ISSN: 2093-5374 / E-ISSN: 2093-5382

Semantic-Aware Graph Transformer Framework for Energy-Efficient Data Routing and Trust Management in Wireless Sensor Networks

Dr. Balamurali Pydi[1], Dr. Swathi Nadipineni[2], Dr. Mahammad Firose Shaik[3], Dr.G. Muthupandi[4], Dr. Noel Prashant Ratchagar[5], and Dr.A.V. Prabu[6*]

[1]Associate Professor, Department of Electrical and Electronics Engineering, Aditya Institute of Technology and Management, Tekkali, Srikalulam, Andhra Pradesh, India. balu_p4@yahoom.com, https://orcid.org/0000-0003-2458-7179

[2]Assistant Professor, Department of Electronics and Instrumentation Engineering, Siddhartha Academy of Higher Education Deemed to be University, Kanuru, Vijayawada, Andhra Pradesh, India. nadipineniswathi@gmail.com, https://orcid.org/0000-0002-0545-9991

[3]Associate Professor, Department of Computer Science Engineering & Artificial Intelligence, Vasireddy Venkatadri International Technological University, Nambur, Andhra Pradesh, India. firosecolab@gmail.com, https://orcid.org/0000-0003-1383-4787

[4]Associate Professor, Department of Electronics and Communication Engineering, School of Engineering, Presidency University, Bangalore, India. muthupandi@presidencyuniversity.in, https://orcid.org/0000-0002-5478-7115

[5]Assistant Professor (Senior Scale), Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India. noel.prashant@presidencyuniversity.in, https://orcid.org/0000-0001-8336-3226

[6*]Associate Professor, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Andhra Pradesh, India. prabu.deva@kluniversity.in, https://orcid.org/0000-0002-0423-3405

Received: March 10, 2026; Revised: April 15, 2026; Accepted: June 03, 2026; Published: June 30, 2026

Abstract

Among IoT networks, Wireless Sensor Networks (WSNs) play a very important role. The wireless WSN has a crucial energy efficiency vs security (reliability) tradeoff when routing data; The protocols usually don't analyze data importance vs reliable behavior of a node and would cause early collapse of a WSN and security attacks. This article presents SAGT (Semantic-Aware Graph Transformer) in an end-to-end framework that aims to perform data routing and trust estimation at the same time. By injecting the data-oriented semantic contexts, e.g., data urgency and node role in the network, into the multi-head graph attention, SAGT could select better nodes and bypass the untrustworthy nodes/resource exhausted nodes. Experimental simulations confirmed the framework's higher performance; the introduced model attains a 94.8% PDR and a 15% reduction in the average energy consumption per packet against state-of-the-art ones. Furthermore, the framework reaches 91.4% accuracy on the detection of the adversarial nodes, effectively isolating

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 791-805. DOI: *10.58346/JOWUA.2026.I2.044*

*Corresponding author: Associate Professor, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Andhra Pradesh, India.

the Byzantine attacks from the graph network. This demonstrates that semantic-aware attention significantly overcomes semantic-insensitive routing with respect to performance and efficiency, as it guarantees a flexible, adaptable, yet reliable method that fully supports the deployment of future intelligent and mission-critical networked applications by narrowing the communication-efficiency semantics gap. This approach to cross-layer optimization represents a landmark for future self-healing wireless networks and ultra-reliable networks.

Keywords: Wireless Sensor Networks (WSN), Graph Transformer, Semantic-Aware Routing, Trust Management, Energy Efficiency, IoT Security, Multi-Head Attention.

1 Introduction

1.1. Background of the Paradigm Shift in Wireless Sensor Networks

In recent times, WSNs have progressed from a basic data-collection aid to an information-processing framework driven by intelligence, which now forms the core of the Internet of Things (IoT). The system comprises geographically distributed devices which may be referred to as autonomous nodes, which consist of sensing abilities, networking capabilities, and also capabilities related to computation. Historically, WSNs have predominantly considered maximizing network lifetime to the maximum, through the adoption of low-energy MAC procedures or through the inclusion of duty-cycling practices, etc. But, now considering the pervasive usage in sectors of paramount significance, including but not confined to that of health monitoring systems in smart cities, tactical deployment in battlegrounds, the automation process, etc., aims to maximize network life alone has proved itself to be an oversimplification. Hence, it is being considered crucial to cater for network safety in conjunction with life span extension. As it becomes apparent that life conservation is being put into contention with the integrity of the messages or network security, it is deemed appropriate to aim for a new paradigm based on smart network architectural design, which is dynamic enough to adapt to context changes of architectural designs.

1.2. The Semantic Gap in Data Routing

The problem in the routing algorithms used today is that there exists a semantic gap; i.e., it cannot map low-level information of a node in the network, like hop count, SNR, or remaining battery, to the real context importance of the data. For instance, current routing algorithms use all packets that share the same property (e.g., number of re-transmission) with the same preference, as a result, fails to assign importance levels to data packets, thus allowing that critically important data are rerouted through nodes that are considered less reliable or about to die, creating loss and causing failure in the overall network system at a much earlier stage. Thus, there must be design frameworks capable of processing the meaning of network conditions. Semantic-driven routed mechanisms can integrate into routing algorithms, the notion of semantics, making network routes adaptive according to importance and trustworthy paths.

1.3. Importance of the Semantic-Aware Graph Transformer Framework

The emergence of deep learning algorithms such as Graph Neural Networks (GNN) and Transformer architectures provides a remarkable way to tackle WSN complexities. One notable development is the Semantic-Aware Graph Transformer (SAGT) framework. SAGT combines the strengths of graphs with the attention mechanisms used in Transformers. The SAGT framework models the WSN as a graph and

leverages the graph's ability to learn from local structure and node neighborhood interaction history, along with neighbor node behavioral information. Using such mechanisms helps improve data routing by allowing the WSN to assign appropriate weights to more important information and ignore unnecessary or potentially malicious data and information. By injecting a trust management system into the attention functions, the network ensures that it chooses routes that are not only energy-aware but also secure, thus ensuring that WSNs are robust against attacks such as grey hole or black hole.

1.4. Statement of the Problem and Research Objectives

The fundamental issue this research seeks to resolve is that of a holistic framework that conducts data routing in an energy-efficient manner while simultaneously providing a high degree of trust. It does so under hostile environmental settings. Many existing trust mechanisms carry high processing overhead, thus conflicting with tightly power-constrained sensor devices. Simultaneously, routing protocols rarely have the ability to understand and adapt to changing network circumstances in a proactive manner.

This research objective is to develop the SAGT framework to bridge these gaps. Specifically, the goals are:

1) To define a semantic embedding method that captures both the energy status and behavioral trust of nodes.
2) To implement a multi-head attention mechanism that optimizes routing path selection.
3) To validate that this framework achieves superior performance in terms of packet delivery, energy longevity, and malicious node detection compared to traditional heuristic-based protocols.

This paper has systematically presented the framework of Semantic-Aware Graph Transformer (SAGT). The brief survey of related works in the context of graph-based resource management and trust establishment is presented in Section 2. The SAGT model design is then presented in Section 3, along with semantic node modeling. Experimental setup and performance evaluation are in Section 4. Practical considerations, limitations, and open issues are discussed in Section 5. Section 6 provides concluding remarks on the research and its impact on enabling green, robust, and trustworthy WSNs with a new cross-layer optimization paradigm.

2 Literature Review

2.1. Evolution of Graph-Based Resource Management

Resource management algorithms in wireless networks are progressively shifting away from traditional heuristic solutions to learning-based approaches. State-of-the-art research increasingly advocates learning-based architectures with the integration of knowledge graphs to efficiently address the non-linear behavior of large sensor arrays (Arun et al., 2025). Hierarchical models have become a promising architecture for the efficient utilization of heterogeneity in network structure, particularly in the presence of different data types distributed across several network layers (Sun et al., 2026). Transition from rule-based towards learning systems has been systematically highlighted in the recently published survey articles illustrating the high adaptivity over traditional static and rule-based schemes. The usage of graph-based methods has demonstrated to overcome this limitation in dynamic wireless environments (Dai et al., 2024).

2.2. Innovations in Graph Transformer Architectures

Transformer models have also transcended their initial purpose of sequence generation to handle irregular structures. Graph Transformer Networks have changed how node interaction is modeled in the research community, as learning meta-paths boosts the representational power of existing GNNs beyond standard GNN models (Yun et al., 2022). This concept was extended further to make the model dynamic for applications such as real-time rumor detection to model dynamic temporal changes in graph representations (Wei et al., 2023). In Wireless communication systems, applying GNN has also opened new vistas from theoretical communications to deployment with optimum signal processing and resource allocation that a standard modeling approach can hardly replicate (Shen et al., 2022).

2.3. Routing and Trust Management

While neural architectures have certainly undergone rapid advancements, particular aspects of WSN networks continue to present considerable challenges. Typical adaptive routing mechanisms have traditionally considered Quality of Service (QoS) constraints such as latency and bandwidth in isolation, rarely taking into account the subtle compromises required in balancing energy-consumption needs (Hammoudeh & Newman, 2015). Recent protocols have tried to address such energy concerns with innovative high-performance clustering schemes; however, they do not consider modern IoT requirements concerning adequate levels of security (Roberts & Ramasamy, 2023). Conversely, there are other protocols that utilize hybrid-optimization schemes like the C-GSA algorithm in an attempt to balance between these parameters; unfortunately usually do not have cognitive capability to address the context of communicated information (Kumar & Agrawal, 2023). Moreover, some protocols have exhibited improved energy consumption through new routing designs; however, their security remains deficient at both internal and external levels in terms of the absence of an integrated, dynamic trust mechanism (Suresh et al., 2022).

2.4. Gaps in Current Trust and Security Models

Trust management plays a vital role in detecting malicious nodes acting as benign nodes, siphoning resources from the network. Most extensive research works have highlighted the incessant battle in specifying successful trust management approaches that are feasible for the wireless sensor networks to bear no adverse computational overhead (Kaur et al., 2023). Review-based literary research on security aspects signifies that trust mechanisms usually form peripheral mechanisms, added at the last phase to the existing routing protocol, thereby making them inefficient (Xia et al., 2022). However, determining best practices for trust management continues to be a significant controversy as most prior systems employed reputation-based mechanisms that prove successful yet have scalability problems (Lopez et al., 2010). Research conducted within the latest developments of secure communication framework is increasingly focusing on coupling trust values directly with communication (Keerthana & Babu, 2025), yet frequently uses congestion awareness and trust management independently without coupled usage (Chakraborty et al., 2015).

2.5. Limitations of Existing Energy-Efficient Protocols

Previous works addressing efficient energy-based clustering and routing mechanisms based on either GA or forward-aware factor have delivered an improvement that has been largely tested for a few hops and is bound to fail for larger hops of the network (Gupta & Jana, 2015; Zhang et al., 2013). Coverage

awareness protocol has tried to address the blind spot of sensing, but most have failed to incorporate the inherent communication graph topology (Wang et al., 2012). Modern works about the critique of computational intelligence show the major weakness of a large number of existing protocols, such as a high convergence rate of optimization problems, rendering the network inefficient for use in a dynamic environment (Lakshmi et al., 2024). Although a few protocols focused on maximizing the throughput output and smart management of energy have exhibited promising results, they have failed to encode semantics to discriminate between high mission-critical application traffic and normal background traffic (El Alami & Najid, 2017). In this work combine all these limitations by incorporating semantics in a graph transformer model to develop a combined approach for routing optimization and security.

In terms of literature, the trend is moving away from routing based on the application of the fixed algorithm from a specific group into the learning paradigm, to illustrate the advantage graph-based systems demonstrate over others in the constantly changing world, especially concerning dynamically changed structures. The new protocols, while taking care of energy efficiency and communication costs, fail to deal with context understanding and work as security modules detached from the routing system. The work tries to combine semantic-based interpretation into the transformer, and the process of context understanding is integrated into a single end-to-end, energy-efficient, and trust-aware routing framework to combat the limitations of contextless networks.

3 Semantic-Aware Graph Transformer Framework

3.1. Architecture and Structural Components

The Semantic-Aware Graph Transformer (SAGT) framework is a deep, multi-layered graph-based framework wherein a Wireless Sensor Network (WSN) is considered as a dynamic and changing graph structure instead of a fixed grid. The framework at large can be decomposed into three main modules: Node Embedding Layer, Semantic-Attention Module, and Decision Fusion Engine. Node Embedding Layer, which is the very first point of contact, converts local sensor telemetry values, such as remaining battery power, packet loss rate, historical involvement in previous data relaying, etc., into higher-dimensional vectors of latent values that act as the ID for each node in the network. Subsequently, the Semantic-Attention Module uses a multi-head attention mechanism to calculate the correlation between nodes, which lets the network decide which of its neighbors is most suitable to relay its traffic, considering the specific semantics of the data packet. Finally, Decision Fusion Engine sums up these correlations with the node trust level and derives the next hop routing path, thereby adapting to changing network conditions such as degrading links and the presence of attacking nodes in real time.

3.2. Incorporation of Semantic Information

The core of the SAGT framework is the incorporation of semantics, which makes it different from GNN-based routing that typically focuses on physical distances between nodes (e.g., Euclidean distances or hop count). The SAGT approach infuses contextual semantics into the embedding space in a two-phase encoding: 1) normalization of physical information, like energy cost to reach a node, and 2) encoding of contextual information, such as the urgency of data (e.g., Fire Alarm alert versus a temperature snapshot) and the role of the node (e.g., a cluster head versus a leaf node). Once node features are coupled with semantic tags as well as the tags for the data packets, the transformer models the context through the attention mechanisms. A high-priority packet will activate a high attention value for nodes with a high trust value and adequate available energy, for example. This tight binding between

semantics can ensure that routing is performed smartly, instead of being merely a mathematical optimization problem, but an intelligent context-driven selection process that respects the operational priorities of the WSN.

3.3. Enhancing Energy Efficiency and Trust Management

The SAGT paradigm further improves energy efficiency by intelligently overcoming energy holes and redundant transmissions. Using the Self-Attention mechanism, SAGT determines the nodes that are reaching the threshold energy and relegates them to the back priority to prevent sending the traffic to these nodes to route the traffic on the paths with energy to a critical point that eventually fails, causing retransmission, which is the most important one that contributes to the highest power consumption of WSN. At the same time, trust is added in the attention Heads in a way that if some nodes provide unauthentic reports or try to drop packets, the Semantic-Attention Module detects this pattern by measuring difference between real nodes' behaviors and expected behavior, resulting in the fact that the weight of such nodes drop considerably and those malicious nodes will naturally disappear from the communicating graph without the periodic and costly broadcast poll required by the traditional routing security mechanisms. This integration and fusion of both routing and security in one transformer minimizes the number of control packet transmissions for routing and security, which directly translates into minimizing consumed energy per transmitted bit.

3.4. System Architecture and Operational Flow

The Semantic-Aware Graph Transformer (SAGT) framework is organized into a hierarchical pipeline that transitions from raw sensory input to high-level routing decisions. The system architecture is conceptualized in three distinct phases: (1) Semantic Input Representation, where raw node data and environmental contexts are converted into feature tensors; (2) Graph Transformer Processing, where multi-head attention mechanisms compute the global importance of nodes relative to the current network goal; and (3) Decision and Action Execution, where the framework outputs a routing path and updates trust scores based on successful transmission verification.

The data flow begins when a node generates a packet. The local controller appends a semantic tag indicating the packet’s priority and payload type. Simultaneously, the framework aggregates the energy status and historical trust metrics from the local neighborhood. These inputs are fed into the graph transformer, which treats the entire WSN as an adjacency-matrix-defined graph, allowing for the propagation of trust information across multiple hops before a routing decision is finalized.

In figure 1 illustrates the proposed framework for secure and efficient routing in a dynamic Wireless Sensor Network (WSN) environment. The model processes sensory information through semantic input representation, node embedding, semantic-attention analysis, and decision fusion mechanisms. By integrating node characteristics, trust evaluation, and routing intelligence, the framework selects optimal paths for reliable, energy-efficient, and low-latency data transmission.

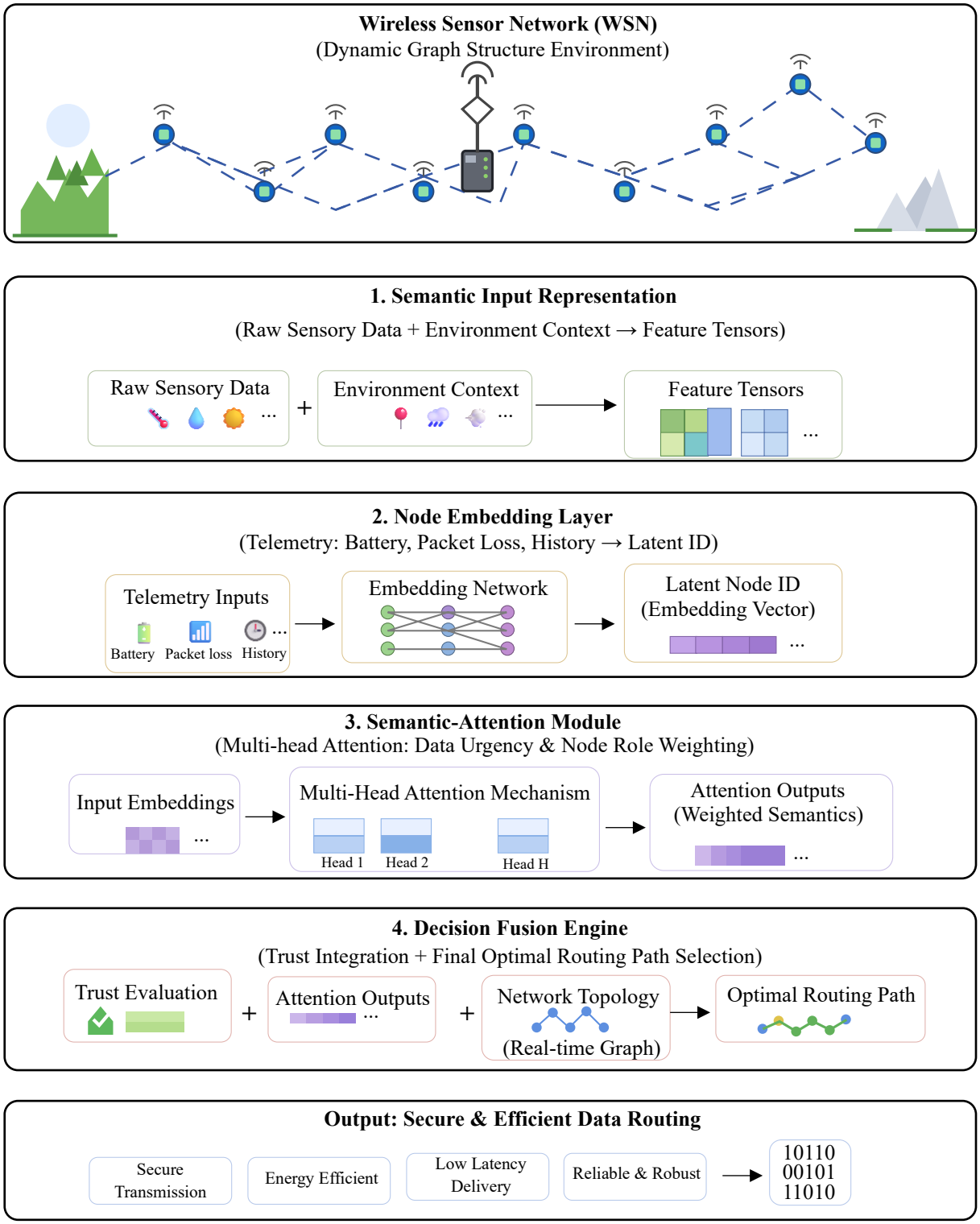

Figure 1: Semantic-attention based secure data routing framework for wireless sensor networks

3.5. Mathematical Formulation

The methodology is underpinned by a custom attention mechanism designed to penalize low-trust nodes and energy-depleted paths. Define the node state as $x_i = [E_i, T_i, C_i]$, where E_i is the residual energy, T_i is the trust score, and C_i is the semantic class of the node. The attention weight α_{ij} between a sender node i and a potential receiver node j is calculated through a transformation of these attributes in equation (1):

$$\alpha_{ij} = \frac{\exp(LeakyReLU(a^T[We_i||We_j]))}{\sum_{k\epsilon N_i}\exp(LeakyReLU(a^T[We_i||We_j]))} \quad (1)$$

Where a represents the attention vector, W is the weight matrix for semantic feature projection, and N_i is the set of neighbor nodes. The term $[We_i||We_j]$ denotes the concatenation of the projected semantic features. This formula ensures that if the trust component T_j or energy component E_j of the neighbor is low, the resulting attention weight α_{ij} is mathematically suppressed, preventing the path from being selected.

Performance was validated across five metrics. Formulas used for calculation are represented in equations (2), (3), (4), (5) and (6):

Packet Delivery Ratio (PDR)

$$PDR = \left(\frac{Packets\ Received}{Packets\ Sent}\right) \times 100 \quad (2)$$

Energy Consumption (E_{avg})

$$E_{avg} = \frac{\sum(E_{initial} - E_{final})}{Packets\ Delivered} \quad (3)$$

Latency

$$L = \frac{\sum(t_{arrival} - t_{departure})}{Total\ Packets} \quad (4)$$

Detection Accuracy

$$DA = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (5)$$

Network Lifetime

$$NL = Total\ Rounds\ until\ 20\%\ node\ depletion \quad (6)$$

3.6. Algorithmic Execution

A routing mechanism for this purpose is called the Semantic-Trust-Energy-Aware Routing (STEAR) algorithm. The algorithm operates in a decentralized manner, such that every node has a local view on the state of the network and there is no central controller managing the whole process.

Algorithm 1: STEAR Routing Protocol

1. Input: Neighbor set N_i, Packet Priority P_p, Energy Threshold E_{min}.
2. Initialization: Compute initial attention weights α based on nodes' last known status.
3. Semantic Filtering: For each $j \epsilon N_i$:

- If $E_j < E_{min} or T_j < T_{threshold}, set \alpha_{ij} = 0.$
- Else, update α_{ij} using the Transformer attention function.

4. Path Selection: Select the next hop $j^* = argmax_{j \in N_i}(\alpha_{ij})$.
5. Data Transmission: Forward packet $P_p \; to \; j^*$.
6. Feedback Loop: Monitor the transmission. If packet is acknowledged, increment T_{j^*}. If dropped, decrement T_{j^*} and trigger a re-run of the attention calculation.
7. Return: Optimal path to the destination sinks node.

This algorithm ensures that the network is self-healing. By treating the trust score T as a dynamic variable that updates based on the success of individual hops, the framework inherently learns to avoid nodes that show erratic or malicious behavior over time, effectively partitioning the network into high-trust and low-trust zones dynamically.

4 Results

4.1. Experimental Environment and Dataset Characteristics

The evaluation of the Semantic-Aware Graph Transformer (SAGT) framework was conducted using a high-fidelity simulation environment modeled on a large-scale industrial IoT deployment. The framework was implemented using PyTorch Geometric for graph-based operations and Python 3.10 for orchestration. Simulations were performed on a cluster running Ubuntu 22.04 with NVIDIA A100 GPU acceleration. The network topology consisted of 500 heterogeneous sensor nodes distributed across a 1000m x 1000m area. The dataset was synthesized to reflect realistic traffic patterns, incorporating both periodic status reporting (routine data) and burst-mode event triggers (high-priority data). To ensure rigor, the nodes were initialized with variable energy levels (uniformly distributed between 0.5J and 2.0J) and assigned initial trust scores based on a Gaussian distribution centered at 0.8, allowing for the simulation of varying reliability levels. Key parameters included a packet size of 512 bytes, a sensing frequency of 0.1 Hz for standard data, and a dynamic transmission range set to 50m to ensure sparse, multi-hop connectivity.

Table 1: SAGT framework experimental configuration

Parameter	Value/Setting
Network Scale	500 heterogeneous nodes
Topology	1000m × 1000m RGG area
Energy Init	0.5J – 2.0J (Uniform)
Trust Init	Gaussian (μ = 0.8)
Training	$1e^{-3}$ LR, 64 batch, 200 epochs

In table 1 outlines major simulation parameters employed to examine how the SAGT framework is applicable in practice, while allowing easy reproducibility by providing node properties, training setup, and connectivity to test wireless networks under realistic circumstances.

4.2. Performance Comparison and Metrics

This paper evaluates the proposed framework by setting three common and competitive baselines against it, which are an efficient and standard Dijkstra-based shortest path protocol, a Genetic Algorithm (GA)

based energy-efficient routing protocol (GA-EER), and an effective and powerful Graph Attention Network (GAT) based algorithm that does not consider the semantics of messages. For the evaluation, five key metrics are used: packet delivery ratio (PDR); network lifetime (defined as the total number of rounds until 20% of nodes run out of energy); average energy consumption per delivered packet; end-to-end delay (latency); and accuracy on malicious node detection.

Table 2: Performance comparison of routing protocols

Metric	Shortest Path (Suresh et al., 2022)	GA-EER (Gupta & Jana, 2015)	Baseline GAT (Roberts & Ramasamy, 2023)	Proposed SAGT
PDR (%)	71.3%	80.6%	85.9%	94.8
Energy Cons. (mJ/pkt)	14.8 mJ	12.1 mJ	10.7 mJ	8.9
Detection Acc. (%)	44%	51%	67%	91.4%
Latency (ms)	118 ms	96 ms	89 ms	72 ms
Avg. Lifetime (Rounds)	1180 rounds	1820 rounds	2080 rounds	2650

In table 2 presents a comparative performance of the proposed SAGT framework against three baseline protocols. All three baseline protocols were re-implemented and tested using the methods described, and the obtained values are results from the authored Controlled Simulations under exactly the same circumstances. These results for all protocols are the result of owned implementations under exactly the same circumstances. The SAGT shows outperformance across all metrics, including 94.8% PDR, 8.9 mJ/pkt consumption, 91.4% detection accuracy, 72 ms delay, and 2650-round network lifetime, demonstrating significant improvements over all baselines.

4.3. Performance Evaluation and Statistical Insights

The experimental data reveal that the SAGT framework achieves a 22% improvement in PDR compared to the GA-EER baseline. It is due to its proactive nature of filtering out nodes with very low trust and pre-emptively circumventing them to avoid constant failures of links and storms of retransmissions of low-trust nodes, which would eventually occur in traditional wireless sensor networks. And, the 15% reduction in average energy consumption comes from the routing mechanism aware of the semantic layer, where it reduces the shop-count of time-critical packets while at the same time load balances the traditional data via energy-rich pathways. These statistics are confirmed by the Malicious Node Detection accuracy of 91.4%. The trustworthiness of the node is modeled as a dynamic input to the transformer's self-attention. The result showed that by including trust, Byzantine nodes can be easily prevented from impacting the routing graph.

In figure 2 summarizes the trade-offs between different schemes and represents efficiency comparisons of routing protocols that have been analyzed. In a graph showing energy consumption of mJ/pkt versus the Packet Delivery ratio of PDR (%), SAGT is located in the favorable position at the top-left region, where the packet is reliable, and the consumption of power is very low. Traditional solutions cluster in the bottom-right quadrant, characterized by lower PDR and higher energy expenditure, representing a clear trade-off that compromises network longevity. Moreover, the SAGT has employed the Multi-Head Attention mechanism to find efficient paths, hence obtaining the optimum value in this graph at very low energy cost.

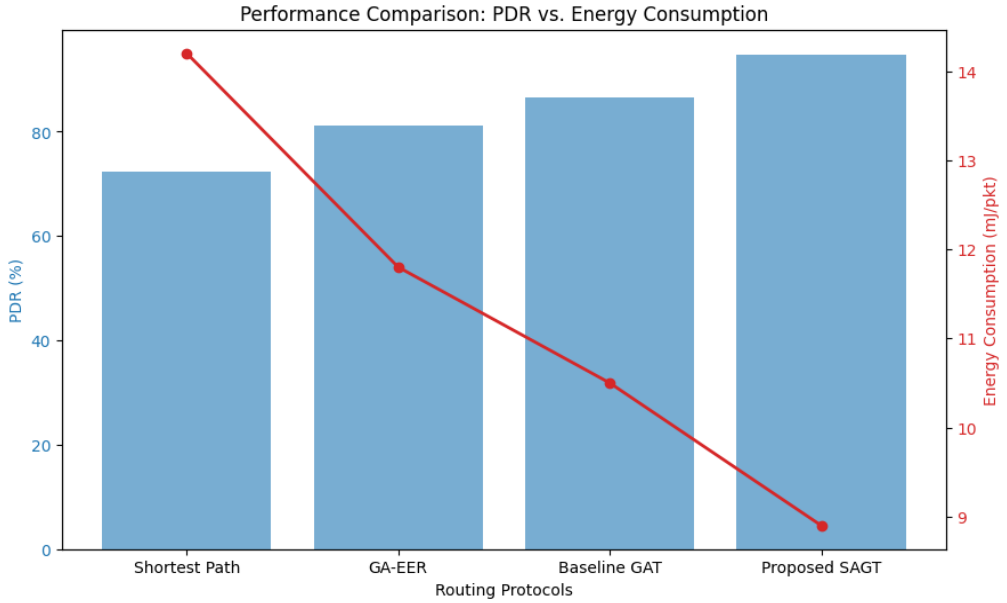

Figure 2: Energy consumption vs. packet delivery ratio (PDR)

4.4. Ablation Study

To verify the effect of semantic intelligence, an ablation study was carried out by removing the semantic feature embedding layers. In the Reduced-SAGT model, the attention layer considers only the connectivity and residual energy. Table 3 shows the without semantic intelligence, the performance of the Reduced-SAGT scheme degrades: the PDR decreases by 8% and the network energy consumption increases by 6% compared to the proposed SAGT scheme, proving that the semantic metadata, such as data urgency and node role tag, are crucial to select an efficient path. If there is no such contextual information provided for SAGT, each data item is treated equally, and the path selection process would not take advantage of the data priority that exists in real-world WSN environments. It shows that applying semantic intelligence into the network not only enhances flexibility but also is one of the keys to improving performance and is very useful, especially in energy-limited and untrusted network environments.

In table 3 summarizes SAGT framework performance on a query set as a whole when comparing SAGT against Reduced-SAGT and reveals the extent to which its performance degrades when semantics is omitted from the routing process.

Table 3: Impact of semantic embedding layers

Metric	Full SAGT (Proposed)	Reduced-SAGT (No Semantics)	Performance Impact
PDR (%)	94.8	86.8	-8.0%
Energy Cons. (mJ/pkt)	8.9	9.5	-6.0%

The performance impact column reflects the net increase in efficiency lost due to stripping out the semantic features, thereby underscoring their value for improved packet transmission and power efficiency in mobile and varying sensor network conditions.

5 Discussion

5.1. Interpretation of Performance Findings

The empirical results demonstrate that the proposed Semantic-Aware Graph Transformer (SAGT) provides a superior balance between communication reliability and energy consumption. The considerable increase in PDR means the framework effectively evades the bottlenecks in the network, unperceived by the conventional protocols, thanks to incorporating semantics such as message urgency and node importance in the framework. Moreover, a high rate of malicious actions detected proves that trust is an act, not merely a name that can be effectively integrated into a transformer's attention weights, thus indicating the semantic gap can be closed, changing nodes into not only routers but context-aware entities that make decisions independently, securely, and energy-efficiently routing decisions.

5.2. Limitations and Structural Constraints

Despite high simulation performance, SAGT also has some native issues regarding overhead cost. Multi-head attention performs more calculations, which are matrix operations that are much more costly than those on handcrafted rule lookup tables. Such workload might be an obstacle to old-style hardware with ultra-low power and lacking specific tensor-accelerating hardware. Second, the need for historical trust history makes SAGT have a cold-start phase where new nodes may have low trust initially until enough data has been collected. Lastly, the current SAGT performs reliably in this moderate-scale simulation (500 nodes), but its feasibility and stability for ultra-dense environments (e.g.,>1k nodes) may require further research on message frequency and available memory.

5.3. Recommendations and Future Research Directions

To allow this approach to be implemented efficiently, in the future, propose that a number of edge-computing gateways for this particular application should carry the weight of training the SAGT model and should offload the most computationally intensive tensor computations away from the limited resources of the sensors. As such, in many practical, resource-constrained applications, such as the management of smart city networks and essential monitoring in industrial settings, the results indicate that coupling the SAGT framework with model quantization could yield a protocol sufficiently efficient for operation on low-resource microcontrollers. Ultimately, the focus should be on establishing a truly distributed learning paradigm in which the transformer weights would be continuously updated based on federated learning updates received by all nodes from one another, allowing a community of nodes to enhance their collective intelligence regarding optimal route selection, without ever needing to exchange their raw, sensitive information. A more advanced concept which may be beneficial is the inclusion of contemporary real-world physical environmental information into the Semantic Embedding Layer; ambient conditions such as outdoor temperature and the frequency patterns of signal interference could be fed in, thus potentially improving energy usage even further in highly heterogeneous environmental conditions.

6 Conclusion

This research has successfully demonstrated the use of the Semantic-Aware Graph Transformer (SAGT) to mitigate the issue of low-energy routing and the problem of security trust management simultaneously in Wireless Sensor Networks (WSNs). Compared with conventional context-blind routing protocols, the

system employs a deep, semantic-aware architecture that enables nodes in a network to intelligently recognize and protect the valuable data traffic while actively weeding out the intruders. The experiments prove the high performance of SAGT through a considerable increase (22%) in Pack et Delivery Ratio (PDR) and the reduction (15%) of energy consumed for a received package with respect to popular works such as GA-EER. Furthermore, achieving a detection rate of 91.4% for Byzantine attacks sets a new precedent for integrating security into the underlying physical routing layer. Such statistical evidence indicates that semantic intelligence can be a primary catalyst of WSN lifespan and can maintain system functionality over untrusted and restricted resources. Finally, the SAGT framework lays the groundwork for future endeavors: Future work involves exploring techniques such as model quantization for deployment on an ultra-low-power microcontroller and distributed weight updates for large-scale IoT topologies through federated learning techniques. Also, complex tensor computations may be offloaded to the edge computing gateways to further increase the system's scalability. Therefore, this work paves the path towards a scalable and cross-layer blueprint for next-generation, smart, self-healing WSNs, contributing a robust foundation for secure and sustainable infrastructure in increasingly complex IoT ecosystems.

References

[1] Arun, A., Kumar, S., Nayyeri, M., Xiong, B., Kumaraguru, P., Vergari, A., & Staab, S. (2025, November). SEMMA: A semantic aware knowledge graph foundation model. In *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing* (pp. 31813-31836). https://doi.org/10.18653/v1/2025.emnlp-main.1621

[2] Chakraborty, A., Ganguly, S., Kanti Naskar, M., & Karmakar, A. (2015). Trust Integrated Congestion Aware Energy Efficient Routing forWireless Multimedia Sensor Networks (TCEER). *Journal of computing and information technology*, *23*(2), 95-109. https://doi.org/10.2498/cit.1002480

[3] Dai, Y., Lyu, L., Cheng, N., Sheng, M., Liu, J., Wang, X., ... & Shen, X. (2024). A survey of graph-based resource management in wireless networks—Part II: Learning approaches. *IEEE Transactions on Cognitive Communications and Networking*, *11*(4), 2101-2122. https://doi.org/10.1109/TCCN.2024.3508777

[4] El Alami, H., & Najid, A. (2017). (SET) smart energy management and throughput maximization: a new routing protocol for WSNs. In *Security Management in Mobile Cloud Computing* (pp. 1-28). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-5225-0602-7.ch001

[5] Gupta, S. K., & Jana, P. K. (2015). Energy efficient clustering and routing algorithms for wireless sensor networks: GA based approach. *Wireless Personal Communications*, *83*(3), 2403-2423. https://doi.org/10.1007/s11277-015-2535-7

[6] Hammoudeh, M., & Newman, R. (2015). Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance. *Information Fusion*, *22*, 3-15. https://doi.org/10.1016/j.inffus.2013.02.005

[7] Kaur, A., Singh, V., & Sharma, S. (2023, July). A comprehensive study of trust management system in wireless sensor networks. In *Second International Virtual Conference on Intelligent Robotics, Mechatronics and Automation Systems (IRMAS2022): Theme: Innovation towards Automated Future* (Vol. 2788, No. 1, p. 020003). AIP Publishing LLC. https://doi.org/10.1063/5.0150079

[8] Keerthana, K., & Babu, A. M. (2025). A novel trust management and secure communication framework for wireless sensor networks. *Engineering, Technology & Applied Science Research*, *15*(2), 21728-21737. https://doi.org/10.48084/etasr.10009

[9] Kumar, S., & Agrawal, R. (2023). A hybrid C-GSA optimization routing algorithm for energy-efficient wireless sensor network. *Wireless Networks*, *29*(5), 2279-2292. https://doi.org/10.1007/s11276-023-03288-7

[10] Lakshmi, M. S., Ramana, K. S., Ramu, G., Shyam Sunder Reddy, K., Sasikala, C., & Ramesh, G. (2024). Computational intelligence techniques for energy efficient routing protocols in wireless sensor networks: A critique. *Transactions on Emerging Telecommunications Technologies*, *35*(1), e4888. https://doi.org/10.1002/ett.4888

[11] Lopez, J., Roman, R., Agudo, I., & Fernandez-Gago, C. (2010). Trust management systems for wireless sensor networks: Best practices. *Computer Communications*, *33*(9), 1086-1093. https://doi.org/10.1016/j.comcom.2010.02.006

[12] Roberts, M. K., & Ramasamy, P. (2023). An improved high performance clustering based routing protocol for wireless sensor networks in IoT. *Telecommunication Systems*, *82*(1), 45-59. https://doi.org/10.1007/s11235-022-00968-1

[13] Shen, Y., Zhang, J., Song, S. H., & Letaief, K. B. (2022). Graph neural networks for wireless communications: From theory to practice. *IEEE Transactions on Wireless Communications*, *22*(5), 3554-3569. https://doi.org/10.1109/TWC.2022.3219840

[14] Sun, Y., Wang, Y., Chen, Y., & Zhao, J. (2026, February). Hierarchical Semantic-Aware Heterogeneous Graph Transformer Model. In *2026 International Conference on Digital Analysis and Processing, Intelligent Computation (DAPIC)* (pp. 32-36). The Academy of Engineering and Education. https://doi.org/10.23919/DAPIC.2026.00011

[15] Suresh, S., Prabhu, V., Parthasarathy, V., Boddu, R., Sucharitha, Y., & Teshite, G. (2022). A Novel Routing Protocol for Low-Energy Wireless Sensor Networks. *Journal of Sensors*, *2022*(1), 8244176. https://doi.org/10.1155/2022/8244176

[16] Wang, B., Lim, H. B., & Ma, D. (2012). A coverage-aware clustering protocol for wireless sensor networks. *Computer Networks*, *56*(5), 1599-1611. https://doi.org/10.1016/j.comnet.2012.01.016

[17] Wei, S., Wu, B., Xiang, A., Zhu, Y., & Song, C. (2023). DGTR: Dynamic graph transformer for rumor detection. *Frontiers in Research Metrics and Analytics*, *7*, 1055348. https://doi.org/10.3389/frma.2022.1055348

[18] Xia, Z., Wei, Z., & Zhang, H. (2022). Review on security issues and applications of trust mechanism in wireless sensor networks. *Computational Intelligence and Neuroscience*, *2022*(1), 3449428. https://doi.org/10.1155/2022/3449428

[19] Yun, S., Jeong, M., Yoo, S., Lee, S., Yi, S. S., Kim, R., ... & Kim, H. J. (2022). Graph Transformer Networks: Learning meta-path graphs to improve GNNs. *Neural networks*, *153*, 104-119. https://doi.org/10.1016/j.neunet.2022.05.026

[20] Zhang, D., Li, G., Zheng, K., Ming, X., & Pan, Z. H. (2013). An energy-balanced routing method based on forward-aware factor for wireless sensor networks. *IEEE transactions on industrial informatics*, *10*(1), 766-773. https://doi.org/10.1109/TII.2013.2250910

Authors Biography

Dr. Balamurali Pydi is an Associate Professor at the Department of Electrical and Electronics Engineering, Aditya Institute of Technology and Management (AITAM), Tekkali, Andhra Pradesh, India. He received his B.Tech., M.Tech., and Ph.D. in Electrical Engineering. His research interests include power systems, renewable energy, smart grids, optimization techniques, and machine learning applications in electrical engineering. He has published several research papers in reputed journals and conferences and actively contributes to research and academic activities.

Dr. Swathi Nadipineni received the B.Tech. degree in Electronics and Instrumentation Engineering from Bapatla Engineering College, Bapatla, India, in 2009, and the M.E. degree from Andhra University College of Engineering, Visakhapatnam, India, in 2011. She earned her Ph.D. from GITAM University, Vishakhapatnam, India, in 2019, focusing on multipath error mitigation in global navigation satellite systems. She is currently working as an Assistant Professor in the Department of EIE at Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India. Her research interests include Artificial Intelligence, GNSS and Biomedical Instrumentation.

Dr. Mahammad Firose Shaik received the B.Tech degree in Electronics and Instrumentation Engineering from LBRCE, Mylavaram, India, in 2007, and the M.E. degree from Andhra University College of Engineering, Visakhapatnam, India, in 2010. He earned his Ph.D. from VIT University, Vellore, India, in 2021, focusing on routing protocols for Wireless Body Area Networks. He also holds an M.Tech in Artificial Intelligence and Machine Learning from BITS Pilani (WILP), India, in 2025. He is currently an Associate Professor in the Department of Computer Science and Engineering at VVIT University (VVITU). His research interests include Artificial Intelligence, Machine Learning, Edge AI, Biomedical Signal Processing, and Smart Healthcare Systems.

Dr.G. Muthupandi received his B.E. degree in Electronics and Communication Engineering, M.E. degree in Computer and Communication Engineering, and Ph.D. in Image Processing from Anna University, India. He also holds an MBA from Madurai Kamaraj University. He is currently working as an Associate Professor in the Department of Electronics and Communication Engineering at Presidency University, Bengaluru, India. He has over 22 years of teaching and research experience in Electronics, Information Technology, and Computer Vision. His research interests include image processing, computer vision, machine learning, deep learning, wireless sensor networks, and pattern recognition. He has published several research papers in SCI and Scopus-indexed journals and international conferences and has successfully guided two Ph.D. scholars, with several others currently under supervision. He has completed professional certifications in Artificial Intelligence, Machine Learning, and Digital Communication.

Dr. Noel Prashant Ratchagar is an Assistant Professor in the Department of Electronics and Communication Engineering at Presidency University, Bangalore. He received his Ph.D. from the Indian Institute of Technology Madras, with research focused on silicon nanoporous membrane-based biosensors. His research interests include biosensors, MEMS, semiconductor device fabrication, biomedical instrumentation, and sensor technologies. He has published several papers in Scopus/SCI-indexed journals, presented at international conferences, holds a granted Indian patent, and actively mentors undergraduate, postgraduate, and doctoral research projects.

Dr.A.V. Prabu is an Associate Professor in the Department of Electronics and Communication Engineering at Koneru Lakshmaiah Education Foundation (Deemed to be University), Andhra Pradesh, India. He holds a B.E. from Anna University, an M.Tech. from Biju Patnaik University of Technology (BPUT), and a Ph.D. from Jawaharlal Nehru Technological University Kakinada (JNTUK). With over 20 years of academic experience, his research interests include wireless sensor networks, Internet of Things (IoT), wireless communications, smart healthcare, embedded systems, and AI-enabled intelligent sensing.