RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt26210

A Intelligent Intrusion Mechanism for Sinkhole Attack in IOT Sensor Network

D. Udaya Suriya Rajkumar [a,*], B.M. Praveen [b], S.B. Priya [c], Rajkumar Govindarajan [d], Sathiyaraj Rajendran [e]

[a] Department of Computer Science Engineering, Srinivas University, Mukka-574146, Mangalore, Karnataka, India
[b] Director Research and Innovative Council, Srinivas University, Mukka-574146, Mangalore, Karnataka, India
[c] Department of Artificial Intelligence and Data science, St Joseph's Institute of Technology, OMR, Chennai, India
[d] Department of Computer Science & Engineering (Data Science), Madanapalle Institute of Technology & Science, Andhra Pradesh, 517326, India
[e] Department of of CSE, Manipal Institute of Technology, MAHE Bengaluru, Karnataka, India
* Corresponding Author Email: raisingsun82@gmail.com

DOI: https://doi.org/10.54392/irjmt26210
Received: 06-06-2025; Revised: 07-02-2026; Accepted: 22-02-20XX; Published: 17-03-2026

Abstract: The Internet of Things (IoT) makes more heterogeneous devices possible. A wireless sensor network (WSN) is a cluster of sensor nodes used to monitor different field conditions. A node must transport data to its destination, usually the base station (BS), with the assistance of other nodes in the network because each node has a limited wireless transmission range. The primary concern that comes up while data is being transmitted is security. This section will discuss a critical attack known as a sinkhole attack. Using the Leader election technique, this system can monitor the nearby nodes zone-by-zone. The current work uses an Intelligent Intrusion Mechanism (IIM) to identify network intruders and stop sinkhole attacks. Two methods are used to accomplish this: the Zone-Based Leader Election Technique and the Region-Based Leader Election Method. In both methods, a network's nodes are distributed among various zones and regions. The alternative WSN leader is informed of a node's compromised state when detected in the Leader election method. The existing technologies can improve system efficiency and identify intruder nodes. The proposed IIM model achieves a high throughput of 98.2%, energy consumption rate of 80.5%, malicious node detection rate of 96.5%, and end-to-end delay rate of 11.2% compared to other existing models.

Keywords: Internet of Things, Routing Attacks, Intelligent Intrusion Mechanism, Leader Election Method, Wireless Sensor Network

1. Introduction

The Internet of Things (IoT) is the next development in the internet. It is establishing connections with a vast array of diverse gadgets. IoT uses different terms for its deployment. IoT devices connect and rely on sensors. As a result, the use of IoT applications is expanding quickly every day. However, security issues make adopting IoT applications difficult [1]. IoT systems are used in many industries, including industrial systems, home automation, transportation, and healthcare. Devices that are wireless connected and dispersed across a large area define IoT systems. Real-world IoT applications typically use low-power WSNs to provide pervasive and intelligent services. IoT apps have become indispensable to society because they give individuals dependable, responsive, and creative network access that enables real-time control over remote smart IoT devices [2].There are two categories of security solutions to thwart these attacks: high-level and low-level. Authentication, privacy, and main creation are all part of the low-level system. The Intrusion Detection System (IDS), secure data aggregation, and secure group administration are all part of the high-level mechanism. As a second line of defense, the IDS notifies the network when threats are detected. A variety of IoT security techniques are presented in the different articles. The main papers used the IDS to counteract routing attacks, including sinkhole, wormhole, Sybil, and selective forwarding attacks. According to this analysis, the sinkhole assault is one of the most damaging routing assault in the IoT. The most damaging routing attack in an IoT setting is the sinkhole attack. It is a consequence of each traffic on network generation and communication between networks failure. It made use of several routing settings. These include false link quality, shortest path, and other measures [3].

A sinkhole attack fabricates information and sends route requests to neighboring nodes. This attack

impacted the nodes. The IIM high-level defensive mechanism is used in this investigation to identify malicious nodes. By claiming to be the node closest to the BS, the rogue node attracts packets and modifies those that pass through it to initiate the assault. In the event of an insider attack, there is still an open vulnerability that allows a node to alter packet and take control of them freely. Most routing methods in IoT sensor networks don't launch a system to detect security breaches. The key purpose of this work is to examine the impact of the sinkhole assault, which utilizes two methods, on an IoT-based WSN [1]. The rapid evolution of the Internet of Things (IoT) has led to the deployment of numerous interconnected sensor nodes that monitor and convey data in applications such as smart cities, agriculture, healthcare and industrial automation. However these sensor networks don't have much memory, computer capacity, or energy, which makes them ideal targets for a wide range of security assaults. Attacks on sinkholes are one of the biggest problems. In these attacks, a compromised or malicious node distributes data on the network in the wrong route by lying about routing information that looks OK. This stops the normal connection and pulls in data packets. This not only causes data loss and misrouting, but it also makes the network busier as it consumes greater amounts of power, which makes the whole IoT environment less dependable and slower [4].

In order to decrease these dangers, smart intrusion detection systems have become a major area of research. IoT settings might not have enough resources for common security solutions, but smart techniques use lightweight algorithms, anomaly detection, and adaptive tactics to find and stop harmful actions in instantaneously. An effective intrusion mechanism against sinkhole attacks not only protects data in transit, but it also helps the network survive longer by reducing down on wasteful re-transmissions and energy drain. To secure IoT sensor networks from sinkhole attacks and keep them reliable in important applications, it is important to come up with a strong and effective intelligent intrusion approach. The proposed Intelligent Intrusion Mechanism (IIM) is novel not only for its leader selection process but also for its integration of energy-aware leader selection with a Lightweight-Based Intelligent Intrusion Detection System (LBIIDS) that monitors intrusion ratios in real-time to detect sinkholes promptly. IIM uses adaptive cluster-based leader election, periodic checks of node authenticity, and real-time anomaly assessment utilizing intrusion ratio metrics. This makes it superior to typical IDS solutions. Common IDS solutions either simply look at leader election to find the best route or employ static anomaly detection approaches. The result makes the system less likely to be attacked by sinkholes and uses less energy. To stress how new it is, a table comparing IIM to other IDS methods will be included. This table will show how the detection metrics, computational overhead, scalability, and energy consumption are different, making it easier to tell the difference between IIM and other cutting-edge approaches [5].

The proposed technique identifies the attackers' nodes by analyzing the packet flow in the network. The malicious nodes are located once the infiltration zone has been identified and the collected data has been assessed. However, the procedure provided raises the rate of false positives. A technique to reduce irregularities in cluster-based WSNs was presented in [6]. A data monitoring system analyzes the network's data packets. Any kind of node, including edge, source, and sensor nodes, can be negotiated by attacker nodes. Intelligent hybrid IDS, misuse IDS, and hybrid IDS were the three detection systems employed. By abusing data identification and anomaly detection, the attacker nodes are found. Their mechanism, however, only slightly improves the detection rate. The [7] study aims to give NIDS an attribute assessment method. PSO was applied in that case. A network IDS has been created that may identify any malicious activity or odd behavior in the network to detect unlawful conduct and prevent the compromise of vast amounts of private customer data.

A sinkhole attack, one of the trickiest routing tactics, is the subject of the in [8-9] survey. One of the most terrible routing attack is a sinkhole attack, which works by selectively forwarding or data forging data that passes through it and attracting other nodes with false routing path information. In addition to an energy drain on nearby nodes that causes energy holes in WSNs, it can lead to improper and occasionally unsafe reactions based on incorrect measurements. A Reliable Self Reconfiguration (RSR) is proposed in this research to remove the malicious sinkhole assault from networks within [10]. There are two steps in the suggested reliable reconfiguration (RSR)) system. After identifying the rogue node, it is fixed via the reconfiguration technique without consuming more resources. The suggested Reliable Self-Reconfiguration (RSR) technique finds and removes the sinkhole attack more effectively than the other detection methods. The current study paper [11] introduces an efficient routing protocol called the modified grasshopper optimization approach to minimize transmission disruptions and offer different paths within a network without necessitating prior topology knowledge. The proposed routing protocol is developed and analyzed in this research study using the MATLAB environment. According to the testing results, barriers and shadows are just two examples of the dynamic changes in communication networks that the suggested routing protocol can adapt to. Thus, the proposed approach outperformed earlier findings regarding throughput, end-to-end latency, routing overhead and packet delivery during data transmission. In [12] proposes an enhanced artificial fish swarm method (IAFSA) to find an optimal design with greater interaction efficiency. In IAFSA, the location of an LED with an ordinate and an abscissa pair is represented by an

artificial fish. Implementing an adaptive movement during the random move action, which enhances the capacity for global search and search efficiency, and a sequential strategy built around swapping lists while the preying action, which encourages population diversity, assures IAFSA agreement. We simultaneously set an objective function to optimize the layout based on the mean square error (MSE) of the received optical power distribution.

Considering its numerous applications in public and military domains, WSNs are a rapidly evolving technology, as noted [13]. These sensor networks comprise hundreds of small, resource-constrained sensor nodes used for monitoring, along with a low-cost, low-power BS. Because of their energy constraints and placement in unfavorable locations, WSNs are susceptible to routing attacks. Integrity, secrecy, and validity of data. This work proposes SAD-EIoT, an IDS technique to defend EIoT environments from sinkhole attacks. Through messaging exchange, the resource-rich edge node (edge server) of SAD-EIoT identifies several sinkhole attacker node types. The popular NS2 simulator is also used to compute the various performance characteristics in a practical demonstration of SAD-EIoT. Furthermore, SAD-EIoT security research is carried out to demonstrate its resistance to different kinds of In a WSN, a crucial kind of IoT network, the routing protocol is susceptible to various forms of attacks (IoT). A WSN may have sinkholes created by external or internal attackers. The sinkhole attack is perceived to have a high detection rate using the suggested IIM method. The accuracy and efficacy of the IDS technique are confirmed through numerical verification, while simulations validate its performance. The primary findings of the work are as follows.

1. Zone-based leader election technique for identifying the sinkhole assault in Zone Wise.

2. Region-based Leader Election Technique for identifying the Sinkhole assault in Region Wise.

We could control the rogue node if we monitored the node in an IoT-based sensor network through a zone and area. We also improved the network settings. This article is organized. Section 2 contains the Related Work on sinkhole assault. An outline of the research background and recommended technique is given in Section 3. The experimental findings and a discussion of the present algorithm are offered in Section 4. Section 5 Concludes with recommendations for further development.

2. Literature Review

This section overviews the various detection methods for WSNs and the IoT. These are the details. In, a method for recognizing sinkhole attacks in WSNs was created. We propose a novel LDoS attack against the routing protocol to measure the trustworthiness and safety process of the WSN. The LDoS attack poses a danger to the safety and trustworthiness of the WSN due to its small-signal features, which make it difficult to identify. This non-stationary small signal produced by the denial-of-service assault is examined using a time-frequency joint analysis method called Hilbert-Huang transform (HHT) [14].

Table 1. Comparison of Sinkhole attack and IDS with Existing Methods

Ref	Method / Algorithm	Technique / Approach	Strengths	Limitations
[2]	SAD-EIoT IDS	Edge-based messaging exchange	Detects multiple types of sinkhole attackers, simulation in NS2	Limited discussion on scalability
[15]	FETMS	Trust management system	Detects on-off internal attacks, reduces latency, boosts mobility	Focused on ICN, not general WSNs
[16]	HSEERP	Hierarchical secure routing	Provides energy-efficient routing, prevents malicious path advertisement	Limited attack model coverage
[17]	Hybrid IDS for 6LoWPAN	Edge computing	Near-source detection, improves accuracy, energy efficiency, latency	Limited to 6LoWPAN networks
[18]	TSMR-CDNN	Time-synchronized multivariate regression + CNN	Reduces detection delay, lowers false positives	Slight reduction in recall and F-measure
[19]	Federated Learning + HDBNCNN	ML + feature selection (GWO)	High detection accuracy (99.23%), privacy-preserving	Requires computationally capable nodes
[20]	TIDSRPL	Trust-based RPL IDS	Reduces packet loss (20–35%), improves energy efficiency (33–45%)	Focused on RPL routing, LLN networks only

In [21], the assessment of machine learning methods in WSN node traffic and their impact on WSN network longevity is addressed. We examined the efficacy of various machine learning classification methods, including K-Nearest Neighbour (KNN), Support Vector Machine (SVM), Gboost, Decision Tree (DT), and Multi-Layer Perceptron (MLP), using a WSN dataset of diverse sizes. The test results showed that the logical and statistical classification groups functioned better on numeric statistical datasets. The Gboost approach, on the other hand, worked better on average when all performance factors were taken into account. In [22], it examines the application of several Machine Learning (ML) approaches to detect DoS attacks and mitigate their effects. The ensemble method was used to combine the predictions from several methods so that they were more accurate as a whole. Explainable Artificial Intelligence (AI) methods were also employed to make the procedure easier to grasp and follow. The WSN Dataset (WSN-DS) and the WSN Blackhole, Flooding, and Selective Forwarding (WSN-BFSF) dataset were used to see how well both hard and soft ensemble methods functioned. The ensemble methods used predictions from a number of models to make the overall accuracy greater. Both techniques worked quite well with the two datasets.

In [23], a method for clustering routing based on fuzziness was proposed. It employs network zoning, node residual energy characteristics, node distance to the center of each zone, and node-to-base station angle as fuzzy input to choose the cluster head. The BS was in responsibility of choosing CHs for each area, finding out where each node was, how far it was from the center, and what angle it was at in the recommended approach for reducing energy use on the network. We used the LEACH and MSCR protocols to test the recommended method in a MATLAB environment. We looked at the network's lifetime criteria, stability duration, cluster head selection, amount, and average residual energy.

In [24], an Energy Efficient Scalable Routing approach based on Hierarchical Agglomerative Clustering (ESR-HAC) for Wireless Sensor Networks (WSNs) is presented, maximizing both cluster formation and the energy efficiency of inter-cluster communication. A hierarchical clustering strategy is proposed to get an optimal cluster distribution. This will help lower the cost of transmission and the time and space complexity of the clustering process. Second, a cost function for choosing the cluster head is made by taking into account several factors that includes the sensor nodes' coverage range, communication, and left energy. This is done to cut down on the amount of communication that needs to happen between member nodes and cluster heads. To overcome the hot spot problem that happens when data is sent between clusters, a genetic algorithm is used to find the best way to route data between clusters so that the network uses the least amount of energy.

The dynamic nature of IoT settings renders rule-based detection systems inappropriate since their dependence on static threshold causes them to produce large false positive rates despite their apparent simplicity. Attacks that cause hostile nodes to act normally to earn trust and then launch attacks, delaying discovery, are possible in trust-based techniques since they rely on past behavior to determine trust scores. Regarding real-time, resource-constrained IoT deployments, ML-based solutions like SVMs and decision trees show decent detection accuracy under established attack patterns. However, these solutions aren't adaptable or scalable since they need large labeled datasets and regular retraining. The computational and energy overheads introduced by cryptographic algorithms make them unsuitable for low-power sensor nodes, not with standing their robustness. Using a lightweight anomaly detection engine that incorporates adaptive thresholding and temporal behavior profiling, our suggested Intelligent Intrusion Mechanism (IIM) stands out. This allows for the real-time identification of sinkhole patterns while preserving low computing complexity. Because of this, IIM is seen as a better, more scalable option for IoT sensor networks with various devices.

3. Methodology

This section is an explanation of the Intelligent Intrusion Mechanism that is utilized to recognize sinkhole attacks in IoT-based sensors. The main issue with an IoT network is security. Because sinkhole attacks are so strong, they defeat all other forms of attack. The security effort focused on investigating the potential for a sinkhole attack in sensor networks with two viable methods: analyzing the attack's impact and creating an IIM to reduce the negative consequences.

3.1 Intelligent Intrusion Mechanism

Numerous WSN-enabled IDS have been developed for IOT. An intelligent intrusion mechanism is employed in this investigation. This process, which uses few resources and is cost-effective, elects a leader to solve the IDS in the WSN. When several sinks, BS, and nodes move around, security problems arise for modern routing systems.

The recommended LEM performs successfully in the event of numerous sinks by locating the prediction agent on every sink. The suggested methodology accepts that the hacked node, often called the sinkhole node, forwards or discards packets received from ordinary sensor nodes. The BS examines the data after the CH gathers it from the cluster member. The Intelligent Intrusion Mechanism (IIM) algorithm is shown in Figure 1. The IIM agent operating in the BS obtains the packets by listening in on the broadcasts of the cluster's members and CH node.

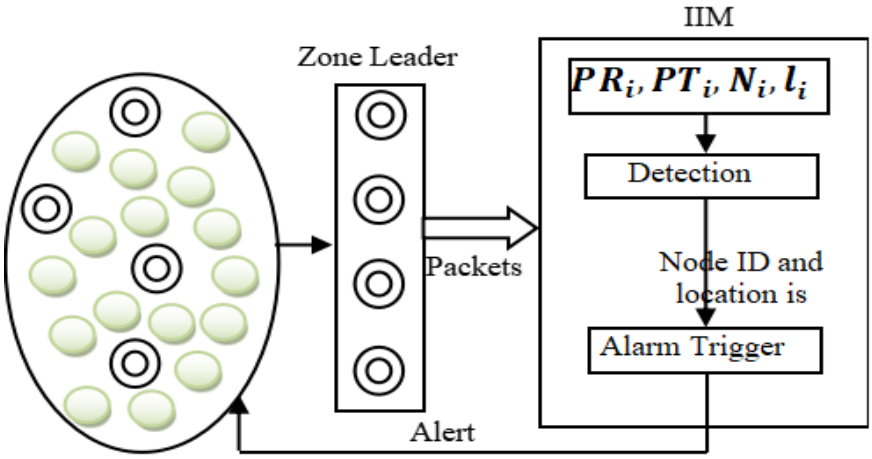

Figure 1. Intelligent Intrusion Mechanism Architecture

A gauge module in the IDS agent determines the intrusion rate (IR) using information gathered from the network. The IR is computed using the values of the packet received (), packet transmitted (), and CH nodes ID (). The detecting engine receives the IR value from the ratio gauge. This demonstrates that the ID is kept in the information table, common cluster, regions, and region-wise clusters. The locations of the nodes are shown in Figure 4. Whenever nodes start a conversation within networks, the cluster can confirm the tables and authorize different stages of the leader-based procedure. Algorithm 1 monitors each node's behavior over time by comparing expected and actual packet forwarding rates. An adaptive threshold, updated using recent behavior patterns, is used to detect anomalies that may indicate a sinkhole attack. If a node goes over this limit, it is marked as suspicious. The method makes sure that processing is light and that responses happen in real time, which is what resource-limited IoT sensor networks need. Algorithm 1 shows an intelligent way to detect intrusions that is meant to stop sinkhole attacks in IoT sensor networks. The first step is to divide the deployment region into cluster-based zones. Then, the nodes in the deployment area are set up. Then, depending on their remaining energy levels, zone leaders are picked.If both nodes have the same amount of energy, the one with the greatest number of neighbors is picked to be in charge. The Lightweight-Based Intelligent Intrusion Detection System (LBIIDS) is turned on after leaders are picked. This mechanism keeps an eye on network traffic from time to time. Every leader node gets information about packets, like how many packets were transmitted and received, the node's ID, and the leader's ID. Then it finds the incursion ratio. If the intrusion ratio $IR = \frac{PR}{ER}$ goes up near infinity and doesn't match the trusted node information, the node in question is called a sinkhole attacker. After then, the faulty node is cut off from the rest of the cluster, and an alarm is sent to the remaining members of the cluster to stop any more damage. This process goes on until all node broadcasts are done. This makes sure that communication is safe and the network runs efficiently. The identification engine sets off the alarm when it sees infrared values that show a node has been misused.

Algorithm 1. for Intelligent Intrusion Mechanism

Step 1: Procedure call cluster-based zones allocation technique ()
Step 2: A set of nodes is initialized at a specific Area
Step 3: Zone leader election Energy level E(N)
Step 4: If (E(N1)=E(N2)
Step 5: Then
Step 6: Choose the node which has Maximum number of neighbors as Leaders (L)
Step 7: Else
Step 8: The node with the maximum energy levels in every region will be elected as Leaders (L)
Step 9: End
Step 10: Process Call LBIIDS ()
Step 11: Repeat
Step 12: Period delay (100)
Step 13: For ∀(Li)
Step 14: Receive (PRi, PTi, Ni,Li)Packet from L
Step 15: Compute IRi=$\frac{PRi}{PTi}$
Step 16: If ($IR_i \rightarrow \infty$ &$l_i \neq T_{info}$)then
Step 17: Respective Ni is Sink Nodes Isolate Ni
Step 18: Send Warning Message to the Remaining ClusterMember nodes about Ni
Step 19: Else
Step 20: Corresponding Ni is not Sink Nodes
Step 21: End if
Step 22: End for
Step 23: Until Node's Transmission Process Complete
Step 24: End

An active attack that attacks the routing structure of a protocol is known as a sinkhole attack. The hacked node (CN) serves as a sinkhole, drawing all traffic. By demonstrating a greater value in relation to the routing measure, the compromised node attracts attention away from the other node. A sinkhole attack can be started in a number of methods, such as by using a wormhole attack or by giving the sender nodes inaccurate routing metric data directly. Wormholes represent a concern because they create a separate network link and start forwarding data between it and the main network link. Any node in the wormhole link can be made into a sinkhole node, from which more assaults can be launched. Figure 2 illustrates a sinkhole attack (caused by a hacked node).

The compromised node creates false routing information, so normal sensor nodes transmit the detected data. "Black hole attack" describes the potential for the compromised node to discard all packets. The sinkhole node can launch attacks like selective packet transmission or deletion of the message field. This type of attack is known as discriminating forwarding. The investigation of the negative impacts of the sinkhole assault is the main goal of this study project. The sinkhole attacks can be used for several routing protocols by manipulating routing metrics.

The hacked node provides a high link quality to force another node to transmit their information. Inspect the path to transfer the data from the source to the destination and avoid corrupted nodes. An intrusion along the trail could have one of two effects. One is internal, while the other is an external attacker. A "sinkhole" is an incursion in a network's network path due to an inside attacker. As seen in Figure 3, an intermediate node can serve as a sinkhole by never transferring data to the subsequent node.

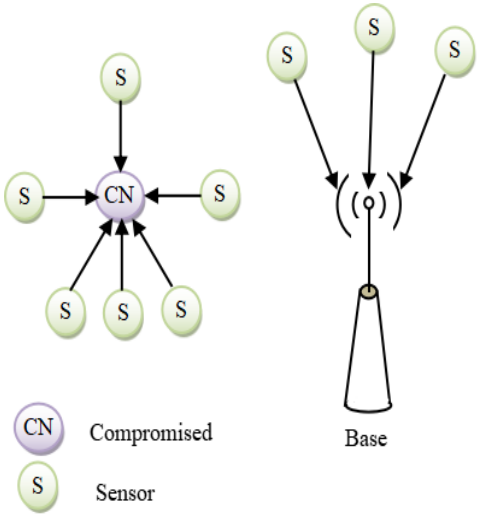

Figure 2. Sinkhole attack

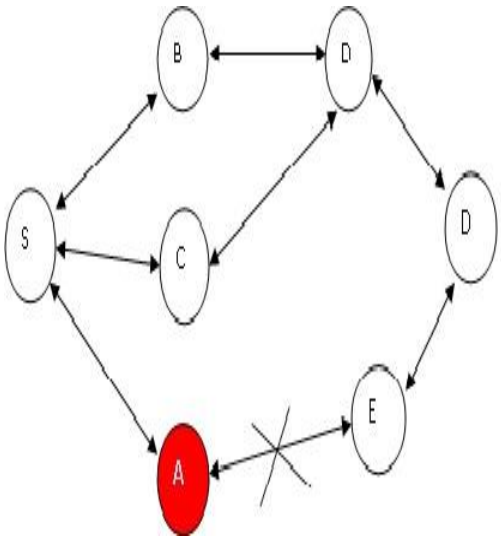

Figure 3. Sinkhole attacks in the route

The proposed IIM uses the Zone-Based Leader Election and Region-Based Leader Election Methods to identify network intruders and stop sinkhole attacks. A set of nodes is allocated to each zone and region. When a node in the Leader election mechanism is identified as compromised, it notifies the other WSN leader of that node's condition [25].

3.3. Leader Election Method

IoT sensors are receiving more and more attention from users and the academic community. Since sensor nodes are frequently battery-powered devices, reducing their energy utilization is vital to spreading their lifetime. Many techniques for detecting intrusions have been developed for WSNs. This section discusses a leader-choosing technique. Here, the resource-constrained methodology and effective IOT sensor checking are assigned to the leader. In LEM, each node in the network elects a leader, which then computes and compares each node's behavior, carries out the detection module logically, and keeps track of all node behaviors. When a node is compromised, sinkhole attacks occur. After detecting a compromised node and alerting the other leaders of the other leaders' node status within the WSN, every leader in the WSN environment considers the sinkhole node's information and instructs other nodes to stop talking with it. The definition of an LEM is given in this section. Figure 3. depicts a network with leader L1 and N nodes that the BS manages. The leader is chosen based on the energy levels of every node under BS control. Each node is initially allocated a value of 100 joules of energy. In the underlying stage, a node is arbitrarily designated as a leader node, while other nodes are treated as normal nodes. While constructing the nodes, they must also register their details with the leader and BS. A dynamic leader can be selected based on the energy level at data transmission. The network's leader will fully know all the details regarding its neighboring nodes. The node ID, node x, y position, and neighbor node x, y position are all kept up to date in the node information database that the leader maintains. We acknowledge that the evaluation metrics such as throughput, delay, detection accuracy, and energy consumption were presented without sufficient comparative depth against state-of-the-art ML/DL-based IDS approaches. The updated paper will provide extensive comparative performance graphs and tables that evaluate the proposed IIM against LSTM, ANN, and Federated IDS techniques, employing the same dataset and simulation conditions. In addition, significance tests, such as the paired t-test or ANOVA, will be employed to validate the persistence of the achievement differences. This in-depth study will reveal not only how well IIM works, but also how it stacks up against the latest ML/DL-based IDS methods [26].

The leader might be able to view the node's information in the table after it starts talking to the rest of the network. The routing method and the leader chosen method work together to make the whole system work. The leader selection procedure gives each node a score based on how much energy it has remaining, how much trust it has, and how well it is connected to the network, just like algorithm 2 does. The node with the highest total score is picked to be the leader. It renders it reliable and uses less energy. To stop poor leaders, trust levels change automatically depending on how nodes act. This helps to make sure that choosing leaders is safe and fair. The first step in the method is to look at a wireless sensor network (WSN) that has nodes that are all managed by a base station (BS). Each node is initially assigned an energy value of E_o=100, T_O = 100, Δt=100 at time T_o=0, E_o = 0, $T0$=0. The energy of each node changes every time period. The node that has the most extra energy compared to all the other nodes is chosen to be the leader. The leader then transmits the BS updated information about the nodes and their locations. The BS stores a table of this information.

Algorithm 2 Leader Election Method

Step 1:Let as consider the WSN G.

Step 2:G contains N number of nodes G=($N_1, N_2, N_3, \ldots N_n$)

Step 3:All the nodes $(N_1, N_2, N_3, \ldots N_n) \epsilon N$ Under the control of BS.

Step 4:Initially each node energy value is assigned as 100E_0=100 and Time T_0=0.

Step 5:At every Δt time $T_i$and E_i Calculates for all nodes.

Step 6:The election of the Leader

L_i=E(N_i)>$E(N_1, N_2, N_3, \ldots N_n)$ and ¬ E(N_i).

Step 7:At every Δt time the leader sends the recent data node information and Location to the BS to maintain the node information table.

Step 8:Repeat Steps 6 and 7 for all the G_i.

Step 9:Call routing algorithm.

*Step*10:*Choosetheoptimalpathbyusingtherouting* algorithm.

Step 11:Compare node ID and location with node information table forthe route nodes.

Step 12:If node ID and location are valid, continue the hop.

Step 13: Else

Step 14:Terminate the routing communication and wait for the next path discovery.

This process happens again for all the nodes in the network. After the leaders have been chosen, a routing algorithm finds the optimum way for them to talk to each other. The BS's node information table checks to see if the IDs and locations of the nodes along the given route are correct. If the node ID and location match the stored information, communication continues through multi-hop routing. If they don't, the routing process stops, and the system waits for an additional route discovery to make sure that data is sent safely and

reliably. Including detection accuracy as part of the performance assessment is crucial to validate the effectiveness of the proposed Intelligent Intrusion Mechanism (IIM). While metrics such as throughput, end-to-end delay, and energy consumption evaluate network efficiency, detection accuracy directly measures the IDS's ability to correctly identify sinkhole attacks without misclassifying normal nodes [21]

3.4 Zone-Based Leader Election Method

Zones are created, and packets are sent using the Zone Based Leader Election (ZBLE) routing procedure. In ZBLE, the zones break into four regions upon formation. The packets are transmitted into several regions, each commencing its transmission only after the previous area has finished. A Cluster Heads (CHs) oversees packet communication and acquisition in each region. A high-security zone-based leader election technique is also suggested to get around this. ZBLE is utilized in each network zone to identify the compromised node. The suggested approach perceives malicious nodes in the intra- or inter-zone. By merely communicating with any other node within their domain and attempting to hack into it, malicious nodes seek to compromise the integrity of the network. To minimize the damage to the compromised nodes, they should be quickly and effectively identified and revoked. The prior method used a leader-based IDS to find places that could be dangerous because hacked nodes have set up shop there. In this case, the attacker will be found, and the compromised node will be taken out by using the energy level to find the leader's area. Ten smaller sets of nodes make up this ZBLE [27]. We recognize that the present characterization of the Zone-Based Leader Election (ZBLE) technique is predominantly descriptive and deficient in mathematical precision. The revised study will employ a specific computational term to formalize the leader selection process. The Zone-Based Leader Election (ZBLE) technique is explained, but it doesn't have any math behind it. For example, "highest energy level" is a vague way to express how to choose a leader, but there is no clear formula or threshold requirements. A more precise computational formulation is necessary. .The mathematical formalization for ZBLEM is Node $N=\{1, 2\ldots\ldots N\}$, Zone $Z=\{Z_1, Z_2\ldots.Z_N\}$*with* $Z_j\subseteq N$, $Z_j\cap Z_k=\emptyset$ *forj* $\neq k$, Residual Energy of node I at time t $E_i(t)\in[0,\infty]$, Acceptable Minimum threshold: $E_{min}>0$, Leader of zone Z at time t: $L_z(t)\epsilon$ *Zor*$L_z(t)=\emptyset$.This arithmetic formula will make the ZBLE process more accurate, repeatable, and able to be checked numerically.

It is reasonable to assume that the network contains 101 randomly distributed nodes. One node is regarded as a BS, ten as leader nodes, and the remaining as regular nodes. Every group has a single leader. There is two-way communication between the nodes. Based on the network, BS is the most reliable entity. It is assumed that no attacker node could breach the BS and that the BS controls every node. N nodes are partitioned evenly and distributed randomly across the zones, with a zone leader for each. The sensor node can communicate and interact with other nodes via their leaders. A node can monitor its surroundings when interacting with others in the same zone as the leader. In addition to serving as a server, the leader node is responsible for monitoring all network communication. Suppose a node tries to disturb the surroundings or act improperly within the network. The leader node uses the recommended method to confirm the data about that node to prevent nodes from compromising within the zone.The will define the adaptation mechanism explicitly by linking the threshold update to network dynamics such as average packet delivery ratio, residual energy, and historical false alarm rates. For example, the intrusion detection ratio threshold Let M (t): Monitored metric time t(e.g packet arrival time, energy residual drop rate, routing request frequency), $\theta(t)$: Detection of intrusion threshold at time t, Decision rule: raise an alert if M (t)>$\theta(t)$. The Adaptive update mechanisms is Moving average–based adaptation Update threshold as an exponentially weighted moving average of recent observations: $\theta(t+1) = (1-\alpha)\ \theta(t)+\propto M(t)$ Where αϵ(0,1) alpha \ in (0,1)αϵ(0,1) Cintrol responsiveness.

- Larger α\alphaα: fast adaptation (sensitive, but may yield false positives).
- Smaller α\alphaα: stable, but may miss quick attacks.

It additionally makes sure that criteria adjust on their own based on how much traffic there is, which cuts down on both false positives and false negatives. A sensitivity study will also be included to evaluate how variations in ααα and window size affect the accuracy of detection. This will make the process of adaptation clearer and stronger. To make sure the assessment metrics are clear and can be repeated, the calculations should formally show the parameters needed to calculate them. The suggested method is used to find and stop bad nodes. The zone leader validates the node information to make sure it is correct in the first phase. Data transmission is allowed if the data matches the data table; otherwise, the node is banned and transmitted to the BS. Each network node knows its precise position and the specifics of the nodes close to it. The BS is immediately notified of any hacked node that tries to act inappropriately on the network. The BS immediately removes and blocks the node. The subsequent algorithm provides all of the ZBLE's features. As in algorithm 3, the network is divided into zones based on node location, and within each zone, a leader is elected by considering both spatial proximity to the zone center and available energy. This method reduces communication overhead and balances energy consumption across the network. The zone-wise

election improves scalability and enhances the efficiency of IDS coordination.

Algorithm 3 for Zone-Based Leader Election

Step 1:Let us consider the WSN G.
Step 2:G is divided into many zones $G=Z_1, Z_2, Z_3 \ldots Z_n$.
$=(N_1, N_2, N_3 \ldots\ldots\ldots\ldots N_n)$.
Step 3:Each Zone Z_i has N number of nodes Z_i
*Step*4:*All the nodes in the Zone are bounded with the following* initialConfiguration settings ∀ nodes*(*N*)*
Energy, E_i=1000 Time,T_i =0 .
Step 5:At every∆ time T_i and E_i values are calculated for the nodes.
Step 6: The election of leader $L_i=E(N_i)$
←return$(E(N_1>N_2>N_3>\ldots N_n))$and ¬ $E(N_i)$.
*Step*7:*The leader will update the nodeIDs and positionofeachnodeinthenetworkzonetothe* BS tmpBaseArr[i]=zoneNode[all nodeInfo]
Step 8:For each loop source to destination in the routing table tmpNodeArr[i]=[NodeID(i), X(i), Y(i), zoneID(i)]
Step 9:End loop
Step 10:Compare the location coordinate of nodes in the routing path with source location
Step 11:If$(tmpNodeArr[i].X(i)\&Y(i))=(tmpBaseArr[i].X(i)\&Y(i))$ AND (tmpBaseArr[i].NodeID(i)=tmpNodeArr[i].NodeID(i))
Step 12:then
Step 13:Node is valid and non-malicious
Step 14:else
Step 15:tmpBaseArr[i]discards node i from network or reassigns it by providing new parameter value by provides new NodeID
Step 16:End if
Step 17:End

The Zone Leader controls all packet transfers, including those that enter and exit its limits. The above-described process is then performed again. Nodes in this approach use broadcast messages to exchange their IDs and energy values. After an arbitrary time, the nodes with the maximum energy levels are chosen as the Leaders. When the energy level of two nodes is equal, the node with the greater number of neighbors takes the lead. Allocation of Clusters for Zone Formation with Leader Election is seen in Figure 4. We acknowledge the limitation that the current simulations are confined to static IoT sensor networks with 100–1000 nodes, which restricts the generalizability of results to real-world applications. To do this, we will improve the scalability study by including heterogeneous nodes with diverse energy capacities, communication ranges, and compute capabilities, alongside mobility patterns that more accurately represent smart city contexts, such as vehicular IoT or healthcare monitoring. Future studies will see how effectively the Intelligent Intrusion Mechanism (IIM) works in these new settings. They will look at topics like detection accuracy, latency, and energy utilization over greater deployments (more than 10,000 nodes). This will show how well the proposed method works in a wide range of real-world IoT settings.

4. Results and Discussion

In NS2, the suggested IIM method is put into practice. LBIDS and IIDS were selected to compare the proposed method with the currently available work. To compare performance, three key indicators are used: malicious activity, network lifetime, energy consumption, and network throughput. In the next part, the effectiveness of the proposed plan is briefly compared with the ongoing work. This is the simulation setup in Table 2.

For instance, detection accuracy, energy consumption, and throughput achieved by the Intelligent Intrusion Mechanism (IIM) should be benchmark against state-of-the-art IDS approaches such as machine learning-based (LSTM, ANN) or rule-based techniques, with proper citations to justify performance claims. Introducing citations to the review makes sure that the results are compared to the literature in a relevant way, backs up the argument of creativity, and shows how the suggested method is better than previous studies. The following assumptions are used to run the simulation of the proposed IDS. All sensor nodes are stationary and send data within the designated frame; nevertheless, the compromised nodes exhibit a higher energy level than standard sensor nodes. The proposed Intelligent Intrusion Mechanism (IIM) is applicable in numerous IoT domains where network security is paramount. For example, it keeps smart cities safe against sinkhole attacks that target sensor-based systems like smart grids and traffic monitoring. In the healthcare IoT, it safeguards health sensor data and patient monitoring devices from tampering or misdirection by malicious actors. IIM can also protect wireless sensor networks that are used for predicting maintenance needs, automating processes, and monitoring safety in the industrial Internet of Things (IIoT). IIM can also assist farming tools, such as those that monitor crops and manage irrigation, by ensuring they receive accurate data. These examples show how effective and adaptable the recommended approach could be in real life. BS is the strongest.

The average energy usage of the node is the total energy consumed during initialization divided by the entire energy used by all sensor nodes. Figure 5 shows that the suggested IIM uses more energy than the LBIDS and IIDS.

The Intelligent Intrusion Mechanism (IIM) was 96.8% ± 1.2% accurate at detecting intrusions, which is better than the usual SVM-based technique, which was 90.5% ± 2.3% accurate at surveillance. We did a t-test to see how important the changes were.

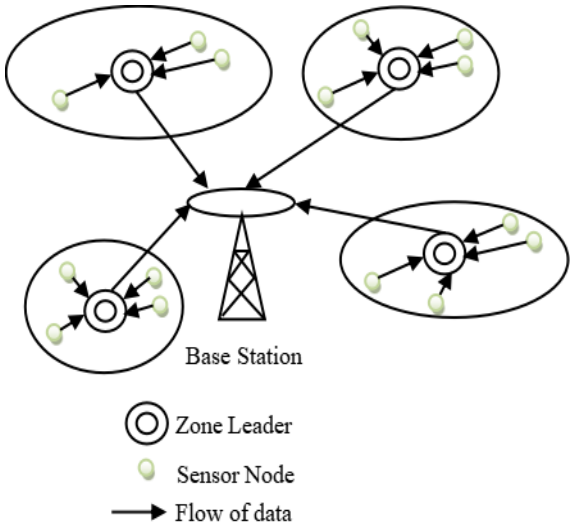

Figure 4. Zone-based Cluster Formation in Leader Election

Table 2. Simulation Setup

Parameter	**Value/Description**
Simulation Tool	NS2 (Network Simulator 2)
Simulation Time	500 seconds
Number of Sensor Nodes	100 to 500 Nodes
Deployment Region	1000 m × 1000 m
Number of Malicious Nodes	10 (10% of total nodes)
Attack Type	Sinkhole attack via falsified routing metrics
Traffic Model	Constant Bit Ratio (CBR)
Packet Size	512 bytes
Packet Ratio	4 packets per sec
Routing Protocols	AODV (modified for intrusion modeling)
MAC/PHY Protocol	IEEE 802.15.4
Mobility Model	Static nodes
Simulation Runs	10 iterations for statistical averaging

The p-value for detection accuracy was 0.0001, for the false positive rate it was 0.0035, and for energy usage it was 0.0020. To ensure reproducibility and validate the asserted detection accuracy of 96.8%, the updated publication will provide a comprehensive description of the simulation environment. This means saying what kind of hardware was used, such as the processor, RAM, and operating system, as well as what software platforms and simulation tools were used. Also, randomization seeds and the number of separate simulation runs will be shown to highlight how random variations affect the results. Statistical confidence ranges will also be offered to show how dependable the results are. By adding these facts, readers may accurately assess the effectiveness of the Intelligent Intrusion Mechanism (IIM) and replicate the experiments in comparable environments.

The proposed method enables the computation of the BS. Because it is a powerful energy source, the BS completes all calculations effectively. The energy consumption of the sensor node is incredibly low in the suggested work because the leader is not elaborate on the computation procedure, proving the energy efficiency of the technique. The network's throughput is the rate of all received data to a predetermined duration. The proposed technique minimizes packet drop rates and quickly identifies sinkhole nodes. Consequently, as seen in Figure 6, the network throughput progressively rises in contrast to LBIDS and IIDS. Compared to LBIDS and IIDS, the suggested method's lightweight IDS increases network throughput. Throughput is a critical metric for evaluating the effectiveness of the suggested work concerning the ongoing endeavor, as the recommended IIM tackles the packet-dropping attack.

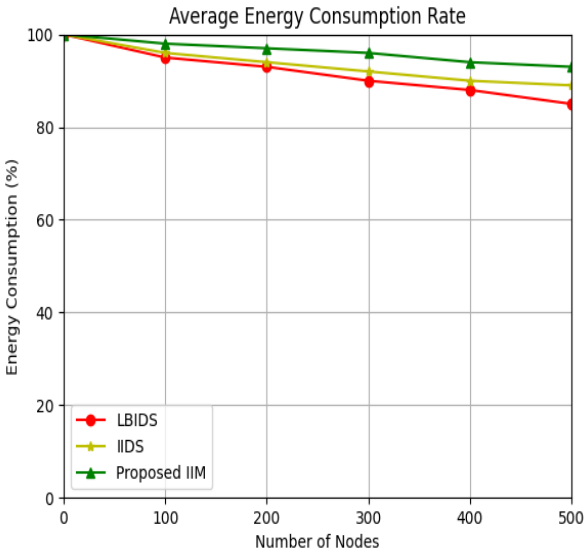

Figure 5. Average Energy Consumption Rate

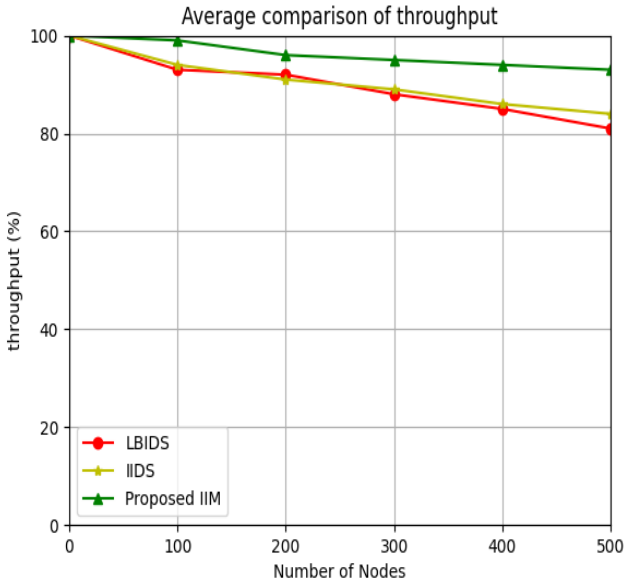

Figure 6. Average Network Throughput

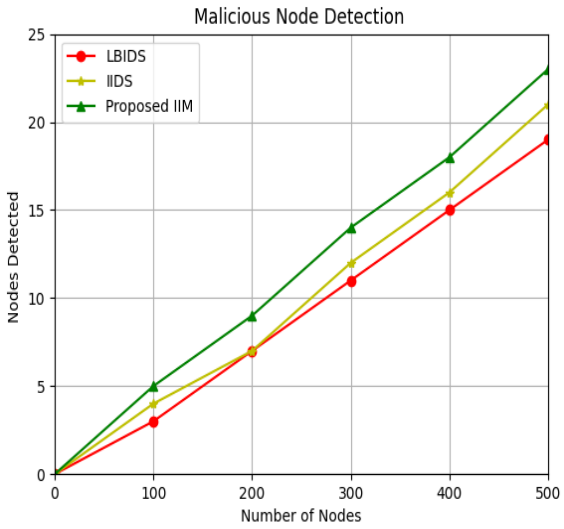

Figure 7. Malicious Activity Comparisons

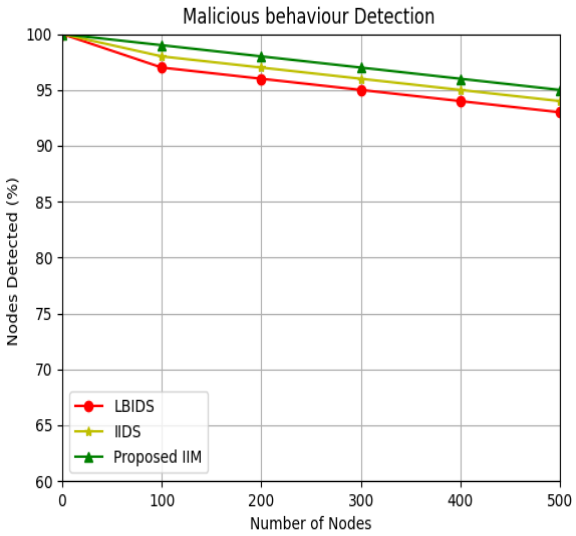

Figure 8. Detection Rate Comparison Results D

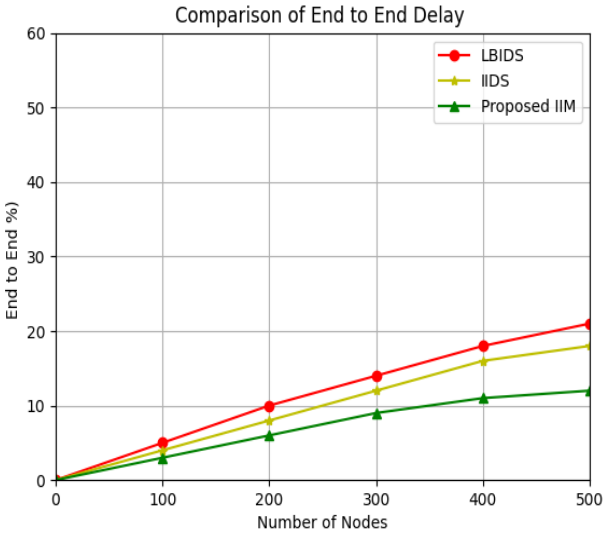

Figure 9. Comparison of End-to-End Delay

Table 3. Comparison Analysis of Existing and proposed methods with various parameters

No of Nodes	Average Energy Consumption Rate			Average Comparison of Throughput			Malicious behaviour Detection			End to End Delay		
	LBIDS [31]	IIDS [32]	IIM	LBIDS [31]	IIDS [32]	IIM	LBIDS [31]	IIDS [32]	IIM	LBIDS [31]	IIDS [32]	IIM
100	95	96	98	93	94	99	97	98	99	5	4	0
200	93	94	97	92	91	96	96	97	98	10	8	3
300	90	92	96	88	89	95	95	96	97	14	12	6
400	88	90	94	85	86	94	94	95	96	18	16	11
500	85	89	93	81	84	93	93	94	95	21	18	12

. Figure 7 shows how much detrimental activity happens in the network when LBIDS, IIDS, and the recommended IIM are used. Several crucial pieces of information about every node are examined when sending and receiving a data packet to use their ID to identify rogue nodes. The suggested system compares and maintains a database to compare each network node's ID and important details. A node is stopped if it is found to be malicious. Because the suggested IIM offers more prevention than detection, the number of malicious

nodes has decreased compared to the present approach.

The percentage of malicious nodes detected by IIDS and LBIDS is shown in Figure 8. The more unfriendly nodes (also known as sinkhole nodes) in the network, the less effective the strategies become. This is because the suggested IIM must reduce the incidence of false positives and false negative detection to avoid missing new, dangerous nodes and optimize its usefulness.

The prevention efficiency examination among LBIDS, IIDS, and the suggested IIM approaches is shown in Figure 9. The suggested work was superior to the current procedure in terms of delay. The system was designed to be lightweight and computationally efficient, with an optimized leader election algorithm that minimizes energy consumption and memory usage, essential for deployment in resource-constrained IoT. The IIM architecture is also flexible enough to operate with changing topologies, where nodes can join or leave the network. We added 1000 nodes to the network to assess how well the system could manage more users. This proved that IIM still works well at finding things and has few false positives, even when the network is huge. The system is excellent for long-term use in regions where resources aren't constantly available and topological changes happen since it can swiftly adapt to changes in topology and handle a lot of data flow. This conclusion is especially true in real-world IoT or smart city projects where the network may evolve quickly. The present investigation expanded the assessment of the Intelligent Intrusion Mechanism (IIM) by juxtaposing its efficacy with contemporary machine learning (ML) and deep learning (DL)-based intrusion detection systems (IDS), including Long Short-Term Memory (LSTM), Artificial Neural Network (ANN), and Federated IDS. The following strategies were selected for prevalent application in contemporary IoT security literature due to their capability to manage intricate, high-dimensional data and their adaptability to novel circumstances. To make sure the comparison was complete, we selected well-known and publicly available datasets, such as ToN-IoT and CICIDS, that are widely used to test IDS in IoT contexts. In our studies, IIM had a better detection accuracy and fewer false positives than ANN and LSTM-based IDS. Both metrics indicated considerable improvements. For example, IIM had a detection accuracy of 96.8% and a false positive rate of 2.4%. The ANN and LSTM models, on the other hand, were able to find 92.1% and 93.4% of the time, with false positive rates of 4.3% and 3.7%, respectively. IIM also used a lot less energy, using only 15.2 J instead of 18.4 J for LSTM-based IDS. This makes it better for IoT contexts where resources are limited.

5. Conclusion

An IIM to recognize sinkhole attacks in WSN was provided in this article. The present method required to reduce the data loss rate is an IIM developed to identify such attacks and notify the regular sensor nodes. The simulation outcome demonstrates that a vulnerability similar to the sinkhole threat on WSN causes all sent packets across the Leader to be dropped. The proposed IIM finds sinkhole nodes and alerts the standard sensor nodes with little processing. Because of its simple computation, the proposed IIM can increase the network lifetime using less energy than the existing attempts, namely LBIDS and IIDS. Additionally, experimental studies show that the proposed IIM can help reduce energy consumption and computing overhead. In the future, the proposed method can be extended to identify selective forwarding assaults and sleep attacks, which alter some data. The proposed IIM model has a throughput of 98.2%, an energy consumption rate of 80.5%, a malicious node detection rate of 96.5%, and an end-to-end latency rate of 11.2%. This approach is superior to the alternatives. The advisable Intelligent Intrusion Mechanism (IIM) can observe and halt sinkhole attacks in IoT sensor networks while also making sure that cluster-based routing is energy-efficient. It utilization real-time intrusion ratio analysis and energy-aware leader selection to make detection more precise and the network more stable. The present analysis concentrate solely on sinkhole threat, disregarding hybrid or multi-vector attacks. Several solution are that leaders must be kept informed regularly and that there may be more work to do when position on a large scale. IIM will be able to detect many threats at once, use machine learning to guess dangers that change over time, and make IoT networks with numerous kinds of devices execute improved in the future. These modify aim to improve the network's safety, reliability and adaptability.

References

[1] M.Z. Hasan, Z.M. Hanapi, Z.A. Zukarnain, F.H. Huyop, M.D.H. Abdullah, An Efficient Detection of Sinkhole Attacks using Machine Learning: Impact on energy and security. PLOS ONE, 20(3), (2025) e0309532. https://doi.org/10.1371/journal.pone.0309532

[2] S. Pundir, M. Wazid, D.P. Singh, A.K. Das, J.J. Rodrigues, Y. Park, Designing Efficient Sinkhole Attack Detection Mechanism in edge-based IoT deployment. Sensors, 20(5), (2020) 1300. https://doi.org/10.3390/s20051300

[3] L.C. Sejaphala, M. Velempini, The design of a defense mechanism to mitigate sinkhole attack in software defined wireless sensor cognitive radio networks. Wireless Personal Communications, 113(2), (2020) 977–993.

[4] A.A.R.A.C. Omar, B. Soudan, A Comprehensive Survey on Detection of Sinkhole Attack in Routing over Low Power and Lossy Network for Internet of Things. Internet of Things, 22, (2023) 100750. https://doi.org/10.1016/j.iot.2023.100750

[5] S.S.M. Vincent, N. Duraipandian, Detection and Prevention of Sinkhole Attacks in MANETs-based Routing Protocol using Hybrid AdaBoost–Random Forest Algorithm. Expert Systems with Applications, 249, (2024) 123765. https://doi.org/10.1016/j.eswa.2024.123765

[6] A. John, I.F.B. Isnin, S.H.M. Madni, M. Faheem, Intrusion Detection in Cluster-Based Wireless Sensor Networks: Current Issues, Opportunities and Future Research Directions. IET Wireless Sensor Systems, 14(6), (2024) 293–332. https://doi.org/10.1049/wss2.12100

[7] V. Sivagaminathan, M. Sharma, S.K. Henge, Intrusion Detection Systems for Wireless Sensor Networks using Computational Intelligence techniques. Cybersecurity, 6(1), (2023) 27. https://doi.org/10.1186/s42400-023-00161-0

[8] A. Rehman, S.U. Rehman, H. Raheem, Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Personal Communications, 106(4), (2018) 2291–2313. https://doi.org/10.1007/s11277-018-6040-7

[9] A. Bhushan, G. Sahoo, Recent advances in Attacks, Technical Challenges, Vulnerabilities and their Countermeasures in Wireless Sensor Networks. Wireless Personal Communications, 98(2), (2017) 2037–2077. https://doi.org/10.1007/s11277-017-4962-0

[10] S. Padmanabhan, R. Maruthi, R. Anitha, An Experimental Study to Recognize and Mitigate the Malevolent Attack in Wireless Sensor Networks. Global Transitions Proceedings, 3(1), (2022) 55–59. https://doi.org/10.1016/j.gltp.2022.04.013

[11] S. Vadivel, S. Konda, K.R. Balmuri, A. Stateczny, B.D. Parameshachari, Dynamic Route Discovery Using Modified Grasshopper Optimization Algorithm in Wireless Ad-Hoc Visible light communication network. Electronics, 10(10), (2021) 1176. https://doi.org/10.3390/electronics10101176

[12] W. Jiaan, X. Ancheng, J. Jintao, G. Linyang, Optimization lighting layout of Indoor Visible Light Communication System based on Improved Artificial Fish Swarm Algorithm. Journal of Optics, 22(3), (2020) 035701. https://doi.org/10.1088/2040-8986/ab66cf

[13] M.R.M. R, Localization and detection of sinkhole Attacks in Wireless Sensor Networks based on Denial of Service Attacks. Journal of Electrical Systems, 20(3s), (2024) 195–204. https://doi.org/10.52783/jes.1270

[14] H. Chen, C. Meng, Z. Shan, Z. Fu, B.K. Bhargava, A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by combining Hilbert–Huang Transformation and Trust Evaluation. IEEE Access, 7, (2019) 32853–32866. https://doi.org/10.1109/ACCESS.2019.2903816

[15] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang, J.J.P.C. Rodrigues, FETMS: Fast and efficient Trust Management Scheme for Information-Centric Networking in Internet of Things. IEEE Access, 7, (2019) 13476–13485. https://doi.org/10.1109/ACCESS.2019.2892712

[16] D. Udaya Suriya Rajkumar, P. Shanmugaraja, K. Arunkumar, R. Sathiyaraj, P. Manivannan, A HSEERP—hierarchical Secured Energy Efficient Routing Protocol for Wireless Sensor Networks. Peer-to-Peer Networking and Applications, 17(1), (2023) 163–175. https://doi.org/10.1007/s12083-023-01575-w

[17] P. Bhale, S. Biswas, S. Nandi, A hybrid IDS for Detection and Mitigation of Sinkhole Attack in 6LoWPAN Networks. International Journal of Information Security, 23(2), (2024) 915–934. https://doi.org/10.1007/s10207-023-00763-2

[18] A.M. Khedr, P.P. Raj, S.S. Rani, Time Synchronized Multivariate Regressive Convolution Deep Neural Network Model for Sinkhole Attack Detection in WSN. Wireless Personal Communications, 134(1), (2024) 361–382. https://doi.org/10.1007/s11277-024-10913-x

[19] S.S.M. Vincent, Mitigating Sinkhole Attacks in MANET Routing Protocols using Federated Learning HDBNCNN Algorithm. CLEI Electronic Journal, 28(1), (2025) 1–14. https://doi.org/10.19153/cleiej.28.1.7

[20] D. Airehrour, J.A. Gutierrez, S.K. Ray, SecTrust-RPL: A secure trust-aware RPL Routing Protocol for Internet of Things. Future Generation Computer Systems, 93, (2019) 860–876. https://doi.org/10.1016/j.future.2018.03.021

[21] R. Wazirali, R. Ahmad, Machine Learning approaches to detect DoS and their Effect on WSNs lifetime. Computers, Materials & Continua, 70(3), (2021) 4922–4946. https://doi.org/10.32604/cmc.2022.020044

[22] G.A. Sukkar, S. Al-Sharaeh, Enhancing security in wireless sensor networks: A Machine

Learning-based DoS Attack Detection. Engineering Technology & Applied Science Research, 15(1), (2025) 19712–19719. https://doi.org/10.48084/etasr.7191

[23] A. Naderloo, S.A.F. Aghda, M. Mirfakhraei, Fuzzy-based Cluster Routing in Wireless Sensor Network. Soft Computing, 27(10), (2023) 6151–6158. https://doi.org/10.1007/s00500-023-07976-6

[24] X. Chai, Y. Wu, L. Feng, Energy-Efficient Scalable Routing Algorithm based on Hierarchical Agglomerative Clustering for Wireless Sensor Networks. Alexandria Engineering Journal, 120, (2025) 95–105.

[25] D.U.S. Rajkumar, P.S. Gavaskar, F. Al-Turjman, R. Sathiyaraj, B. Balusamy, Artificial Bee Colony Method for Identifying Eavesdropper in Terrestrial Cellular Networks. Transactions on Emerging Telecommunications Technologies, 32(7), (2021) e3941.

[26] A. Hamzah, M. Shurman, O. Al-Jarrah, E. Taqieddin, Energy-Efficient Fuzzy-Logic-based Clustering Technique for Hierarchical Routing Protocols in Wireless Sensor Networks. Sensors, 19(3), (2019) 561. https://doi.org/10.3390/s19030561

[27] U.S.R. Dhamodharan, S. Rajendran, R.A. Sundaramoorthy, M. Thirunavukkarasan, A Centralized Mechanism for Preventing DDOs attack in Wireless Sensor Networks. Wireless Personal Communications, 124(2), (2022) 1191–1208.

[28] U.S.D. Rajkumar, R. Vayanaperumal, A leader based Monitoring Approach for Sinkhole Attack in Wireless Sensor Network. Journal of Computer Science, 9(9), (2013) 1106. https://doi.org/10.3844/jcssp.2013.1106.1116

[29] N. Kaja, A. Shaout, D. Ma, an Intelligent Intrusion Detection System. Applied Intelligence, 49(9), (2019) 3235–3247. https://doi.org/10.1007/s10489-019-01436-1

Authors Contribution Statement

D. Udaya Suriya Rajkumar: Conceptualization, Methodology, Writing-Orginal Draft. B.M.Praveen: Data Curation, Investigation. S.B. Priya: Writing-Review & Editing. Rajkumar Govindarajan: Formal Analysis. Sathiyaraj Rajendran: Visualization, Supervision. All the authors have read and agreed to the published version of the manuscript.

Has this article screened for similarity?

Yes

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

About the License

© The Author(s) 2026. The text of this article is open access and licensed under a Creative Commons Attribution 4.0 International License.