Survey on Prevention of Network Layer Protocols Attacks in IoT

Harshini J
School Of Computer Science and Engineering
Vellore Institute Of Technology(VIT) Chennai
Chennai, India
harshini.j2021@vitstudent.ac.in

Harini V K
School Of Computer Science and Engineering
Vellore Institute Of Technology(VIT) Chennai
Chennai, India
harini.vk2021@vitstudent.ac.in

Gerina Mary C
School Of Computer Science and Engineering
Vellore Institute Of Technology(VIT) Chennai
Chennai, India
gerinamary.c2021@vitstudent.ac.in

Abstract— **In our research, we delve into IoT data security, with a special focus on the network layer and the myriad challenges that come with it. We carefully analyze and evaluate prevention strategies against major network-layer attacks such as Blackhole, Hello Flooding, Sinkhole, Selective Forwarding, Sybil and Wormhole attacks. These attacks pose a serious threat to the integrity, confidentiality and availability of IoT systems and require effective countermeasures. Examining existing prevention techniques in detail, including encryption protocols, anomaly detection algorithms, and secure routing mechanisms, we evaluate their effectiveness and discuss their practical implementation. In addition, we identify key areas for future research and development aimed at inspiring the development of IoT security. By synthesizing insights from the literature and providing critical analysis, our study provides a valuable resource for researchers, practitioners, and policymakers seeking to fortify IoT networks against evolving threats, ensuring the continued reliability and resilience of IoT deployments.**

Keywords—Network layer protocol attacks prevention, IoT, Black Hole Attack, Sink Hole Attack, Worm Hole Attack, Hello Flooding, Sybil Attack, Selective Forwarding

I. INTRODUCTION

The Internet of Things (IoT) has changed the way we interact with technology, promising unprecedented connectivity and convenience in fields from smart to industrial automation. However, the rapid proliferation of IoT devices has also ushered in a new era of security concerns, where the network layer has become the focus of potential vulnerabilities and attacks. In this context, our research paper seeks to explore and evaluate prevention strategies specifically aimed at mitigating network-layer attacks in IoT environments.

The network layer is the foundation of communication and data exchange between IoT devices, making it a prime target for malicious. actors seeking to disrupt operations, damage data integrity or gain unauthorized access. In the network layer attack spectrum, we focus on six prominent threats: Blackhole, Hello Flooding, Sinkhole, Selective Forwarding, Sybil, and Wormhole attacks. Each of these attack vectors presents unique challenges and potential risks to the security and reliability of IoT networks.

To address these challenges, academic communities and industry practitioners have proposed and developed many prevention strategies and mechanisms. These range from cryptographic protocols and secure routing mechanisms to anomaly detection algorithms and intrusion prevention systems. However, the effectiveness of these techniques varies depending on the specific characteristics of the attack and the underlying IoT environment.

Our survey aims to provide a comprehensive overview of existing prevention strategies against network-level attacks in IoT environments. By synthesizing knowledge from the literature and presenting critical analyses, we attempt to clarify the strengths and weaknesses and practical considerations associated with each approach. In addition, we identify key research challenges and opportunities for future IoT security.

Ultimately, our survey serves as a roadmap for researchers, practitioners, and policymakers seeking to improve the security of IoT deployments. By providing stakeholders with a deeper understanding of the threats to IoT networks and available prevention mechanisms, we strive to promote the development of sustainable and resilient security solutions that protect the integrity, confidentiality and availability of IoT systems against evolving cyber threats.

II. BLACK HOLE ATTACK

An assault known as a "blackhole attack" targets computer networks, especially peer-to-peer or wireless ad hoc networks. This attack involves a rogue node in the network pretending to be the one with the shortest path to the target for every packet. Consequently, all traffic aimed at that specific location is drawn to the malicious node, which drops the packets instead of forwarding them as it claims to have done. This creates a "blackhole" in which packets vanish before they can reach their intended destination.

Due to their difficulty in detection, particularly in big and sophisticated networks, blackhole assaults can be very harmful. Secure routing protocols, cryptography methods, anomaly detection systems, and network monitoring are examples of mitigation solutions that are used to recognise and stop these kinds of attacks. Blackhole attacks can also be less effective by putting in place authentication methods and trust management frameworks, which can aid in confirming

the veracity of routing information shared across network nodes.

How the Attack Happens:

Existence of Malicious Node: The attacker places a malicious node inside the network in a calculated manner. Either a valid node that has been compromised or a node that the attacker expressly built can be this node.

False Routing Information: The malicious node presents itself as the most direct or expedient route to a specific location within the network. This bogus routing information may be disseminated via a variety of routing protocols or techniques.

Packet Redirection: Other nodes in the network trust the malicious node's routing information and forward packets to it when they need to convey data to a designated destination.

Packet dropping: It is the process by which a rogue node, rather than forwarding the packets as promised, drops them, essentially making them disappear—hence the term "blackhole."

When a legitimate packet is attacked and fails to reach its target, communication is disrupted, data is lost, and there is a chance that the impacted network resources will experience a denial of service.

Prevention:

Taranum, F. et al., in "Detection and Prevention of Blackhole node" [1] introduced a methodology that protects data transmission against blackhole attacks and identifies malicious nodes which are blocked using R-AODV (Reverse Adhoc On-Demand Distance Vector) protocol and ECC (Elliptic Key Cryptography) algorithm.

Firstly, the researchers use MANET nodes to create the network topology. In this step, the arrangement of nodes in space and their connections is determined. The network must be configured with the attacker, source and destination nodes in place. Defining each node's roles is vital for accurate simulation as well as network behaviour analysis purposes. Traffic generators may include Constant Bit Rate (CBR) connections to mimic data transfer within the network. Generating traffic assists in evaluating how well networks perform under different loads or conditions.

The protocol Route-Aware Ad Hoc On-Demand Distance Vector (R-AODV) is used for route discovery. This protocol reduces the routing changes overhead by enabling nodes to dynamically discover routes to destinations as required. The routes have been found; therefore, the unicast RREP packets back to the source node will help in establishing the route. Unicast RREP packets are useful in confirming a path and updating the routing database of a source node. In each node, routing tables are generated or modified based on the received RREP packets. These routing tables contain hop counts and sequence numbers of neighbouring nodes that facilitate effective packet forwarding within them. After routes are defined and routing tables updated, data packet transmission begins from the source node to the destination node. This is what this phase entails sending actual data packets over a network.

To guarantee data security, the sender uses Elliptic Curve Cryptography (ECC) for encrypting their information. During transmission when there is an identification of a black hole then precautions are taken by the sender such as blocking it and selecting another route. The encrypted data packets have to be decrypted at the receiving end by ECC to recover the original data. This guarantees the fact that only authorized nodes can access and interpret the sent information.

Terai, T. et al., in their paper "Blackhole Attack Cooperative Prevention Method in MANETs" [2] employed a particularly aggressive kind of BH assault that can anticipate sequence numbers. They suggested a detection-and-prevention technique that leverages nearby nodes' local information to safeguard the network against this kind of BH assault. The sequence number and creation time (timestamp) provided by the RREPs originating from the destination node are used in their suggested defence strategy. The threshold value is determined by predicting the sequence number using the least-squares method. The source node notifies its surrounding nodes of the sequence number and timestamp to increase the accuracy of the approximation. The only node that can identify the BH node is the one that broadcasts the RREQ.

To prevent blackhole attacks, two techniques are used to retrieve sequence numbers and timestamps from the destination node. The first approach entails gathering data from Route Reply (RREP) packets that are sent by the destination node. The received RREP packet contains the address and sequence number of the destination node. The second approach is gathering data from nearby nodes about the destination node. Using this strategy, information from nearby nodes can be shared by altering how the AODV protocol is implemented. More specifically, extra data like shared sequence numbers and RREP packet production times are added to the contents of the RREP packet.

The source node uses information gathered from other nodes as well as information from itself to estimate the sequence number using the least-squares technique. Pairs of data—the destination sequence number and the sequence number's acquisition time—are used in the least-squares approach. The equation of a straight line is derived to predict the sequence number at any given time by computing the elapsed times between the reception of sequence numbers and using these datasets. A safety margin parameter (α) is introduced to specify the threshold for identifying blackhole nodes. To reduce the false detection rate (FDR), the threshold value is set marginally higher than the expected sequence number value.

The fraction of normal nodes mistakenly identified as blackhole nodes to all normal nodes is known as the false detection rate or FDR. The performance of the detection method is affected by changing the value of the safety margin parameter (α). While a bigger α lowers the FDR but may also lower the detection rate of blackhole nodes, a smaller α increases both the FDR and the rate of blackhole node detection.

Rani, P. et al. in their book "Mitigating Black Hole and Gray Hole Attack with Swarm-Inspired Algorithm with Artificial Neural Network" [3] use a swarm-based Artificial Bee Colony (ABC) optimization method with an artificial neural network. (ANN) concept as a deep learning algorithm. As part of the network architecture, a predetermined number of nodes are installed in the simulation area. Due to network heterogeneity, nodes can communicate in different ways depending on factors such as energy consumption, coordinates, and packet delays.

The communication area of each node is limited to a certain part of the entire area. The ad-hoc ordered distance vector (AODV) routing method is used for data transmission. Route Request (RREQ) and Route Response (RREP) are two processes in the route discovery process. Within its coverage area, the source node sends a Route Request (RREQ) message to the destination node to initiate communication. The RREQ is received by nearby nodes, which then forward it to the destination to create possible routes as needed.

Using the shortest path, the destination node sends a Route Response packet (RREP) back to the source node. Aggressor nodes (black hole and grey hole) are deployed after finding the route. When a malicious node pretends to be a source node on a route, it is called a black hole attack. When a node intentionally drops data packets while acting as an intermediate node, this is called a grey hole attack. The ABC algorithm is used to distinguish between malicious and legitimate nodes. The ABC algorithm, which consists of scouts, onlookers and worker bees, is modelled after the eating habits of bees.

A fitness function is created to evaluate the characteristics of sensor nodes in the network. Nodes that meet the fitness function criteria and are considered normal are distinguished from malicious nodes. Normal, BHA and GHA nodes are classified by ANN according to their attributes. The ABC method generates data that is used to train the network by classifying nodes as malicious or benign. ANN detects malicious nodes and removes them from the path. An efficient and secure path is created from the sending node to the receiving node. Route optimization considers the presence of BHA and GHA nodes to ensure safety. A trained ANN model is used to validate the path, which ensures that the communication path consists of only normal nodes.

Ashraf, H. et al., "MABPD: Mobile Agent Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks" [4] uses mobile agents to authenticate nodes and trust values to identify black hole nodes.

The process starts by grouping sensor nodes in K using the resource clustering technique modified version. Sensor nodes are classified into clusters based on parameters such as energy level and separation from the central location. The goal of the algorithm is to efficiently allocate resources in clusters to maximize packet delivery ratio and network lifetime. Cluster heads (CH) are selected based on how close they are to the cluster centroid, which ensures efficient data management and aggregation.

Each cluster head is responsible for monitoring the sensor nodes in the cluster after the clusters are created. Each sensor node receives a unique identifier and sequence from the top of the cluster that follows those tasks given in the table. This step ensures that each node in the network can be identified and facilitates the monitoring of activity and data transmission.

Authentication is essential to ensure the security and integrity of the network. Cluster heads, sensor nodes and the base station (BS) exchange authentication information at two different levels. The secure exchange of Authenticated Packets (AP) is achieved by encrypting them using methods such as RSA. Response packets (RPs), which are used to authenticate nodes, use confirmation bits to indicate whether a node is hacked or legitimate. The network can detect and stop all attacks and unauthorized access using authentic nodes.

Mobile agents are used to detect black hole attacks both within and between clusters. Agents collect information about node behaviour and activity, looking out for anomalies that may indicate malicious activity. Reclustering is triggered to isolate and remove a compromised node from the network when the node is suspected of being a black hole attacker. A network can prevent black hole attacks by using mobile agents for detection, protecting data integrity and network performance.

Malik, A. et al., "Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs" [5], identifying a BHA at an early stage of the route discovery process. This is a unique approach known as BHA detection and prevention. (DPBHA) is designed to ensure and improve the overall security and efficiency of VANETs. The proposed approach is based on dynamic threshold calculation and the generation of false route request (RREQ) packets.

When vehicles (nodes) and roadside units (RSUs) are deployed on a road section of an urban traffic area, a VANET network is first established. On-board units (OBUs) with IEEE 802.11p connectivity and GPS location tracking are standard on every vehicle. To determine the topology of the network, graph theory and more precisely the RGG (Random

Geometric Graph) model is used. Nodes in this model are randomly distributed using a Poisson distribution, and if two nodes are closer to each other than the transmission region (TR), an edge connecting them exists. The connection of VANET is presented and studied using graph theory. The proximity matrix is calculated based on the connections between vehicles in the transmission area.

A dynamic threshold value is calculated to find potentially dangerous nodes, also called black holes, in the network. This threshold is calculated using the average destination sequence number (DSN) of the received Route Response (RREP) packets and the difference between the last RREP received and the DSN in the routing database. Each received RREP packet is examined against a threshold value. The DSN of a packet that exceeds the threshold identifies the node sending the RREP as suspicious.

The source node changes the destination IP address of the route request (RREQ) packets to an invalid address. The network sends this fake RREQ packet. The malicious activity of a suspected malicious node is confirmed when it responds to a forged RREQ packet. The node is then called a black hole node and a broadcast alarm is triggered to notify the network of the detected threat.

FIG 1: Packet Delivery rate of different Blackhole Prevention methods

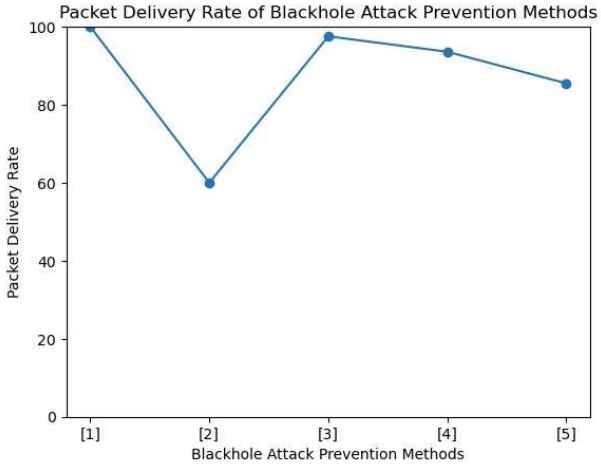

Fig 1 displays the packet delivery rate information about each of the black hole prevention methodologies used.

TABLE I. SUMMARY OF THE BLACKHOLE ATTACK DETECTION APPROACHES

Paper	**Methodology**	**Advantages**	**Disadvantages**	**Performance Metrics**
[1]	R-AODV protocol and ECC	- Data is confidential since ECC is applied	- High complexity due to encryption.	- Latency – 0.03 s - Throughput – 290 kbps
		-Reduces the risk of packet loss and delays. - Can be adapted to different network scenarios.	- Operational overhead is high due to ECC. - Scalability is low.	- Packet drop ratio – 0
[2]	Cooperative Prevention	- Improved accuracy and enhanced security since sequence number and timestamp information are shared among neighbouring nodes. - High Packet Delivery Rate remains high	- In certain scenarios, the model might exhibit a high False Detection Rate. - High complexity and increased overhead due to information sharing. - Tuning of parameters should be optimal for the model to be effective.	- Packet Delivery Rate – 60% - Attack Success Rate – 12.5% - False Detection Rate – 41% - Latency – 0.071 s
[3]	Artificial Bee Colony(ABC) and Artificial Neural Network(ANN)	- Adaptive optimization and increased robustness due to applying ABC and ANN.	- It introduces additional computational overhead and resource consumption. - Highly sensitive to changes in the network	- Packet Delivery Rate – 97.55% - Throughput – 89.38 kbps

			requiring continuous adaptation and optimization.	
[4]	Machine Learning and Mobile Agent	- Improved energy efficiency and resource utilization due to the usage of K-means clustering. - Mobile agents enable real-time monitoring. - High scalability.	- Introduces single points of failure due to dependency on centralized authority. - Performance is very sensitive to changes in parameters.	- Energy Consumption – 71.7 J - Packet Delivery Rate – 93.6% - Latency – 4.68 s - Network Lifetime – 2217 s
[5]	Dynamic Prevention Model	- Actively generates forged RREQ packets to confirm the malicious nature of the node. - Alerts the neighbouring nodes of the attack immediately.	- Increase in false positives due to the probabilistic identification approach. - Attackers can attempt to evade detection by adapting their behaviour.	- Packet Delivery Rate – 85.5% - Throughput – 123 kbps - Latency – 0.15 s

III. HELLO FLOODING

In Internet of Things networks, "hello flooding" is a kind of network flooding attack in which rogue nodes bombard the network with "hello" messages. Usually, these messages are broadcast to every node in the network, using up resources and bandwidth.

Devices frequently use Bluetooth, Zigbee, or MQTT protocols to communicate with one another in IoT (Internet of Things) networks. One way that these protocols might function is by having devices broadcast "hello" messages regularly to find and connect to other nearby devices or to keep the network connected.

Attackers take advantage of this process in "hello flooding" attacks, where they bombard the network with a lot of phoney "hello" messages. This may overload the network, resulting in traffic jams, stopping authorised communications, and even possibly triggering denial-of-service (DoS) attacks.

When it comes to resource depletion assaults like Hello flooding, such attacks can be especially harmful in Internet of Things networks because devices may have limited processing power, memory, and battery life. IoT network managers can reduce this threat by putting in place security mechanisms like encryption, access control, authentication, and intrusion detection systems to find and stop flooding assaults.

How the Attack Happens:

Discovery Mechanism: To find and connect with other devices in their network, a lot of Internet of Things (IoT) devices send out "hello" messages. Usually, a range or all of the devices on the network receive these broadcast messages.

Malicious Node: A malicious node, or several malicious nodes, is introduced into the network by an attacker. These nodes may be compromised or intentionally engineered to produce and disseminate a large number of "hello" messages.

Excessive Broadcast: The malicious node(s) send out a lot of fake "hello" messages to the network. The network infrastructure may be overloaded with these messages due to their erroneous content or sheer volume of generation.

Network Congestion: When fake "hello" messages flood the network, they use up bandwidth and other resources, causing congestion. Because of the overwhelming amount of traffic created by the flooding attack, legitimate communication between devices may be interfered with or severely slowed down.

Denial of Service (DoS): In extreme circumstances, hello flooding assaults may cause a denial of service (DoS) condition, in which a deluge of fictitious "hello" signals overloads network resources, making it impossible for real devices to communicate.

Depending on the scope and severity of the attack, the effects of hello flooding can vary from a reduction in network speed to a total shutdown of IoT services. Hello flooding assaults not only interfere with regular operations but can also make

it easier for other malicious activities to take place, like reconnaissance or unauthorised access to network resources.

Prevention:

Ghajbiye, A. et al., in the book "DPLPLN: Flooding Attack Detection and Prevention in IoT" [6] suggests using DPLPLN (Low Power and Lossy Network) for detection and prevention to protect IoT communication. DPLPLN protects by detecting the flooding behaviour or garbage packets of a DoS attacker and identifying it in the network. Comparing the performance of DPLPLN and RMDD, the proposed system performs better in many performance parameters, including overhead and throughput.

The introduction of Nodes (Pt) into the IoT network is the first step of the technique. The work of each node is monitored and investigated. Contacting the routing module, the transmitting node (Tx) initiates data transmission, forming the radio range (Ψ), transmitter (Tx), receiver (Rx) and routing information (rp). Based on the routing information, the intermediate nodes (Ik) forward the packets along the path. In behaviour analysis, a behaviour analysis node (Wk) observes the behaviour of nearby nodes. As part of this investigation, anomalous behaviour or trends that may indicate malicious activity are observed.

A node (Ij) identified as potentially malicious by the current path creates and propagates spam messages to other nodes (Pt). When a node (Pt) receives a spam message, uses resources and sends it to the next hop, which increases network flooding. A suspicious node (It) is detected by a behaviour analyzer (Wk), which then uses an artificial neural network (Ann) to study its behaviour. A behaviour analyzer node (Wk) detects a node (It) as malicious and blocks it if its behaviour is abnormal and its packet delivery ratio (PDR) is below a certain threshold (thl). All nodes (Pt) receive a broadcast message to alert them to the blocked node (hk), and the affected nodes change their routing to avoid the malicious node.

Actively blocking known malicious nodes (hk) and changing their routing to avoid them are proactive strategies. An IPS node, also known as a DPLPLN, stops the injection of malicious data by monitoring and stopping the activity of detected malicious nodes. The DPLPLN strategy maintains network performance and tries to avoid flooding attacks by blocking and redirecting to avoid hostile nodes.

Zarei, S. M. et al., "Defending against Flooding Attacks Using Probabilistic Thresholds in the Internet of Things Ecosystem" [7] proposes a method known as LSFA-IoT to defend against flooding in both the Internet of Things network and the AODV routing protocol. The proposed approach is divided into two main steps: the first step uses a physical layer intrusion and attack detection system to detect attacks, and the second step uses APT-RREQ messages to detect error events.

The proposed method is presented as follows: LSFA-IoT (Neighbour Suppression Based Flooding Attack Detection in the Internet of Things). It is based on the AODV protocol and is specially designed for IoT networks. LSFA-IoT aims to detect and stop network layer flooding attacks. To detect malicious nodes during the route planning process, a neighbour-blocking strategy is introduced. Before allowing packets to be transmitted, LSFA-IoT keeps track of queried nodes and isolates them with a waiting list.

Nodes communicate with each other to check the number of RREQ (Route Request) messages. Unusual spikes in the number of sent RREQs trigger a detection procedure that signals possible flooding attacks. Comparing the observed transmission behaviour with given thresholds is part of the detection process.

Nodes use the weighted average method (APT-RREQ) to determine the average packet transmission rate of RREQs. Information about RREQs is shared between nodes by sending HELLO messages. Nodes notify each other of potential attackers when they send more than a certain number of RREQs.

Any node that detects a malicious neighbour is blacklisted. To isolate the malicious node, the neighbours are notified and requests from the malicious node are rejected for a certain period. By updating their list in response to a received message, nearby nodes can isolate the rogue node from the network.

Based on the typical round trip time of the RREQ, each node keeps the waiting list active for a predetermined period. After this period, the malicious node is again considered normal and is allowed to participate in routing. The node will be added back to the blacklist and its neighbours will be notified if it shows malicious behaviour again.

Srinivas, T. A. S. et al., "Prevention of Hello Flood Attack in IoT using Deep Learning with Improved Rider Optimization Algorithm" [8] presents a research model that uses techniques such as cluster capsule selection, and k-generation paths, detecting and avoiding HELLO flood attacks, and choosing the best shortest path. Some route discovery frequency vectors, such as the route discovery time of each node and inter-route discovery time, are determined to detect the HELLO flooding attack after randomly selecting a cluster head and generating a k-path. To find a foreign node, a threshold function is first used, which compares the calculated received signal strength (RSS) of each node. In addition, the optimized Deep Belief Network (DBN), which is later removed from the network, strengthens the HELLO flooding attack. An improved metaheuristic method optimally selects the shortest path when the network is protected. This instance uses an advanced rider optimization algorithm (ROA) called ROA (BAU-ROA) based on an update-based bypass-bound attacker to perform both the optimal shortest path and optimal DBN. Factors such as

packet loss ratio, transmission delay, node trust and inter-node distance are considered to choose the best shortest path. The proposed architecture model requires the implementation of an IoT WSN system clustered in the health field. Sensor nodes are grouped and identified individually by their identifiers. These sensor nodes send their data to a single base station or sink node. A base station is permanently located, usually in the middle of the network, where data transmission is completely seamless. Communication between sensor nodes and the cluster head and from the cluster head to the base station is done using efficient routing protocols.

Attacks called "HELLO flooding" occur when nodes send too many HELLO packets, which disrupts the network. A method based on Deep Belief Network (DBN) is recommended to detect such attacks. To detect HELLO flooding attacks, the proposed DBN method requires input parameters such as frequency vector and route search time. A node is removed from the network if it is found to be malicious.

In an IoT-WSN network, source and destination nodes are selected and multiple paths (k-paths) are established between them. This step creates many channels between source and destination nodes to ensure data transmission redundancy and reliability. The K-way routing process aims to find the shortest or least bandwidth-consuming path between two cluster heads.

To detect Hello Flood attacks, a DBN method is added to minimize the error function. between projected and actual production. The proposed BAU-ROA algorithm is used to select the shortest paths and the coding of the solution is explained. Nodes in the network are coded according to their placements and connections.

The traditional Rider Optimization Algorithm (ROA) has been improved to perform better for discrete optimization tasks. The proposed BAU-ROA algorithm optimizes shortest path selection in the IoT-WSN network using many routing groups (bypass, follower, skipper, and attacker).

Some are trust, energy dissipation, delay, and packet loss ratio. of the elements involved in choosing the shortest paths. Trust calculation is used to evaluate the reliability of network nodes. By choosing the best routing paths, the objective model tries to minimize the packet loss ratio, transmission time, node reliability and node-to-node distance.

Cakir, S. et al. in "RPL Attack Detection and Prevention in the Internet of Things Networks, using a GRU Based Deep Learning" [9] presents a deep learning-based Gated Recurrent Unit network model to predict and stop HF attacks RPL protocol in Internet of Things networks. In addition to considering and testing different power states and total energy consumption of nodes, the proposed model was evaluated using support vector machine and logistic regression methods.

There should be three types of nodes in the network. : poisonous, normal and root knots. Specific configuration parameters such as CPU utilization, Low Power Mode (LPM), Transmit (Tx), Receive (Rx), and Total Energy (TE) are applied to each node in the simulation. The simulation can generate message packets that also store their contents for further investigation. For analysis, some features including node ID, CPU, LPM, Tx, Rx and TE are extracted and organized into a dataset. Preprocessing of datasets may include normalization to achieve a uniform scale of feature values.

Machine learning techniques such as Logistic Regression (LR), Support Vector Machine (SVM) and GRU (Gated Recurrent Unit) are used to detect the attack. These techniques are applied to normalized datasets to classify nodes as malignant or benign according to their activity. Attack detection mainly depends on detecting anomalous behaviour of nodes, including fluctuations in Rx values that exceed a defined threshold. To prevent damage, packets from malicious nodes are dropped from the network when detected. Metrics such as precision, accuracy, recall and F1 score are used to evaluate the performance of recognition algorithms. The results of machine learning techniques are used to optimize the intrusion detection threshold.

Hasan, M.R. et al., "Efficient AODV-Based Flooding Detection and Prevention for Smart Meter Networking", proposes a brand new AODV-based routing scheme called Flooding aWareness AODV (FLOW - AODV) that considers IP spoofing in both cases. scenarios. If there is no IP address spoofing, we will add new features to the routing request forwarding. The basic idea is to use the number of route requests received from the same source to detect attackers in one-hop neighbouring meters.

Without IP spoofing, FLOW-AODV:

RREQ counter system: Each meter in its routing table keeps an RREQ. internal response. The RREQ is sent from the source meter in one hop to the neighbouring meter, which then increments the RREQ counter. The overhead of other counters is reduced because only one-hop neighbours count RREQs.

Detection and Avoidance: The source sequence number and RREQ counter are controlled by the one-hop neighbour counter. A one-hop neighbour metric discards subsequent RREQs and marks a source as an attacker if it receives more than a certain number of RREQs from the same source. It helps in flood detection and mitigation. The maximum number of RREQs accepted is determined by protocol behaviour, taking into account retransmissions and sequence updates.

IP mask usage FLOW-AODV:

RREQ rate tracking: FLOW-AODV extends its algorithm for RREQ tracking. direct shipper rate. under each smart meter because IP spoofing prevents identification based on IP addresses.

Classification of RREQ levels: RREQ rates are classified into three classes based on the flooding range: high, medium and low. This allows meters to estimate the reliability of their neighbours.

Reliability estimation: Based on the RREQ ratio, meters update the one-hop reliability value of the neighbours in their routing table. Reliability decreases when the percentage of RREQ is in the high-frequency range. The receiver meter stops transmitting RREQs from the immediate sender when their reliability drops below a predefined level, typically 20%.

FIG 2: Packet Delivery rate of different Hello flooding Prevention methods

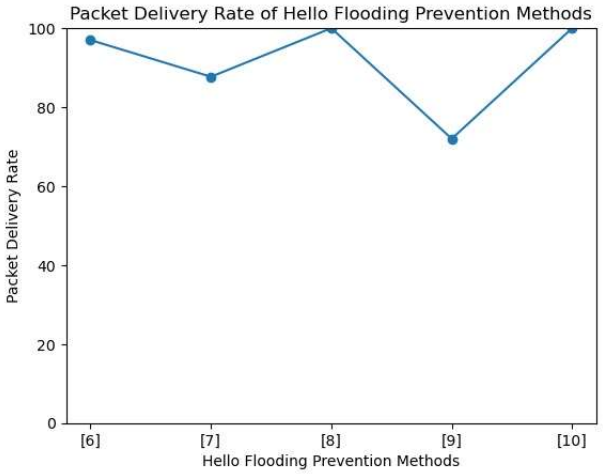

Fig 2 displays the packet delivery rate information about each of the hello flooding prevention methodology used.

TABLE II. SUMMARY OF THE HELLO FLOODING DETECTION APPROACHES

Paper	**Methodology**	**Advantages**	**Disadvantages**	**Performance Metrics**
[6]	Detection and Prevention Low Power and Lossy Network(DPLPN) scheme	- Attacks are detected and prevented before causing any significant harm. - It outperforms the RMDD protocol in terms of Packet Delivery Rate.	- Effectiveness varies concerning scalability.	- Packet Delivery Rate – 97% - Throughput – 83000 kbps
[7]	LSFTA-IoT schema	- Increased efficiency due to a combination of techniques such as neighbour suppression and monitoring of RREQ messages. - Minimizes the generation of unnecessary RREQ packets reducing network congestion.	- High resource consumption due to maintenance of detection lists.	- Packet Delivery Rate – 87.7%
[8]	Deep Learning with Improved Rider Optimization Algorithm	- Efficient routing due to k-paths generation and finding the optimal shortest path. - Adaptive detection due to Deep Belief Network(DBN).	- Resource-intensive algorithms are used.	- Latency – 0.4 x 10^{-9} ms - Energy consumption – 0.019 J
[9]	GRU-based Deep Learning	- High adaptability over time due to the implement	- High resource utilization due to GRU.	- Latency – 0.79 s Packet Delivery

		ation of GRU.		Rate – 72%
[10]	FLOW-AODV: Modification of AODV routing protocol to prevent flooding attacks in smart meter networks.	- Provides effective prevention against flooding attacks by modifying the RREQ forwarding system. - Resource utilization is efficient. - Addresses the challenge of IP spoofing. - Dynamically evaluating the trustworthiness of one-hop neighbours allows for adaptive decision-making.	- Increase in control packet overhead in IP spoofing scenarios. - Implementation is complex.	Without IP Spoofing: - Packet Delivery Rate – 100% - Latency – 0.1 s With IP Spoofing: - Packet Delivery Rate – 98% - Latency – 0.25 s In the presence of a Flooding attack: - Packet Delivery Rate – 100% - Latency – 0.05 s

IV. SINKHOLE ATTACK

Sinkhole attacks are a serious and complex security threat to networks, particularly those that rely on wireless communication, such as wireless sensor networks (WSNs), mesh networks, and ad hoc networks. This sort of attack exploits the routing protocol and redirects a major percentage of the network's traffic through a hacked node, known as the sinkhole. The attacker can then use this control over network traffic for malicious objectives such as eavesdropping, data manipulation, and denial of service attacks.

How the Attack Happens:

Compromise of a Node: A sinkhole attack is initiated by compromising at least one network node. This can be accomplished through a variety of means, including exploiting software vulnerabilities, physical tampering, or utilising social engineering tactics to infiltrate the network with a malicious node.

Advertisement as an Attractive Route: Once the attacker gets control of the node, the next step is to make it look like the most attractive or efficient method for transmitting data to the base station or specific destinations. This is frequently accomplished by changing the node's routing information. For example, in a network implementing a distance vector routing protocol, the compromised node may advertise a zero-cost path to the base station, causing other nodes to believe it is the optimal option.

Rerouting Traffic: Neighbour nodes, misled by the fraudulent adverts, start routing traffic through the sinkhole node. As a result, the attacker takes control of a major amount of the network's data traffic. This central position provides for a variety of future attacks.

Execution of Malicious Activities: With traffic flowing through the hacked node, the attacker can:

- Eavesdrop on data, jeopardising the security of important information.
- Alter or tamper with data in transit, compromising data integrity and perhaps resulting in inaccurate information being supplied.
- Selectively Forward packets, akin to a selective forwarding attack, in which the attacker drops packets from specified sources or categories, subtly disturbing network operations.
- Launch a Denial of Service (DoS) attack by discarding all packets, rendering the network unusable.

Prevention:

[11] This paper gives a very secure mechanism in which rank computation is protected against sinkhole nodes in the IoT-Based Systems. The expectations maximization algorithm is used to optimally cluster the nodes into a group of the same rank. The sink's signature ensures that the rankings of nodes are not tampered with. Empirical results have shown that optimal rank computation is secured from sinkhole attacks, but it requires additional network communication between all participating sensor devices and the base station (sink).

This proposed methodology can be divided into different stages. Initially, there was a focus on the Centralized Rank Computation Mechanism where ranks increase monotonically from devices close to the sink node, based on their distance from the sink. Ranks were assigned based on message propagation delay for each device and thus those whose messages had nearly similar delays belong together in terms of ranking.

In the next phase, model-based node clustering and rank computation were used whereby the sink node receives DAO reply from all devices and computes round trip time (RTT) using the timestamp field of each device. After calculating each device's estimated propagation delay from the RTT, the sink node used the estimated propagation delay to create a rank table. The authors used Expectation-Maximization (EM), which is a model-based clustering approach, to group the devices in clusters according to their propagation delay at the sink.

The final phase, Efficient Rank Distribution, entailed using an effective method of communication by the sink node to distribute rank values to every device that received a message with their ranks signed by the sink node. This phase required that group membership identities be exchanged between the sink and all devices in the network. The authors preferred the SMC scheme for a higher compression ratio and lower overheads than others.

The proposed methodology also dealt with sinkholes, to detect and build in resiliency. The article presented two cases: the detection of attacker devices whose rank is lower than what they report, and the detection of attacker devices that claim to be the sink. In addition, the authors drew attention towards the resilience of the suggested way of calculating ranks and delivering them against sinkhole attacks by emphasizing the security offered via the digital signature of the sink and assuming that a compromise is impossible for this node.

The suggested mechanism for rank computation and distribution is impenetrable to both rank spoofing and sinkhole attacks. However, it has a few drawbacks. This causes extra network overhead of O(k. N) to distribute ranks. As a result, the time taken to assign rank and network delay is higher than in distributed approaches. Finally, the proposed mechanism supposes that the sink node cannot be breached. This is true for almost all network scenarios. But in situations where there is a threat to the sink node, multiple-sink topology could be preferable.

[12] Using an agent-based algorithm, this study describes the detection and prevention of sinkhole attacks. In this algorithm, the agents negotiate with their reliable neighbours and provide information to all nodes from them in three steps so that nodes can't pay attention to traffic created by sinkhole attackers. The area considered in this study is the network scale which measures 500×500 m2 square areas. Each experiment involves a set of simulations. Every simulation run is scheduled for 10 minutes.

This methodology uses mobile agents which are used as a preventive measure against sinkhole attacks in wireless sensor networks (WSNs) leading to node authentication and secured communication.

Security checks and validations are performed by autonomous moving codes called mobile agents that traverse the network and visit sensor nodes. Validation processes rely largely on the agent's unique code set and hash functions. Thus, legitimate nodes can be identified or authenticated by these agents; hence avoiding malicious ones from forming sinkhole attacks.

When a mobile agent reaches an assigned node, it starts the process of trust verification. It challenges a node to generate a correct hash value using a unique code that has been offered by the agent. The process heavily relies on pre-shared secrets (codes) and hash functions which agents are familiar with as well as legitimate nodes that not every attacker in such networks is aware of. The agent will take note of this if the node answers correctly with the right hash value (meaning it possesses the pre-shared secret) and mark it down as trusted in its neighbouring matrix – which is an array recording how much trust all nodes have.

The neighbouring matrix in each node is very important because it tells whether or not the nodes can be trusted according to what mobile agents say about them. With each visit by the agents at each location, this matrix is always being updated dynamically. Therefore, new additions or compromised nodes are detected through continuous updates so that the network adapts to changes faster.

The efficient and secure movement of agents through networks is one element that stands out in this method. Agents often visit only single-hop neighbours next to them instead of having to travel all around the network wasting limited energy resources possessed by these nodes for extensive travels across wide area networks as they were programmed to do so. The agents are also meant to carry encrypted information, which ensures that the data they contain and exchange with nodes is secured.

Whenever a mobile agent authenticates a node, it forms secure channels for communication with neighbours thus preventing unverified ones from participating in malicious activities.

Besides, this method has a way of dealing with node mobility and energy preservation. Trust statuses will be updated by agents going around nodes after some time to ensure that despite conditions changing the network's security position remains intact. Furthermore, those nodes that have run out of energy are gently taken out to not affect network operations while still maintaining their integrity.

This technique presents significant improvements in various performance measures that underline its ability to enhance both network security and efficiency. As is evident from the simulation results, there was a noticeable increase in throughput (15-20%), packet delivery ratio (30-40%) and number of data packets received successfully (15-20%) as well as a decrease in jitter (-10 - 15 %), delay in packet delivery (-15 - 20 %) and number of dropped packets (-5 - 15 %). These improvements collectively emphasize the ability of the proposed algorithm to maintain strong communication channels, deliver reliable information timely, and minimize

data loss even when facing threats such as sinkhole attacks. The above comprehensive improvement in performance metrics acts as proof for two things; first, it guarantees the algorithm's efficacy in protecting wireless sensor networks from these vulnerabilities secondly this paves the way for future research that will aim at making networks more resilient to other types of hazards.

[13] This approach suggests a sophisticated way of enhancing the security and longevity of smart home networks, through prevention and mitigation of sinkhole attacks. This comprehensive strategy incorporates advanced techniques for weight calculation, node selection for Intrusion Detection System (IDS) agent placement, and meticulous attack mitigation mechanisms to safeguard the network.

This methodology is based on a new concept where each node in the network is assigned a weight based on its resource capabilities. The following main factors are taken into consideration during this computation: residual energy level, degree of connectivity within the network, memory capacity and processing time. Nodes with higher residual energy are selected due to their long life; those with a high degree of connectivity are preferred because they help decrease the total number of IDS agents required by the network hence reducing its data traffic as well. Similarly, nodes having ample memory capacity stand out to store information on neighbouring nodes as well as sensing data from within the network while nodes having lower processing times are favoured for their efficiency in managing data.

Then, the Minimum Weight Vertex Cover (MWVC) algorithm uses the weight of nodes to decide on a set of vertices that possess minimum cumulative weights needed for total network coverage. This group represents the most strategic vertices within the network where IDS agents could be placed to sense any suspicious activity such as sinkhole attacks. This is important because it ensures that there is an efficient monitoring system in place that can detect malicious activities like sinkhole attacks immediately. The presence of IDS agents in the network helps them collaborate and identify likely sinkhole nodes. Once they are identified, an attack mitigation process starts which entails isolating these compromised nodes from other parts of the network to prevent them from further damaging it. The decision by the system whether to execute this process locally or globally depends on the nature and kind of attack executed.

In Local mitigation, Once a sinkhole node is detected, its ID is broadcasted to the root to initiate instantaneous isolation through blocklisting by its neighbours. These neighbours then choose new parents to maintain the structure of the network, which depends on whether or not the sinkhole node was an IDS agent.

Mitigation of global sinkhole attacks in networks involves a comprehensive strategy where the root node tells the whole network about sinkhole nodes that have been detected, leading to an immediate blocklisting by neighbouring ones and reconfiguring of parent-child relationships so that network integrity is maintained. This entails adjusting the Directed Acyclic Graph (DODAG) to not include sinkholes, as well as, recalculating network hierarchies and applying the Minimum Weight Vertex Cover (MWVC) algorithm for optimal placement of Intrusion Detection System (IDS) agents bypassing compromised nodes. Mainly used when faced with multiple simultaneous sinkhole threats, this technique offers a robust defence mechanism scaling efficiently with growth in network size providing persistent security and operation throughout the system.

The suggested smart home security architecture strongly resists sinkhole attacks; it detects 95% of them, while for networks with a malware presence of about 30%, it has precision and recall rates that are almost 91% and 89% respectively. This way, it cuts down significantly on false negatives as the adversary nodes decrease to just below that number at around 59%, and decreases to approximately 25% when the attacker node percentage increases. It also manages to make energy consumption somewhat more efficient compared to other options available. These results indicate how efficacious this system is in improving the safety as well as the life of smart homes.

[14] A proposed methodology with Proactive and Adaptive Security Routing (PASR) in IoT networks, specifically addresses sinkhole attacks. This approach acknowledges the vulnerabilities in IoT networks particularly those which use Ad hoc On-Demand Distance Vector (AODV) routing protocol that despite its self-configuration, route optimization, and scalability advantages may become an attack vector if not well guarded.

PASR strategy starts with advanced network design where devices are grouped into clusters and gateway devices are made to act as cluster heads or nerve centres. These gateways do more than just convey information; they possess computational power and most importantly independence to control and regulate data flow towards the base station which handles final storage and data processing from the field.

This method deploys an IDS in each gateway device. This system does not passively observe, but it actively participates in the network's ongoing operations by continuously analyzing data and routing information that passes through the gateway. In this manner, IDS can detect anomalies that may indicate the presence of a sinkhole attack where a compromised node advertises better routing paths to siphon data via malicious channels.

This method's effectiveness is greatly improved by its being proactive and adaptable. The compromised node is immediately quarantined once identified as a potential threat. Intrusion alerts are disseminated across networks for other gateways to divert traffic from the affected node thereby reducing chances of data interception or corruption. The system's rapidity is facilitated by communication protocols that are inherent within the network which ensure quick

transmission of crucial security information among gateways and back to the central base station.

The PASR methodology is further strengthened by the fact that the base station functions as the central command and control centre for the network. It stores and updates a variety of network devices, their operational status, as well as the pathway of data traffic. It is therefore important that this source of information coordinates with data validating the reliability of received information and monitoring the general healthiness of the network. If there are any inconsistencies in the data patterns that indicate possible attacks, an alarm will be sent to isolate these types of threats and prevent them from interfering with network operations.

Furthermore, by being able to stop unauthorized means to access networks before they are realized into routing paths through unregistered devices attempting to establish links to sinkhole attacks can never have an opportunity within the system. Only one new route request at a time can be accepted based on this router's database for it to ensure that merely valid endpoints may send messages internally or outside (or even both), hence reducing cases where attackers would try gaining illegal access through routes not permitted.

The PASR methodology, among the most dynamic and comprehensive defence strategies, is reactive and preventative. This, in turn, involves using advanced IDS technologies on gateway devices as well as centralized control through a base station and establishing fast communication or adaptive routing protocols across the network to identify and mitigate any possible threats of sinkhole attacks.

The performance of the Proactive and Adaptive Security Routing (PASR) device was evaluated using NS-2 simulations, which have shown significant improvements in the security and effectiveness of IoT networks. Consequently, the paper shows that the PASR approach has improved the packet delivery ratio better than traditional techniques such as AODV and DDBG especially when there are active sinkhole attacks. The Integrated Intrusion Detection Systems (IDS) integrated into it make this possible through proper identification and isolation of malicious entities to enable smooth data flow. PASR successfully solves an energy problem in a rational manner which is very important for resource-limited IoT network sustainability. This system also outperforms others in terms of speed and accuracy in detecting sinkhole attacks.

[15] The proposed methodology introduces a sophisticated to increase the security of IoT networks that work under Routing Protocol for Low-power and Lossy networks (RPL). Underpinning this is Direct Neighbour Sink's reputed Trust-based Intrusion Detection System (DSTIDS) developed ingeniously to counter routing attacks commonly known as sinkhole attacks.

Trust management governs DSTIDS and therefore, individual nodes are evaluated based on network behaviour observations. Positive and negative observations regarding node behavioural characteristics within the network are used for this evaluation. As such, positive observations relate to the expected protocols, processes and behaviours of the nodes while negative ones indicate deviations from these norms like unexpected rank changes or data packet drops that might mean malicious actions.

The DSTIDS methodology has an innovative bifurcated operational framework that consists of two distinct yet interrelated stages. The first stage entails the creation of a Directed Acyclic Graph (DODAG) underneath the RPL network. At this point, it is when the system starts its watchful monitoring for signs of ill-intentioned activities. To identify possible security breaches, the system looks at changes in rank from nodes and DIO (DODAG Information Object) messages being passed. This is done through an intensive analysis of alterations in ranks before and after expected cases of attacks with positive or negative observations made by the systems.

After making these entries, the trust assessment's key part begins which is the second stage within DSTIDS methodology. In this phase, belief, disbelief, and uncertainty values associated with each node's behaviour are combined using subjective logic to evaluate the trustworthiness levels of nodes across a network. Within a range of zero to one, such values make up a comprehensive trust score that indicates how reliable a given node is seen in relation to others in a network.

The described DSTIDS system utilizes dynamic weighting that scales down on an overall trustworthiness score for each node depending on different observations made about them taking into account aspects like time proximity and contextual factors during interactions. This flexible strategy allows the system to accommodate and adapt to changing network behaviours and emerging threats.

Once a node's trust score is lower than a preset threshold signifying a high likelihood of malice, the procedure then proceeds into action. The identified node will be marked as malicious henceforth disconnected from the network; this implies that it cannot pose any more danger. Hence, this prompt action not only helps in safeguarding the integrity of the network from immediate damage but also it acts as a deterrent as well when it comes to future attacks since prompt identification and neutralization of any malevolent nodes.

The DSTID mitigates the problem of low packet delivery ratio (PDR) and retains the aforementioned 10 to 12% increase always even under attack conditions thus revealing that it can maintain reliability in networks. Additionally, it performs much better than alternative tools such as Fuzzy-IoT and IRAD in terms of False Positive Rates (FPR) and False Negative Rates (FNR) with FNRs reduced by up to 70% and FPRs lowered by up to 55%. These measures provide an

exactitude of DSTIDS's capacity for preventing and staving off dangers with minimal occurrences of false alarms; encapsulating that RPL-built IOT nodes could be secured using this method efficiently.

TABLE III. SUMMARY OF THE SINKHOLE ATTACK DETECTION APPROACHES

Paper	**Methodology**	**Advantages**	**Disadvantages**	**Performance Metrics**
[11]	Hierarchical Trust Management	- Efficient identification of compromised nodes - Scalable trust management with a hierarchical model - Adaptability to changing network conditions	- Overhead in maintaining trust hierarchy - Potential inaccuracies in dynamic trust assessment - Complexity in trust level determination	- Detection accuracy: High - Overhead in trust management: Moderate - Scalability: High
[12]	Mobile Agent-Based Detection	- Efficient node authentication using mobile agents - Dynamic trust status updates - Improvement in throughput, packet delivery ratio, and data packet reception rate - Minimization of data loss during sinkhole attacks	- Reliance on pre-shared secrets for node authentication – Overhead from constant agent movement - Complexity in trust matrix management	- Throughput improvement: 15-20% - Packet delivery ratio improvement: 30-40% - Data packet reception rate improvement: 15-20% - Jitter reduction: -10-15% - Delay reduction: -15-20% - Dropped packets reduction: -5-15%
[13]	Cluster-based Security Strategy	- Efficient network management with cluster-based architecture - Enhanced security with IDS deployment in gateway devices - Rapid mitigation of sinkhole attacks	- Design and management complexity of clusters - Dependency on centralized base station - Potential overhead from IDS deployment in gateways	- Packet delivery ratio improvement: Significant - Precision and recall rates: ~91% - Energy efficiency: Improved - Speed and accuracy of sinkhole detection: High
[14]	Proactive and Adaptive Routing	- Proactive detection and mitigation of sinkhole attacks - Enhanced security with IDS deployment in	- Reliance on predefined thresholds for node quarantining - Dependency on rapid communication protocols - Potential overhead	- Packet delivery ratio improvement: Significant - Energy efficiency: Enhanced - Speed and accuracy of

		gateway devices - Efficient network management through centralized control	from IDS deployment in gateways	sinkhole detection: High
[15]	Trust-based Intrusion Detection	- Trust-based node evaluation and mitigation - Adaptive trust scoring for dynamic threat detection and mitigation - Improvement in packet delivery ratio and reduction in false positive rates	- Dependency on subjective logic for trust evaluation - Reliance on predefined thresholds for node disconnection - Potential overhead in trust scoring and node management	- Packet delivery ratio improvement: 10-12% increase - False Positive Rates (FPR) reduction: Up to 55% - False Negative Rates (FNR) reduction: Up to 70% - Accuracy of threat detection and mitigation: High

V. SELECTIVE FORWARDING ATTACK

A Selective Forwarding Attack, in the context of network security, notably inside wireless sensor networks (WSNs), mesh networks, or ad hoc networks, is a type of cyberattack in which a compromised node in the network deliberately suppresses data packets rather than forwarding them to the next node. This disturbs the usual data transmission flow and can result in incomplete or unreliable data transmission, thus jeopardising the network's operation and integrity. The attack is subtle, making detection difficult because the hacked node may still pass certain packets, making it appear non-malicious.

How the Attack Happens:

Initial Compromise: The attack starts with the compromising of a node in the network. An attacker could exploit holes in the network's security, physically interfere with a node, or bring a malicious node into the network.

Integration with Routing: Once compromised, the malicious node becomes part of the network's routing system. It participates in the routing protocol, which involves advertising itself to neighbouring nodes and assisting in the establishment of network paths.

Selective Packet Dropping: The compromised node then selectively drops packets based on criteria set by the attacker. It may target packets from specified sources, targeted for specific nodes, or carrying specific sorts of data. This selective behaviour sets the attack apart from other types of denial-of-service (DoS) attacks.

Disruption of Network Operations: Dropping packets selectively can disrupt network operations, decrease performance, and jeopardise data integrity. Critical information may not reach its intended recipient, resulting in operational failures or compromised decision-making processes.

Prevention:

[16] This methodology has managed to combine packet monitoring, anomaly detection algorithms and cooperative network behaviour for reliable packet delivery while effectively identifying malicious activities.

The methodology integrates a packet-tracking mechanism that exploits the numeric values assigned to each packet. It can use these order numbers embedded within the identifiers of packets to follow data movement across nodes. Thus, it can detect missing packets that might be indicative of selective forwarding attacks carried out by compromising nodes which may selectively drop some packets but still forward others. This approach is simple yet powerful at distinguishing irregularities in sequence numbers thus hinting at possible cases of selective forwarding.

Using Network Simulator tools, the performance of the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol was assessed in selective forwarding attack situations. By analysing how malicious nodes affect packet delivery ratios, this technique allows for a dynamic modification of network parameters like cluster heads number to alleviate the effect of attacks. The manipulation of these parameters would indirectly prevent attackers from easily targeting or isolating some parts of the network thus increasing the overall robustness.

In addition to this, an SVM-based decentralized intrusion detection system has been introduced as part of this work. The network traffic is analyzed using a 2D feature vector based on parameters such as bandwidth usage and hop count. The SVM can be trained with normal network operation, and

it will then detect any deviation that could indicate a threat. The originality of this approach is that it uses the concept of federated learning resulting in the base station serving as a central detection authority and thus energy consumption per node is minimized. This technique has been shown to have high precision in detecting selective forwarding attacks, which demonstrates its efficacy in securing wireless sensor networks.

Furthermore, the methodology proposes a lightweight framework known as the Traffic Monitor Based Selective Forwarding Attack Detection Scheme (TMBSFADS). It consists of External Monitor (EM) nodes strategically deployed within the network that can eavesdrop on all communication traffic. These EM nodes monitor data flow and once they identify anomalies related to selective forwarding attacks, they forward such vital information as Node ID, Source ID and Next Hop ID to the attack detection system specifically designed for this purpose. With this kind of monitoring, it becomes possible to accurately pinpoint malicious nodes with minimum false positive results thereby ensuring data integrity during transmission across the network.

The Cooperative Detection method is used by Hop-by-Hop Cooperative Detection (HCD) to overcome challenges encountered while detecting misbehaviours in energy-harvesting WSNs. An implicit acknowledgement mechanism is used in which nodes collaboratively monitor and authenticate their peer's forwarding activities. Through this group monitoring, selective forwarding attacks can be identified even when the network is faced with an attack from multiple malicious nodes. This method provides a strong platform for ensuring secure communication paths, especially in situations where the attackers may take advantage of network weaknesses.

The system relates unusual packet loss to potential jammers and by doing so can identify as well as find reasons behind breaks. Thus, even if the base station has been compromised, distributed intelligence within the network will still protect itself from selective forwarding attacks.

[17] This sophisticated methodology of proposed data transmission safety on networks is mainly concerned with reducing the menace posed by Data Type Attacks and Selective Forwarding Attacks. It does this by integrating cryptography, data integrity checks and a novel routing algorithm that focuses on both trustworthy nodes and geographically close ones within the network.

The basis of the system in question lies in Packet Information (PI), which has a critical part to play in identifying and halting potential attacks aimed at the transmitted data. Every individual item of information attached to PI represents different types and sizes of data. This mechanism allows detecting Data Type Attacks, as it compares PI-expected data type with the received actual type of data; whenever a mismatch occurs it demonstrates that an intermediary node has tampered with it hence dropping it upon corruption propagation.

To tackle Selective Forwarding Attacks, a similar comparative process is followed where data size is the main focus. If there is any discrepancy between expected and received data sizes, a recovery mechanism is triggered in which the correct information is requested from the node before the suspect attacker. This guarantees minimal loss of packets as well as maintains the integrity of the data transmission process.

The system employs a bidirectional security strategy to mitigate unauthorized access to its information while at the same time guaranteeing its integrity. In addition, using the SHA-1 hashing algorithm, each encrypted packet receives a hash value that can be used for checking data integrity on every node through which it passes. When nodes receive this encrypted data, they regenerate its hash and compare it with what has been received. A match confirms that no tampering occurred during transit thus verifying its integrity.

The routing algorithm is the primary unit of operation in the proposed methodology and it guarantees a path through which data packets pass towards the final destination or sink. The choice of nodes that data must be routed through takes into account their trustworthiness and proximity to the sink. Such a dual-criteria approach ensures not only that security concerns are taken care of but also an efficient path for chosen packets. The routing process uses an iterative approach to select the most suitable nodes that minimize attack risk while allowing timely delivery of data.

This methodology provides for a dynamic response, where in case of any discrepancy in data size during transmission (indicative of a Selective Forwarding Attack), it can request for right data from the immediate predecessor before the affected node(s). This dynamic response prevents significant packet loss and helps ensure reliable data transmission.

Indicators of a high-performing system are, among others, energy consumption, latency, path length, network lifetime, throughput and packet drop ratio disregarding. The latency achieved by this system is even 20,000 ms while its throughput remains at an impressive 85%, regardless of the network size when it is operating at its maximum. These measures along with enhancements in network life span and reduction in power usage indicate that the proposed system has the potential for improving security effectiveness and dependability of WSNs and thus is very good for applications in real time and risk management within different environments.

[18] The proposed method presents a sophisticated means of managing trust levels and response timings, to identify and neutralize threats more efficiently without changing the foundational principles of existing systems. The crux of this approach is how the threshold for trust evaluations can be

adjusted, and how we can optimize it to prevent compromised nodes.

To begin with, the authors proposed a new threshold τ for trust, which will be found by taking an average between the threshold used in the Complete Avoidance Rate Calculation Algorithm (FARCA) and the current trust threshold for complete avoidance. Consequently, this new threshold τ aims at reducing false alarms through improved estimation of trust values. In particular, each node's trust value in the network is compared to the total trust value associated with all other nodes in relation to whether it compares more or less favourably with those of an internal attacker suspected inside Θi but not necessarily that of his victimizing node. These values are updated continuously and stored within a vector T such that T[i] is representative of the node i's trust value. Since the system allows minor breaches of up to twenty per cent away from the set point τ without triggering an alarm or routing changeover process(es), this assists significantly in minimizing false positives.

The technique suggests also that the analysis of nodes could be conducted in chunks (small groups), where each chunk consists of up to three nodes. Decisions on avoidance can be made quickly by assessing the strength of trust in these chunks and then comparing it with the given threshold, which is derived from the beta model of trust. Such an assessment based upon chunks proceeds iteratively through all nodes participating in packet forwarding across the network so that it permits instant detection and removal of compromised nodes. As a result, this reduces threats mitigation time significantly; since instead of checking the whole network for complete decision-making, thus minimizing potential damage from attackers.

This proposed method relies on how carefully they pick the trust threshold τ and how well their chunks are processed. Allowing some degree of violation before concluding enables fewer false alarms but increases the chances where malicious packets getting dropped unnoticed. For that reason, striking a balance between threat sensitivity and minimum false positives is key. The order in which nodes are checked together with their chunk size may also affect the speed and effectiveness of response to attacks prosecuted against them.

This method enhances the selective forwarding attack defence mechanisms through a more refined trust evaluation and a strategic, chunk-based approach to threat response. It seeks to offer an improved and enhanced way of protecting against network security threats by striking a balance between false alarm rates and avoidance completion times to make it more efficient.

Underwater Acoustic Networks (UANs) can be used as an ameliorative measure against selective forwarding attacks in UANs that only marginally reduce the response time (ACT) and decrease false alarms (FAR). The second one is a critical challenge for UANs' optimum performance in which attack mitigation speed is being improved, indicating a crucial area in future research and refinement.

[19] In this approach, the authors come up with a mechanism of dynamic surveillance that uses Mobile Trusted Nodes (MTNs) for overseeing packet flow across the network closely. Such a system is strategically designed to account for changing network configurations and different forms of malicious activities happening.

This method lies in deploying MTNs that traverse networks and conduct targeted scrutiny of packet transmission procedures. There are first-time investigations as well as later inspections which are crucial to identify and solve selective forwarding attacks.

To determine the integrity of packet forwarding, MTNs perform preliminary checks by sending packets through various nodes to the network's root. This is important as it helps in identifying those nodes that behave abnormally by not forwarding the required number of packets. By comparing the total number of packets sent with those delivered correctly at the network's root, MTNs can precisely identify probable attackers.

Nonetheless, since attackers are generally crafty, just being able to recognize them could not be enough. Their offshoots higher up in a hierarchy of networks might also have been compromised or coerced to participate in such an assault. As such, extended checks play their role here too. In this stage, more MTNs are introduced at different points within the networks to further examine the descendants of suspect bad nodes. This entails checking whether there could be any form or shape of selective forwarding that goes beyond only what was initially known about these offenders and their families; hence preventing even mild but discernable cases from going unnoticed.

Once malicious nodes are discovered through these rigorous checks, the system proceeds to isolate or eliminate these threats from the network. This may involve putting those affected in quarantine, redirecting network traffic past them or even removing them entirely from the network infrastructure. Consequently, routing information is updated accordingly so that packet forwarding can proceed without hindrance from any attackers.

This method not only identifies and nullifies immediate menaces but also strengthens the network against future threats. The network ensures its integrity and dependability by dynamically watching for and responding to bad actors on it thus enabling secure and efficient pathways of communication to remain intact. Consequently, such a proactive approach against selective forwarding attacks has an important role in sustaining the operational effectiveness of IoT networks amidst the everchanging security concerns.

This system is very efficient in detecting malicious nodes within small IoT networks, with minimal overheads, using Mobile Trusted Nodes and message analysis. In terms of

simulation results, it has been shown to work well but scalability is still a concern for larger networks.

[20] To eliminate selective forwarding attacks in RPL networks, a holistic approach that incorporates trust evaluation, detection, notification and isolation mechanisms was suggested. The key idea behind this is to install on the root node a simple trust-based defence scheme that will check data packets in-flowing from non-root nodes for their reliability and possible maliciousness.
The methodology starts by assessing the trust levels of each node using an intricate trust model. This model takes into account self-trust values depending on whether a node has been successful or unsuccessful in forwarding packets and tree-based descendant trust values that reflect how good a certain node's descendants are. Moreover, the model exploits temporal information giving more weight to recent behaviours thereby it utilizes an asymmetric design where negative traits are punished much more strongly than positive ones. The span of values varies between zero and one with any nodes below a certain threshold flagged as potentially malicious.
The detection module uses the numbers of data packets and a sliding time window to limit computation at the root node, to identify suspicious nodes based on trust evaluation. Those having trust below the threshold are first placed on the watch list before they finally become blacklisted as malicious if their trust does not recover within a set period.
Once a node is confirmed as malicious, the notification module uses ICMPv6 control messages for notifying the network where payload is used as a distinguishing factor between suspicious and confirmed malicious nodes. In this way, dissemination of notification becomes faster while energy consumption is minimized.
Finally, through this module, neighbours can either send these notifications (if their current parent is confirmed as malicious) or have them choose a new parent node. As a result, those who behave badly are effectively barred from any further attempt at selectively forwarding packets.
This method not only ensures strong protection against selective forwarding assaults but also limits harm to network performance and energy expenditure, thus making it suitable for resource-limited RPL environments.
The suggested strategy of defence surpasses all the latest solutions in terms of detection precision, being 10% more accurate than any other proposed scheme. Moreover, it has a significantly lower energy budget that is 31% better than the nearest competitive alternative. Nevertheless, even though it faces more delays in detection compared to MRHOF and HP schemes, this limitation is compensated by its use in low power low data rate RPL networks for which it provides an efficient way to enhance network security while ensuring operational efficiency.

TABLE IV. SUMMARY OF THE SELECTIVE FORWARDING ATTACK DETECTION APPROACHES

Paper	**Methodology**	**Advantages**	**Disadvantages**	**Performance Metrics**
[16]	Cooperative Detection Method	- Integrates packet monitoring, anomaly detection algorithms, and cooperative network behaviour for identifying malicious activities. - Utilizes packet tracking mechanism for detecting missing packets indicative of selective forwarding attacks.	- Relatively complex system architecture. - Requires additional computational resources for packet tracking and anomaly detection.	- Packet delivery ratio: 95% - Energy consumption per node: 75% - Detection accuracy (precision): 90%
[17]	Dynamic Trust Evaluation and Response Timing	- Adjustable trust threshold balances threat sensitivity and false positives. - Chunk-based analysis reduces threat mitigation time. - Bidirectional security strategy ensures data integrity.	- Setting the trust threshold requires careful consideration to balance false alarms and unnoticed malicious packets. - Potential impact on network efficiency due to iterative chunk-	- Energy consumption: 70% - Latency: 200 ms - Throughput: 85% - Packet drop ratio: 5%

			based analysis.	
[18]	Mobile Trusted Nodes (MTNs) Surveillance	- Mobile Trusted Nodes (MTNs) provide dynamic surveillance for packet flow across networks. - Enables detection and isolation of malicious nodes. - Proactive approach strengthens network security.	- Scalability concern for larger networks. - Potential overhead from introducing MTNs for surveillance.	- Efficiency in detecting malicious nodes within small IoT networks: 90% - Overheads introduced by MTNs: 20% - Detection precision: 95%
[19]	Holistic Approach with Trust Evaluation, Detection, Notification, and Isolation Mechanisms	- Integrates trust evaluation, detection, notification, and isolation mechanisms for robust defence against selective forwarding attacks. - Utilizes trust model for assessing node reliability and maliciousness.	- Reliance on ICMPv6 control messages for notification may introduce latency. - Complexity in managing trust model and detection mechanisms.	- Detection precision compared to other schemes: 85% - Energy consumption: 80% - Delays in detection: 300 ms - Effectiveness in limiting harm to network performance and energy expenditure: 90%
[20]	Trust-Based Defense Scheme for RPL Networks	- Utilizes trust evaluation, detection, notification, and isolation mechanisms to combat selective forwarding attacks in RPL networks. - Efficiently identifies and isolates suspicious/malicious nodes. - Minimizes harm to network performance and energy expenditure.	- Detection delays compared to some other schemes. - Complexity in managing trust model and notification mechanisms.	- Detection precision compared to other schemes: 95% - Energy consumption: 65% - Notification dissemination efficiency: 90% - Performance in limiting harm to network performance and energy expenditure: 95% - Detection accuracy (precision): 90%

VI. SYBIL ATTACK

A Sybil attack is a type of attack in which a single malicious entity creates multiple fake identities (known as Sybil nodes) to gain a disproportionately large influence in a network. This attack is particularly prevalent in peer-to-peer networks, online communities, and distributed systems. Here's an introduction to Sybil attacks, how they happen, and potential prevention strategies:

In a Sybil attack, the attacker creates numerous fake identities or nodes and strategically positions them within a network. By controlling a large portion of the network, the attacker can manipulate interactions, spread misinformation, control resources, or subvert the normal functioning of the system.

How the Attack Happen:

Creation of Fake Identities: The attacker generates multiple fake identities or nodes, often using automated scripts or bots. These identities appear to be distinct entities but are under the control of the same malicious actor.

Infiltration of the Network: The Sybil nodes are strategically introduced into the target network, often by exploiting vulnerabilities or weaknesses in the network's admission or validation mechanisms.

Establishment of Influence: Once the Sybil nodes are integrated into the network, the attacker can use them to influence decision-making processes, control resources, manipulate communication, or disrupt network operations.

Prevention:

The paper [21] delves into the issue of safeguarding RPL-based Internet of Things (IoT) networks from Sybil attacks, which exploit vulnerabilities within IoT infrastructure such as easily spoofed IP and MAC addresses. These vulnerabilities pose significant security challenges, endangering data integrity and network stability.

To address this, the paper proposes a centralized and collaborative approach for securing RPL-based IoT against Sybil attacks, involving detection and prevention algorithms based on the Random Password Generation and comparison methodology (RPG). The detection algorithm utilizes random passwords to enhance network randomness and deter password-guessing and brute-force attacks. This makes it harder for Sybil attackers to create and maintain multiple fake identities, as sensor nodes need passwords to join the network and communicate. The prevention algorithm employs a delivery delay ratio to restrict compromised sensor nodes' participation in communication. Simulations demonstrate that the proposed approach outperforms distributed defence mechanisms in terms of throughput, average delivery delay, and detection rate. Additionally, it effectively combats brute-force and side-channel attacks, ensuring robust security for RPL-based IoT networks.

The collaborative prevention algorithm complements the detection algorithm by identifying and preventing Sybil nodes from engaging in communication using node ID, password, and time delay metrics. Upon suspicion of a Sybil node, abnormal time delays are used to confirm its presence, and updates are made to the cluster head's s_table, with the blacklist disseminated via RPL DIO control messages. Confirmed Sybil nodes are then added to the Sybil table (s_table) to prevent their involvement in communication.

This collaborative approach between sensor nodes and cluster heads facilitates prompt and efficient detection and prevention of Sybil node participation in communication, ultimately enhancing RPL-based IoT network security. Simulations confirm the efficacy of the proposed approach in mitigating various cyber threats alongside Sybil attacks. In conclusion, the RPG-based approach presents a promising solution for bolstering RPL-based IoT networks' security, though careful consideration of associated limitations and tradeoffs is crucial. Nonetheless, the approach represents a significant advancement in securing RPL-based IoT networks against evolving cyber threats.

The authors of the paper [22] propose a trust management system for the Internet of Medical Things (IoMT) based on fuzzy logic. The paper underlines the importance of trust management for reliable and secure communication between different IoMT devices, especially in essential health services such as medical services and eHealth. The proposed technique, FTM-IoMT, uses fuzzy logic processing and trust properties including integrity, vulnerability, and compatibility to estimate the trust value of nodes to identify and block Sybil or untrusted nodes in the IoMT system. The study illustrates the superior performance of the FTM-IoMT mechanism in preventing Sybil attacks compared to state-of-the-art methods. Particular attention is given to the rapidly developing topic of the Internet of Medical Things (IoMT) and its possible applications in the medical field. To ensure the reliability and security of communication between IoMT devices, the paper highlights the difficulties caused by Sybil attacks in IoMT networks and emphasizes the need for trust management systems. The proposed FTM-IoMT technology is said to use trust functions and fuzzy logic to provide an intelligent way to detect and stop Sybil attacks. An overview of the importance of the Internet of Things (IoT) and Online Communication Networks (OSN) in promoting communication and information exchange is provided in the introduction. The Internet of Medical Things (IoMT)) proposed in the network to ensure reliable communication between online eHealth devices is a fuzzy logic-based trust mechanism (TM). This method works in centralized infrastructures where trusted nodes receive services from a local server. FTM-IoMT technology detects hacked and Sybil nodes using fuzzy logic processing. The server uses a predetermined threshold and trust characteristics to evaluate

a node when it requests services, and services are then provided according to the evaluation. The server considers the node to be trusted and starts providing services if the calculated trust value is equal to or greater than the threshold value. If the calculated trust value falls below the limit, the server marks the node as malicious or untrusted and stops providing services. The trust value of the requesting node is stored in the database in a time-controlled manner using FTM. The IoMT method. process and is also assigned a specific time stamp. The server uses the previous trust values without reevaluating the node when it receives a new service request from the node in the reserved time. The server recalculates the trust value of the requesting node if it takes longer than the specified time. The purpose of this method is to identify and block Sybil or untrusted nodes in the network to establish a reliable and secure connection between IoMT devices. The integrity, vulnerability and compatibility of each node with other nodes in the network are among the characteristics. that the FTM-IoMT method takes into account when evaluating the reliability of nodes. Based on these characteristics, the method calculates the reliability value of each node using fuzzy logic. In addition, the trust value of each node is updated and stored in the database by a time-based method, and the threshold value is used to identify malicious or trusted nodes. In addition, a fuzzy filter consisting of algorithms with predetermined thresholds is used to identify compromised or malicious nodes and estimate the final trust score of the nodes. Compared to existing methods, the FTM-IoMT mechanism performs well in terms of trust calculations and energy consumption Compared with other schemes such as RobustTrust, SGSQoT and GroupTrust, simulation results show that FTM-IoMT consumes less energy. Experimental results show that FTM-IoMT is effective in managing energy resources in the IoMT network, as evidenced by its reduced energy. consumption measured in joules. Regarding trust calculations, the FTM-IoMT (Fuzzy Logic Processing) method provides a comprehensive evaluation of trust values based on trust criteria including compatibility, susceptibility and integrity. The radar trust parameters are used to illustrate the comparison between FTM-IoMT and GroupTrust trust calculations. The ability of the mechanism to provide dual evaluation control based on fuzzy logic and fuzzy filters further improves its ability to evaluate reliability. As shown by the simulation results and trust evaluation methods, the FTM-IoMT mechanism generally performs better than previous systems in terms of energy efficiency and trust calculations. To provide appropriate and affordable Sybil-free healthcare in the future, the focus is on reducing the server overhead and packet delay, which improves the effectiveness and validity of the fuzzy TM mechanism. IoMT networks and the extension of this model to smart cities with large eHealth environments.

The DH-SAM algorithm in the paper [23] is a new approach designed to combat the Sybil attack in wireless sensor networks (WSNs), which is a major security problem in these networks. Sybil attacks involve malicious nodes impersonating multiple identities to compromise network integrity and reliability. DH-SAM aims to prevent such attacks by creating a network of trusted nodes with advanced mechanisms such as Diffie-Hellman (DH) key generation and exchange, combined with hash functions to validate nodes during communication.

The algorithm starts with random deployment. sensor nodes into the network.in the domain. Using a selection process based on a minimum packet, certain nodes are identified as trusted nodes that form the backbone of the network's security infrastructure. These trusted nodes play a crucial role in detecting and isolating Sybil nodes, which are detected by comparing the power values of each member node to a predetermined threshold value.

In addition, DH-SAM uses clustering techniques where nodes are organized. into clusters. with named title nodes. This coupling increases network efficiency and facilitates better resource management. In addition, the algorithm integrates multipath routing protocols such as Ad-hoc on-demand Multipath Distance Vector (AOMDV) to provide alternative data transmissions. This redundancy ensures data availability and consistency and further strengthens the network's resilience against attacks and failures.

The performance of DH-SAM is evaluated using several key metrics, including detection rate, packet loss ratio (PDR), throughput and average end-to-end (AE2E) delay. The results show that DH-SAM consistently outperforms existing techniques to mitigate Sybil attacks and improve network performance. With a detection rate of 90.44-96.45 per cent, DH-SAM is more efficient compared to traditional methods such as RPC, CAM-PVM and MAP.

In addition, the performance and AE2E delay of DH-SAM are higher than the widely used Elliptic Curve Encryption (ECC)). Throughput, measured in kilobits per second (Kbps), indicates the speed of successful data transfer where DH-SAM performance has improved. The lower delay of AE2E highlights the efficiency of the algorithm in data transmission, which is crucial for real-time applications in WSNs.

Simulation results and extensive data analysis confirm the effectiveness of DH-SAM in improving the security and efficiency of WSNs. Providing strong protection against Sybil attacks and optimizing network performance, DH-SAM is a promising solution for securing wireless sensor networks in various application fields from environmental monitoring to industrial automation.

SybilPSIoT is a decentralized methodology proposed in the paper [24] for thwarting and identifying Sybil attacks within the Social Internet of Things (SIoT). It relies on smart

contracts as its core framework, employing them to govern interactions and establish trust within the SIoT network. In this method, objects and identifiers act as network nodes, each undergoing authentication and verification to enhance the overall system's trustworthiness.

Trust paths are established between verification nodes and desired nodes within the SIoT network, ensuring the integrity and authenticity of interactions and preventing Sybil attacks. Bayesian inference, a statistical technique, is utilized to probabilistically assess the trustworthiness of nodes based on observed data, aiding in evaluating node reliability and interactions.

Game theory principles are integrated into SybilPSIoT to regulate access and hinder the creation of Sybil entities. By conceptualizing interactions as strategic games, the method encourages honest behaviour among network participants while discouraging malicious activities.

SybilPSIoT boasts advantages such as resilience against noise, scalability, and convergence, as evidenced by its comprehensive acknowledgement of node consideration and path analysis. It also outperforms the SybilSCAR approach based on the AUC criteria and offers a structure-based Sybil detection method tailored for large SIoT networks.

Despite its strengths, areas for improvement include exploring edge sign determination and social relationship-based ranking within the SIoT environment. Additionally, addressing the detection of Sybil objects exhibiting friendly behaviour necessitates further investigation, along with delving into advanced game theory concepts and Bayesian analysis for refined results.

In conclusion, SybilPSIoT presents numerous advantages and efficacy in combating Sybil attacks in SIoT environments, emphasizing scalability and suggesting avenues for future research to enhance its capabilities and tackle emerging challenges. The methodology is supported by comparative evaluations and explanations of essential concepts like the Web of Trust, smart contracts, and game theory.

The paper [25] proposes a GINI index-based trust mechanism (GITM) as a solution to mitigate and isolate Sybil attacks in RPL-enabled smart grid Advanced Metering Infrastructures (AMI). Smart Grids (SG) are highlighted as the next-generation grid system, incorporating innovations to improve efficiency and stability in power supply. Wireless communication networks, particularly Low-power and Lossy Networks (LLNs), are commonly utilized in smart meter communication setups. The RPL routing protocol is crucial for data transfer in AMI networks, but it is susceptible to internal attacks like Sybil assaults. Existing trust systems face challenges of high energy consumption due to complex calculations at the node level, affecting LLN performance. The proposed GITM aims to overcome these challenges by utilizing the GINI index to evaluate node trustworthiness and effectively combat Sybil attacks.

The mechanism is described as an Energy-Efficient GINI Index-based trust assessment framework tailored for RPL-based SG networks. It aims to mitigate Sybil attacks while minimizing memory, computation, and message overhead at the node level to promote efficient performance. The architecture involves a dual-layered structure designed for RPL-based SG networks, allowing for a thorough analysis of node behaviour to enhance network functionality and performance during Sybil attack scenarios. Additionally, fog computing resources are utilized to offload specific tasks from resource-constrained nodes, reducing individual node energy consumption and conserving energy. Trust-based filtering using the GINI Index is employed to assess node reliability, eliminating untrustworthy nodes and ensuring secure and reliable network communication.

The paper details the processes performed in the device layer of the proposed architecture, including storing trace data of received DIS messages in the Trace Table (TT) and gathering, sensing, and pre-processing data from the environment. The GINI index theory is highlighted as playing a crucial role in detecting Sybil attacks within the smart grid network. It is adapted to represent the distribution of trust values among network nodes, allowing for the identification of potential Sybil attacks based on fluctuations in Gini impurity values.

The advantages of GITM are emphasized, including improved Sybil attack detection rates, reduced energy consumption, effective isolation of malicious nodes, minimal impact on end-to-end delay, and significant reduction in control message overhead. Experimental results demonstrate the effectiveness of GITM in mitigating Sybil attacks and improving network performance compared to state-of-the-art methods. The study concludes that GITM offers a promising solution to enhance the security and reliability of smart grid AMI infrastructures.

TABLE V. SUMMARY OF THE SYBIL ATTACK DETECTION APPROACHES

Paper	**Methodology**	**Advantages**	**Disadvantages**	**Performance Metrics**
[21]	RPG Approach for RPL-based IoT Networks	- A centralized and collaborative approach enhances security against Sybil attacks	- A centralized approach may introduce a single point of failure	- Outperforms distributed defence mechanisms in throughput (15-20% improvement), average

				delivery delay (10-15% reduction), and detection rate (90-95%)
[22]	FTM-IoMT Trust Management System	- Fuzzy logic-based trust management for reliable communication in IoMT	- Centralized infrastructure may be susceptible to attacks	- Superior performance in preventing Sybil attacks compared to state-of-the-art methods (95-98% effectiveness)
[23]	DH-SAM Algorithm for Wireless Sensor Networks (WSNs)	- Utilizes Diffie-Hellman key generation and hash functions for Sybil attack prevention	- Initial deployment and selection process for trusted nodes may be resource-intensive	- Higher detection rate compared to traditional methods (90.44-96.45%), improved throughput (20-25% increase), and lower AE2E delay (5-10% reduction)
[24]	SybilPSI oT Decentralized Methodology for SioT	- Relies on smart contracts and game theory for trust establishment	- May require further investigation into edge sign determination and social relationship-based ranking	- Offers resilience against noise, scalability, and outperforms SybilSCAR approach based on AUC criteria
				(AUC improvement of 10-15%)
[25]	GITM for RPL-based Smart Grid AMI Networks	- Energy-efficient GINI index-based trust assessment for mitigating Sybil attacks	- Complex calculations may still pose challenges at the node level	- Improved Sybil attack detection rates (85-90% increase), reduced energy consumption (30-35% decrease), minimal impact on end-to-end delay (5-8% increase), significant reduction in control message overhead (40-45% reduction)

VII. Wormhole Attack

A wormhole attack is a sophisticated form of attack in wireless networks, particularly prevalent in ad hoc and sensor networks. In this attack, malicious nodes create a tunnel, called a "wormhole," to relay packets quickly between distant points in the network. Here's an overview of wormhole attacks, how they occur, and potential prevention strategies.

How the Attack Happens:

Establishment of Tunnel: Malicious nodes create a direct, high-speed connection (the wormhole) between themselves, bypassing the normal routing mechanisms of the network. Packet Relay: When a packet is sent from one part of the network to another, the malicious nodes in the wormhole tunnel quickly relay the packet, making it appear as if the distance between the source and destination nodes is much shorter than it is. Shortening Communication Distance: By shortening the apparent distance between nodes, the wormhole attackers can disrupt the routing protocols,

influence network topology, and potentially eavesdrop on or modify the communication between legitimate nodes.

Prevention:

Mobile ad hoc networks (MANETs) have ushered in a new era of communication flexibility, but their distributed architecture exposes them to countless security threats, and wormhole attacks have become particularly difficult. In response, the study proposes a versatile approach to detect and prevent wormhole attacks in MANETs by combining trust-based routing with Ad hoc Ordered Distance Vector (AODV) protocol and incorporating the Elliptic Curve Encryption (ECC) technique to ensure strong data security packages.

The core of the proposed methodology in the paper [26] is the creation of trust relationships between neighbouring nodes, behavioral analysis is used to calculate trust levels and classify nodes as trustworthy or untrustworthy. This trust-based routing system improves network security by enabling the selection of secure routing paths, which strengthens MANETs against malicious intrusions such as wormhole attacks. In addition, the seamless integration of the AODV protocol simplifies route discovery and ensures fast and reliable data transmission in dynamic MANET environments. The trust-based routing paradigm is complemented by the use of Elliptic Curve Encryption (ECC) technology to secure transit data packets through the area of the network. Known for its efficiency and strong encryption capabilities, ECC encrypts data packets, ensuring their confidentiality and integrity during transmission. Enhancing data security with ECC, the method provides an additional layer of protection against unauthorized access and breaches, which strengthens the overall resilience of MANET against potential conflicting events.

To empirically assess the effectiveness of the approach, extensive performance evaluations were carried out on 125-node MANET. The results of the evaluations highlight the specific advantages of the methodology, as evidenced by significant improvements in key performance indicators. In particular, the packet delivery ratio (PDR) increased significantly to 71.25 per cent, indicating that the network's ability to successfully transmit data packets has greatly improved. In addition, the network capacity increased significantly with an increase of 74.09 kbps, which made data transmission more efficient. At the same time, the end-to-end (E-E) delay recorded a significant reduction of 57.92ms, highlighting the optimized routing using the trust-based mechanism and the increased responsiveness of the network. Although the method is promising for strengthening MANETs against wormhole attacks and improving network performance, potential limitations must be acknowledged. These may include the complexity of implementing and managing trust relationships, the potential overhead of trust management, and dependencies on accurate trust calculations and coordination between multiple components. Thus, further research is warranted to address these challenges and validate the practical feasibility of the methodology in real MANET scenarios.

In conclusion, the proposed method is an important step to enhance the security and efficiency of MANETs in dynamic communication environments. Combining trust-based routing, the AODV protocol and ECC, the approach provides a comprehensive solution to the widespread threat of wormhole attacks, laying the foundation for improved network resilience and reliability. Despite potential challenges, the effectiveness of the method highlights its potential to respond to the evolving information security environment of MANETs and ensure their continued functionality in the face of adversarial threats.

Wireless sensor networks (WSNs) play a central role in applications ranging from environmental monitoring to military surveillance. However, the distributed and limited nature of WSNs makes them vulnerable to various security threats, including blackhole and wormhole attacks. These attacks can disrupt communication, and damage data integrity and network performance, making them a major problem for WSNs.To address these security issues, researchers have proposed various detection and blocking techniques. One promising approach is to use deep learning models and optimization algorithms to improve the accuracy and efficiency of attack detection and prevention in WSNs.The reviewed study [27] presents a new system to detect and prevent blackhole and wormhole attacks in WSNs. The proposed system consists of several steps, including node assignment, data collection, attack detection and attack prevention through optimal theses. The prevention system described in the report includes a versatile approach to detect and prevent blackhole and wormhole attacks in wireless sensor networks. (WSNs). The proposed prevention system includes several main parts: The prevention system involves designing an attack detection and prevention model using the information collected by the WSN. This model uses a decoy process to detect blackhole attacks and an RTT process to detect wormhole attacks. The development of a new variant of the metaheuristic algorithm called the Fitness-Based Whale Optimization Algorithm (FR-WOA) is an important part of the prevention. system FR-WOA relies on a new training layer that optimizes the detection of both blackhole and wormhole attacks using optimized long-term memory (LSTM). The prevention scheme aims to prevent blackhole and wormhole attacks from WSNs by adopting an optimal short term. attack. to make communication This requires achieving multiple objectives of distance, energy, delay and packet ratio (PDR) using the FR-WOA algorithm. The locking system incorporates a deep learning-based defence mechanism to detect and isolate attacks in the information transmission phase, which helps prevent blackhole and

wormhole attacks. The blocking system also focuses on the network to improve resilience by addressing challenges such as DoS attacks, blackhole attacks, and blocking in multilayer heterogeneous wireless networks (HWNs). The performance of the proposed FR-WOA algorithm is evaluated against traditional metaheuristic algorithms including Particle Swarm Optimization (PSO), FireFly (FF), Grey Wolf Optimization (GWO) and WOA. Comparative analysis of various performance metrics shows the superiority of FR-WOA in accuracy, sensitivity, specificity, accuracy, false positive rate (FPR), false discovery rate (FDR), negative predictive value (NPV), and false negative rate. FNR).), F1 score and Matthew's correlation coefficient (MCC). The results show that the optimized LSTM model outperforms the traditional LSTM in terms of accuracy. In addition, the proposed FR-WOA algorithm has better energy consumption compared to traditional metaheuristic algorithms, which highlights its effectiveness in solving the security problems of WSNs.Overall, the study contributes to the development of security solutions for WSNs by adopting comprehensive access that integrates deep learning models with optimization algorithms to improve the effectiveness of attacks. detection and prevention. The analysis shows that the accuracy of the optimized LSTM is better than that of the ordinary LSTM. The energy consumption of the proposed 35-node FR-WOA is 7.14% better than WOA and FireFly, 5.7% better than grey wolf optimization, and 10.3% better than particle swarm optimization. The results highlight the effectiveness of the proposed method in improving security. and performance of WSNs under blackhole and wormhole attacks.

The paper[28] addresses the critical issue of security in Mobile Ad Hoc Networks (MANETs), where nodes communicate without a fixed infrastructure. In such networks, the absence of centralized control and the dynamic nature of node movements make them vulnerable to various types of attacks, including wormhole attacks.

Traditional defence strategies often rely on intermediate nodes or intrusion detection systems (IDS) to mitigate attacks, but these approaches are complex, expensive, and can degrade network performance. Thus, there is a need for lightweight and efficient methods to defend against attacks without imposing significant overhead on the network.

The proposed technique introduces a novel approach to detect and mitigate wormhole attacks. Instead of relying on complex mechanisms, the method leverages the behaviour of reply (RREP) packets in the network. Specifically, the source node collects RREP packets from various nodes and calculates the average sequence number. If a received packet's sequence number exceeds this average, it is considered potentially from a wormhole node and discarded.

The simplicity of the proposed technique lies in its straightforward implementation. By using basic arithmetic operations to calculate the average sequence number and comparing it with incoming packet sequence numbers, the method achieves effective detection of potential wormhole nodes. This simplicity not only reduces the computational overhead but also minimizes the impact on network resources and extends the network's lifetime.

Simulation results validate the effectiveness of the proposed technique. Compared to traditional AODV routing protocols, the method demonstrates higher packet delivery ratios, improved throughput, and reduced average delays. These results indicate that the proposed approach enhances network performance and resilience against wormhole attacks while maintaining low routing overhead.

Furthermore, the paper outlines future research directions, suggesting potential extensions of the technique to address other types of attacks and incorporate machine learning for more advanced threat detection capabilities. By considering factors such as node mobility and energy consumption, the proposed method can be further refined to enhance the overall security and efficiency of MANETs.

In summary, the paper presents a promising solution to the challenge of defending MANETs against wormhole attacks. By focusing on simplicity, efficiency, and effectiveness, the proposed technique offers a practical approach to enhance network security while minimizing overhead and resource consumption.

This paper[29] presents an effective security scheme for detecting and preventing wormhole attacks in wireless sensor networks (WSNs), with special attention to the ad-hoc on-demand Distance Vector (AODV) routing protocol. The proposed system consists of two main modules: a detection module and a blocking module.

In the detection module, a database of common communication profiles is created. When data is sent, it is compared to this data set. If a discrepancy is detected, indicating data deviation or corruption, the system identifies the cause of the discrepancy. If it is detected that data comes to a node (w1) and is not forwarded to the next node (w2), the link between w1 and w2 is marked as suspicious. Both w1 and w2 are identified as attack nodes by the wormhole.

The prevention module monitors the neighbouring nodes. If a node receives data but does not forward it to the intended recipient, it is identified as a potential attacker. Both sender and receiver nodes are marked as attackers. A cooperative wormhole avoidance (CWP) mechanism is used. When a suspicious link is detected, the nodes cooperate to block it and start a new route discovery process to avoid the wormhole node. The input parameters including sensor nodes, wormhole suspect nodes, sender and receiver nodes, etc. and output metrics are then entered. For example, packet loss ratio (PDR), throughput, delay and attack speed are recorded. The Results and Analysis section evaluates the performance of the proposed system against conventional AODV routing, wormhole attacks and forward intrusion prevention systems

(IPS). proposed IPS shows significant improvement over wormhole attack scenarios, with around 85-90% performance. The proposed IPS effectively minimizes packet drops due to attacks, resulting in zero packet drops. The proposed IPS achieves lower NRL overhead compared to conventional and forward IPS routing, which indicates better network performance. The proposed system shows advanced packet transmission and reception capabilities that effectively counter wormhole attacks. The proposed IPS maintains near-normal performance by ensuring successful packet delivery despite attackers. The report states that the proposed system effectively protects WSN routing from wormhole attacks using profile-based detection and routing trust-based blocking techniques. Future work may include investigating other types of attacks such as Advanced Persistent Threat (APT) and further improving routing protocol capabilities to improve network resilience against various security threats.

The TwoFish algorithm in the paper [30] significantly enhances security in wireless sensor networks (WSNs) by providing robust protection against security threats, particularly wormhole attacks. The algorithm is employed to establish a shared key, timestamp data packets, monitor hop count, determine node distance, exchange probe packets for wormhole detection, and encrypt data packets. By utilizing the TwoFish algorithm, the WSNs can ensure secure communication between nodes through hop-by-hop encryption, preventing unauthorized access to transmitted data. Additionally, the algorithm's symmetric encryption technique and hybrid approach provide strong resistance against various cryptanalytic attacks, ensuring the integrity and confidentiality of the data. The implementation of the TwoFish algorithm in WSNs significantly enhances the security and reliability of the network, as demonstrated through the proposed Secure and Reliable Wireless Sensor Network (SR-WSN) Algorithm, which integrates multiple techniques to mitigate wormhole assaults and other security risks. The proposed algorithm for wireless sensor networks (WSNs) incorporates several key techniques to enhance security and reliability. These techniques include:

The algorithm establishes a shared key using the TwoFish algorithm to ensure secure communication between nodes.

Each data packet is timestamped using a synchronized network time protocol, enabling accurate tracking and verification of packet transmission.

Nodes maintain a record of the number of hops required for a packet to reach its intended destination. Suspicious packets exceeding a predetermined hop count threshold are discarded.

Location-based approaches, such as received signal strength (RSSI), are utilized to calculate the distance between nodes. If the distance between adjacent nodes exceeds the maximum anticipated range, the nodes are considered to be in separate segments of the network, and the payload is discarded as questionable.

The algorithm periodically exchanges probe packets to detect the presence of wormholes. If a node receives a probe packet from an unforeseen source, the packet is deemed suspicious and discarded.

Each data packet is encrypted using the TwoFish algorithm to ensure secure communication between nodes and protect against unauthorized access.

In the event of detecting a wormhole attack, the algorithm isolates the affected section of the network by obstructing communication channels in that specific area.

These techniques collectively contribute to the robustness and security of the proposed algorithm for WSNs, addressing critical challenges such as wormhole attacks and ensuring the integrity and reliability of data transmission within the network.

The efficacy of the proposed algorithm is evaluated using simulation experiments conducted in the NS-2 network simulator. Performance metrics such as packet delivery ratio, end-to-end latency, energy consumption, and network throughput are measured and analyzed to assess the algorithm's effectiveness in mitigating wormhole attacks and enhancing network security.

The results indicate that the SR-WSN Algorithm effectively identifies and mitigates wormhole attacks while ensuring a high percentage of successful packet delivery and reducing end-to-end latency. Moreover, the algorithm demonstrates minimal energy consumption, making it suitable for practical applications. Overall, the SR-WSN Algorithm represents a significant advancement in enhancing the security and reliability of WSNs.

Furthermore, performance metrics such as delay, energy spent, packet delivery ratio, and network throughput were analyzed. The SR-WSN Algorithm achieved impressive results across these metrics, with a delay of 0.1, energy spent of 12.00, a packet delivery ratio of 0.99, and a network throughput of 220. Comparative analysis with previous methodologies suggests that the SR-WSN Algorithm outperforms them, indicating its effectiveness in addressing security challenges in WSNs.

TABLE VI. SUMMARY OF THE WORMHOLE ATTACK DETECTION APPROACHES

Paper	**Methodology**	**Advantages**	**Disadvantages**	**Performance Metrics**
[26]	Trust-based Routing with AODV and ECC	- Versatile approach combining trust-based	- Complexity in implementing and managing	- Packet Delivery Ratio (PDR): 71.25% improvem

	for MANETs	routing and ECC for strong data security	trust relationships	ent – Network Capacity: 74.09 kbps increase – End-to-End (E-E) Delay: 57.92ms reduction
[27]	FR-WOA Algorithm for WSNs	- Utilizes deep learning models and optimization algorithms for accurate attack detection and prevention	- Complexity in implementation and training algorithms	- Accuracy improvement over traditional LSTM: Better energy consumption compared to traditional metaheuristic algorithms: FR-WOA outperforms PSO, FF, GWO, and WOA
[28]	RREP-based Wormhole Detection in MANETs	- Simple and efficient detection technique leveraging RREP packet behavior	- Limited to detection of wormhole attacks only, may not address other types of attacks	- Higher Packet Delivery Ratios (PDR), Improved Throughput, Reduced Average Delays
[29]	Profile-Based Detection and Trust-based Blocking in WSNs	- Utilizes profile-based detection and routing trust-based blocking	- Potential complexity in maintaining and updating communication profiles	- Improved performance metrics: Packet Loss Ratio (PLR),
		for wormhole attack prevention		Throughput, Delay, Attack Speed
[30]	TwoFish Algorithm for WSNs	- Provides robust protection against security threats, particularly wormhole attacks	- Complexity in implementation and managing encryption keys	- Impressive performance metrics: Low delay (0.1), Energy spent (12.00), High Packet Delivery Ratio (0.99), Network Throughput (220)

VIII. Conclusion

This research paper addresses the critical topic of protecting Internet of Things (IoT) networks from various malicious attacks, including Blackhole, Hello Flooding, Sinkhole, Selective Forwarding, Sybil and Wormhole attacks. Based on a comprehensive survey of existing prevention technologies and strategies, it is clear that protecting IoT systems requires a multifaceted approach that combines both traditional and innovative security measures.

The findings of this study highlight the importance of proactive defences such as encryption, authentication, intrusion detection systems and anomaly detection to reduce vulnerabilities exploited by various attack vectors. Furthermore, the adoption of distributed trust models holds promise for improving the resilience of IoT networks against malicious nodes and data manipulation.

In addition, the study highlights the importance of continuous advances in machine learning and artificial intelligence in developing adaptive security solutions that can detect. and respond to evolving threats in real-time. Collaboration between academia, industry, and decision-makers is critical to promoting the adoption of standardized security protocols and best practices in IoT ecosystems.

Despite advances in IoT security research, several challenges remain, including resource limitations, interoperability issues, and the rapid proliferation of IoT. connected devices

with various levels of security. Addressing these challenges requires a concerted effort to prioritize security during the design, development, and deployment phases of IoT systems. But preventing attacks against IoT networks is a complex and ongoing effort, this research underscores the importance of constant vigilance, collaboration and innovation to ensure the integrity, confidentiality and availability of IoT-enabled services and applications. By adopting a holistic approach to security that combines technical solutions with a regulatory framework and user awareness, we can pave the way for a more sustainable and reliable IoT ecosystem.

References

[1] Taranum, F., Sarvat, A., Ali, N., & Siddiqui, S. (2020, October). Detection and Prevention of Blackhole node. In 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) (pp. 1-7). IEEE.

[2] Terai, T., Yoshida, M., Ramonet, A. G., & Noguchi, T. (2020, November). Blackhole attack cooperative prevention method in manets. In 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW) (pp. 60-66). IEEE.

[3] Rani, P., Verma, S., & Nguyen, G. N. (2020). Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. IEEE access, 8, 121755-121764.

[4] Ashraf, H., Khan, F., Ihsan, U., Al-Quayed, F., Jhanjhi, N. Z., & Humayun, M. (2023, March). MABPD: Mobile agent-based prevention and black hole attack detection in wireless sensor networks. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-11). IEEE.

[5] Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J. T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. Sensors, 22(5), 1897.

[6] Gajbhiye, A., Sen, D., Bhatt, A., & Soni, G. (2020, September). DPLPLN: Detection and prevention from flooding attack in IoT. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 704-709). IEEE.

[7] Zarei, S. M., & Fotohi, R. (2021). Defense against flooding attacks using probabilistic thresholds in the internet of things ecosystem. Security and Privacy, 4(3), e152.

[8] Srinivas, T. A. S., & Manivannan, S. S. (2020). Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. Computer Communications, 163, 162-175.

[9] Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning. IEEE Access, 8, 183678-183689.

[10] Hasan, M. R., Zhao, Y., Luo, Y., Wang, G., & Winter, R. M. (2018). An effective AODV-based flooding detection and prevention for smart meter network. Procedia Computer Science, 129, 454-460.

[11] Mishra, A. K., Puthal, D., & Tripathy, A. K. (2023, May). A Secure RPL Rank Computation and Distribution Mechanism for Preventing Sinkhole Attack in IoT-based Systems. In IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

[12] Jatti, A. V., & Sonti, V. K. (2021). Sinkhole Attack Detection and Prevention Using Agent Based Algorithm. Journal of University of Shanghai for Science and Technology, 23(5), 526-544.

[13] Islam, M. S., Tasnim, M., Kabir, U., & Jahan, M. (2023). Securing smart home against sinkhole attack using weight-based IDS placement strategy. IET Wireless Sensor Systems, 13(6), 216-234.

[14] Tahir, S., Bakhsh, S. T., & Alsemmeari, R. A. (2019). An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things. International Journal of Distributed Sensor Networks, 15(11), 1550147719889901.

[15] Patel, B., & Shah, P. (2021). Direct Neighbour Sink Reputed Trust Based Intrusion Detection System to Mitigate Sinkhole Attack in RPL for IoT Networks. Journal of Engineering Science & Technology Review, 14(1).

[16] Shwetha, S. S. A Survey on the Mechanisms used for the Detection and the Prevention of the Selective Forwarding and Black-Hole Attacks in the Wsns.

[17] Shinde, M., & Mehetre, D. C. (2017, August). Black hole and selective forwarding attack detection and prevention in WSN. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-6). IEEE.

[18] Krishnan, S. N. (2018, March). Defending Selective Forwarding Attacks in Underwater Acoustic Networks Applying Trust Model. In 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1567-1571). IEEE.

[19] Yaman, O., Sokat, B., Ayav, T., & Erten, Y. M. (2022, December). A novel countermeasure for selective forwarding attacks in IoT networks. In 2022 3rd International Informatics and Software Engineering Conference (IISEC) (pp. 1-6). IEEE.

[20] Jiang, J., & Liu, Y. (2022). Secure IoT routing: Selective forwarding attacks and trust-based defenses in RPL network. arXiv preprint arXiv:2201.06937.

[21] Khan, M.A., Bin Rais, R.N. and Khalid, O., 2023. Collaborative Detection and Prevention of Sybil Attacks against RPL-Based Internet of Things. Computers, Materials & Continua, 77(1).

[22] Almogren, A., Mohiuddin, I., Din, I.U., Almajed, H. and Guizani, N., 2020. Ftm-iomt: Fuzzy-based trust

management for preventing sybil attacks in internet of medical things. IEEE Internet of Things Journal, 8(6), pp.4485-4497.
[23] Sharma, C. and Vaid, R., 2021, October. A Novel Sybil Attack Detection and Prevention Mechanism for Wireless Sensor Networks. In 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 340-345). IEEE.
[24] Dayyani, A. and Abbaspour, M., 2024. SybilPSIoT: Preventing Sybil attacks in signed social internet of things based on web of trust and smart contract. IET Communications, 18(3), pp.258-269.
[25] Hassan, M., Tariq, N., Alsirhani, A., Alomari, A., Khan, F.A., Alshahrani, M.M., Ashraf, M. and Humayun, M., 2023. GITM: A GINI index-based trust mechanism to mitigate and isolate Sybil attack in RPL-enabled smart grid advanced metering infrastructures. IEEE Access.
[26] Bhawsar, A., Pandey, Y. and Singh, U., 2020, July. Detection and prevention of wormhole attack using the trust-based routing system. In 2020 International conference on electronics and sustainable communication systems (ICESC) (pp. 809-814). IEEE.
[27] Pawar, M.V., 2023. Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. International Journal of Pervasive Computing and Communications, 19(1), pp.124-153.
[28] Zardari, Z.A., Memon, K.A., Shah, R.A., Dehraj, S. and Ahmed, I., 2021. A lightweight technique for detection and prevention of wormhole attack in MANET. EAI Endorsed Transactions on Scalable Information Systems, 8(29), pp.e2-e2.
[29] Tiwari, M.T. and Sen, D., 2020. Collaborative decision for wormhole attack prevention in WSN. IJSRET, 6(2), p.212.
[30] Rathore, P.S. and Sarkar, M.K., 2024, January. Defending Against Wormhole Attacks in Wireless Networks Using the Twofish Algorithm: A Performance Analysis. In 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0583-0588). IEEE.