International Journal of Communication Systems

WILEY

RESEARCH ARTICLE

SmartRoute Optimization Network: Anomaly-Aware Energy-Efficient Routing for Real-Time Landslide Monitoring in WSNs

G. V. Soni Meera[1] | R. Isaac Sajan[2]

[1]Department of Electronics and Communication Engineering, Marthandam College of Engineering & Technology, Kuttakuzhi, Tamil Nadu, India | [2]Department of Electronics and Communication Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India

Correspondence: G. V. Soni Meera (sonimeeragv@gmail.com)

Received: 10 March 2025 | **Revised:** 18 July 2025 | **Accepted:** 13 December 2025

Keywords: energy-efficient routing | malicious node detection | outlier management real-time landslide monitoring | SmartRoute optimization network

ABSTRACT

Wireless sensor networks (WSNs) are crucial for applications such as environmental monitoring, smart cities, and disaster detection, but they face significant challenges from malicious nodes, outliers, and routing inefficiencies. These issues hinder network performance and reliability, while existing solutions often fall short due to high computational demands and limited scalability. This paper introduces the SmartRoute optimization network: anomaly-aware energy-efficient routing for real-time landslide monitoring in WSNs (SRON), an innovative framework designed to enhance reliability and energy efficiency in WSNs, especially for landslide monitoring. The SRON framework integrates three core methodologies: dynamic position bias for malicious node detection, grouped query attention for precise outlier management, and SmartPPO for optimized routing. The dynamic position vias module identifies and isolates malicious nodes to prevent false data from disrupting network accuracy. The grouped query attention mechanism improves outlier detection by clustering sensor readings, thereby filtering anomalies and reducing false alarms. Furthermore, the integration of PPO with the attention sink mechanism enhances routing efficiency, enabling energy-aware, reliable data transmission while focusing on critical data points. The developed SRON framework is rigorously tested in Python using more complex simulation parameters, achieving a malicious node detection accuracy of 96%, an outlier detection accuracy of 95%, and a routing efficiency improvement of 94%. These results underscore SRON's capability to address modern WSN challenges, offering a comprehensive, adaptive, and resource-efficient solution for real-time landslide detection and other critical monitoring applications in complex environments.

1 | Introduction

Real-time landslide monitoring using wireless sensor networks (WSNs) [1] faces significant challenges not only from environmental factors but also from the presence of malicious nodes [2] and outliers [3] that can compromise data integrity and network performance. Malicious nodes are those that intentionally disrupt the network by injecting false data, dropping packets, or even disabling other nodes. Outliers, on the other hand, refer to abnormal data readings resulting from sensor malfunctions, environmental noise, or unexpected changes in the monitored parameters. Both malicious nodes and outliers can severely affect the reliability of landslide predictions and the overall functionality of WSNs.

In addressing these issues, research has used different methods and approaches. For identifying malicious nodes, anomaly detection techniques [4, 5] on have been very much used [6, 7]. In fact, these methods scan the behavior of individual nodes against the expected patterns and point out those that do

© 2026 John Wiley & Sons Ltd.

abnormal activities, such as unusual data transmission rates or energy consumption profiles. Machine learning algorithms [7], including supervised and unsupervised models [8, 9], have been explored to classify nodes based on historical data and real-time behavior, enhancing the network's ability to distinguish between benign and malicious activities.

Outlier detection techniques were added to WSNs for landslide monitoring. Statistical techniques such as z-score analysis [10] are applied with an interquartile range (IQR) [11] for identification and data point filtration to ensure valid readings feed into the final analysis. More advanced techniques, including data fusion [12] and consensus algorithms [13], have been used to make sensor data more robust by averaging inputs from several nodes toward a consensus of the best measurements. Other adaptive thresholding methods [14, 15] have also been proposed, which can adaptively adjust the sensitivity levels according to environmental conditions, thus helping to differentiate between normal fluctuations in data and actual outliers.

Despite all these developments, there still remain some serious shortcomings of the existing approaches that treat malicious nodes and outliers. Hence, they may have very high false positive rates (FPRs), flagging benign nodes as malicious or not actually detecting the threats at all. Moreover, the machine learning models are generally very data-intensive to train and computationally expensive, which is not feasible in all the resource-constrained WSN environments. Other variations include reputation-based systems [16, 17], in which the existence of a collusive attack is still probable due to groups of miscreant nodes collaborating to stay ahead in the network.

The challenges of routing in the presence of malicious nodes and outliers add another layer of complexity. Traditional routing algorithms [18, 19] were designed with no consideration of the compromised nodes and therefore are sensitive to disruptions from data falsification or node failures. The overhead in terms of communication and energy consumption in routing protocols against attacks degrades the overall performance of the WSN. Most of the existing approaches rely on static routing paths that do not adapt to changing network conditions or the presence of unreliable nodes, leading to increased delays in data transmission and reduced resilience against potential attacks.

In summary, despite the various techniques that have been proposed to detect malicious nodes, identify outliers, and enhance routing in WSNs for real-time landslide monitoring, significant challenges remain. Current methods face problems with adaptability, scalability, and trade-off between security and performance. There is a need for novel methods to combine anomaly detection, data fusion, and robust routing protocols to produce a sustainable monitoring system in the sense that it should remain of high accuracy and reliability even under adversarial conditions and environmental variability.

This paper will achieve next-generation advanced routing protocols and detection mechanisms, besides integration of machine learning techniques for WSNs with Smart Resilient Optimal Network (SRON) method:

- Malicious Node Detection: Incorporating a dynamic position bias module that can detect and isolate malicious nodes in the network. This prevents false data injection through the detection of inconsistencies in sensor behavior, thus maintaining the integrity of the data being transmitted and enhancing the overall security of the WSN.
- Effective Outlier Management: By implementing the grouped query attention mechanism, the SRON effectively manages outliers and minimizes false alarms while it is implemented in the SRON. The grouped query attention segments data for the accurate processing of sudden fluctuations in sensor readings to identify anomalous data points and handle them without damaging the integrity of the monitoring system
- Optimized routing: The SRON framework significantly improves data accuracy and optimizes routing through SmartPPO the integration of the proximal policy optimization (PPO) with attention sink mechanism. By utilizing the attention sink to filter out redundant information, the system focuses on critical environmental data, ensuring that only the most relevant readings are processed. The incorporation of PPO facilitates energy-efficient routing by determining the most reliable paths for data transmission, ensuring the timely delivery of crucial information for landslide detection and response. Together, these features enhance the overall effectiveness of real-time monitoring efforts.

This paper is organized as follows: Section 2 reviews relevant research on the topic. Section 3 presents the proposed methodology. Section 4 presents the experimental results and their analysis. Finally, Section 5 draws conclusions.

2 | Related Work

Several researchers developed systems in the context of improving detection and efficiency of WSNs using secure routing protocols and intrusion detection mechanisms, while these proposed solutions bring many merits, scalability, complexity, and the dynamic nature of such networks present great challenges.

Wang et al. [20] proposed a malicious node detection strategy for WWSNs using dynamic trust management integrating type-2 fuzzy logic to evaluate multiple factors for trust assessment in node nodes. This technique does comprise a dynamic mechanism that updates the trust value by dynamically changing the environment condition due to extreme scenarios of deployment. However, some drawbacks of this method include the complex implementation of fuzzy logic with significant computational resources and difficulty in defining and measuring trust factors, which can affect the reliability and timeliness of the detection of malicious nodes.

Zhai et al. [21] proposed a secure detection service for WSNs that uses a lightweight timestamp-based message authentication code integrated with exclusive OR network coding to monitor and manage message integrity in real time. This approach allows for the simultaneous detection of pollution and

replay attacks while maintaining low communication bandwidth and computational complexity. The correctness of the detection mechanism is demonstrated, and performance evaluations indicate that it incurs minimal overhead compared with traditional MAC–based schemes and consumes less energy than other joint detection strategies. However, this relies on time synchronization that is not easily implemented in dynamically changing environments, and without strict maintenance, it creates vulnerabilities, and the scope of the detection service is very narrow due to its focus on pollution and replay types of attacks.

A recent transformer architecture with a spatio-temporal attention mechanism was proposed by Kumar et al. [22] to design a dynamic context-capturing deep learning model for anomaly detection in WSNs that automatically identifies anomalous data streams induced by interference or malfunctioning nodes through the sensing of the dynamic context of the sensor data. The model, developed and evaluated on a dataset that was publicly available of a water treatment plant setting, demonstrates impressive performance characteristics, such as accuracy and F1-score, precision measures that have outperformed other state-of-the-art in the domain. However, there may also be drawbacks. Complexity of models might assume vast computational resources for either the training or the real-time inference and would rely for effective training on high-quality labeled datasets that are certainly not always readily available in more diverse operational environments.

Revanesh et al. [23] proposed an approach that intends to extend the lifespan of WSNs with intelligent energy management models and also enhanced the routing protocols of LEACH and EESR for improved performance in the area of WSNs. Utilizing the LMNN in a more refined manner, the system ensures improvements in energy efficiency with proper data quality; the need for fewer sensors becomes possible with this approach, making the environment monitor effective. Further, from the results, it can also be concluded that the introduced IDS based on the ANN-ILMNN methodology is efficient enough to realize anomaly detection through the optimum features. The main disadvantages of this approach include the complexities and computational overhead associated with the implementations of neural networks that could limit scalability in large WSN deployments and require a fair amount of training data for efficient learning.

Kalaivanan et al. [24] have proposed energy-efficient and reliable data collection protocol (EERDCP), which very effectively reduces these drawbacks by using WSNs with drone technology to monitor landslides in landslide-prone areas in real time. The system starts by deploying many sensor nodes continuously collecting data on soil condition, pressure of water, and rainfall in the area. The data are routed through a tap root-based routing topology where nodes are selected based on residual energy and distance using fuzzy logic. The gathering drones minimize the need for long-range transmission, hence minimizing the draining of battery life. This approach increases monitoring efficiency as well as minimizes man risk, but it may find challenges in remote or difficult terrains of connectivity, thereby requiring continuous enhancement in terms of network reliability.

The critical issues in WSNs include unbalanced distribution of sensor nodes, inefficient energy consumption, and low network lifetime. All the above problems are covered by Niti et al. [25], who gave the three-tier extended energy efficient clustering hierarchy (TEEECH) algorithm. TEEECH-based technique offers enhanced cluster head selection by the ADV-LEACH2 algorithm and utilizes the modified fuzzy-C mean clustering technique to uniformly distribute the SN among the clusters. The process begins by first choosing the cluster heads based on their energy and distance from the base station. Subsequently, it constructs the clusters that are energy optimized. This has the profound effect of increasing the network stability and overall lifetime of the WSN. The proposed TEEECH approach provides a significant improvement in energy efficiency and network performance, though, of course, at the cost of added complexity in implementation besides computational resources compared with traditional methods.

Energy consumption is among the main issues in WSNs that usually result in the early failure of a node and reduction of lifetime in the network. Yin et al. [26] discuss a clustering routing protocol known as tuna swarm optimization and fuzzy control (TSFC), which is based on the problem of drawbacks associated with the clustering protocols. This technique initializes the network parameters. Then, it clusters the network by using TSO to optimize the structure of the cluster and decrease communication distances. The fuzzy controller then assesses the fitness of nodes for the CH by ranking the residual energy and distance metrics of various candidate nodes. Then, it manages the normal nodes on how they conduct the transmission toward the base station under the CHs so that there is good data fusion and communication. The advantages are energy efficiency enhancement and longer network lifetime. The drawback is the complexity of implementing the fuzzy control mechanism.

Techniques between sensor nodes always cause uneven energy consumption problems in energy efficiency and the longevity of the network. Therefore, Vipul et al. [27] developed an enhanced fuzzy–based energy-efficient routing protocol called E-FEERP using the dynamic clustering technique via particle swarm optimization with a fuzzy-based routing approach by selecting the best route to BS based on the node energies and distances to BS. This approach improves network performance with enhanced throughput and a high packet delivery ratio (PDR) at low energy consumption. However, the major limitation of E-FEERP is that it has increased computational complexity in comparison with the other relatively simpler protocols that need greater processing power and more time to implement.

Energy inefficiency leads to reduced network lifetime and maximum packet loss in the network during data transfer. This limitation may be overcome with the assistance of the meta inspired Hawks fragment optimization system presented by Meenakshi et al. [28]. The operational principle of this system bases its approach on the heuristic wing antfly optimization (HWAFO) algorithm to ensure selection of proper cluster heads and routing pathways for maximizing the delivery rate of data along with minimizing power consumption. The benefit is the ability to allow high throughput along with a low packet drop ratio; a possible drawback might be that this algorithm would be complex and require more computational capabilities.

Tumula et al. [29] proposed the enhanced bio-inspired energy-efficient localization (EBEEL) for WSNs to overcome some of the most challenging problems identified within the context of disasters. Those are data aggregation, bandwidth limitation, scalability issues, energy consumption, and QoS. Inspired by the biological systems with a nature of adaptation, self-organization, and auto healing, it improved routing efficiency (RE) and resistance capabilities to environmental disasters. However, EBEEL would still suffer from shortcomings of potential complexity in implementation, reliance on accurate localization, and the need to continue evolving with environmental changes, which increases overhead and may slow down response time in emergencies.

3 | System Model

The SRON framework operates through a structured sequence of data collection, filtering, and optimized routing to ensure reliable landslide monitoring in WSNs. Initially, environmental data such as rainfall, slope angle, and soil saturation are collected from sensor nodes and preprocessed to remove noise and detect outliers. The filtered data are then processed through the attention sink mechanism, which eliminates redundant information and prioritizes critical environmental inputs. To maintain data integrity, the system identifies and isolates malicious nodes using dynamic position bias and filters outliers through the grouped query attention mechanism. Following this, the PPO algorithm dynamically selects the most energy-efficient and reliable routing paths, avoiding flagged malicious nodes and unstable network regions. Finally, the refined data are analyzed by a prediction model to assess landslide risks and generate timely alerts in high-risk scenarios. This process is governed by Equation (1):

$$Output(D_i) = \sum_{i=1}^{N} \left(AS(D_i) \times PPO(Route((D_i))) - M(D_i) - O(D_i)\right) \tag{1}$$

where $AS(D_i)$ filters redundant data through the attention sink, $PPO(Route((D_i)))$ routes it efficiently, and $M(D_i)$ and $O(D_i)$ account for malicious nodes and outliers, respectively. This integrated approach enhances reliability, efficiency, and the accuracy of real-time landslide predictions.

3.1 | Proposed Methodology

This paper will create a robust framework for critical challenges of WSNs. Those critical challenges include the following: malicious nodes, outliers, and energy efficient routing through advanced techniques in machine learning. The architecture and methodologies proposed are detailed in Figure 1.

Figure 1 represents the anomaly-aware grouped query attention–based crossform transformer designed for sensor data processing. This architecture uses an encoder–decoder structure to effectively handle grouped and weighted aspects of input data, with a focus on anomaly detection. This transformer architecture enhances anomaly detection in sensor networks by leveraging Dynamic position bias ensures temporal and structural coherence across the inputs and outputs. Grouped query attention allows the model to focus on key aspects of the data while minimizing noise.

3.1.1 | Data Preprocessing

The crossform transformer model uses a labeled landslide dataset with multi-sensor environmental inputs such as soil moisture, rainfall, ground vibration, temperature, and slope angle, with each data sample annotated by landslide risk levels (low, moderate, high risk). The data preprocessing stage begins by handling missing sensor readings using linear interpolation, while outlier values are filtered through z-score thresholding. All features are normalized using min–max scaling to maintain consistent input ranges. To preserve temporal dependencies, the continuous sensor streams are segmented into fixed-size time windows, and relevant statistical features such as mean, variance, and trend are extracted. Furthermore, data augmentation techniques like temporal shifting, random dropout of sensor streams, and SMOTE are applied to address class imbalance and improve model robustness.

3.1.1.1 | Risk Area Detection With Crossform Transformer. Following data preprocessing, the processed multi-sensor inputs are passed into the crossform transformer architecture. The pipeline starts with an input embedding layer, which transforms both continuous and categorical features into a unified high-dimensional representation suitable for deep learning. The model architecture is based on an encoder–decoder structure, where the encoder captures relevant spatial and temporal patterns from multi-sensor inputs, and the decoder predicts the landslide risk level or event occurrence. A key highlight of the model is its use of grouped query attention to focus on grouped environmental factors (e.g., rainfall and soil moisture together), and dynamic position bias to effectively capture temporal dependencies within segmented time windows. The training is performed in a fully supervised manner using a weighted cross-entropy loss function, where higher weights are assigned to positive landslide events to counteract class imbalance and prioritize high-risk detection. For optimization, the AdamW optimizer is employed along with an adaptive learning rate scheduler that adjusts the learning rate dynamically based on validation performance. To prevent overfitting, early stopping is used, where training halts if the validation loss fails to improve over a set number of epochs. Training is conducted using mini-batch gradient descent, processing the data in smaller batches to ensure stable and efficient convergence. The model is trained for a fixed number of epochs, with regular validation checks, ensuring generalization to unseen data and robustness against overfitting. This training setup ensures the crossform transformer effectively captures the intricate relationships between environmental factors and landslide occurrences.

The SRON architecture is designed to provide robust monitoring and response capabilities for landslide detection by leveraging data processing, malicious node isolation, outlier management, and energy-efficient routing mechanisms. In the overall workflow, sensor nodes collect environmental data, such as soil moisture, temperature, and vibration,

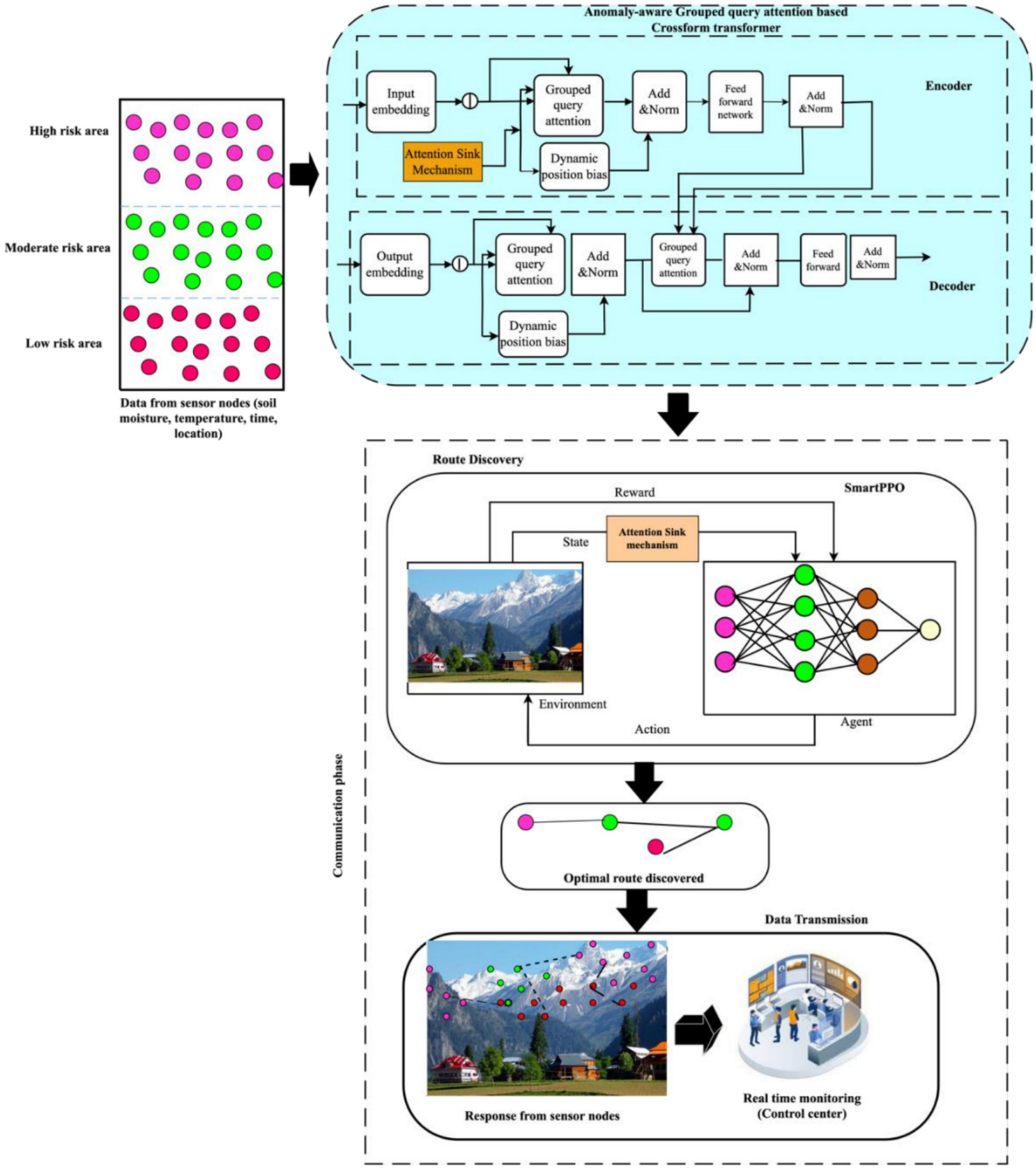


FIGURE 1 | Architecture of SmartRoute optimization network.

which are then processed to identify risk areas, outliers, and malicious nodes. A crossform transformer aggregates and prioritizes critical data by applying an attention mechanism. Malicious nodes are detected and isolated by calculating a deviation score, while outliers are identified by comparing data points to cluster means. An optimized routing protocol, enhanced with PPO, ensures that data travels through secure and efficient paths, avoiding hotspots, malicious nodes, and areas marked as high-risk. Finally, the system calculates a landslide risk score L based on environmental variables by using Equation 2:

$$L = \sum_{i=1}^{n} w_i x_i \tag{2}$$

where w_i are weights representing the importance of each environmental factor x_i. This score triggers alerts and automated response protocols if a threshold is exceeded.

The input data get the transformations first from input embedding to its encoder–decoder pipeline, taking the input, converting it into embedding with the help of hierarchically multi-level encoded captures and grouping it accordingly according to multi-sensory input from grouped query attention, which allows contextual similarity detection among diverse multiple sensors inputs and, for that purpose, performs aggregate operations as an ensemble representation for recognizing anomalies in streams of diversified data along relations among any given sets. To preserve the temporal and spatial order of the data, a dynamic position bias module adds dynamic positional information to the grouped queries. The add and norm residual connections stabilize the learning process following the attention operation. Feature transformation and representation capability are enhanced by a feedforward network. The output from the encoder is the sensor data that are grouped and weighted according to the importance of various attributes for anomaly detection. Output embedding is used in the decoder flow, and the output or the previous input to the autoregressive task is transformed to an embedded form. In this decoder, grouped query attention focuses selectively on important parts of the encoded input. The decoder uses dynamic position bias, which maintains sequence structure and uses add and norm in decoding information while refining through feedforward layers. Finally, cross attention between the encoder and decoder provides efficient mapping from the input to output while taking effective care of group-wise anomalies.

At the heart of the SRON framework lies the crossform transformer module; it serves as a central component to identify landslide risk areas by cross-checking data across numerous sensors to focus on critical environmental factors such as soil moisture, seismic activity, and ground stability. This assigns different importance levels to each sensor reading using multi-head self-attention mechanisms. Thus, the model can focus on areas where environmental shifts are more likely to signal potential landslides.

The attention mechanism in the crossform transformer is mathematically represented by:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{3}$$

where Q, K, and V are query, key, and value matrices derived from the sensor data. The scaling factor d_k ensures numerical stability by adjusting the scores. This formula well quantifies the importance of different sensor readings, showing regions of significant change and down-weighting stable or irrelevant data. The attention-driven approach will allow the system to maintain awareness continuously over high-risk zones, thus facilitating more precise landslide prediction and timely alerts. The architecture of the crossform transformer ensures to maintain data integrity by essentially acting as a preliminary filter by segmenting the risk-prone areas from stable regions. Such information, detected within these specific regions with sudden environmental changes, is further processed using downstream modules. Furthermore, the segmentation abilities of the transformer allow the SRON framework to contextualize the sensor readings and provide an understanding with multiple dimensions to each of the identified risk areas.

3.1.1.2 | Malicious Node Detection and Isolation via Dynamic Position Bias. The crossform transformer first analyzes network data to identify critical regions, which are then passed to the dynamic position bias module for further evaluation. This module is designed to detect hostile nodes that may introduce malicious data by masking environmental measurements or distorting communication patterns. Meanwhile, the SRON framework continuously monitors sensor nodes, tracking key metrics such as energy consumption, packet forwarding rates, and connectivity patterns. Nodes exhibiting anomalies—such as unusually high energy usage, irregular packet forwarding, or inconsistent connectivity compared with the majority—are flagged as suspicious. The dynamic position bias module quantifies these deviations mathematically, enabling real-time identification of potentially malicious nodes without relying on predefined attack signatures. The workflow of dynamic position bias is given in Figure 2.

The detection process relies on calculating a behavioral deviation score D_i for each node i:

$$D_i = \sum_{j=1}^{m} \left| B_{i,j} - Expected_j \right| \tag{4}$$

where $B_{i,j}$ represents the historical average of metric j of node i calculated across trusted, previously identified benign nodes over a sliding window of recent rounds. This expected value acts as a baseline to measure deviations from normal behavior, and $Expected_j$ is the expected value of this metric. The $Expected_j$ value is determined by calculating the average value of a specific metric j (such as energy consumption, packet forwarding rate) across a set of trusted nodes that have been previously identified as benign. To ensure the detection process remains adaptive to recent network conditions, this calculation is performed over a sliding window of recent rounds. Specifically, the metric values of all trusted benign nodes are collected over the most recent W rounds, and the expected value is computed as the average of these observations. This sliding window approach helps to capture the normal behavior trends in real time. The resulting $Expected_j$ serves as a baseline reference point, against which the current behavior of any node is compared with detect abnormal or potentially malicious deviations. The expected value of metric j is computed using Equation (5):

$$Expected_j = \frac{1}{N \times W} \sum_{n=1}^{N} \sum_{w=1}^{W} Metric_{j,n,w} \tag{5}$$

This equation is used to determine if a node is behaving maliciously based on its energy consumption, packet forwarding, and connectivity metrics.

$$T_{malicious} = B_1 \cdot E_i + B_2 \cdot P_{f,i} + B_3 \cdot C_i + B_4 \cdot D_i \tag{6}$$

where E_i is the energy level of node i, $P_{f,i}$ the Packet forwarding rate of node i, C_i is the connectivity score of node i (e.g., number of neighbors), D_i is the delay or response time of node i, and B_1, B_2, B_3, and B_4 are weights representing the importance of each parameter in identifying malicious behavior.

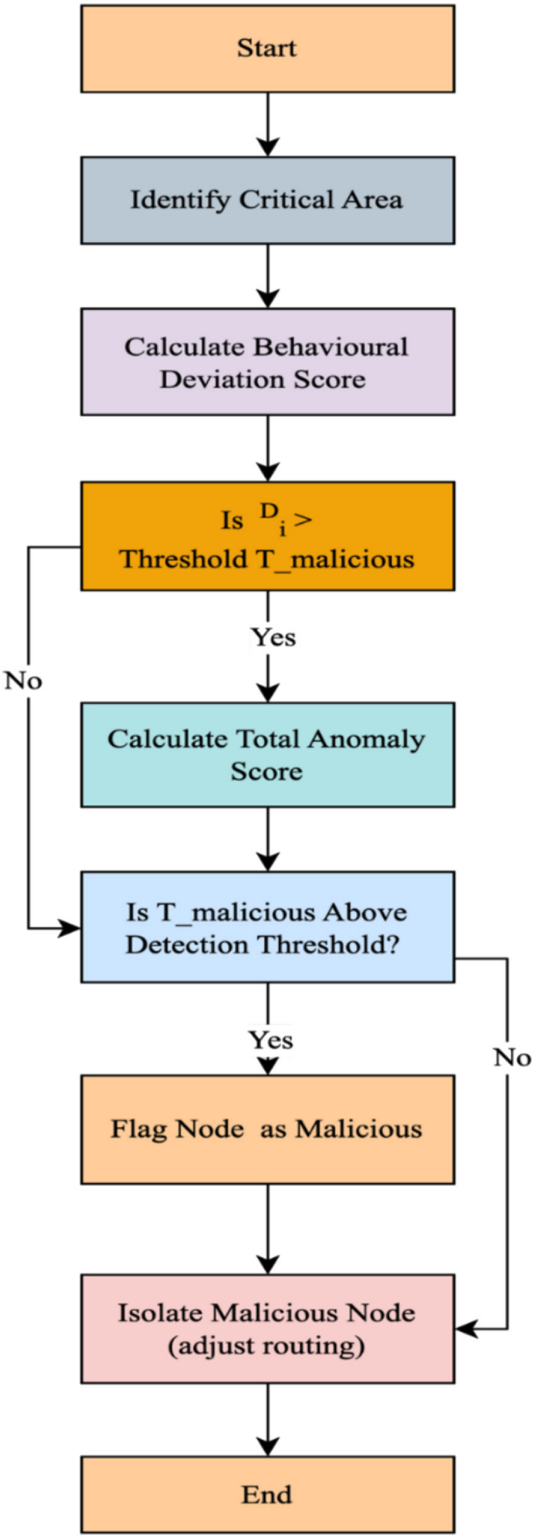


FIGURE 2 | Workflow of dynamic position bias.

If the anomaly score D_i exceeds a predefined threshold $T_{malicious}$, the node is flagged as malicious. The dynamic position bias module adjusts routing decisions to avoid the flagged nodes. The isolation of such potential threats from participating in data transmissions is thus achievable. As a result, the network security is preserved, given that malicious nodes cannot introduce false data nor influence routes. While Equation (4) quantifies the deviation of a node's behavior from the network norm (expected values), Equation (6) computes an overall maliciousness score by linearly combining individual metrics using predefined weights. This allows the system to flexibly prioritize certain metrics (e.g., energy, delay) depending on environmental and operational context. The deviation score from Equation (4) can optionally be included as an additional term in Equation (6) for composite anomaly scoring.

The adaptive nature of the dynamic position bias allows it to recalibrate its detection criteria in real time, responding to patterns of attacks or changes in the network topology. When the patterns emerge to show suspicious activities, it would update its threshold values to ensure high detection accuracy (DA). It is especially useful in landslide areas where environmental conditions and sensor readings may change abruptly.

3.1.1.3 | Outlier Management With Grouped Query Attention Mechanism. After the malicious node is identified, the grouped query attention mechanism will continue to screen the data for outliers. In landslide detection, spikes or falls in sensor readings can be caused by environmental setting changes, sensor errors, or interference from external sources. These outliers are detected and controlled in a grouped query attention mechanism not to cause false alarms or disrupt routing processes. The grouped query attention mechanism manages outliers of sensor data by clustering reading based on geographic proximity and environmental similarity. Each cluster of readings $X = \{x_1, x_2, \ldots \ldots x_n\}$ is processed to identify outliers using statistical deviation.

This mechanism segments data into clusters based on geographic or environmental similarity, allowing it to compare sensor readings within localized contexts. For each data point x_i within a cluster, an outlier score $O(x_i)$ is computed as follows:

$$O(x_i) = \frac{|x_i - \mu_X|}{\sigma_X} \tag{7}$$

where μ_X and σ_X are the mean and standard deviation of the cluster X.

This equation assesses whether a node's behavior is significantly different from the expected norm, indicating it as an outlier

$$T_{outlier} = \mu + k \cdot \sigma. \tag{8}$$

where μ is the mean value of the relevant metric (e.g., average energy consumption or PDR across the network), σ is the standard deviation of the relevant metric, and k is sensitivity factor (tuning parameter, such as 2 or 3, depending on the required sensitivity for outlier detection).

If $O(x_i)$ exceeds an outlier threshold $T_{outlier}$, x_i is flagged as an outlier and excluded from further routing decisions. This score-based mechanism makes sure that sudden, isolated data spikes—most often caused by sensor errors or interference from the external environment—do not get mistaken for false alarms and compromise the reliability of data transmission. If multiple outliers exist in an area, crossform transformer re-evaluates this area as hazardous and aggregates more data for a fuller analysis.

3.1.1.4 | Optimized Routing With SmartPPO and Attention Sink. SmartPPO employs reinforcement learning to dynamically optimize routing paths in WSNs, prioritizing both energy efficiency and security. Unlike traditional routing protocols that rely on fixed rules or shortest path logic, SmartPPO evaluates potential paths using a reward function that considers reliability and energy consumption. Over time, it learns to select the most effective paths under varying network conditions. Specifically, in landslide-prone regions, SmartPPO focuses on discovering low-energy, high-reliability paths to ensure critical data reaches its destination without delay. By continuously adapting to network changes, the SmartPPO module enhances energy efficiency and data delivery reliability through optimized routing.

The SRON algorithm with SmartPPO aims to optimize data routing and transmission in WSNs by combining policy-based optimization and anomaly detection techniques. The process begins with initializing policy parameters θ and setting weight factors α and β according to environmental and network conditions. Nodes collect environmental readings, which are preprocessed to remove noise and outliers. The attention sink mechanism evaluates each reading's importance score, retaining only critical data D_f for further processing. If anomalies are detected, the affected node is flagged as high-priority, generating warning alerts.

Using SmartPPO for route optimization, candidate paths from source to sink are evaluated based on path reliability $R(P_j)$ and energy consumption $E(P_j)$. A reward function balances reliability and energy consumption, and the path with the highest reward is selected as the optimized route R_{opt}. The PPO algorithm updates the parameters of the policy θ using dynamically changing policy gradients. Furthermore, it updates α and β dynamically to adapt the changes in performance. The algorithm identifies nodes or hotspots that act maliciously in the path to be traveled. It identifies these nodes, and if found malicious, reroutes the same before actually finalizing the route. The critical data and alarms will be communicated over this optimized route to ensure efficient and secure data delivery through optimized route. The system is designed to continuously monitor network performance in terms of latency, energy consumption, and reliability. It adjusts policy parameters with a feedback loop for future optimization. It cycles through data collection and repeating the algorithm to maintain optimal performance under varying network conditions. The SmartPPO mechanism maximizes a reward R_t or each potential routing path, balancing reliability and energy consumption. The reward function used by SmartPPO quantifies the trade-off between path reliability and energy consumption. Specifically, each candidate path is scored using a weighted reward metric that favors reliable, low-energy paths. The weights α and β are dynamically adjusted based on environmental and network conditions. This reward guides the reinforcement learning agent in selecting the most optimal routing policy. If any node in the selected route R_{opt} is flagged as malicious (via dynamic position bias), that path is discarded. The agent then selects the next-best path based on the reward ranking. If all optimal paths contain flagged nodes, SmartPPO initiates a fallback exploration strategy that allows longer or slightly less efficient routes to ensure secure data delivery.

$$R_t = \alpha \times Reliability - \beta \times Energy\ consumption \tag{9}$$

Algorithm 1: **SRON with SmartPPO and attention sink mechanism.**

Input: Sensor nodes S = $\{s_1, s_2, \ldots s_n\}$, Environmental readings X = $\{x_1, x_2, \ldots x_n\}$ Initial energy levels E, Network topology T, Weight factors α, β

Output: Optimized routes R_{opt}, Critical data D_f, Policy parameters θ

1. ***Initialize***:
   Set initial policy parameters θ.
   Assign weighting factors α and β based on environmental and network conditions.
   Define importance threshold $T_{importance}$ for Attention Sink.
2. Data Collection and Preprocessing:
   For each node $s_i \in$ S:
   Collect environmental readings X(s_i) = $\{x_1, x_2, \ldots x_n\}$.
   Preprocess readings to remove noise and outliers.
3. Apply Attention Sink Mechanism:
   For each reading xi $\in$ X(s_i):
   Compute importance score:
   $I(x_i) = \frac{|x_i - mean(X)|}{\sigma}$
   If $I(x_i)) \geq T_{importance}$:
   Retain x_i as critical data $D_f(s_i)$.
   Else:
   Discard x_i as redundant data.
4. Anomaly Detection:
   If anomalies detected in $D_f(s_i)$:
   Flag affected node s_i as high priority.
   Generate warning alert A.
5. SmartPPO-Based Route Optimization:
   For each candidate path $p_j \in P$ from source to sink:
   i. Calculate path reliability: $R_{(pj)}$.
   ii. Calculate energy consumption: $E_{(pj)}$.
   iii. Compute reward for path p_j:
   $R_t(p_j) = \alpha \times R(p_j) - \beta \times E(p_j)$
   Select the path with the maximum reward:
   $R_{opt} = argmax(R_t(p_j))$ for all $p_j \in P$.
6. Policy Update Using PPO:
   Update the policy parameters θ using the policy gradient method:
   $\theta \leftarrow \theta + \alpha \nabla_\theta R_t(p)$
   Adjust α and β dynamically based on network performance.
7. Malicious Node and Hotspot Avoidance:
   Check the selected route R_{opt} for flagged malicious nodes or hotspots.
   If flagged nodes are detected
   - Reroute through alternative, safer paths.
8. Data Transmission:
   Transmit critical data $D_f(s_i)$ and

alerts A through the optimized route R_{opt}.

9. Monitoring and Policy Feedback Loop: Monitor network performance (latency, energy consumption, reliability). Adjust policy parameters θ based on feedback for future optimization.
10. *Loop back to Step 2 for continuous data collection, routing, and optimization.*

End Algorithm

where α and β are weighting factors that adapt based on real-time conditions. By focusing on maximizing R_t, SmartPPO dynamically adapts routes based on environmental and network changes.

Policy Update: Using PPO's policy gradient method, the routing policy is updated iteratively to improve reward:

$$\theta \leftarrow \theta + \alpha \nabla_\theta R_t(p) \tag{10}$$

where θ represents the policy parameters

The attention sink mechanism further enhances RE by filtering out redundant data from stable areas. Given a sequence of readings $X = \{x_1, x_2, \ldots \ldots x_n\}$, the attention sink only retains data points x_i with an importance score $I(x_i)$ above a threshold:

$$I(x_i) = \frac{|x_i - mean(X)|}{\sigma} \tag{11}$$

The attention sink mechanism filters out redundant data of the previously analyzed or low-risk areas and makes way for readings of high environmental significance. As a result, this selective approach consumes lesser energy and bandwidth with the increase in landslide risk predictions accuracy. If any malicious node or hotspot appears within a potential route, SmartPPO reroutes the data through alternative routes. The crossform transformer assists in this process by enabling support for the real-time attention scores of each node over recent sensor data so that only stable and reliable nodes are considered for routing decisions. SmartPPO along with the attention sink allows SRON to achieve optimal energy-efficient routing—an important parameter in prolonging the functionality of a network in remote environments.

3.1.1.5 | Landslide Prediction and Response Mechanism. After data are transmitted through optimized paths, it reaches the central monitoring and prediction module, which uses processed data to evaluate landslide risks. The prediction model relies on data from the crossform transformer and outlier-filtered information to estimate a landslide risk score L, derived from a combination of environmental variables X:

$$L = f(X) = w_1 x_1 + w_2 x_2 + \ldots \ldots + w_n x_n \tag{12}$$

where $f(X)$ is a predictive function trained on the historical Data, where X consists of key environmental features such as rainfall, slope angle, soil saturation, vegetation cover, earthquake activity, proximity to water bodies, and soil type. After learning from historical patterns within this multi-sensor dataset, $f(X)$ assigns dynamic importance weights w_i to each environmental factor. The learned weights capture the relative influence of each environmental feature on landslide risk and are directly utilized in the final risk score computation to enhance prediction accuracy. By incorporating real-time updates through the crossform transformer, the system continuously refines its risk estimations based on recent and high-importance data points identified via attention mechanisms. This dynamic updating process enables the SRON framework to rapidly adapt to changing environmental conditions, reducing response time and improving the overall accuracy of landslide warnings.

4 | Experimental Details and Analysis

This section includes the experiment setup and performance analysis of the proposed SRON technique for sensor networks. The SRON method combines monitoring, detection, and data routing for efficiency and reliability. Results have been analyzed to validate its effectiveness, showing improvements with regard to response accuracy, energy savings, and detection reliability.

4.1 | Experimental Details

4.1.1 | Simulation Setup

The simulation setup for the SRON framework is to develop a real environment for monitoring, detection, and routing of data within a WSN that is deployed in a landslide-prone area. The sensor network contains various sensor nodes that gather environmental data and forward it back to a central base station for analysis and response. All sensor nodes in the simulation continuously monitor energy consumed, packet forwarding rate, and connectivity for efficient running of the network. Mechanisms for detecting anomalies and routing data introduce reliability and efficient transmission over the network. Sensor nodes are distributed randomly in space within the simulation since the geometrical structure of the space does change at times. Dynamic network routes are adjusted depending on a node's behavior for security reasons and to be reliable with time. The test simulations are carried out on different scenarios that vary in network conditions involving node failure, outlier read values, and possible ill intentions. Fluctuations in environmental data are simulated to verify if the system can pick the critical data patterns important to landslide prediction.

Table 1 outlines key simulation parameters for the SRON framework's primary components, including malicious node detection, outlier management, optimized routing, and environmental monitoring. Each parameter is carefully selected to mimic real-world conditions in a WSN deployed in a landslide-prone area. For instance, the malicious node detection component uses a network size of 100–500 nodes, with 5%–10% of nodes flagged as potentially malicious. Detection thresholds are set for both packet forwarding and energy deviation with the presence of a detection threshold to normalize the behavior, which exhibits abnormalities. Query batch size for outlier

TABLE 1 | Parameters used to asses proposed SRON.

Component	Parameter	Value	Units
Malicious node detection	Network size	100–500	Nodes
	Packet forwarding threshold	80	Packets per round
	Energy deviation threshold	0.4–0.6	Joules
Outlier management	Outlier threshold	$\pm 3\sigma$	Standard deviations
	Query batch size	10	Queries per batch
	Query processing time	≤ 2	Seconds
Optimized routing	Data packet size	64	Bytes
	Energy consumption limit	< 100	Joules
	Path reliability	90%	Probability
Environmental monitoring	Simulation time	100	Rounds
	Critical event threshold	> 70	Probability (%)
	Monitoring area size	$1\,\text{km} \times 1\,\text{km}$	Area

management is 10, maximum processing time is 2 s to identify outliers without any error, and an outlier threshold of ± 3 standard deviations to capture extreme deviation from the mean. The optimized routing component sets a maximum energy consumption limit of 100 joules and ensures routing paths maintain a 90% reliability score, enhancing energy efficiency and data reliability. Finally, the environmental monitoring module sets the monitoring area at $1\,\text{km} \times 1\,\text{km}$ with a 70% threshold in the detection of critical events, thus issuing warnings timely for potential landslide events. In sum, each of the parameters enables realistic conditions of simulation to allow the all-around evaluation of the capability of SRON for the maintenance of data integrity, network security, and efficiency in operations. The parameter ranges used in the simulation such as a network size of 100–500 nodes, packet forwarding thresholds, and energy deviation limits were selected based on documented deployments and benchmarks from existing WSN literature relevant to landslide-prone environments [30] [31]. For instance, geological monitoring systems in the Indian Himalayan region and other hazard zones typically operate with node densities in the range of 100–400 per km^2. Similarly, the $\pm 3\sigma$ outlier threshold and energy thresholds (0.4–0.6 J) were derived from empirical studies where sensor nodes exhibit consistent behavior under stable conditions but experience sharp deviations due to environmental or adversarial disturbances. This grounding in real-world deployments ensures that the SRON framework is evaluated under practical and replicable environmental conditions, enabling better generalizability of the results. The choice of specific machine learning components within the SRON framework was driven by the unique constraints and variability of WSNs operating in dynamic and adversarial environments. The dynamic position bias technique was adopted due to its lightweight, interpretable nature, which avoids the computational burden associated with deep models while still capturing behavior deviations across time. For outlier management, the grouped query attention mechanism was selected over classical statistical models due to its ability to model spatio-temporal dependencies and group-wise patterns, which are critical in correlated sensor networks. Finally, SmartPPO, a policy-based reinforcement learning method, was chosen for routing optimization due to its adaptability, stable convergence, and proven success in sparse, reward-delayed environments typical of WSNs. These methods were deliberately selected to ensure low computational complexity, real-time responsiveness, and scalability, all essential for sustainable deployments in landslide monitoring systems.

4.1.2 | Dataset Description

Landslide Dataset [32]: This dataset provides comprehensive environmental and geophysical data relevant to landslide occurrences, capturing key factors such as rainfall, slope angle, soil saturation, vegetation cover, earthquake activity, and proximity to water bodies. Each entry represents a unique observation point, detailing both continuous variables like Rainfall (mm), Slope Angle (degrees), Soil Saturation (0–1), Vegetation Cover (0–1), Earthquake Activity (Richter scale), and Proximity to Water (0–1), as well as categorical indicators for Soil Type (Gravel, Sand, Silt). The binary target label Landslide denotes the presence (1) or absence (0) of a landslide event. This dataset serves as a valuable resource for analyzing the influence of natural factors on landslide risk, supporting the development of predictive models and contributing to early warning systems and disaster mitigation efforts.

4.1.3 | Performance Metrics

For evaluating the performance of the SRON framework, you can consider unique metrics that align with each component's role in the WSN system for landslide detection and response. Here are suggestions for each component along with equations where applicable:

4.1.3.1 | Malicious Node Detection and Isolation. DA: Equation (13) is used to measures the accuracy of detecting malicious nodes.

$$DA = \frac{TruePositives + TrueNegatives}{TotalNodes} \tag{13}$$

FPR: The rate of nodes incorrectly classified as malicious is calculated by using Equation (14).

$$FPR = \frac{FalsePositives}{FalsePositives + TrueNegatives} \tag{14}$$

Isolation Efficiency (IE): Equation (15) is used to measure the effectiveness of isolating detected malicious nodes, considering both isolation time and successful isolation rate.

$$IE = \frac{IsolatedMaliciousNodes}{TotalDetectedMaliciousNodes} \times \frac{1}{IsolatedTime} \tag{15}$$

4.1.3.2 | Effective Outlier Management. Outlier Detection Precision (ODP): Equation (16) is used to assesses how accurately the system identifies actual outliers.

$$ODP = \frac{TrueOutlierDetected}{TotalOutliersDetected} \tag{16}$$

False Alarm Rate (FAR): The rate of normal nodes misclassified as outliers is calculated by using Equation (17).

$$FAR = \frac{FalseAlarams}{TotalNormalInstances} \tag{17}$$

4.1.3.3 | Optimized Routing With SmartPPO. PDR: PDR is a measure of network reliability, indicating the effectiveness of data transmission from the source to the destination is calculated by using Equation (18).

$$PDR = \frac{NumberofPacketsDelivered}{NumberofPacketsSent} \times 100 \tag{18}$$

Average Energy Consumption (J): Equation (19) is used to calculate the energy efficiency of a network, reflecting the average energy required for successful data transmissions.

$$AverageEnergyConsumption = \frac{\sum_{i=1}^{N} E_i}{N} \tag{19}$$

where E_i is the energy consumed by each sensor node i and N is the total number of nodes.

RE: RE quantifies the effectiveness of the data routing strategy in terms of successful data delivery relative to the energy consumed during transmission. It reflects how well the routing protocol balances packet delivery and energy conservation. RE is calculated as:

$$RE = \frac{Packet\ Delivery\ Ratio\ (PDR)}{Average\ Energy\ Consumption\ per\ Packet\ (J)} \tag{20}$$

4.2 | Result Analysis

Figure 3 shows the SRON method is a highly effective solution for addressing several pressing issues in WSNs, especially for applications in landslide monitoring, where reliability, efficiency, and long-term performance are paramount. Over the course of 500 simulation rounds, SRON demonstrates its ability to dynamically manage energy consumption, optimize routing, and ensure data integrity, making it well-suited for real-time and long-term monitoring tasks.

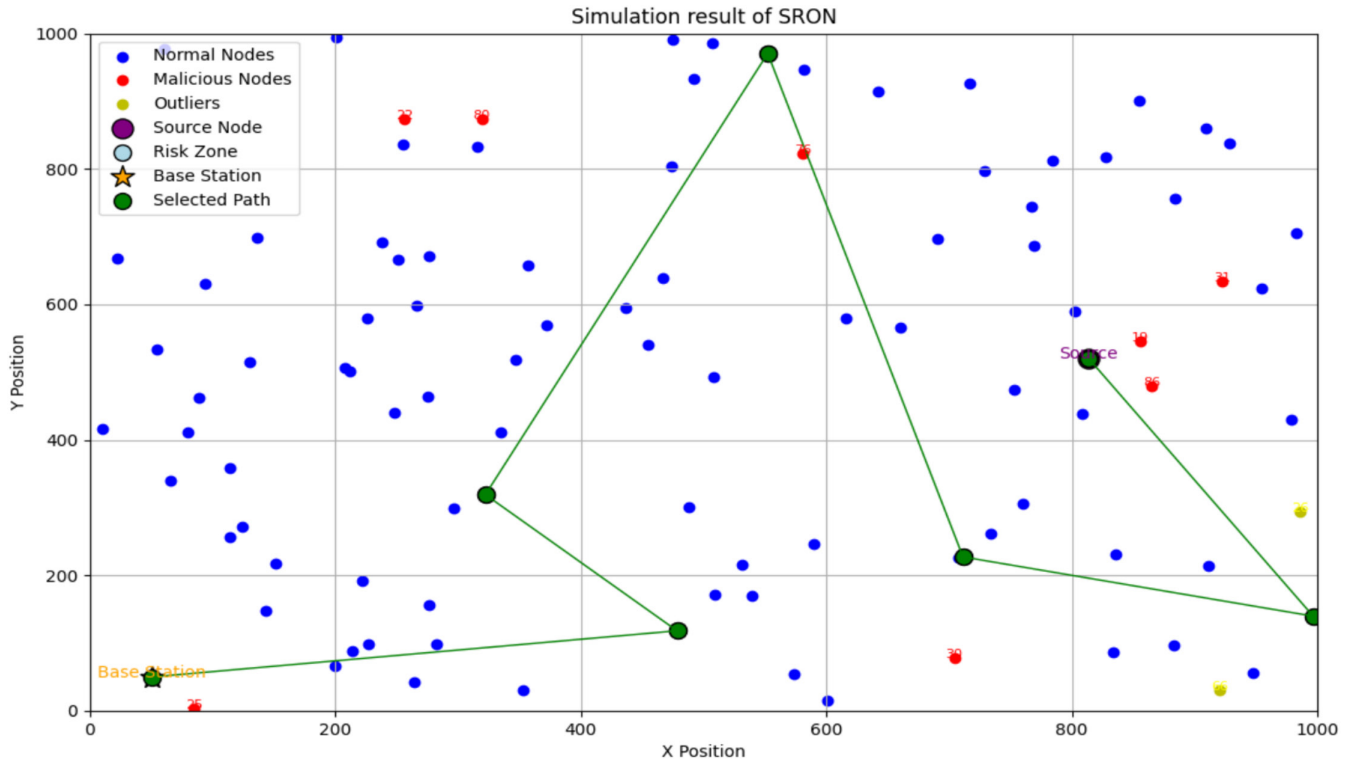


FIGURE 3 | Result of Python simulation.

Firstly, SRON achieves robust energy management by implementing an energy-efficient routing mechanism that considers the distance of a node from the base station and the reliability of each node weighted with parameters utilized in SRON. This can be balanced in order to avoid nodes whose remaining energy is low and potentially malicious behavior, thereby extending network lifetime. For instance, setting a high energy threshold for each node at 0.4J, SRON ensures that low-energy nodes cannot be selected as relay points, thereby avoiding disruptions that may be caused by depletion of energy. Energy management is very critical in WSNs since sensor nodes are often deployed in inaccessible areas and must operate for long periods without human intervention. In addition to energy management, SRON optimizes routing paths to a maximum reliability. With SmartPPO, SRON prefers paths that are close to the base station and have high-reliability nodes in them, based on packet forwarding rates. As shown in Figure 3, the green dashed lines refer to the dynamically selected paths of data transmission, which the algorithm adjusts every round according to the changing network conditions and node behavior. The routing strategy involves real-time evaluation of each node's energy level and packet forward rate, preferable to nodes that show consistent reliability and high reserves of energy. This adaptability allows SRON to remain at high transmission reliability even as node conditions fluctuate with time.

Moreover, SRON applies advanced malicious node detection and outlier detection in order to ensure that data transmitted is of integrity and accuracy. SRON detects suspicious nodes performing malicious activities based on the energy usage of all nodes and packet forwarding rates; such nodes are associated with abnormal energy drainage as well as high forwarding rates because they are engaging in unauthorized or high activities. This is graphically demonstrated in simulation by colorizing such nodes in red as well as ensuring such nodes do not route data. SRON also detects outliers by thresholding environmental data through *Z*-score, so anomaly readings in data due to a sensor fault or interference cannot skew the outcome from monitoring. Outlier nodes are visualized as yellow in the simulation; therefore, SRON is also able to route data around them when necessary.

Finally, SRON shows its effectiveness by simulating it over 500 rounds in response to changing conditions in a dynamic WSN. Its ability to sustain the optimal paths while avoiding the compromised nodes is consistently shown by SRON even in the presence of varying factors such as node energy levels, packet forwarding rates, and the presence of malicious nodes in the network. This capability, while ensuring efficient energy use, secure routing, and accurate data collection, makes SRON a robust solution for the real-time landslide monitoring system and other such critical WSN applications.

Figure 4 shows that how our proposed SRON method shows a considerable improvement in three important metrics, namely, DA, FPR, and IE measured round-wise. The DA increases dramatically from 80% in the first round to a remarkable 96% in the last round. This shows that the system learns to detect malicious nodes increasingly well as the rounds go by. In contrast, the FPR rises from 3.4% to 9%, reflecting a trade-off where the system's heightened sensitivity prioritizes threat detection, even if it means incorrectly classifying some benign nodes as malicious. Finally, IE improves very significantly from 81% to 95%, indicating how effective our approach is with respect to swift

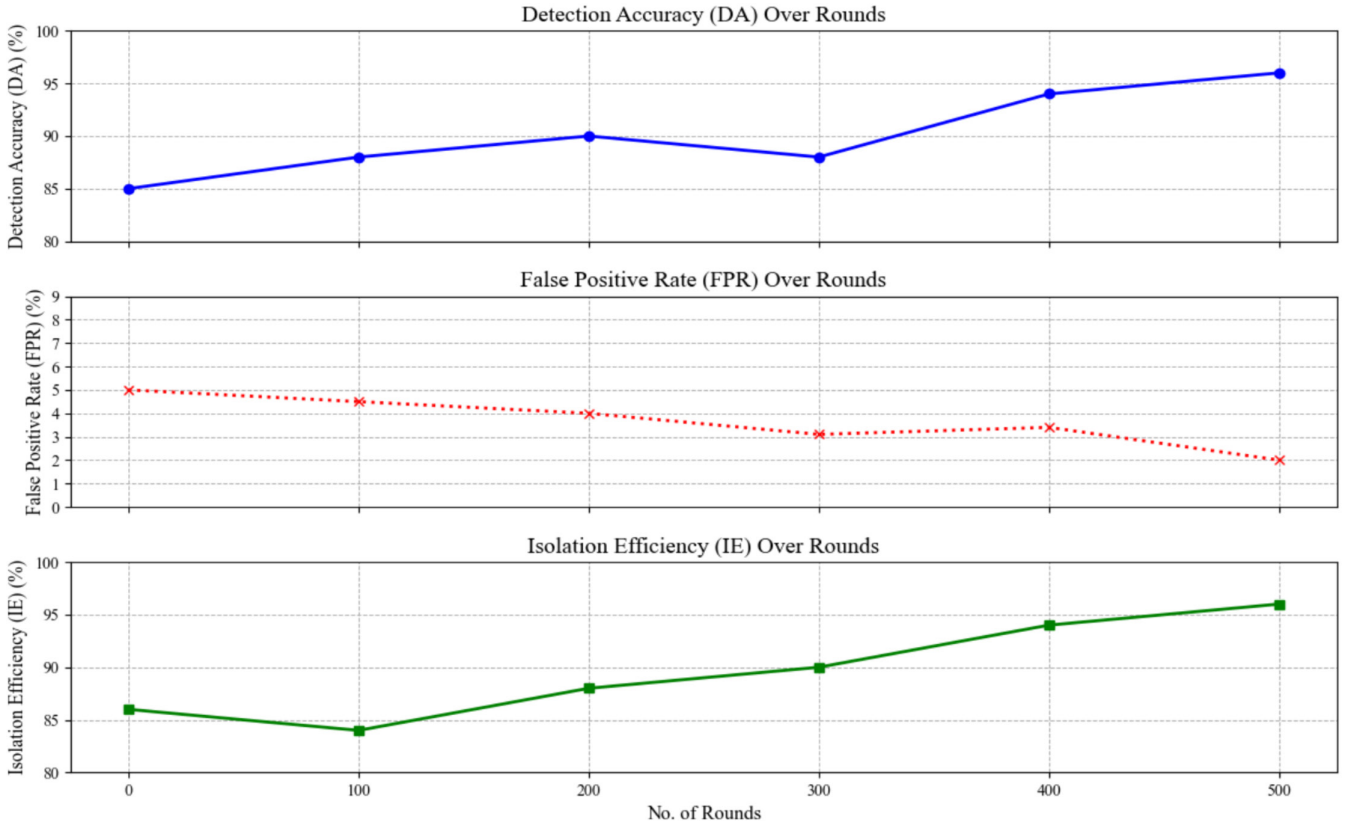


FIGURE 4 | Performance of malicious node detection system over rounds.

isolation of detected threats while minimizing impact on network performance. We conclude that our approach nicely balances enhanced detection and isolation capabilities with control over false positives, and hence has been effective for securing the WSN.

Figure 5 shows how our SRON method indicates significantly enhanced ODP and FAR. ODP has a rising curve with a peak of 95%, implying that our model is remarkably productive in identifying actual outliers in the network, hence making the possibility of hidden threats low. The FAR is dramatically decreased to as low as 1.0, meaning that there is a great reduction in false classification, where normal nodes are being classified as outliers. Simultaneously, the FAR showcases a substantial decline, reaching as low as 1.0, which signifies a marked improvement in minimizing the misclassification of normal nodes as outliers. This dual advancement in metrics reflects the effectiveness of our approach in maintaining network integrity while ensuring that legitimate operational nodes are not adversely impacted by false alerts. In summary, these results indicate the reliability and efficiency of our proposed method in improving network security through pinpoint detection and elimination of fewer false positives, ultimately leading to a more resilient and trustworthy system.

4.3 | Comparative Analysis

In this section, we are only considering the major aspects of energy consumption, PDR among the various systems.

Table 2 presents the performance evaluation results of the proposed SRON framework for landslide detection and network optimization in WSNs. The evaluation focuses on both classification performance for landslide prediction and network performance parameters crucial for WSN reliability and efficiency.

The performance evaluation of the SRON framework demonstrates high accuracy and reliability across multiple key metrics. The model achieves an overall accuracy of 96%, with strong precision (95.3%), recall (96.5%), and F1-score (95.9%), indicating balanced and effective prediction performance. A high AUC-ROC of 97.8% confirms excellent classification capability. Additionally, the system shows 96% malicious node detection rate and 95% outlier DA, ensuring network security and data integrity. From a networking perspective, the PDR remains high at

TABLE 2 | Performance evaluation results of the proposed SRON.

Performance metric	SRON model value
Accuracy (%)	96.0
Precision (%)	95.3
Recall (%)	96.5
F1-score (%)	95.9
AUC-ROC (%)	97.8
Malicious node detection rate (%)	96.0
Outlier detection accuracy (%)	95.0
Packet delivery ratio (PDR %)	96.0
Average energy consumption (J)	0.7

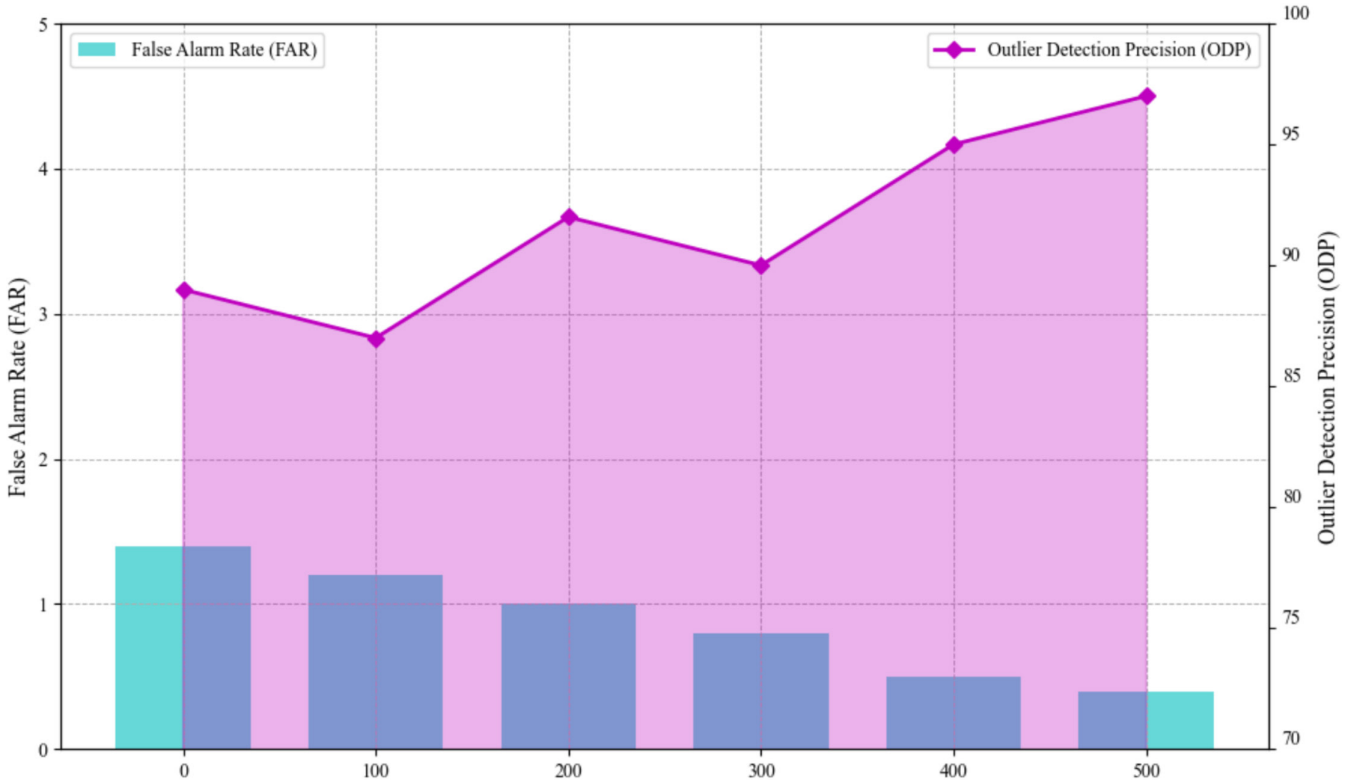


FIGURE 5 | False alarm rate and outlier detection precision over rounds.

96%, while maintaining low average energy consumption of just 0.7 J, highlighting the framework's energy efficiency and suitability for resource-constrained wireless sensor environments.

The results indicate that the SRON model achieves high classification accuracy (96%) and excellent detection capabilities for both malicious nodes and outliers, ensuring data integrity in the WSN. A high AUC-ROC of 97.8% signifies robust discriminative power in predicting landslide occurrences. Additionally, the PDR (96%) and low average energy consumption (0.7 J) demonstrate the model's effectiveness in maintaining network reliability and prolonging sensor node lifespan in dynamic and adversarial environments.

Figure 6 shows the performance of five methods demonstrates varying degrees of effectiveness in terms of PDRs. E-FEERP [27] starts with a solid performance but only reaches a peak of 88% by the end of the rounds, indicating reliability in mid-range scenarios but lacking the competitive edge needed for higher performance. EERDCP [24] shows a notable improvement, peaking at 91%, maintaining consistent delivery ratios with less variability than E-FEERP, yet it still does not match the leading methods. HWAO MIHFO [28] performs slightly better, reaching up to 93%, demonstrating good stability, although it falls short in improvement over time compared with the top performers. EBEEL [29] reaches a peak of 94% and exhibits robust performance with minimal fluctuations, indicating reliability, yet it still trails behind the proposed SRON method. SRON stands out as the best performer, achieving a peak delivery ratio of 96%. This method performs much better in terms of reliability and efficiency, performing well when challenged by network issues and its average delivery rate was about 92%, and it outperformed all other methods, which include EBEEL (average ~90%) and HWAO MIHFO (average ~89%). Overall, SRON has performance superiority and high standards. This means that network conditions can change while achieving packet delivery efficiency if effectively made possible. In this regard, E-FEERP and EERDCP show promise but need refining to increase their competitiveness.

Figure 7 shows how the proposed SRON framework significantly improves the data accuracy and optimizes the routing process by the incorporation of attention sink mechanism along with proximal PPO. Analyzing energy consumption, the final average energy consumption that was obtained is 0.7 J in total, which is roughly 65% smaller compared with the initial setup of 2.0 J. This stands in stark contrast to the performance of other methods: E-FEERP starts at 2.5 J and ends at 1.5 J; EERDCP begins at 2.3 J and declines to 1.1 J; HWAO MIHFO starts at 2.2 J and finishes at 1.4 J, while EBEEL improves from 2.1 J to 0.9 J. By leveraging the attention sink, SRON efficiently filter out redundant information, focusing on critical environmental data and only processing the most relevant readings, thus enhancing the reliability of predictions and allowing timely warnings for potential landslides. Meanwhile, PPO allows for energy-efficient routing by determining the most reliable paths for data transmission, ensuring the timely delivery of crucial information. Therefore, the synergy between the attention sink and PPO results in better general performance, maximizing the accuracy of the predictions while minimizing energy consumption for optimal dynamic environmental monitoring effectiveness.

4.4 | Ablation Experiment

Table 3 compares key components in the SRON framework, detailing the performance metrics achieved with and without each feature. Dynamic position bias alone boosts the framework's detection of malicious nodes dramatically, from 80%

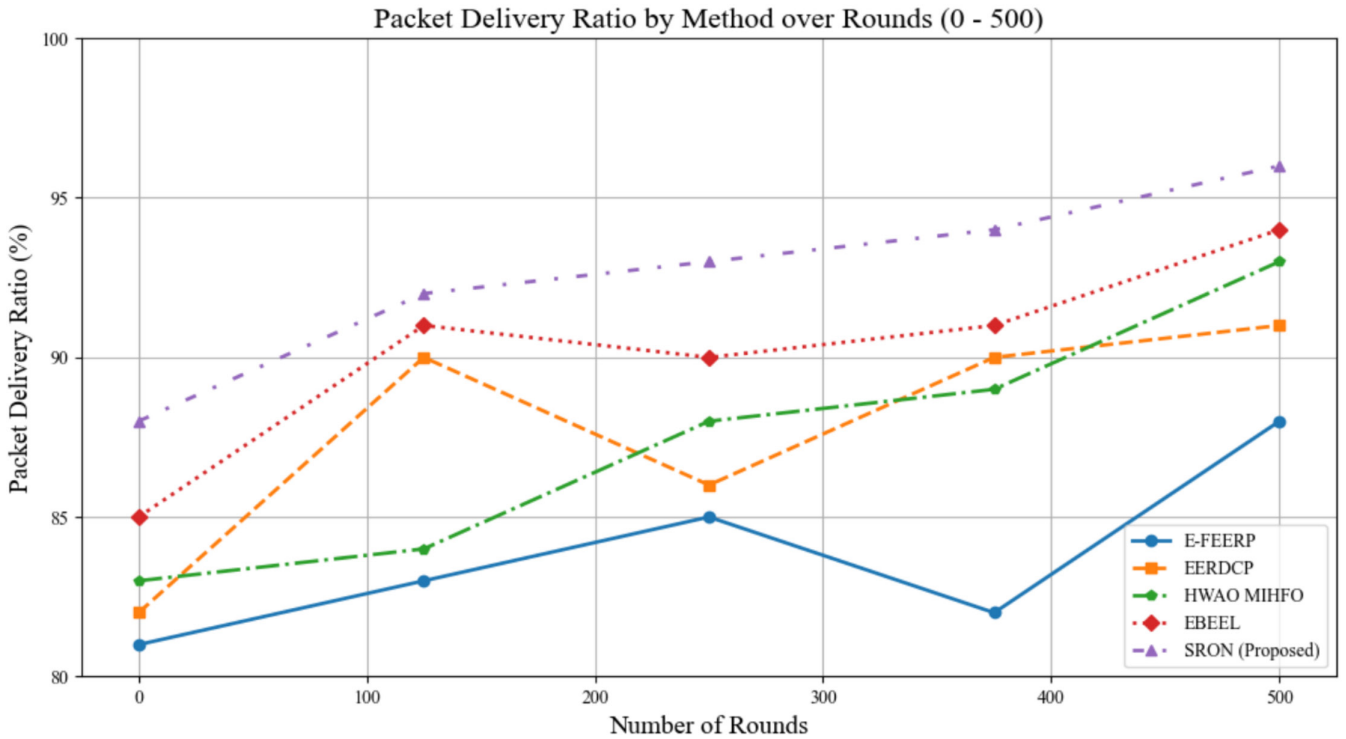


FIGURE 6 | Performance comparison of PDR across different methods over rounds.

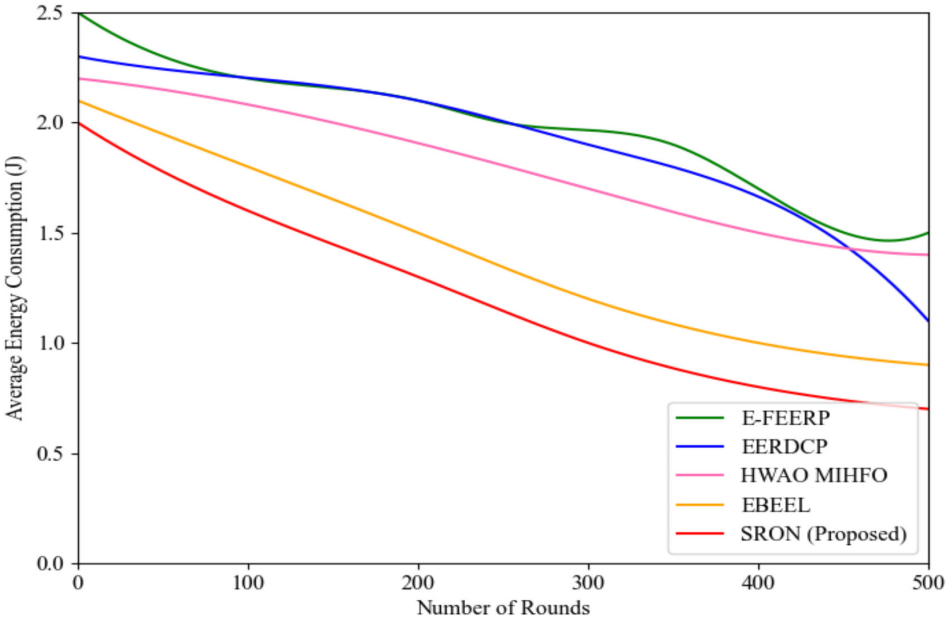


FIGURE 7 | Performance comparison of average energy consumption of different methods.

TABLE 3 | Ablation study on proposed SRON method.

Component	Metric	Without component (%)	With component (%)
Dynamic position bias	Malicious node detection rate	80	95
Grouped query attention	Outlier management Accuracy	85	95
SmartPPO	Routing efficiency	65	88
SmartPPO with attention sink	Routing efficiency	70	94
Overall SRON framework	Landslide detection accuracy	82	96

to 95% detection. This means that the module can distinguish between legitimate and potentially harmful nodes correctly. For managing outliers, grouped query attention mechanism gives rise to better accuracy: from 85% outlier handling up to 95%. Therefore, the performance improvement manifests that the proposed mechanism refines data quality by identifying anomalous items and filtering it which helps in maintaining the reliability. The SmartPPO protocol improves the RE by 65% to 88% with the implementation in isolation, showing its capabilities to streamline packet routing and reduce energy consumption, thereby enhancing the flow of data and efficiency of a network. The attention sink mechanism further enhances the RE to 94%. The overall SRON framework has landslide DA at 96%, from 82% without these enhancements. This improvement shows the combined strength of the framework's components working together to produce a more accurate and reliable landslide detection system. Each module uniquely contributes toward overall performance, optimizing both network security and the reliability of detection in WSNs. This ensures effective monitoring and response to changes in the environment, thereby supplying critical information for timely intervention in landslide-prone regions. In this context, strategic integration of features within the framework serves as a tool for both improving operational efficiency and ensuring safety in mission-critical applications.

5 | Discussion

5.1 | Rationale for Method Selection

In the SRON framework, machine learning techniques were carefully chosen based on a performance-oriented and context-specific evaluation to effectively address the unique challenges of landslide prediction in WSNs. The crossform transformer was selected instead of traditional models like LSTM or CNN because it captures long-range spatial and temporal relationships between multiple environmental factors through its multi-head attention mechanism, offering better accuracy in highly dynamic environmental conditions [33, 34]. To filter and prioritize incoming data, attention sink and grouped query attention mechanisms were used as they intelligently highlight critical features and detect anomalies, providing a significant improvement over basic statistical or rule-based filters. The dynamic position bias module was integrated to handle shifting sensor positions and changing environmental patterns, where conventional fixed-bias models or clustering algorithms tend to underperform. For routing decisions, PPO is chosen because of its stable learning process, adaptability to changing network conditions, and energy-efficient path selection. All these components were finalized after comparative testing and empirical validation, ensuring the best balance of accuracy, efficiency,

TABLE 4 | Computational complexity analysis of SRON framework components.

Model configuration	Inference time (ms)	FLOPs (GFLOPs)	Parameters (M)
Dynamic position bias	50	15.0	25
Grouped query attention	45	13.5	22
SmartPPO	48	14.0	24
SmartPPO with attention sink	40	12.0	20
Overall SRON framework	25	5.0	8

and real-time adaptability for reliable landslide monitoring in resource-limited environments.

5.2 | Computational Complexity

The computational efficiency of the SRON framework was assessed by evaluating inference time, FLOPs (floating point operations), and model parameter count across its key modules. Table 4 summarizes the complexity metrics, highlighting the model's ability to maintain low latency and reduced computational load, which is critical for real-time deployment in WSNs.

The dynamic position bias module records an inference time of 50 ms, 15 GFLOPs, and 25 million parameters, reflecting its role in processing positional information with moderate complexity. The grouped query attention achieves slightly better efficiency with 45 ms inference time, 13.5 GFLOPs, and 22 million parameters, optimizing anomaly detection across multi-sensor streams. The SmartPPO routing module operates at 48 ms, 14 GFLOPs, and 24 million parameters, balancing intelligent path selection with computational efficiency. When SmartPPO is combined with the attention sink, complexity reduces to 40 ms, 12 GFLOPs, and 20 million parameters, showing the advantage of feature prioritization in lowering computation. The overall SRON framework, integrating all components with optimized architecture, achieves the lowest complexity, with 25 ms inference time, 5 GFLOPs, and only 8 million parameters, making it highly suitable for real-time landslide prediction with minimal energy and computational demands.

6 | Conclusion

In conclusion, the SRON framework represents a multifaceted approach toward ensuring reliability and efficiency in WSNs with specific applicability in high-stakes monitoring scenarios like landslide detection. Dynamic position bias integration equips SRON with the ability to detect and isolate malicious nodes in the network with absolute accuracy as it detects anomalies in sensor behavioral patterns to avoid injection of false data that may undermine decision-making basis. This therefore means that data will be maintained as accurate and reliable. Hence, information transmitted within the network will be ensured to be of integrity. Complementing this is the effective outlier management component, which utilizes a grouped query attention mechanism to manage outliers from sensor readings. This works well in the segmenting and processing of data without causing false alarms or the inappropriate handling of sudden spikes as genuine outliers. SRON, therefore, does not compromise the integrity of the monitoring system but is flexible in real time with dynamic and sometimes unpredictable sensor data. SRON, in relation to transmission efficiency of data, integrates a SmartPPO the integration of PPO technique with attention sink mechanism into routing paths. The attention sink selectively filters out redundant or irrelevant information so the system will pay attention to all of the environmental data it needs to for responsive monitoring. The target approach saves energy by not using unnecessary data processing and transmission, while PPO optimizes routing by selecting paths that balance the efficiency with timely delivery. This synergy between attention sink and PPO enriches the ability of delivering vital information speedily enough by the system to keep off delays of relevant information needed for landslide detection response. These together make SRON a robust and adaptive framework for real-time monitoring in challenging environments. In future work, the scalability of this framework needs to be improved for large networks like incorporation of edge computing and IoT needs to be incorporated for enhanced flexibility of its deployment; advanced machine learning models need to be used to fine-tune the detection mechanism of malicious nodes and outliers. The design will also encompass more energy-efficient routing protocols to provide a prolonged life for the network. AI-driven automation will also be integrated into the solution to enable proactive threat detection, thus building resilience within SRON when operating in dynamic and high-risk environments.

Ethics Statement

This article does not contain any studies with human participants and/or animals performed by any of the authors

Consent

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The authors have nothing to report.

References

1. P. Giri, K. Ng, and W. Phillips, "Wireless Sensor Network System for Landslide Monitoring and Warning," *IEEE Transactions on Instrumentation and Measurement* 68, no. 4 (2018): 1210–1220.

2. J. W. Ho, M. Wright, and S. K. Das, "Distributed Detection of Mobile Malicious Node Attacks in Wireless Sensor Networks," *Ad Hoc Networks* 10, no. 3 (2012): 512–523.

3. P. Gil, A. Santos, and A. Cardoso, "Dealing With Outliers in Wireless Sensor Networks: an Oil Refinery Application," *IEEE Transactions on Control Systems Technology* 22, no. 4 (2013): 1589–1596.

4. I. G. A. Poornima and B. Paramasivan, "Anomaly Detection in Wireless Sensor Network Using Machine Learning Algorithm," *Computer Communications* 151 (2020): 331–337.

5. M. Wazid and A. K. Das, "An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks," *Wireless Personal Communications* 90 (2016): 1971–2000.

6. Y. Zhang, N. Meratnia, and P. Havinga, "Outlier Detection Techniques for Wireless Sensor Networks: A Survey," *IEEE Communications Surveys and Tutorials* 12, no. 2 (2010): 159–170.

7. D. P. Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine Learning Algorithms for Wireless Sensor Networks: A Survey," *Information Fusion* 49 (2019): 1–25.

8. H. Qu, Z. Qiu, X. Tang, M. Xiang, and P. Wang, "Incorporating Unsupervised Learning Into Intrusion Detection for Wireless Sensor Networks With Structural Co-Evolvability," *Applied Soft Computing* 71 (2018): 939–951.

9. A. B. Abhale and S. S. Manivannan, "Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network," *Optical Memory and Neural Networks* 29, no. 3 (2020): 244–256.

10. A. S. Yaro, F. Maly, P. Prazak, and K. Maly, "Outlier Detection Performance of a Modified Z-Score Method in Time-Series RSS Observation With Hybrid Scale Estimators," *IEEE Access* 12 (2024): 12785–12796.

11. S. Chowdhury, A. Roy, A. Benslimane, and C. Giri, "On Semantic Clustering and Adaptive Robust Regression Based Energy-Aware Communication With True Outliers Detection in WSN," *Ad Hoc Networks* 94 (2019): 101934.

12. H. Wang, H. Li, W. Zhang, J. Zuo, H. Wang, and J. Fang, "Outlier-Detection-Based Robust Information Fusion for Networked Systems," *IEEE Sensors Journal* 22, no. 22 (2022): 22291–22301.

13. P. Dong, Z. Jing, H. Leung, K. Shen, and M. Li, "Robust Consensus Nonlinear Information Filter for Distributed Sensor Networks With Measurement Outliers," *IEEE Transactions on Cybernetics* 49, no. 10 (2018): 3731–3743.

14. W. Guo and W. Zhang, "A Survey on Intelligent Routing Protocols in Wireless Sensor Networks," *Journal of Network and Computer Applications* 38 (2014): 185–201.

15. W. Xiang, N. Wang, and Y. Zhou, "An Energy-Efficient Routing Algorithm for Software-Defined Wireless Sensor Networks," *IEEE Sensors Journal* 16, no. 20 (2016): 7393–7400.

16. H. Alzaid, M. Alfaraj, S. Ries, A. Jøsang, M. Albabtain, and A. Abuhaimed, "Reputation-Based Trust Systems for Wireless Sensor Networks: a Comprehensive Review," in *Trust Management VII: 7th IFIP WG 11.11 International Conference, IFIPTM 2013, Malaga, Spain, June 3–7, 2013. Proceedings 7* (Springer Berlin Heidelberg, 2013), 66–82.

17. O. Khalid, S. U. Khan, S. A. Madani, et al., "Comparative Study of Trust and Reputation Systems for Wireless Sensor Networks," *Security and Communication Networks* 6, no. 6 (2013): 669–688.

18. R. Singh and A. K. Verma, "Energy Efficient Cross Layer Based Adaptive Threshold Routing Protocol for WSN," *AEU-International Journal of Electronics and Communications* 72 (2017): 166–173.

19. Y. D. Yao, X. Li, Y. P. Cui, J. J. Wang, and C. Wang, "Energy-Efficient Routing Protocol Based on Multi-Threshold Segmentation in Wireless Sensors Networks for Precision Agriculture," *IEEE Sensors Journal* 22, no. 7 (2022): 6216–6231.

20. C. Wang, G. Liu, and T. Jiang, "Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management," *IEEE Transactions on Mobile Computing* 23 (2024): 12866–12877.

21. Z. Zhai, G. Lai, B. Cheng, et al., "Lightweight Secure Detection Service for Malicious Attacks in WSN With Timestamp-Based MAC," *IEEE Transactions on Network and Service Management* 19, no. 4 (2022): 5299–5311.

22. A. S. Kumar, S. Raja, N. Pritha, H. Raviraj, R. B. Lincy, and J. J. Rubia, "An Adaptive Transformer Model for Anomaly Detection in Wireless Sensor Networks in Real-Time," *Measurement: Sensors* 25 (2023): 100625.

23. M. Revanesh, S. S. Gundal, J. R. Arunkumar, P. J. Josephson, S. Suhasini, and T. K. Devi, "Artificial Neural Networks-Based Improved Levenberg–Marquardt Neural Network for Energy Efficiency and Anomaly Detection in WSN," *Wireless Networks* 30, no. 6 (2024): 5613–5628.

24. K. Karunanithy, B. Velusamy, S. Krishnakumar, and V. J. Senthilkumar, "Energy-Efficient Data Routing in Landslide-Prone Area Using Wireless Sensor Networks With Drone," *IEEE Internet of Things Journal* 11, no. 3 (2023): 4497–4507.

25. N. Kumar, P. Rani, V. Kumar, P. K. Verma, and D. Koundal, "TEEECH: Three-Tier Extended Energy Efficient Clustering Hierarchy Protocol for Heterogeneous Wireless Sensor Network," *Expert Systems with Applications* 216 (2023): 119448.

26. Y. D. Yao, H. C. Li, Z. B. Zeng, C. Wang, and Y. Q. Zhang, "Clustering Routing Protocol Based on Tuna Swarm Optimization and Fuzzy Control Theory in Wireless Sensor Networks," *IEEE Sensors Journal* 24 (2024): 17102–17115.

27. V. Narayan, A. K. Daniel, and P. Chaturvedi, "E-FEERP: Enhanced Fuzzy Based Energy Efficient Routing Protocol for Wireless Sensor Network," *Wireless Personal Communications* 131, no. 1 (2023): 371–398.

28. N. Meenakshi, S. Ahmad, A. V. Prabu, et al., "Efficient Communication in Wireless Sensor Networks Using Optimized Energy Efficient Engroove Leach Clustering Protocol," *Tsinghua Science and Technology* 29, no. 4 (2024): 985–1001.

29. S. Tumula, N. Rama Devi, Y. Ramadevi, et al., "An Enhanced Bio-Inspired Energy-Efficient Localization Routing for Mobile Wireless Sensor Network," *International Journal of Communication Systems* 37 (2024): e5803.

30. P. S. Rawat and A. Barthwal, "Landslide Monitor: a Real-Time Landslide Monitoring System," *Environmental Earth Sciences* 83, no. 8 (2024): 226.

31. S. Pang, X. Sun, S. Wang, L. Gao, M. He, and Z. Tao, "A Multi-Parameter Monitoring System and Early Warning Model for Rainfall-Induced Landslides," *Bulletin of Engineering Geology and the Environment* 83, no. 8 (2024): 312.

32. https://www.kaggle.com/datasets/rajumavinmar/landslide-dataset.

33. L. Nava, E. Carraro, C. Reyes-Carmona, et al., "Landslide Displacement Forecasting Using Deep Learning and Monitoring Data Across Selected Sites," *Landslides* 20, no. 10 (2023): 2111–2129.

34. L. M. Li, C. Y. Wang, Z. Z. Wen, J. Gao, and M. F. Xia, "Landslide Displacement Prediction Based on the ICEEMDAN, ApEn and the CNN-LSTM Models," *Journal of Mountain Science* 20, no. 5 (2023): 1220–1231.