

Detecting Blackhole Nodes in IoT Environment using Logistic Regression-Based Trust-Based Security (LRTS)

C. Balakumar^{1*} and S. Vydehi²

¹Department of Computer Science,
Dr. SNS Rajalakshmi College of
Arts and Science (Autonomous),
Coimbatore, India

²Department of Information
Technology, Dr. SNS Rajalakshmi
College of Arts and Science
(Autonomous), Coimbatore, India

*E-mail: balakumar.cbk@gmail.com

Received for publication
May 12, 2025.

Abstract

Black hole attacks pose a critical threat to Internet of Things (IoT) networks by maliciously dropping data packets, severely disrupting communication, and compromising network reliability. These attacks exploit the lack of robust security mechanisms in common routing protocols, leading to significant data loss and network performance degradation. Addressing this vulnerability is essential to ensure the secure and efficient operation of IoT systems. This paper proposes an intelligent detection mechanism leveraging logistic regression (LR) and trust metrics to predict whether a node exhibits black hole behavior. Trust parameters such as end-to-end delay (ED), packet delivery ratio (PDR), energy consumption (EC), and reputation trust (RT) are employed as features in a LR model. The model is trained using stochastic gradient descent (SGD), initializing coefficients and a threshold for integrated trust (IT), and iteratively updating them based on the dataset. In the prediction phase, the learned coefficients compute IT values for unseen nodes, which are then classified as Trusted or Malicious. Simulation results confirm the effectiveness of the proposed model, achieving 85% accuracy—demonstrating a 13% improvement over conventional models with 72% accuracy. This proactive and data-driven approach significantly enhances IoT network resilience by enabling early detection and mitigation of black hole attacks.

Keywords

Internet of Things (IoT), security, blackhole attack, logistic regression, trust

1. Introduction

With the latest technological advancements, the Internet of Things (IoT) has become integral to everyday life. Kevin Ashton coined the term “Internet of Things” in 1999. Initially, it was called “Pervasive Computing” and “Embedded Internet”. Later, it was promoted to radio frequency identification (RFID). Today, IoT is often referred to as the internet of everything, incorporating emerging technologies like artificial intelligence, cognitive computing, and blockchain. IoT comprises interconnected devices, including sensors, digital machines, mechanical

devices, and more, each assigned unique identification numbers and internet protocol addresses for communication and data transfer (Zhou et al., 2018). This connectivity enables seamless communication anytime, anywhere, and among any entities, supporting machine-to-machine (M2M) communication, machine-to-person (M2P) communication, and person-to-person (P2P). Key characteristics of IoT include connectivity, heterogeneity, dynamic environments, unique identification, sensing capabilities, intelligence, scalability, and self-configuration. Similar to the IOS/OSI reference model, IoT adopts a layered architecture, typically comprising the

Sensing or Perception layer, Middleware layer, and Application layer. The Sensing layer, comprising sensors or RFID tags, detects environmental data, which is then processed by the Middleware layer (Yan et al., 2014). However, oversight in considering human-to-computer and human-to-human interactions may occur. The IoT system operates through internet-enabled smart objects equipped with sensors, actuators, processors, and communication devices, collecting data from the environment.

Security in IoT environments is not only susceptible to the threats faced by conventional networks but also to additional risks arising from IoT's inherent characteristics, including computation capabilities, memory, battery capacity, and deployment environment. In IoT networks, nodes rely on each other to complete tasks, as they don't depend on dedicated routers. Consequently, intermediate nodes may become overloaded, leading to resource depletion and potential selfish behavior, undermining cooperation. Moreover, the wireless nature of IoT exposes nodes to various users operating in potentially hostile environments with limited physical protection. Hence, security concerns should extend beyond external adversaries to include attacks originating from compromised nodes within the network. The dynamic nature of IoT further complicates matters, as trust relationships among nodes fluctuate with new node additions or departures, potentially leading to misbehavior and non-cooperation. Consequently, establishing a vibrant mark of defense in IoT in the view of security is challenging, necessitating the identification of untrusted nodes to safeguard highly sensitive IoT applications (Prathapchandran and Janani, 2021).

Furthermore, secure routing is a critical concern in IoT due to its unique characteristics. Routing protocols such as routing protocol for low power lossy network (RPL), dynamic source routing protocol (DSR), and ad hoc on-demand distance vector (AODV), and others aim to ensure timely and lossless information exchange between nodes. However, these protocols are vulnerable to internal routing attacks, meaning a black hole attack, caused by overloaded, selfish, or malicious nodes. Such attacks aim to retain incoming packets for self-benefit, disrupting the network's overall operation. Despite these challenges, ensuring the successful completion of tasks in the IoT environment requires a timely and uninterrupted information flow. Thus, the success of operations in IoT heavily relies on node cooperation, underscoring the critical role of routing security in overall network security (Muthu Ganesh et al., 2022).

The primary aim of the suggested research is to perceive and mitigate black hole attacks within the RPL routing protocol by leveraging logistic regression (LR) and along with quality of service (QoS) metrics.

II. Review of Literature

Due to the distinct nature of networks and other security vulnerabilities, routing security in IoT demands new techniques. Several routing approaches have been identified in the literature.

LR (Akturk et al., 2024 and Charizanos et al., 2024) is one of the Machine Learning Algorithms. It is a statistical tool where the dependent variable can take only two possible values. This tool explores the relationship between two variables, such as dependent and independent variables. The dependent variables can take the forms of discrete, continuous, and categorical. The proposed model adopt the feature of LR to classify and predict the behavior of nodes. In the training phase, the proposed model makes use of QoS Metrics to predict the node behavior. Therefore, the dependent variable describes the node behavior as trusted or untrusted whereas the independent variable encompasses the QoS metrics.

The logistic function, described in Eqs. 1 and 2:

$$p = \frac{1}{1 + \exp(-z)} \quad (1)$$

$$p = \frac{1}{1 + \exp(-(b_0 + b_1 \cdot x_1 + b_2 \cdot x_2 + b_3 \cdot x_3))} \quad (2)$$

where p represents the probability of the occurrence of variable y , with a range between 0 and 1.

The LR model employs numerical inputs to make predictions. Within this framework, the QoS metric serves as input, forecasting whether a node's behavior falls into the Trusted or Malicious category, which is considered the outcome. If the calculated probability surpasses a predefined threshold, the prediction categorizes the behavior as Trusted; otherwise, it categorizes it as Malicious.

For the proposed model, LR utilizes four coefficients (b_0, b_1, b_2, b_3) as in Eq, (3) and three input values. For instance:

$$Z = b_0 + b_1 \cdot x_1 + b_2 \cdot x_2 + b_3 \cdot x_3 \quad (3)$$

where b_0 represents the intercept or bias. It is assumed that the contribution significance of the

coefficient b_0 is 1.0, while x_1 , x_2 , and x_3 denote the input values. The learning algorithm is responsible for deriving the appropriate coefficients (b_0 , b_1 , b_2 , b_3) from the provided training data. The LR parameters are optimized using the stochastic gradient descent (SGD) method to obtain the best-fit model parameters.

The SGD algorithm is adept at precisely computing extreme probability LR constants from contribution data. It represents a progressive approach to updating regression coefficients, processing only one sample point (regression error) at a time. This procedure is categorized as an online wisdom algorithm, as classifiers can be incrementally updated during the sample update process. During optimization, each training sample is sequentially passed into the model. The model predicts the training sample based on the current coefficient values, computes new coefficient values based on the prediction error, and applies the classical method to minimize the error in subsequent predictions. This iterative process continues until the model achieves satisfactory accuracy or for a predetermined number of iterations.

The subsequent equivalence is employed as in Eq. (4) to modernize the coefficient (b) at each iteration:

$$b = b + \alpha \cdot (y - p) \cdot p \cdot (1 - p) \cdot x \quad (4)$$

where:

b represents the enhanced constants or weights,

x represents the input value,

y represents the output,

α is the learning rate, determining the extent to which the coefficients learn during each update. It is typically initialized at the outset of the training process. Optimal values typically fall within the range of 0.1–0.3.

Airehrour et al. (2018) introduced the SecTrust-RPL routing protocol, which prioritizes security in IoT networks by addressing routing attacks. This model assesses and evaluates a node's trustworthiness based on successful packet exchanges within a specific timeframe and positive acknowledgments from connected nodes. SecTrust becomes an integral part of the RPL routing protocol, providing defenses against Rank and SYBIL attacks. Alshehri and Hussain (2017) introduced a centralized approach to manage trust in the IoT, fostering secure communication between IoT nodes. This method introduces a super node (SN) acting as the centralized trust manager, dividing the IoT environment into clusters. Each cluster includes a master node (MN) serving as the local trust manager, supervising communication

among multiple cluster nodes (CNs). The SN maintains a central repository containing trust data for all MNs and CNs across the entire IoT framework, while MNs maintain local repositories housing trust values for CNs within their clusters. Centralized trust management emerges as a promising solution to tackle security challenges in the IoT domain.

Djedjig et al. (2015) proposed a method to enhance the trustworthiness of RPL nodes, aiming to mitigate both internal and external RPL attacks. In this approach, each node evaluates trust values for its immediate neighbors based on direct observations and feedback obtained from neighboring nodes. These computed trust values contribute to determining an RPL node's average trustworthiness, which assists in selecting parent nodes. Similarly, Seeber et al. (2013) introduced a trust computing architecture tailored for RPL within cyber-physical systems. This architecture employs a trust platform module (TPM) to establish trust and facilitate key exchange in RPL-based networks. Through the TPM, secure communication among authenticated nodes is facilitated by provisioning keys.

Iuchi et al. (2015) developed a strategy for secure parent node selection to safeguard RPL networks from infiltration by malicious nodes. Their method employs a trust-based threshold mechanism for node assessment. During the route construction phase, each node (x) calculates a threshold based on the maximum and average rank of its neighboring nodes. If a neighbor's rank falls below this threshold, it is considered hostile, and the node prevents it from being considered as a candidate for parent node selection.

In their paper (Govindaral et al., 2023), a trust model is introduced as a pivotal mechanism aimed at bolstering security. Trust assumes a crucial role not only in decision-making but also in the design and analysis of secure distribution systems. By assessing the trustworthiness of nodes, the objective is to enhance both security and routing performance. The primary contribution of another paper (Srinivas and Manivannan, 2021) lies in determining the optimal shortest route path using a hybrid algorithm termed dragonfly based deer hunting optimization algorithm (D-DHOA), which integrates the deer hunting optimization algorithm (DHOA) and the dragonFly algorithm (DA). This integration considers parameters such as trust, distance, delay or latency, and packet loss ratio in the objective model. Consequently, the entire process becomes highly effective in identifying and thwarting two fundamental attacks, namely black hole and selective forwarding, within IoT-WSN in the healthcare sector.

This article (Gnanaprasanambikai, 2024) addresses a significant security threat, namely the black hole attack, within IoT networks using the RPL protocol for data packet routing at the network layer. Recent research suggests that security has not been a top priority for manufacturers, creating an opening for potential attacks to infiltrate networks. To tackle this issue, a trust-based mechanism is developed specifically to mitigate black hole attacks within the RPL protocol. Additionally, Srinivas and Manivannan (2021), Alansari et al. (2023), Bhosale et al. (2022), Srinivas et al. (2020), Shukla et al. (2021), Sahraneshin et al. (2023), and Chakravorty et al. (2023) proposed various security mechanisms to address the black hole attack in IoT.

While security mechanisms like Shared Secret, public key infrastructure (PKI), Digital Signature, Digital Certificate, and Hash functions are effective, they often rely on centralized and predetermined approaches, often involving trusted third parties Bhalaji et al. (2019). However, this reliance can lead to increased computational power, memory consumption, communication bandwidth usage, and battery power consumption, which in turn can degrade the overall network's throughput, availability, and robustness—especially in IoT environments with resource-constrained nodes. Moreover, these techniques can prove inefficient in addressing internal attacks.

III. Proposed Work: Logistic Regression-Based Trust-Based Security (LRTS)

The primary objective of the proposed Lightweight Routing Trust Scheme logistic regression-based trust-based security (LRTS) is to effectively identify and mitigate black hole attacks in IoT networks while predicting the future behavior of nodes to enhance network security and reliability. LRTS is designed to operate in decentralized IoT environments where no central authority exists to evaluate the trustworthiness of devices. Instead, each node independently assesses the reliability of its neighboring nodes based on observed behavior, enabling informed decisions for future interactions.

The network is assumed to consist of n nodes, including some compromised nodes acting as black holes, to evaluate the robustness and effectiveness of the trust model rigorously. Recognizing the inherent constraints in IoT devices—such as limited memory, processing power, and battery capacity—the proposed scheme influences the energy consumption

(EC) associated with continuous monitoring, sensing, and communication processes.

This work focuses on post-authentication node behavior, acknowledging that nodes initially authenticated can exhibit malicious behavior later due to compromise. Each node passively monitors the communication behavior of its adjacent nodes through acknowledgment mechanisms, maintaining situational awareness within the network.

Within the network, two types of nodes exist: trusted and untrusted/malicious. Trusted nodes conduct all network activities, while untrusted nodes, identified as black holes, engage in malicious actions like packet dropping. The LRTS comprises the following phases:

- Trust evaluation & organization of black hole nodes by means of integrated trust (IT)
- Prediction of black hole nodes by means of LRTS

Trust evaluation commences when the performance of the IoT environment deteriorates. In such circumstances, every node within the IoT is tasked with assessing the trustworthiness of its neighboring nodes by using the LRTS model. This proposed mechanism has been integrated into the RPL routing protocol. Trust evaluation can be conducted by each node toward every other node built on numerous trust metrics, including EC, end-to-end delay (ED), packet delivery ratio (PDR), and reputation trust (RT). The collective assessment of these trust metrics is specified as direct trust, as each node directly evaluates. Assuming that over time, node ' i ' seeks to assess the reliability of node ' j ', it will assess the PDR of node ' j ' concerning node ' i '.

The PDR is well-defined as the proportion between the whole data packets forwarded and the total number of data packets received. The term "forwarding" refers to transferring data without any loss or manipulation. In the context of a black hole attack, characterized by the intentional dropping of incoming packets, the PDR is significantly reduced. Malicious entities drop packets intentionally, resulting in fewer packets reaching the destination successfully and thus diminishing the PDR. As genuine nodes are forced to retransmit the dropped packets, both the PDR and collision rate are affected adversely. Moreover, malicious vehicles may disrupt the entire routing operation, further impacting the PDR. Considering these factors, the PDR is considered a critical metric.

In the RPL routing protocol, several control packets are used, including the destination advertisement

object (DAO), destination advertisement acknowledgment (DAO-ACK), DODAG information object (DIO), DODAG information solicitation (DIS), and. Therefore, the PDR is calculated using Eq. (5) below.

$$PDR_{n_{ij}} = \sum_{n=1}^N \beta_i \left(\frac{SF(DIO)_{n_{ij}}}{UF(DIO)_{n_{ij}}} + \frac{SF(DAO)_{n_{ij}}}{UF(DAO)_{n_{ij}}} + \frac{SF(DIS)_{n_{ij}}}{UF(DIS)_{n_{ij}}} + \frac{SF(DAO-ACK)_{n_{ij}}}{UF(DAO-ACK)_{n_{ij}}} \right) + \sum_{n=1}^N \beta_i \left(\frac{SF(DP)_{n_{ij}}}{UF(DP)_{n_{ij}}} \right) \quad (5)$$

In the above equation, where, $i, j = 1, 2, 3 \dots N$, $i \neq j$, $\sum \beta_i = 1$, β_i represents weight factor

$SF(DIO)_{n_{ij}}$ denotes successful forwarding ratio of DIO

$UF(DIO)_{n_{ij}}$ denotes unsuccessful forwarding ratio of DIO

$SF(DAO)_{n_{ij}}$ denotes successful forwarding ratio of DAO

$UF(DAO)_{n_{ij}}$ denotes unsuccessful forwarding ratio of DAO

$SF(DIS)_{n_{ij}}$ denotes successful forwarding ratio of DIS

$UF(DIS)_{n_{ij}}$ denotes unsuccessful forwarding ratio of DIS

$SF(DAO-ACK)_{n_{ij}}$ denotes successful forwarding ratio of DAO-ACK

$UF(DAO-ACK)_{n_{ij}}$ denotes ineffective progressing ratio of DAO-ACK

$SF(DP)_{n_{ij}}$ denotes fruitful progressing ratio of Data Packets,

and $UF(DP)_{n_{ij}}$ denotes unsuccessful forwarding ratio of Data Packets.

Next node 'i' will assess the ED of node 'j'. The following equation is used to evaluate the ED of node 'j' with respect to node 'i'. ED includes all possible delays that have arisen due to the route detection, route dissemination, re-transmission, and relay time. It has been computed using Eq. (6).

$$ED_{n_{ij}} = \frac{\sum_{s=1}^n PR_s - PS_s}{SNP_{n_{ij}}} \quad (6)$$

In the above equation, PR_s denotes the period to arrive at the starting data of the 's'th packet from the starting node 'i' to the ending node 'j'. PS_s denotes the time to start the starting information of the 's'th packet from the starting node 'i' to the ending node 'j'. $SNP_{n_{ij}}$ denotes the total quantity of packets forwarded by node 'i' to node 'j'. Then, EC can be constructed on the following equation. The life of any IoT device might be determined by this factor. The services of any device can be assessed as long as they are alive. Otherwise, they will be treated as dead. Adversaries will try to deplete the energy level of genuine devices by engaging in malicious activities, thereby reducing the energy level of genuine devices. The subsequent Eq. (7) is used to assess the energy level of a node:

$$EC_{n_{ij}} = Transmit_{n_{ij}} * 19.5mA + listen_{n_{ij}} * 21.5mA + CPUtime_{dj} * 1.8mA + LPM_{dj} * \frac{0.0545mA}{32768} \quad (7)$$

Where,

$i = 1, 2, 3 \dots n$

$j = 1, 2, 3 \dots n$

and $i \neq j$

$Transmit_{n_{ij}}$ denotes energy depletion of node 'j' with respect to node 'i' after it is involved in transmission activities

$listen_{n_{ij}}$ denotes energy depletion of node 'j' with respect to node 'i' when it is involved in listening activities

$CPUtime_{dj}$ denotes of CPU utilization time of node j

LPM_{dj} denotes the Low Power Mode of node j.

The suggested approach makes use of a power tracing mechanism (Prathapchandran and Janani, 2021) to trace out the utilization power of participating nodes. Next node i will evaluate the RT of node j with the help of the following equation. Reputation serves as a critical component in trust calculation, representing a form of global trust. In this model RT periodically collects. The following Eq. (8) used to compute the RT.

$$RT_{n_{ij}} = \frac{\sum_{k=1}^m RET_{nsnj}}{m} \quad (8)$$

In the above equation,
 m nodes, the number of devices in the network

RET_{nsnj} denotes recommendation trust provided by the nodes (ns) who had direct interaction with node nj over the period of time.

To calculate the IT by combining all the trust metrics to evaluate the trustworthiness of nodes, we can use a weighted sum approach. Each trust metric (PDR, ED, EC, and RT) is assigned a weight to reflect its relative importance in determining trust. The weights can be determined based on the precise necessities of the IoT environment and the significance of each metric in assessing node behavior. The IT can then be calculated using the following Eq. (9).

$$IT_{vij} = \mu_1 PDR_{vij} + \mu_2 ED_{vij} + \mu_3 EC_{vij} + \mu_4 RT_{vij} \quad (9)$$

In the above equation, $\mu_1 + \mu_2 + \mu_3 + \mu_4 = 1$.

Once the IT is calculated for each node, it can be compared against a predefined threshold value to decide whether the node is trustworthy or not. If IT exceeds the threshold, the node is considered trustworthy; otherwise, it is classified as untrustworthy or malicious. The following Eq. (10) is used to classify the nodes. Based on the IT value, the node can be identified as a Blackhole node or a trusted node.

$$IT_{vij} < \text{Threshold, Blackhole nodes} \quad (10)$$

$$IT_{vij} \geq \text{Threshold, Trusted nodes.}$$

The above threshold value can be fixed per the user's requirements.

Figure 1 illustrates the workflow of the proposed LRTS model. The process begins with initializing model parameters and collecting trust metric data, including PDR, energy delay (ED), EC, and residual energy (RT). After normalizing these features, the LR model is trained via SGD to compute an IT score. Nodes are classified as trusted or malicious based on whether the IT surpasses a defined threshold. The model then predicts the behavior of new nodes, enabling dynamic trust assessment and enhancing network security through continuous monitoring and classification.

The following section discusses the forthcoming performance of the participating devices in the network environment. Algorithm for the proposed work as follows:

Input : Trust Metrics (PDR, ED, EC, and RT)

Output: Classify the nodes as Blackhole or node and predict the node's future behavior

Step 1: Initialize Parameters:

Step 1.1 Define the logistic regression model with coefficients ($b_0, b_1, b_2, b_3, b_4, b_5$) representing the weights for each trust metric.

Step 1.2 Set a Threshold value for Integrated Trust (IT) to classify nodes as Trusted or Malicious.

Step 2: Input Data:

Step 2.1 Obtain the trust metrics data for each node:

PDR, ED, EC, RT

Step 2.2 Classify each node as either Trusted (1) or Malicious (0) based on whether it performed a black hole attack or not.

Step 3: Feature Scaling:

Normalize or scale the trust metric values to ensure uniformity and prevent dominance of certain metrics over others.

Step 4: Training Phase:

Utilize logistic regression to train the model on the input data:

Iterate through the training dataset:

Compute the Integrated Trust (IT) value for each node using the logistic regression equation:
 $IT = b_0 + b_1 \cdot PDR + b_2 \cdot Delay + b_3 \cdot Energy + b_4 \cdot RS$

Compare IT with the Threshold value:

If $IT > \text{Threshold}$, classify the node as Trusted (1).

If $IT \leq \text{Threshold}$, classify the node as Malicious (0).

Update the coefficients (b_0, b_1, b_2, b_3, b_4) using the stochastic gradient descent algorithm:

$b_i = b_i + \alpha \cdot (y - p) \cdot p \cdot (1 - p) \cdot x_i$ where:

α is the learning rate.

y is the actual class label (Trusted or Malicious).

p is the predicted probability of the node being Trusted.

x_i is the value of the corresponding trust metric.

Step 5: Prediction Phase:

After training, use the learned coefficients to predict the behavior of new nodes:

Compute the Integrated Trust (IT) value for each node using the logistic regression equation.

Compare IT with the Threshold value:

If $IT > \text{Threshold}$, classify the node as Trusted.

If $IT \leq \text{Threshold}$, classify the node as Malicious.

Step 6: Output:

The predicted classification (Trusted or Malicious) for each node based on the Integrated Trust value.

The following section discusses the mathematical explanation of the proposed model. Here's a

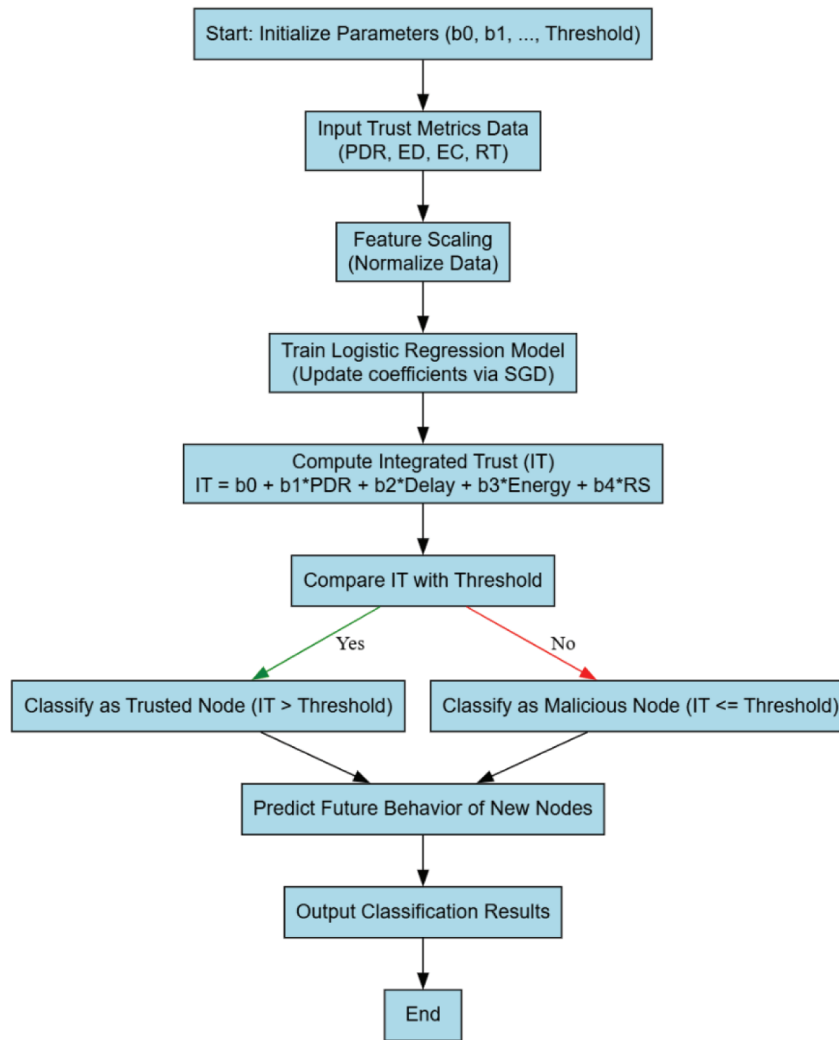


Figure 1: Overview of proposed work. EC, energy consumption; ED, end-to-end delay; IT, integrated trust; PDR, packet delivery ratio; RT, reputation trust; SGD, stochastic gradient descent.

step-wise algorithm representation with a mathematical example:

Step 1: Initialize Parameters:

Define the logistic regression model with coefficients (b0, b1, b2, b3, b4, b5).

Set Threshold value for Integrated Trust (IT).

Example:

Step 1: Assume the coefficient values as follows and set the threshold value for the integrated trust as follows:

b0=0.5
b1=0.2
b2=-0.3
b3=0.1
b4=0.4
b5=-0.2

Threshold value for IT = 0.7

Step 2: Input Data:

Obtain trust metrics data for each node.

Classify each node as Trusted (1) or Malicious or Blackhole (0).

Example:

Node 1: PDR = 0.8, Delay = 10 ms, Energy = 30 J, RS = 0.6, Class = 1 (Trusted)

Node 2: PDR = 0.5, Delay = 20 ms, Energy = 40 J, RS = 0.4, Class = 0 (Malicious)

Step 3: Feature Scaling:

Normalize or scale the trust metric values.

Example:

Normalize PDR, Delay, and Energy values between 0 and 1.

Step 4: Training Phase:

Iterate through the training dataset.

Compute IT for each node using logistic regression equation.

Update coefficients using stochastic gradient descent algorithm.

Compare IT with Threshold to classify nodes.

Example:

For Node 1:

$$IT = 0.5 + 0.2 \cdot 0.8 - 0.3 \cdot 10 + 0.1 \cdot 30 + 0.4 \cdot 0.6 = 0.87$$

$IT > \text{Threshold}$ ($0.87 > 0.7$), so classify as Trusted.

For Node 2:

$$IT = 0.5 + 0.2 \cdot 0.5 - 0.3 \cdot 20 + 0.1 \cdot 40 + 0.4 \cdot 0.4 = 0.61$$

$IT \leq \text{Threshold}$ ($0.61 \leq 0.7$), so classify as Malicious or Blackhole

Step 5: Prediction Phase:

Use learned coefficients to predict behavior of new nodes.

Compute IT for each node using logistic regression equation.

Compare IT with Threshold to classify nodes.

Example:

For a new node:

$$IT = 0.5 + 0.2 \cdot \text{PDR} - 0.3 \cdot \text{Delay} + 0.1 \cdot \text{Energy} + 0.4 \cdot \text{RS}$$

If $IT > \text{Threshold}$, classify as Trusted.

If $IT \leq \text{Threshold}$, classify as Malicious.

Step 6: Output:

Predicted classification (Trusted or Malicious) for each node based on IT value.

Example:

For the new node with PDR = 0.7, Delay = 15 ms, Energy = 35 J, RS = 0.5:

$$= 0.5 + 0.2 \cdot 0.7 - 0.3 \cdot 15 + 0.1 \cdot 35 + 0.4 \cdot 0.5 = 0.71$$

$$IT = 0.5 + 0.2 \cdot 0.7 - 0.3 \cdot 15 + 0.1 \cdot 35 + 0.4 \cdot 0.5 = 0.71$$

$IT > \text{Threshold}$ ($0.71 > 0.7$), so classify as Trusted.

IV. Simulation Results and Discussion

The performance of the proposed LRTS model was evaluated through extensive simulations designed to assess its effectiveness in detecting malicious nodes within wireless sensor networks. Trust assessment metrics such as PDR, ED, EC, and RT were considered to reflect network reliability and node behavior comprehensively. The goal was to demonstrate that the LRTS model can accurately classify nodes as trusted or malicious, thereby improving network security and resource utilization. The simulation was implemented using Python with the LR model trained via SGD. The network consisted of 100 sensor nodes randomly deployed in a 1000 m × 1000 m

area. Simulated traffic included both normal and malicious nodes generating packets under varying load conditions. The key simulation parameters are summarized in Table 1. During the simulation, trust metrics were continuously monitored and normalized. The LR model integrated these features to compute an IT score. A threshold value of 0.5 was chosen for classification; nodes with $IT \geq 0.5$ were considered trusted, while those below were flagged as malicious. The model's accuracy, precision, recall, and F1-score were calculated to evaluate performance.

The primary objective is to detect the Black hole attack. Before doing so, it is crucial to understand its impact on the IoT environment. For this purpose, Black hole nodes will be strategically placed within the IoT environment, and their effect on the packet dropping ratio will be analyzed. The proposed LRTS model will be compared with existing similar models, such as the one proposed by David Airehrour et al. (2019), as well as the traditional RPL routing protocol. The comparison will be based on various concert metrics, including:

Table 1: Simulation parameters

Parameter	Value
Simulator	NS3
Duration	1000 s
Routing protocols	RPL, TRLS, David Airehrour et al. (2019)
No. of Nodes	100
No. of untrusted nodes	10%, 20%....80%
Traffic type	CBR
Propagation model	Nakagami Model
Mobility model	Random Waypoint
MAC type	IEEE 802.11
Mode of channel	Wireless
Data payload	512 B/packet
Simulation area	1000 m × 1000 m
Nodes' speed	5 – 10 – 15 – 20 – 25 (m/s)
Data rate	10.4 Mbps
RPL parameter	MinHopRankIncrease = 256
LR learning rate	0.01
Number of iterations (training)	1,000
Threshold	0.5

CBR, constant bit rate; LR, logistic regression; RPL, routing protocol for low-power lossy network.

- PDR
- Average Delay
- Routing Overhead
- Detection Ratio

a. Packet dropping ratio analysis

Figure 2 illustrates the impact of the packet dropping ratio in a network environment compromised by the presence of Black Hole nodes. It is clearly observed that as the number of Black Hole nodes increases within the network, the packet dropping ratio correspondingly increases at regular intervals of time. This trend indicates a direct correlation between the proportion of malicious nodes and the degradation of network performance. The root cause of this vulnerability lies in the RPL, which inherently lacks integrated security mechanisms to detect or mitigate such internal attacks. Consequently, Black Hole nodes exploit this weakness by maliciously dropping packets instead of forwarding them, resulting in significant data loss and reduced network reliability. This behavior not only hampers effective communication but also affects critical applications relying on consistent data transmission. These findings underscore the urgent need for enhanced security features within RPL to safeguard against packet dropping attacks and maintain network integrity.

b. Packet delivery ratio analysis versus blackhole nodes

Figure 3 illustrates the relationship between the PDR and the presence of Black Hole nodes within the network. As the number of Black Hole nodes increases at regular intervals, the resulting impact on the PDR is systematically analyzed. The figure clearly demonstrates that the proposed LRTS (Lightweight Routing Trust Scheme) model consistently achieves a higher PDR compared to the two existing baseline models. This improvement highlights the effectiveness of the LRTS model in mitigating the adverse effects caused by malicious nodes that drop or manipulate data packets. By incorporating trust-based mechanisms and enhanced detection strategies, the LRTS model effectively isolates Black Hole nodes, ensuring that data packets are routed through more reliable paths. Consequently, the model sustains network reliability and performance even in the presence of increasing internal attacks. These results emphasize the potential of trust-based routing protocols in enhancing the security and robustness of low-power and lossy networks.

The LRTS prototypical reflects QoS metrics such as PDR, ED, EC, and RT to assess the reliability of participating devices, resulting in an IT score. Additionally, LR support is incorporated into the model to identify and eliminate Black Hole devices,

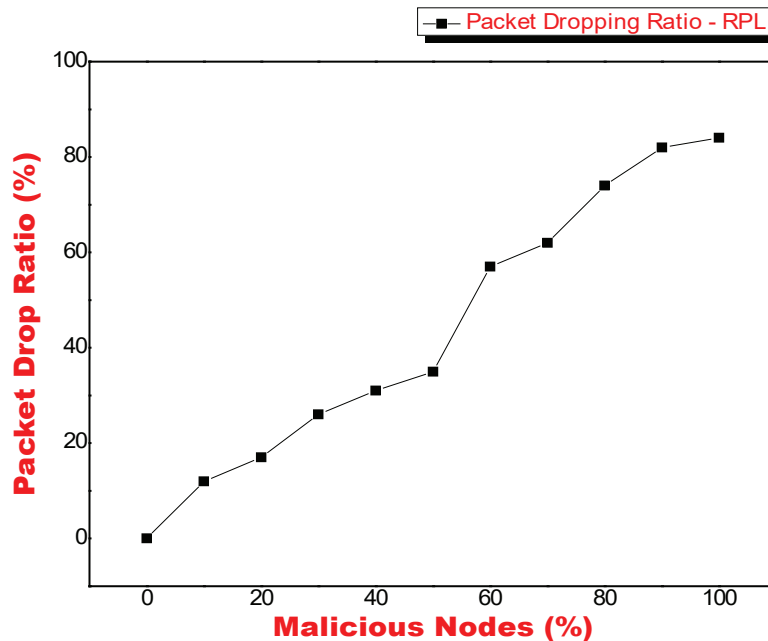


Figure 2: Influence of black hole nodes under normal RPL routing protocol. RPL, routing protocol for low-power lossy network.

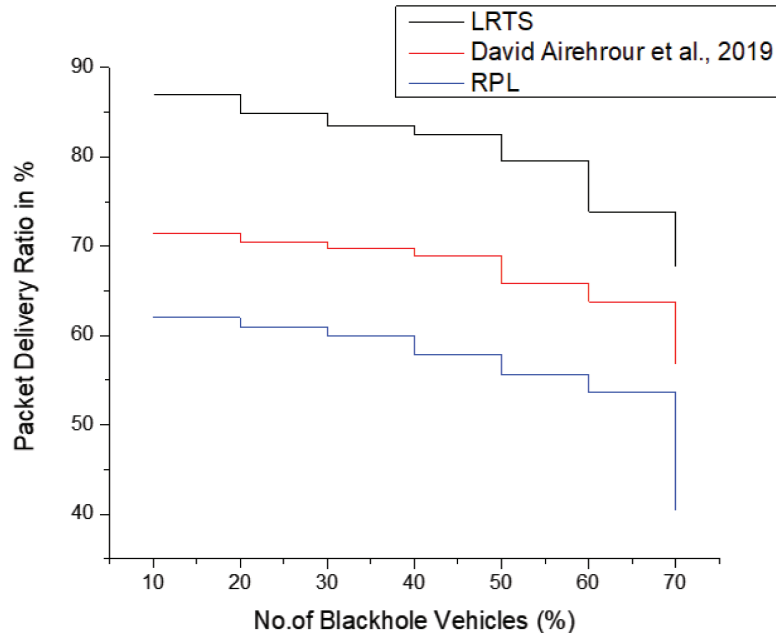


Figure 3: PDR versus % of blackhole nodes. LRTS, logistic regression-based trust-based security; PDR, packet delivery ratio; RPL, routing protocol for low power lossy networks.

consequently cumulative the PDR. In contrast, the model proposed by David Airehrour et al. (2019) only considers PDR as a single metric to evaluate device trustworthiness. Due to this limited measurement approach, the delivery ratio is lower compared to the proposed model and higher than that of RPL. As mentioned earlier, RPL lacks inherent security mechanisms, leading to a very low PDR compared to the other two models.

c. Average delay analysis versus black hole nodes

Figure 4 illustrates the analysis of average delay versus black hole nodes. As the number of nodes surges, the proposed LRTS model exhibits shorter delays compared to the other two models. This improvement can be attributed to the fact that the IoT network primarily consists of trusted nodes, with black hole nodes being effectively removed through trust and LR. Consequently, the absence of black hole nodes results in better delay performance. In contrast, the RPL protocol lacks security mechanisms, making it vulnerable to attacks and leading to increased delays due to retransmissions and other network activities. In David Airehrour et al. (2019), the weaker trust assessment allows for the possibility of black hole nodes, resulting in longer delays compared to the proposed model

and shorter delays compared to the RPL routing protocol.

d. Routing overhead versus black hole nodes

Figure 5 illustrates the routing overhead versus black hole attacks. It is evident from the figure that the sending overhead of the LRTS model is less compared to the other two models. This can be attributed to the effective identification and elimination of black hole nodes in the LRTS model, allowing routing-related information to flow smoothly without encountering difficulties. As a result, the routing overhead is reduced in the suggested model. In contrast, in the model proposed by David Airehrour et al. (2019), where trust evaluation is weaker, the presence of black hole nodes leads to routing issues such as packet dropping and retransmissions, resulting in higher routing overhead. Similarly, in the RPL protocol, the lack of security measures also contributes to routing-related issues, consequently leading to higher routing overhead compared to the LRTS model.

e. Detection accuracy versus black hole nodes

Figure 6 illustrates detection accuracy versus black hole nodes, and it is evident that the detection

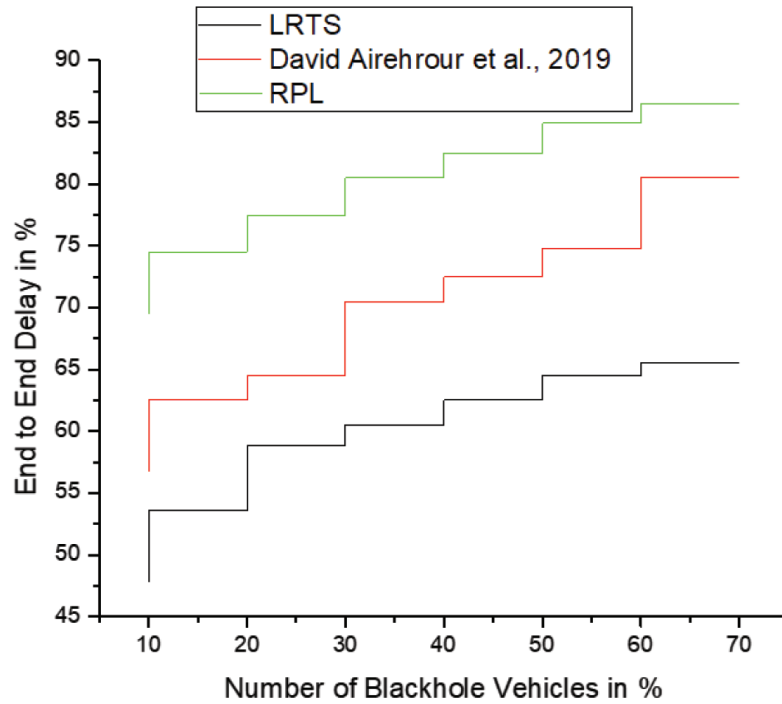


Figure 4: Average delay versus % blackhole nodes. LRTS, logistic regression-based trust-based security; RPL, routing protocol for low-power lossy networks.

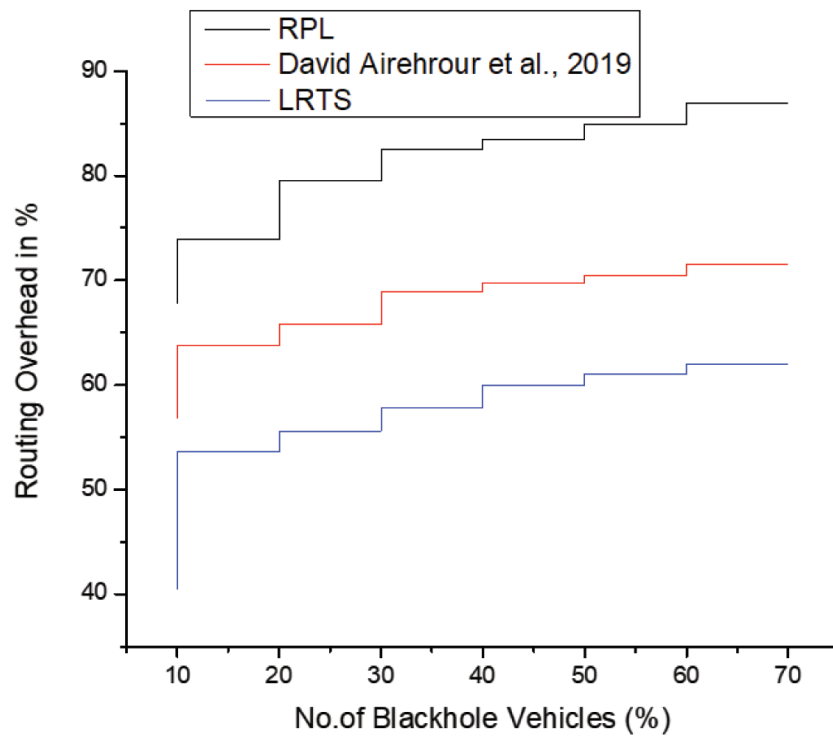


Figure 5: Routing overhead versus % of blackhole nodes. LRTS, logistic regression-based trust-based security; RPL, routing protocol for low power lossy networks.

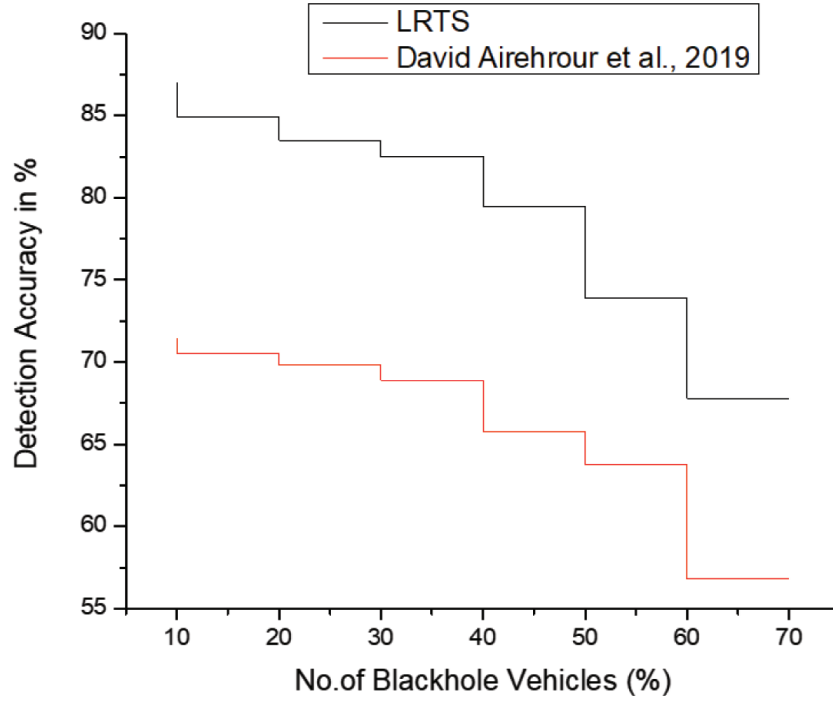


Figure 6: Detection accuracy versus % of blackhole nodes. LRTS, logistic regression-based trust-based security.

accuracy of LRTS is high. This can be attributed to the multiple trust evaluations combined with LR, which enables accurate prediction of future behavior. As a result, the detection accuracy of LRTS is superior to that of RPL (David Airehrour et al., 2019). In contrast, the lower finding correctness in David Airehrour et al., 2019 can be attributed to its poor trust evaluation mechanism. Similarly, RPL exhibits poor detection accuracy compared to the other two models owing to the lack of detection feature within the protocol itself.

V. Conclusion

This research presents a novel trust-based LR algorithm to detect black hole attacks in IoT networks by integrating multiple trust metrics, including ED, PDR, EC, and RT, into a unified IT score. The proposed model leverages LR with SGD for adaptive and efficient classification of nodes as trusted or malicious. Compared to conventional models, which typically achieve an accuracy of 72%, the proposed method achieves an improved accuracy of 85%, representing a 13% increase in detection performance. This improvement underscores the effectiveness of the approach in proactively identifying malicious behavior and enhancing overall network security. As part

of future work, the model can be extended using advanced deep learning techniques such as LSTM or ensemble methods to better capture temporal patterns. Additionally, real-world deployment and the integration of decentralized trust mechanisms using blockchain will be explored to improve further scalability and robustness in heterogeneous IoT environments.

References

- [1] Zhou W, Jia, Y, Peng A, Zhang, Y, & Liu, P (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, 1–1. DOI:10.1109/ijot.2018.2847733.
- [2] Yan Z, Zhang P and Vasilakos A V (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, 42, 120–134.
- [3] K.Prathapchandran and T.Janani, "A Trust Aware Security Mechanism to Detect Sinkhole Attack in RPL Based IoT Environment Using Random Forest - RFTrust" *Computer Networks*, Elsevier, Vol.198, No. 108413, 2021

- [4] V.Muthu ganesh, S.Sivagurunathan, K. Prathapchandran, T. Janani, "Mitigating Blackhole attack in RPL based Internet of Things Using Trust and Machine Learning", *International journal of socio technology and knowledge development*, 2022.
- [5] Akturk, Berkay, et al. "Robust functional logistic regression." *Advances in Data Analysis and Classification* (2024): 1-25.
- [6] Charizanos, Georgios, Haydar Demirhan, and Duygu İçen. "A Monte Carlo fuzzy logistic regression framework against imbalance and separation." *Information Sciences* 655 (2024): 119893.
- [7] Govindaraj, Mahalakshmi, and Suresh Arumugam. "Enhancing IoT Security with Trust-Based Mechanism for Mitigating Black Hole Attacks." *International Journal of Safety & Security Engineering* 13.5 (2023).
- [8] Bhalaji, N., K. S. Hariharasudan, and K. Aashika. "A trust based mechanism to combat black-hole attack in RPL protocol." *ICICCT 2019–System Reliability, Quality Control, Safety, Maintenance and Management: Applications to Electrical, Electronics and Computer Science and Engineering*. Springer Singapore, 2020.
- [9] Gnanaprasanambikai, L. "K-means clustering-based Trust (KmeansT) evaluation mechanism for detecting Blackhole attacks in IoT environment." *International Journal of Computing and Digital Systems* 15.1 (2024): 1-10.
- [10] Srinivas, T., and S. S. Manivannan. "Black hole and selective forwarding attack detection and prevention in IoT in health care sector: Hybrid meta-heuristic-based shortest path routing." *Journal of Ambient Intelligence and Smart Environments* 13.2 (2021): 133-156.
- [11] Alansari, Zainab, et al. "RPLAD3: anomaly detection of blackhole, grayhole, and selective forwarding attacks in wireless sensor network-based Internet of Things." *PeerJ Computer Science* 9 (2023): e1309.
- [12] Bhosale, Snehal A., and S. S. Sonavane. "Wormhole attack detection system for IoT network: A hybrid approach." *Wireless Personal Communications* 124.2 (2022): 1081-1108.
- [13] Srinivas, T. Aditya Sai, and SS Mani Manivannan. "Preventing collaborative black hole attack in IoT construction using a CBHA–AODV routing protocol." *International Journal of Grid and High Performance Computing (IJGHPC)* 12.2 (2020): 25-46.
- [14] Shukla, Mukul, Brijendra Kumar Joshi, and Upendra Singh. "Mitigate wormhole attack and black-hole attack using elliptic curve cryptography in MANET." *Wireless Personal Communications* 121 (2021): 503-526.
- [15] Sahraneshin, Tayebbeh, et al. "Securing communications between things against wormhole attacks using TOPSIS decision-making and hash-based cryptography techniques in the IoT ecosystem." *Wireless Networks* 29.2 (2023): 969-983.
- [16] Chakravorty, Rahul, Jay Prakash, and Ashish Srivastava. "An efficacious neural network and DNA cryptography-based algorithm for preventing black hole attacks in MANET." *Soft Computing* (2023): 1-13.
- [17] Airehrour D, Gutierrez JA, Ray SK (2018) SecTrust-RPL: a secure trust-aware RPL Routing protocol for Internet of Things. *Future Gener Comput Syst*. DOI: 10.1016/j.future.2018.03.021.
- [18] Alshehri M D, and Hussain F K (2017). A Centralized Trust Management Mechanism for the Internet of Things (CTM-IoT). *Lecture Notes on Data Engineering and Communications Technologies*, 533–543. doi:10.1007/978-3-319-69811-3_48.
- [19] Djedjig N, Tandjaoui D, Medjek F (2015) Trust-based RPL for the Internet of Things. In: 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 962–967 20.
- [20] Seeber S, Sehgal A, Stelte B, Rodosek G D, Schnwlder J (2013) Towards a trust computing architecture for RPL in cyber-physical systems. In: *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, pp. 134–137.
- [21] Iuchi K, Matsunaga T, Toyoda K, Sasase I (2015) Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network. In: 2015 21st Asia-Pacific Conference on Communications (APCC), pp. 299–303
- [22] David Airehrour, Jairo A. Gutierrez, Sayan Kumar Ray, SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things, *Future Generation Computer Systems*, Volume 93, 2019, Pages 860-876, ISSN 0167-739X, DOI: 10.1016/j.future.2018.03.021.