, a threshold-based packet loss rate mechanism is used to detect faulty nodes in the network. If the packet loss rate exceeds the threshold means the network will automatically redirects its route from CH to Vice-CH. This approach assures continuous communication process and minimizes packet loss rate.

The combination of behavioral trust, Gannet optimization, and dual cluster head mechanism provides a comprehensive solution to achieve fault tolerance in WSNs. The proposed work not only improve reliability but also enhance energy efficiency and network lifetime. The main contributions of this work are summarized as follows:

- Behavioral trust method used to ensure node reliability
- Gannet- used to select of Primary and Vice Cluster Heads in each cluster.
- Threshold-based packet loss method used to find faulty node.
- Network dynamically take redirection to improve fault recovery

The remainder of the paper is organized as follows. Section 2 literature review based on related work in fault tolerance and trust-based WSNs. Section 3 the proposed methodology. Section 4 discuss simulation results, and Section 5 concludes the paper.

II. Literature Review

Fault tolerance in Wireless Sensor Networks (WSNs) has been widely studied due to the restricted limitations of sensor nodes such as limited battery, unreliable communication, link quality and miscellaneous nodes. Initial research mainly focus on clustering and redundancy methods to improve network stability.

A study carried by Selvi and Manoharan [11] evaluates various techniques which would be clustering based fault detection methods and the researchers mainly aim to improve energy efficiency and communication reliability. In a similar manner, Kaur and Kaur [12] introduced a clustering-based fault tolerance mechanism it consider only to improve network lifetime, instead to find faultdetection capability.

Energy-based fault tolerance mechanism have also beeninvestigated. Aishwarya*et al.* [13] proposed an energy-aware clustering and routing protocol which use backup node to protect the data which is chosen based on residual energy.This technique improves fault recovery but does not find malicious node activityeven it considers only energy as a parameter metric. Similarly, Saroj and Kumar [14] introduced a fuzzy logic clustering approach for fault tolerance, which enhance decision-making while raising computational complexity.

Wang *et al.*[15] present a trust orientedmethod for fault detection leveraging multi-factor assessment. Their approach uses factorlike communication cost and nodesactivity to identify faulty nodes. thus, this method necessitates predefined parameters and lack of dynamic routing. Similarly, trust management techniques discussed in [16] trust parameter metric consider as important metric to identify faulty node and it ensure secure communication in WSNs.

Trust-based clustering has also received more attention from researchers. Gaber*et al.* [17] suggested a trust-based cluster head selection approach utilizing a bio-inspired optimization algorithm. The parameters taken into account in this method are trust, value,energy and node degree.It wouldimproved network lifespan and reliability. But, this method does not address fault recovery during communication.

Security-aware fault tolerance methods has been studied using trust-based routing. Zhang *et al.* [18] developed a fault-tolerant routing protocol using trust and fuzzy logic to improve packet delivery ratio and network stability. Although the approach enhances reliability, but this method does not focus on backup mechanism if the cluster head failure.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Recent works to combined advanced trust evaluation approaches. Studies such as [19] introduced fuzzy trust and outlier detection for secure clustering, malicious node detection with higher accuracy. likewise, trust GAN models have been introduced to enhance fault node detection rates and adjustable to dynamic environments [20]. These method works better of behavioral trust in both faults and attacks.

Inspite of these development, several research gaps remains. Most present methods either focus to reduce energy consumption or security, but not both simultaneously. Many clustering protocols may affects in single point if cluster head once failure mean the entire cluster would be disturbed. Additionally, at present trust based model may not be integrate the effective bio inspired techniques to choose best cluster head.

To analyze these certain restrictions, this paper proposes a behavioral trust-based fault tolerance model combined with Gannet optimization algorithm**.** Differnt from energy-based methods, behavioral trust examine every nodes reliability using packet forwarding activity, packet loss rate, and quality of communication. This helps to detect both faulty and malicious nodes productively. Additional, the incorporation of Gannet optimization selects efficient Primary and Vice Cluster Heads, while removing the issue of single point of failure.

consequently, the proposed approach offers a solution by combining fault tolerance based dual clustering mechanism to improving reliability, security, and network lifespan.

III. Proposed Method

This section explains the proposed **Behavioral Trust-Based Fault Tolerance model** incoporate with the **Gannet optimization algorithm** to select efficient cluster head. This model aim to explore faulty and malicious nodes by utilizing trust parameter which contain threshold range to maintain consistent link quality using a dual cluster head technique.

A. Network Model

Consider a Wireless Sensor Network (WSN) made up of N sensor nodes that are randomly deployed within a sensing region. Each node interacts with adjacent nodes and sends data to the Base Station (BS) via Cluster Heads (CHs).

- Nodes remain fixed position after deployment
- Each node contain same initial energy
- Communication involves multi-hop
- Each cluster has:
  - Primary Cluster Head (PCH)
  - Vice Cluster Head (VCH)

B. Behavioral Trust Model

Behavioral trust have threshold measure of a node's reliability which is observed based on communication activities over a period. In Wireless Sensor Networks (WSNs), all the nodes have responsibility to forward the aggregated data, maintain link qulity for communication, and interact with neighboring nodes. If any diversion indicates the faulty nodes or malicious node should be present in network then the network dynamically redirect all the packets against faulty node. In mathematically, behavioral trust of a node i is denoted as T_i, which shows the reliable node participation in data transmission and forwarding process.

C. Importance of Behavioral Trust

Behavioral trust is mainly important to tolerate the fault if occurs in network to provide continuous and secure link quality due to the following reasons:

- *Fault Detection:* If the network affects by faulty node means that certain node activities like packet dropping or delayed transmission these things able to identify attacker node.
- *Attack Detection:* the malicious node creates the abnormal network such that node called as black hole or worm hole attacker nodes.
- *Reliable Routing:* it often checks the nodes link quality and residual energy for routing and data forwarding to continuously transmit the data from one other.
- *Cluster Head Selection***:** This model assures the reliable node only able to act as Cluster Head (CHs).

In contrast with conventional energy based methods, the behavioral trust aims the secure communication process based on link quality. This generate network should be secure environment.

D. Parameters for Trust Evaluation

Behavioral trust is computed using multiple communication parameters that reflect node performance:

1. Packet Loss Rate (PLR_i)

In trust based network, the Packet Loss Rate (PLR) is combined with behavioral trust assessment to identify malicious nodes. Here, the threshold is used to segment the nodes activity. PLR calculates the number of packet drops to the total number of transmitted packets within the stipulated time.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

This value is compared to the threshold range. If the node exceeds the range means that node consider as suspicious or untrustable node, otherwise the node used for communication.

$$PLR_i = \frac{P_{lost}}{P_{sent}}, T_i = \begin{cases} 1, & PLR_i \le \theta \\ 0, & PLR_i > \theta \end{cases}$$

where PLR_i denotes the packet loss rate of node i, P_{lost} represents the number of packets lost, and P_{sent} indicates the total number of packets transmitted. The parameter θ is the defined threshold value, and T_i is the trust indicator, where 1 denotes a trust node and 0 denotes an untrustable node.

2. Packet Delivery Ratio (PDR_i)

In trust based network, the **Packet Delivery Ratio (PDR)** is used to find how much of packets to be transmitted from source to destination node, if all the packets are sent mean that node consider as trustable node else that node denotes malicious node.

$$PDR_i = \frac{P_{received}}{P_{sent}}, T_i = \begin{cases} 1, & PDR_i \le \theta \\ 0, & PDR_i > \theta \end{cases}$$

Where PDR_i denotes the packet delivery ratio of node i, $P_{received}$ is the number of packets successfully delivered to the destination, and P_{sent} is the total number of packets transmitted. The parameter θ represents the predefined trust threshold, and T_i is the trust value assigned to the node, where 1 indicates a trustworthy node and 0 denotes an untrustworthy node.

***3.** Link Quality Indicator (LQI_i)*

The **Link Quality Indicator (LQI)** is consider one of the significant factor, particularly evaluate the link quality. How much node receives the signal for data sending as well as data receiving period. If the node receives all the packet and optimal link quality to checks the node reliability in the network.

$$LQI = \frac{RSSI - RSSI_{min}}{RSSI_{max} - RSSI_{min}}$$

Where:

- RSSI= Received Signal Strength Indicator of the current signal
- $RSSI_{min}$= Minimum measurable signal strength
- $RSSI_{max}$ = Maximum measurable signal strength

E. Behavioral Trust Computation

The behavioral trust of node i is computed as a weighted combination of the above parameters:

$$T_i = w_1(1 - PLR_i) + w_2 PDR_i + w_3 LQI_i$$

Where, W_1, W_2, W_3, are weight coefficients such that $W_1+W_2+W_3 = 1$

- $(1-PLR_i)$ ensures that lower packet loss increases trust
- PDR_i reflects successful communication
- LQI ensures stable connectivity

1. Threshold-Based Fault Identification

A threshold value T_{th} is defined to classify nodes:

$$Node_i = \begin{cases} Trusted, & T_i \ge T_{th} \\ Faulty/Untrusted, & T_i < T_{th} \end{cases}$$

If T_i is high → node is reliable

- If T_i is low → node is faulty or malicious

2. Ignoring Faulty Nodes in Network Operation

To ensure fault tolerance, nodes identified as faulty are excluded from network operations such as routing and cluster head selection.

This can be mathematically expressed using a selection function:

$$S_i = \begin{cases} 1, & T_i \ge T_{th} \\ 0, & T_i < T_{th} \end{cases}$$

Where:

- S_i = 1 Node is eligible for communication and clustering
- S_i = 0 Node is ignored / excluded

3. Cluster Head Selection

Only nodes satisfying the condition S_i are considered in the Gannet optimization process for selecting Primary and Vice Cluster Heads. This ensures that unreliable nodes are completely removed from critical network functions.

IV. RESULT

The performance evaluation of the proposed **behavioral trust-based Gannet optimization algorithm** is simulated and compared with the standard Gannet optimization algorithm.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

TABLE 1
NETWORK MODEL

Parameter	Value
Number of Nodes	100
Initial Energy	0.5 J
Network Area	100 × 100 m
Simulation Rounds	5000
Packet Size	4000 bits
Base Station	Fixed
Traffic Type	CBR

The obtained results shows that the proposed approach performs better with standard gannet optimization algorithm. In comparison across all the performance metrics are considered. In terms of packet delivery ratio, it works well to produce more success rate due to selecting reliable node with high residual energy. Packet loss rate monitor to ensure which node to drop the packet that node consider to be an unreliable node and malicious node. Further, this method to improve energy efficiency, and reduce overall energy consumption to prolonged the network lifespan. The delay also reduced due to optimally selects the routing process to continuously transmit the data from source to destination.

TABLE 2:
PERFORMANCE METRICS

Metric	Standard Gannet	Behavioral Trust-based Gannet
Packet Delivery Ratio (%)	89.2	96.8
Packet Loss Rate (%)	10.8	3.2
Residual Energy (J)	0.21	0.34
Energy Consumption (J)	0.29	0.16
End-to-End Delay (ms)	210	145
First Node Dead (Round)	980	1450
Half Nodes Dead (Round)	2100	2900
Last Node Alive (Round)	3200	4300

Additionally, the alive and dead nodes simulation rounds indicates that the proposed method highly retain the network for longer duration, with delayed node failures compared to the standard gannet optimization algorithm. Finally the behavioral trust produce longer network, high residual energy and node reliability in wireless sensor network.

Rounds	Alive Nodes		Dead Nodes	
	Standard Gannet	Trust-Based Gannet	Standard Gannet	Trust-Based Gannet
1000	92	98	8	2
2000	65	84	35	16
3000	38	60	62	40
4000	10	32	90	68
5000	0	12	100	88

V. CONCLUSION

This paper proposed a **behavioral trust-based Gannet optimization algorithm** to improve the network performance. The trust calculation method to improve node reliability and residual energy. The simulation results shows that the introduced method performs well compared with conventional gannet optimization algorithm. The compared parameter metrics such as packet delivery ratio, packet loss rate, residual energy, and number of alive node, number of dead nodes. By choosing reliable node to ignore malicious node to ensure continuous routing and efficient data transmission. In future research, this method hybrid with machline learning techniques in dynamic environment. Additionally, investigate with some security mechanism to sophisticated attacks make strengthen the trustworthy sensor network.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[4] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14–15, pp. 2826–2841, 2007.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. IEEE HICSS*, 2000.

[6] S. Singh and M. P. Singh, "Energy-efficient hierarchical clustering in wireless sensor networks: A swarm intelligence approach," *Applied Soft Computing*, vol. 12, no. 12, pp. 3790–3801, 2012.

[7] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proc. IEEE ICNN*, 1995, pp. 1942–1948.

[8] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, 2008.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, 2003.

[10] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.

[11] G. V. Selvi and R. Manoharan, "Cluster based fault identification and detection algorithm for WSN: A survey," *IJCTT*, vol. 4, no. 10, pp. 3491–3495, 2013.

[12] N. Kaur and K. Kaur, "Fault tolerance mechanism using clustering for power saving in wireless sensor networks," *IJETT*, vol. 4, no. 8, pp. 3483–3487, 2013.

[13] C. Aishwarya, P. Padmakumari, and A. Umamakeswari, "Energy aware fault tolerant clustering and routing mechanism for WSN," *Indian Journal of Science and Technology*, 2016.

[14] P. Saroj and S. Kumar, "A novel power efficient clustering technique with fault tolerance using type-2 fuzzy logic," *IJCA*, vol. 181, no. 5, 2018.

[15] N. Wang, J. Wang, and X. Chen, "A trust-based formal model for fault detection in wireless sensor networks," *Sensors*, vol. 19, no. 8, 2019.

[16] A. Kaur *et al.*, "Trust management techniques in wireless sensor networks," *Springer*, 2020.

[17] T. Gaber*et al.*, "Trust-based secure clustering in WSN," *Computer Networks*, vol. 146, pp. 151–158, 2018.

[18] H. Zhang *et al.*, "A security fault-tolerant routing for clustered WSNs," *Journal of Wireless Communications and Networking*, 2016.

[19] Y. Liu *et al.*, "Secure clustering with fuzzy trust evaluation and outlier detection for WSN," 2022.

[20] Y. Liu *et al.*, "GAN-based trust management for secure clustering in WSN," 2022.