Shielding Wireless Sensor Networks: Unveiling Denial-Of-Service Attacks Through Trust and Isolation Forest

K. Kathirvel[1]*, S. Hemalatha[2]

[1,2]Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-641 021.
Email: kkathir.kandasamy@gmail.com
*Corresponding Author

Received: 19.04.2024 Revised : 22.05.2024 Accepted: 27.05.2024

ABSTRACT

Wireless Sensor Networks (WSNs) plays a pivotal role across various domains, such as environmental monitoring and industrial automation. Nevertheless, their decentralized and resource-constrained nature exposes them to security vulnerabilities, notably Denial of Service (DoS) attacks. Detecting and mitigating such threats in WSNs are imperative to uphold operational reliability. This study introduces an innovative methodology employing the Isolation Forest algorithm for DoS attack classification in WSNs. Trust metrics encompassing reliability, contact intimacy, cooperation, energy consumption, and throughput are gathered from sensor nodes to construct datasets. Through the application of the Isolation Forest algorithm on these datasets, anomalies indicative of DoS attacks are discerned. Leveraging the intrinsic characteristics of isolation trees, the algorithm effectively distinguishes between normal network behavior and malicious activities. The efficacy of the proposed approach is demonstrated through a mathematical model, substantiating its ability to detect and mitigate DoS attacks. Experimental findings further validate the effectiveness of our method in accurately identifying DoS attacks with minimal false positives. This method presents a promising avenue for bolstering WSN security and resilience against DoS attacks, ensuring uninterrupted operation and preserving data integrity in critical applications.

Keywords: Wireless Sensor Network, Security, Trust, DoS attack, Isolation Forest

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are intricate systems comprising numerous autonomous sensors distributed across space, utilized for monitoring various environmental or physical conditions such as pressure, motion, temperature, and pollutants (Awan et al., 2022). These sensors collaborate to gather data and transmit it to central locations or servers for necessary actions. WSNs have extensive applications across diverse fields including military surveillance, smart infrastructure, healthcare, and environmental monitoring. They consist of various components such as base stations, sensor nodes, communication protocols, power sources, and data processing units, each playing a specific role in network functionality (Anand, C et al., 2021 and Das et al., 2023).

Sensor nodes, the core components of WSNs, sense the environment and relay information for analysis, while base nodes act as intermediaries between sensor nodes and end-user applications. Communication protocols like Bluetooth Low Energy (BLE) and Zigbee facilitate data transmission (Jinhui et al., 2018). Energy sources, including batteries and energy harvesting mechanisms, power the network, and data processing capabilities manage the vast amount of data generated by sensor nodes. Despite their numerous applications, WSNs face challenges such as security, energy efficiency, scalability, and interoperability. Security, in particular, is a significant concern due to the deployment of WSNs in unattended and critical environments (Pang et al., 2018). Internal compromises and external threats like hackers and viruses jeopardize network integrity. Ensuring confidentiality, integrity, availability, and authentication is crucial to protect sensitive data and maintain network performance (Kodali et al., 2015 and Bangotra et al., 2022).

The main objective of this paper is to enhance WSN security by identifying Denial of Service (DoS) attacks using interpersonal characteristics of nodes such as Packet Delivery Ratio, Throughput, Contact Intimacy, Cooperation, Reliability, and energy. Leveraging these characteristics as datasets, the Isolation Forest algorithm is employed to distinguish between normal and malicious node behavior and predict future node behavior.

The subsequent sections of the paper are structured as follows:

- Section 2: Background, providing context for the proposed work.

- Section 3: Literature Review, identifying research gaps in existing literature.
- Section 4: Discussion of the proposed work.
- Section 5: Illustration of the proposed work's proof of concept through mathematical examples.
- Section 6: Presentation of simulation results.
- Final Section: Conclusion.

2. Background

The proposed model compromises of following background information.

2.1 The Dynamic Source Routing Protocol (DSR)

In Wireless Sensor Networks (WSNs), various routing protocols have been utilized, including Low Energy Adaptive Clustering Hierarchy (LEACH), Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN), Adaptive Periodic Threshold-based Energy Efficient Sensor Network Protocol (APTEEN), Sensor Protocols for Information via Negotiation (SPIN), Ad-hoc On-demand Distance Vector (AODV), and Dynamic Source Routing (DSR) Protocol. Among these, the unique characteristics and advantages of the Dynamic Source Routing (DSR) Protocol make it particularly suitable for WSN environments. This section will delve into the operational principles of the DSR routing protocol and outline the rationale behind its adaptation for WSN environments. The following diagram illustrates the operational framework of the DSR routing protocol (Villalba et al., 2009)

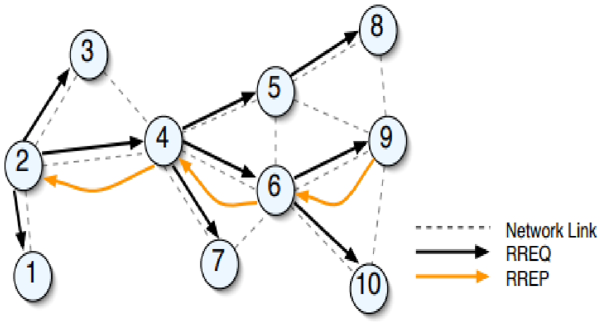


Figure 1. Framework of DSR Routing Protocol

In the Dynamic Source Routing (DSR) protocol (Johnson et al., 1996 and Johnson et al., 2001), two types of control packets are utilized to facilitate route discovery and maintenance: Route Request (RREQ) and Route Reply (RREP). When a source node intends to transmit data to a destination node but lacks a route to it in its route cache, it initiates a Route Request (RREQ) packet. The RREQ packet includes crucial information such as the address of the source node, the address of the destination node, a unique identifier for the request, and a hop count indicating the number of hops the packet has traversed. As the RREQ packet propagates through the network, each intermediate node it encounters appends its own address to the packet before rebroadcasting it, provided it hasn't seen the request previously. This process of appending and rebroadcasting continues until the RREQ packet either reaches the destination node directly or an intermediate node possessing a route to the destination in its cache.

Upon receiving the Route Request (RREQ) packet, either the destination node or an intermediate node equipped with a route to the destination initiates a response by sending a Route Reply (RREP) packet back to the source node. The RREP packet includes crucial details such as the address of the source node, the address of the destination node, a list of nodes delineating the route from the source to the destination, and a route sequence number. The route sequence number plays a pivotal role in ensuring the freshness of the route information. Intermediate nodes that intercept the RREP packet store the route information in their caches for future reference. These control packets, comprising both RREQ and RREP, are integral to the functioning of Dynamic Source Routing (DSR). They facilitate dynamic route discovery, enable adaptation to changes in network topology, and ensure the availability of up-to-date routing information throughout the network, all without the necessity for periodic routing updates.

2.2 Choosing the Dynamic Source Routing (DSR) protocol for Wireless Sensor Networks (WSNs) is justified for various reasons

In this section, the selection of the Dynamic Source Routing (DSR) protocol for Wireless Sensor Networks (WSNs) is justified based on several key factors: its ad hoc nature, source routing capability, reduced overhead, loop-free routes, flexibility, and efficient data delivery.Firstly, WSNs often operate in dynamic and ad hoc environments where node mobility and varying connectivity are common occurrences. DSR's dynamic route discovery mechanism, which occurs on-demand as data packets are transmitted, makes it well-suited for such environments(Villalba et al., 2009). This adaptive behavior allows DSR to swiftly adjust to changes in the network topology, ensuring reliable communication.Secondly, DSR minimizes routing overhead by eschewing periodic routing updates. Instead, routes are established only when necessary, thus reducing the volume of control traffic circulating in the network. This reduction in overhead is particularly advantageous in WSNs, where energy conservation is paramount, as it helps minimize energy consumption, prolonging the network's operational lifespan. Moreover, DSR employs source routing, meaning that the entire route is encapsulated within the packet header. This eliminates the need for intermediate nodes to maintain routing tables, thereby reducing memory and processing requirements. Such efficiency is highly beneficial for resource-constrained sensor nodes commonly found in WSNs (Upadhyay et al., 2016 and Kashyap et al., 2017).

Dynamic Source Routing (DSR) employs sequence numbers to ensure loop-free routing within Wireless Sensor Networks (WSNs). Each node maintains a sequence number for every route it knows about, with routes possessing higher sequence numbers being favoured. This mechanism plays a critical role in preventing routing loops and enhancing the reliability of data transmission across the network. By encapsulating the entire route within the packet header, DSR facilitates efficient data delivery without the dependence on centralized control or infrastructure. This feature is particularly advantageous in scenarios where nodes must communicate directly with each other, bypassing intermediary infrastructure nodes.DSR's inherent flexibility and adaptability further contribute to its suitability for diverse network conditions and application requirements within WSNs. It adeptly handles varying traffic patterns, node mobility, and alterations in network topology, making it well-suited for a broad spectrum of WSN applications. In summary, the dynamic nature, reduced overhead, and source routing capability of DSR make it a compelling choice for WSNs, enabling efficient and adaptive routing while mitigating resource constraints and enhancing energy efficiency (Del-Valle-Soto et al., 2014 and Rabeb et al., 2012).

2.3 The impact of Denial of service (DoS) attack over DSR Routing Protocol

A Denial of Service (DoS) attack targeting a Wireless Sensor Network (WSN) can inflict substantial damage on the network's operational integrity, performance, and dependability. The foremost impact of such an attack is the disruption of regular network operations. By inundating the network with an excessive volume of traffic, assailants can inundate sensor nodes, causing data transmission delays, packet loss, and potentially rendering the network entirely inaccessible. DoS attacks consume critical network resources like bandwidth, processing capacity, and energy. This resource depletion can impede the ability of sensor nodes to execute their designated tasks, thereby diminishing the overall efficiency of the network. The heightened network congestion resulting from a DoS attack can further deteriorate WSN performance. This degradation encompasses increased latency, diminished throughput, and compromised reliability of data transmission, all of which can adversely affect the quality of service for applications reliant on prompt and precise data delivery. DoS attacks can significantly escalate energy consumption in sensor nodes, especially if they involve processing or forwarding a substantial volume of malicious traffic. This heightened energy usage can hasten battery depletion and curtail the operational lifespan of battery-powered sensor nodes, thereby compromising the long-term sustainability of the network (Laghbi et al., 2023).

In certain instances, DoS attacks may serve as a diversionary tactic to obscure other malicious activities, such as data tampering or eavesdropping. By inundating the network with malicious traffic, attackers exploit the ensuing chaos to manipulate or intercept sensitive data transmitted within the network, jeopardizing its integrity and confidentiality. Persistent DoS attacks can also hinder the scalability of WSNs by constraining the network's capacity to accommodate additional nodes or expand its coverage area. This limitation impedes the deployment of new sensor nodes and curtails the growth potential of the network. Overall, the ramifications of a DoS attack on a WSN can be profound, disrupting network operations, compromising data integrity, depleting resources, and undermining the reliability and performance of the network. Implementing robust security measures and proactive mitigation strategies is imperative to shield WSNs against such attacks and uphold their continued functionality and efficacy (Sultan et al., 2022 and Abbas et al., 2020).

2.4 The Isolation Random Forest Algorithm

The Isolation Forest algorithm functions as an unsupervised learning technique designed to pinpoint outliers within a dataset. It capitalizes on the inherent structure of decision trees to achieve this objective. In this algorithm, observations undergo isolation via a process of random feature selection. Following this, a split value is randomly determined within the range of the chosen feature, forming a decision tree-like structure. The path length from the root to a leaf within these decision trees serves as a metric for evaluating the normalcy of a data point. Essentially, this length reflects the number of splits required to isolate a particular sample. Given that outliers are typically scarce compared to regular data points and tend to lie farther away from the main body of the data, they are expected to exhibit shorter average path lengths (Xu et al., 2023).

Consequently, by utilizing decision trees with randomized partitioning, such outliers are anticipated to be identified closer to the root of the tree. This characteristic of the Isolation Forest algorithm makes it effective in detecting outliers within a dataset. By aggregating numerous random decision trees into a forest, the Isolation Forest algorithm tends to generate shorter path lengths for outlier points. This algorithm for outlier detection operates by employing an ensemble of binary decision trees, with each tree referred to as an Isolation Tree (or iTree). Once the ensemble of iTrees, known as the Isolation Forest, is trained, the model training phase concludes. During the scoring phase, each data point undergoes evaluation by traversing through all the previously trained trees. Subsequently, an "anomaly score" is assigned to each data point based on the depth of the tree required to reach that point. This anomaly score is computed by aggregating the depths obtained from each of the iTrees. An anomaly score of -1 is assigned to anomalies, while normal points receive a score of 1. The assignment of scores is determined by the contamination parameter provided, which represents the percentage of anomalies present in the data (Lesouple et al., 2021 and Al Farizi et al., 2021).

3. REVIEW OF LITERATURE

In this section, we discuss the several notable works relevant to the proposed research in addressing security concerns within Wireless Sensor Networks (WSNs).

Cao et al. (2021) introduced a novel Identity-Based Encryption Algorithm (IIBE) aimed at simplifying the key generation process, reducing network traffic, and enhancing network security. This algorithm bridges the gap between traditional public key encryption and identity-based public key encryption by eliminating the need for a public key certificate and associated management overhead, while also addressing key escrow and key revocation challenges effectively. Zhou et al. (2016) proposed a scheme utilizing three types of nodes: Cluster Heads (CHs), Inspector Nodes (INs), and Member Nodes (MNs). INs monitor CH transmissions to safeguard clusters against selective-forwarding attacks, while CHs forward packets from MNs and other CHs. MNs transmit data packets to CHs and assess CH and IN behaviors using a reputation mechanism. The scheme introduces the concept of composite reputation value (CRV), factoring in forwarding rate, detection of malicious nodes, and surplus energy, thereby extending network lifespan by balancing energy consumption.

Haseeb et al. (2019) introduced the Energy-Aware and Secure Multi-Hop Routing (ESMR) protocol, enhancing energy efficiency and multi-hop data security using a secret sharing scheme. The protocol divides the network field into inner and outer zones, forming clusters based on node proximity. Data transmission from cluster heads to the sink node is secured using an efficient secret sharing scheme.Ourrouss et al. (2021) addressed disturbing attacks by implementing a bio-inspired trust management model combining the beta reputation system with Ant Colony Optimization (ACO). This model enhances the Dynamic Source Routing (DSR) protocol by identifying and isolating malicious nodes from participating in data packet transmission. Majumder et al. (2023) presented the CRYPTO-DSR protocol, a cryptography-based dynamic source routing protocol utilizing Johnson's algorithm for route computation and hash functions for securing data packets within nodes.

Ali et al. (2020) introduced a data security approach leveraging a modified version of the Diffie–Hellman algorithm to reduce computational and response times. This approach enhances security by generating hashes for transmitted values and undergoes thorough security analysis to assess its resilience against various attacks. Indeed, within resource-constrained WSN environments, deploying heavyweight security mechanisms like traditional cryptographic methods, key management systems, and blockchain technologies can pose significant challenges due to their computational and resource overhead. Consequently, there is a rising demand for lightweight security solutions tailored specifically to the constraints of WSN devices. Lightweight security solutions offer a balance between security and resource efficiency, rendering them suitable for deployment in WSN environments with limited processing power, memory, and energy. These solutions typically prioritize efficiency while still providing adequate protection against common security threats.

4. Proposed Method

The primary aim of this model is to detect DoS attacks in the WSN environment and forecast the future behavior of participating nodes. The proposed model consists of the following phases:

- Initial assumption and Network Deployment

- Trust evaluation or Dataset Creation
- Identification of nodes and prediction of nodes' future behaviour

4.1 Initial Assumption and Network Deployment

The WSN network consists of N nodes without a central device for assessing or validating node trustworthiness. Each node autonomously evaluates the trustworthiness of participating devices, particularly during instances of degraded network performance. Nodes in the network are resource-constrained, facing limitations in energy, size, memory, and battery capacity. Some nodes are designated as DoS nodes and intentionally integrated into the network environment. The proposed model's effectiveness is assessed exclusively in the presence of DoS nodes. It focuses on a post-authentication mechanism, enabling the model to operate over time after node deployment within the network. Each node passively observes the communication behaviour of its neighbouring nodes and maintains a trust table, storing pertinent trust-related information and status updates of other nodes in the network.

Table 1. Trust Table

Node ID	PDR	T	R	CO	CI	E	Status

In the above table,
Node ID – Denotes the node identification
PDR – Denotes Packet Delivery Ratio
T – Denotes Throughput
R - Denotes Reliability
CO – Denotes Cooperativeness
CI- Denotes Contact Intimacy
E – Energy Efficiency

4.2 Trust metrics Evaluation or Creation of Datasets

To identify or classify DoS attacks, the Isolation Forest algorithm can be utilized, for which a dataset needs to be created to serve as the training set. To accomplish this, the following trust metrics will be calculated: Packet Delivery Ratio, Throughput, Cooperation, Contact Intimacy, and Energy Efficiency. These metrics will be considered as the dataset.

4.2.1 Packet Delivery Ratio (PDR) Calculation

In the Dynamic Source Routing (DSR) protocol, both data and control packets are integral for ensuring the routing functionality in the WSN environment. Consequently, the Packet Delivery Ratio (PDR) of a node can be computed based on these two packet types. In the presence of a DoS attack, the PDR of a node might decrease. Hence, it becomes crucial to calculate the PDR considering the presence of such attacks. The PDR is determined as the ratio of successfully delivered packets (including both control and data packets) to the total number of packets sent (comprising both control and data packets), factoring in the impact of the attack. The following equation is employed to calculate the PDR: Divide the number of successfully delivered packets (both control and data packets) by the total number of packets sent (including both control and data packets), then multiply the result by 100 to obtain the percentage.

$$\mathrm{PDR}_{\mathrm{ninj}}\,(\mathrm{t}) = \frac{\text{Successful Data Packet Delivered}_{\mathrm{ninj}}}{\text{Total data Packets Sent}_{\mathrm{ninj}}}\mathrm{x}100 + \frac{\text{Successful Control Packet Delivered}_{\mathrm{ninj}}}{\text{Total Control Packets Sent}_{\mathrm{ninj}}}\mathrm{x}10 \quad (1)$$

In the above equation,

$\mathrm{PDR}_{\mathrm{ninj}}$ denotes packets delivery ratio of node j with respect to node i over the period of time t.

4.2.2 Throughput Calculation

DoS attack creates impact on Throughput of WSN environment. It is calculated as measuring the rate of successful data packet delivery between nodes. The following equation is used to measure the Throughput.

$$\mathrm{T}_{\mathrm{ninj}}\,(\mathrm{t}) = \frac{\text{Total Data Received}_{\mathrm{ninj}}}{\text{Time Interval}} \quad (2)$$

In the given equation, $\mathrm{T}_{\mathrm{ninj}}$ (t) represents the throughput of node j concerning node i over the time period t. To standardize the throughput value within the range of 0 to 1, it can be scaled by multiplying it by 100. Consequently, the revised equation is as follows:

$$.\mathrm{T}_{\mathrm{ninj}}\,(\mathrm{t}) = \frac{\text{Total Data Received}_{\mathrm{ninj}}}{\text{Time Interval}}\ \mathrm{X}\ 100 \qquad (3)$$

4.2.3 Reliability Calculation

Reliability ensures a node's ability to uphold its functionality and facilitate data transmission even in the presence of a DoS attack. This metric is deemed essential because the occurrence of a DoS attack may lead to performance deterioration and potential disruption in the WSN environment. Reliability can be influenced by two factors: Packet Delivery Ratio (PDR) and Node Availability. The equation used to compute node reliability is as follows:

$$\mathrm{R}_{\mathrm{ninj}}\,(\mathrm{t}) = \mu_{\mathrm{PDR}} \times \mathrm{PDR}_{\mathrm{ninj}}\,(\mathrm{t}) + \mu_{\mathrm{Availablity}} \times \text{Node\_Availablity}_{\mathrm{ninj}}\ (\mathrm{t}) \qquad (4)$$

In the above equation, the notation $\mathrm{R}_{\mathrm{ninj}}$ (t) denotes the reliability of node j concerning node i over the time period t. $\mathrm{PDR}_{\mathrm{ninj}}$ (t)denotes the Packet Delivery Ratio of node j concerning node i over the time period t. μ_{PDR} and $\mu_{\mathrm{Availablity}}$ represent weights assigned to each metric, reflectng their significance in determining reliability. During a DoS attack, nodes may encounter increased packet loss, reduced availability, and heightened susceptibility to malicious activities. Hence, the reliability formula may require additional factors or adjustments to accommodate these effects. These weights can be customized based on network requirements and priorities. The Packet Delivery Ratio can be computed using Equation 1. Node availability refers to the percentage of time a node remains operational and accessible for communication within the network. It can be calculated using the subsequent formula:

$$\text{Availability}_{\mathrm{ninj}}\,(\mathrm{t}) = \frac{\text{Time node is operational}_{\mathrm{ninj}}}{\text{Total observed time}_{\mathrm{ninj}}}\mathrm{x}100 \qquad (5)$$

In the provided equation, $\text{Availability}_{\mathrm{ninj}}$ (t) denotes the availability of node j concerning node i over the time period t. The calculated availability will then be substituted into Equation 4, while Equation 1 will also be substituted, thereby obtaining the reliability of a node.

4.2.4 Cooperation Calculation

This metric ensures whether a node have an ability to cooperate efficiently with others nodes in the environment though adversarial conditions. Therefore, it is refers to the willingness of a nodes to forwarding messages, share resources with other nodes and participate in all the network activities towards to attain a common goal. These things will be happen only if the node is not affected by any kind of attack. Packet forwarding Ratio will determine the cooperation of a node. If cooperation of a node is good, it can capable to share resources with other nodes, forwarding data, collaborate with other nodes to achieve a certain goal. The following equation is used to calculate the cooperation of a node.

$$\mathrm{Co}_{\mathrm{ninj}}\,(\mathrm{t}) = \frac{\text{Packet Forwarding Ratio}_{\mathrm{ninj}}}{\text{Max\_Packet Forwarding Ratio}_{\mathrm{ninj}}}\mathrm{x}100 \qquad (6)$$

$\mathrm{Co}_{\mathrm{ninj}}$ denotes cooperation of node j with respect to node i over the period of time t. The notation $\text{Packet Forwarding Ratio}_{\mathrm{ninj}}$ denotes the packet delivery ratio of node j concerning node i over the time period t, which can be obtained from Equation 1. $\text{Max\_Packet Forwarding Ratio}_{\mathrm{ninj}}$ denotes the maximum packet delivery ratio of node j concerning node i over the time period t.

4.2.5 Contact intimacy Calculation

The contact intimacy of a node can be determined by analyzing two metrics: the communication behavior and connectivity pattern of nodes. This concept denotes the intensity and frequency of interactions between two nodes. In the event of a DoS attack, these factors may be disrupted. An equation is employed to quantify the contact intimacy of nodes.

$$\mathrm{CI}_{\mathrm{ninj}}\,(\mathrm{t}) = \frac{\mathrm{W}_{\mathrm{L}}\mathrm{XL}_{\mathrm{ninj}} + \mathrm{W}_{\mathrm{D}}\mathrm{XD}_{\mathrm{ninj}}}{\text{Max Possible values}_{\mathrm{ninj}}} \qquad (7)$$

In the provided equation, $\mathrm{CI}_{\mathrm{ninj}}$ (t) signifies the contact intimacy of node j concerning node i over the duration of time t. W_{L} and W_{D} are weights attributed to the quantity of communication links and session duration, respectively. These weights indicate the relative significance of each metric in determining contact intimacy. $\mathrm{XL}_{\mathrm{ninj}}$ denotes the total count of communication links established by the node, while $\mathrm{XD}_{\mathrm{ninj}}$ represents the total duration of communication sessions involving the node. The maximum achievable value is the sum of the products of the weights and the corresponding maximum values of XL and XD. This computation can be carried out using the following equation.

$$\text{Maximum Possible Values}_{\mathrm{ninj}}\ (\mathrm{t}) = \mathrm{W}_{\mathrm{L}}\,\mathrm{X}\ \mathrm{Max}_{\mathrm{Links}} + \mathrm{W}_{\mathrm{D}}\,\mathrm{X}\ \mathrm{Max}_{\mathrm{Duration}} \qquad (8)$$

The value calculated above will be substituted into Equation 7 to determine the contact intimacy of node j in relation to node i.

4.2.6 Energy Level Calculation

To calculate the energy level of a node amidst a Denial of Service (DoS) attack, it is necessary to account for the node's energy consumption pattern and any alterations or disturbances induced by the attack. A prevalent method involves monitoring the node's energy usage throughout a defined timeframe and adapting it according to the attack's repercussions. The ensuing equation serves to compute the energy level of a node.

$EE_{ninj}\,(t) = Energy_{Initial} - Energy_{Consumed} + Adjusment_{ninj}$ (9)

The energy efficiency level of node j with respect to node i, denoted as $EE_{ninj}\,(t)$, is determined by considering the initial energy level of the node, denoted as $Energy_{Initial}$, and the energy consumed by the node during the observation period, denoted as $Energy_{Consumed}$. In the formula for calculating the final energy level of a node in the presence of a DoS attack, adjustments are made to accommodate deviations in energy consumption caused by the attack. To calculate these adjustments, it is essential to take into account the specific effects of the DoS attack on the node's energy consumption pattern. The subsequent equation is utilized for this adjustment calculation.

$Adjusment_{ninj} = Attack\_Impact_{ninj} \times Energy\_Consumption_{ninj}$ (10)

Attack Impact $_{ninj}$ denotes the influence of the DoS attack on energy consumption. This could be expressed as a scalar value or a function that encapsulates the severity or magnitude of the attack's impact on energy usage. Determining Attack_Impact $_{ninj}$ involves considering several factors, including the type and intensity of the DoS attack, the node's vulnerability to the attack, and the characteristics of the network environment. Energy_Consumption $_{ninj}$ represents the energy consumed by the node during the observation period.

The determination of the Attack_Impact term relies on various factors, such as the type and intensity of the DoS attack, the node's vulnerability, and the network environment. It can be derived from empirical observations, simulation studies, or analytical models that quantify the attack's influence on energy consumption. Calculating the Attack_Impact involves assessing the severity or magnitude of the DoS attack's impact on energy consumption. The specific formula for this calculation depends on factors like the attack's characteristics, the node's behavior, and the network environment. The following formula is employed for calculating the Attack_Impact.

$Attack\_Impact_{ninj} = \int \quad (Metric1, Metric2, \dots, Metric\ n)$ (11)

Where, Metric1, Metric2, ..., Metric n are the normalized metrics that characterize various facets of the attack's influence on energy consumption. ∫ is a function employed to aggregate and merge the normalized metrics, facilitating the computation of the comprehensive attack impact.

4.3 Identification of DoS attack

After computing the trust metrics, the final trust score of individual nodes can be determined using the following equation.

$T_{ninj} = \mu_1 PDR_{ninj} + \mu_2 T_{ninj} + \mu_3 CO_{ninj} + \mu_4 CI_{ninj} + \mu_5 EE_{ninj}$ (12)

Where, $\mu_1, \mu_2, \mu_3, \mu_4, \mu_5$ are weighting factors.

$\mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 = 1$ and i≠j, i,j=1,2,3,4.....

PDR_{ninj} denotes Packet Delivery Ratio, T_{ninj}

denotes throughput, CO_{ninj} denotes cooperation

CI_{ninj} denotes contact intimacy and EE_{ninj} denotes energy efficiency.

Subsequently, classification can be executed based on the final trust value, employing the following equation.

$\text{if } T < th, \text{DoS attack}$ (13)$\text{if } T \geq th, \text{Geniune node}$

In the provided equation, 'th' represents the threshold value, which can be determined by the user. Upon identifying the node, the status of the node will be updated in the trust table.

Then, the following algorithm will be used to predict the future behaviour of a node with the help of Isolation Forest Algorithm.

Algorithm 1. The proposed model

Input: Dataset comprising trust metrics (Reliability, Contact Intimacy, Cooperation, Energy Consumption, Throughput) for each node and Labels indicating the presence or absence of a Denial-of-Service (DoS) attack for each node.

Output: Classification of nodes as affected by a DoS attack or not, leveraging the Isolation Forest algorithm.

```
Begin
    If (Performance of WSN is satisfied) then
        No need of executing the proposed model
    else
        for (Every node ni evaluates every other node nj)
            Read : Data and Control Packet Delivery Ratio
            Calculate: Packet Delivery Ratio (PDR)
            Read:  Total data received and Time Interval
            Calculate : Throughput
            Read: Node's Availability and PDR
            Calculate: Reliability
            Read: Packet Forwarding Ratio and Maximum Forwarding Ratio
            Calculate: Cooperation Index
            Read: Communication Links, Session Duration and Maximum Possible Values
            Calculate : Contact Intimacy
            Read:  Initial Energy Level, Energy Consumption and Adjustment
            Calculate : Energy Consumption
        End if
    Data Preparation: Collect the dataset containing the calculated trust metrics (Throughput, Reliability, Cooperation, Contact Intimacy and Energy Consumption) and corresponding labels.
    Feature Selection: Determine the trust metrics to be utilized in the analysis based on their relevance and domain expertise.
    Model Training: Train an Isolation Forest model using the dataset containing trust Metrics and configure model parameters such as the number of trees in the forest and the maximum depth of each tree.
    Scoring: Assign a score to each node in the dataset using the trained Isolation Forest model and compute an anomaly score for each node based on its trust metric values.
    Threshold :Apply a threshold to the anomaly scores to classify nodes as impacted by a DoS attack or not. Nodes with anomaly scores below the threshold may be identified as experiencing a DoS attack, while those above the threshold may be considered unaffected.
    Prediction: Utilize the trained model to predict whether new nodes are undergoing DoS attacks based on their trust metric values.
    End
End
```

5. A Proof of Concept: A Mathematical Example

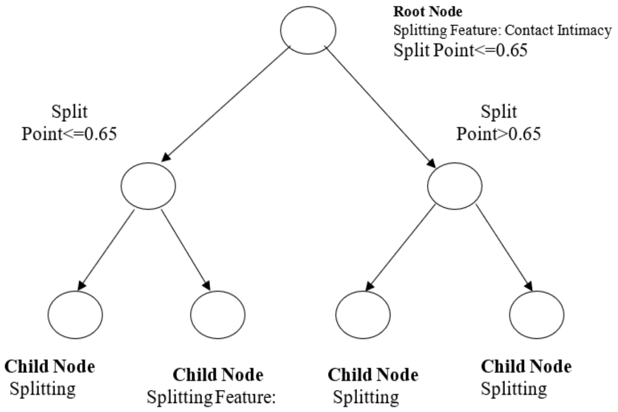
To predict the future behaviour of the node, with the help of Isolation Forest algorithm, the calculated trust metrics can be considered as data sets and the status of a node i.e whether node as DoS or not is also specified. Assume a simplified example with a small dataset and each node in a Wireless Sensor Network (WSN), along with labels indicating whether each node is experiencing a DoS attack or not:

Table 2. Sample Dataset

Node	Reliability	Contact Intimacy	Cooperation	Energy Consumption	Throughput	DoS Attack
1	0.95	0.75	0.80	0.60	0.70	Yes
2	0.85	0.60	0.70	0.55	0.65	No
3	0.90	0.80	0.75	0.65	0.75	Yes
4	0.80	0.70	0.65	0.50	0.60	No
5	0.75	0.85	0.70	0.70	0.80	No
6	0.88	0.65	0.60	0.45	0.55	Yes
7	0.82	0.72	0.68	0.58	0.63	No
8	0.92	0.78	0.72	0.63	0.68	Yes

Now, we will proceed to illustrate the algorithm steps using mathematical examples.

1. Data Preparation:
   - We gather the dataset and arrange it in a tabular format as demonstrated above.
2. Feature Selection (Optional):
   - Let's opt to include all trust metrics in our analysis.
3. Model Training:
   - We train an Isolation Forest model on the dataset. To simplify, let's construct a forest comprising 3 trees and set a maximum depth of 3 for each tree.
4. Scoring:
   - Each node is scored using the trained Isolation Forest model, generating anomaly scores based on their trust metric values.
   - For instance, let's compute the anomaly scores for nodes 1 and 2:
     - Node 1: Anomaly Score = 0.6 (example value)
     - Node 2: Anomaly Score = 0.8 (example value)
5. Thresholding (Optional):
   - We may establish a threshold, such as 0.7, to classify nodes as either experiencing a DoS attack or not.
   - Nodes with anomaly scores below the threshold (e.g., 0.7) might be designated as encountering a DoS attack, while those surpassing the threshold could be deemed normal.
6. Evaluation (Optional):
   - The model's performance is assessed using metrics like accuracy, precision, recall, and F1-score. This involves comparing the model's predictions against the ground truth labels to gauge its efficacy in detecting DoS attacks.
7. Prediction:
   - Utilizing the trained model, we can predict whether new nodes in the WSN are undergoing DoS attacks based on their trust metric values.



In this diagram, the root node initiates the split based on the feature "Contact Intimacy" with a split point of "<= 0.65". Two branches stem from the root node, denoting the resulting child nodes from the split. Each branch is marked with the condition for reaching that node. Rectangles at the end of each branch represent the child nodes. Within each child node, the splitting feature and chosen split point are indicated. This recursive process continues for each child node until individual data points are isolated or a stopping criterion is met. Leaf nodes depict individual data points or subsets of data points isolated by the tree. Optionally, leaf nodes may be labeled with the corresponding data point or subset. Distinct colors or shading can be applied to differentiate between normal and anomaly (DoS attack) data points if desired. Next we calculate the path length hence assume, Contact Intimacy: 0.6, Cooperation: 0.7 Energy Consumption: 0.55,

To calculate the path length for this data point:

1. Begin at the root node.
2. Move to the left child node as the value of "Contact Intimacy" (0.6) is less than or equal to the split point (0.65).
3. As this node is a leaf, the path length is 1, as we have traversed a single edge.

The path length for this data point is 1.

Repeat this process for each data point in the dataset to calculate the path length for all data points in the isolation tree. The path length represents the depth of the leaf node reached during traversal and can be used as a measure of anomaly score in isolation forest anomaly detection algorithms.

Now, let's elaborate on how we computed the anomaly score for data point 1 (Node 1) using the Isolation Tree:

- Traverse Data Point 1 Through the Isolation Tree:
    - Starting from the root node, we assess the splitting condition based on the feature "Contact Intimacy" for data point 1 (0.75).
    - As 0.75 is less than or equal to the split point (0.65) at the root node, we proceed to the left child node.
    - Upon reaching the left child node, we encounter a leaf node, indicating that the path length for data point 1 in this tree is 2 (the number of edges traversed from the root node to the leaf node).
- Anomaly Score Calculation:
    - Given that we have only one tree in this example, the anomaly score for data point 1 is simply the path length (2).
- We iterate through this procedure for every data point, guiding them through the isolation tree and determining their individual path lengths to derive the anomaly score for each. Elevated anomaly scores suggest a higher likelihood of a data point being an outlier or anomaly.
- To forecast whether a new node signifies a DoS attack or not given the provided context and the computed anomaly scores, we can adopt a threshold-based method. We establish a threshold value; data points surpassing it are categorized as DoS attacks, while those falling below it are classified as non-DoS attacks.

Let's consider that we've computed the anomaly scores for the dataset using the isolation forest algorithm, presented as follows:

Table 3. Anomaly Score Calculation

Node	Anomaly Score
1	2.5
2	1.5
3	2.5
4	1.5
5	1.5
6	2.5
7	1.5
8	2.5

Now, let's imagine we've set a threshold value of 2.0. Any data point with an anomaly score greater than or equal to this threshold will be categorized as a DoS attack, while any data point with an anomaly score below this threshold will be deemed not a DoS attack.

Let's forecast whether a new node is a DoS attack or not based on this threshold:

- New Node: Assume we have a new node with an anomaly score of 2.2.
- Threshold Comparison: As the anomaly score (2.2) exceeds the threshold (2.0), the new node is labeled as a DoS attack.

This classification process can be succinctly expressed mathematically:

- Let Anomaly ScorenewAnomaly Scorenew represent the anomaly score of the new node.
- Let ThresholdThreshold denote the predefined threshold value.
- If Anomaly Scorenew≥ThresholdAnomaly Scorenew≥Threshold, then classify the new node as a DoS attack; otherwise, classify it as not a DoS attack.

In our scenario, since the anomaly score of the new node (2.2) surpasses the threshold (2.0), it is identified as a DoS attack.

This threshold-based strategy offers a straightforward approach to predicting whether a new node is a DoS attack or not, relying on the anomaly scores computed using the isolation forest algorithm. Adjusting the threshold permits us to manage the classification model's sensitivity to various anomaly levels.

```
 if AnomalyScore_new >= Threshold:
 return "DoS Attack"
 else:
return "Not a DoS Attack"
```

6. Simulation Results and Discussion

To evaluate the performance of the proposed model against traditional DSR routing protocol and the protocol proposed by Dharini N et al. (2020), a simulation was conducted using the NS3 Simulator tool. The simulation utilized the following parameters:

- Total duration of simulation: 1000 seconds
- Maximum number of nodes: 100 nodes
- Incremental placement of blackhole nodes: 10%, 20%, ..., 80%

These parameters were chosen to comprehensively assess the effectiveness of the proposed model in mitigating the impact of DoS attacks across different proportions of DoS nodes within the network. By incrementally increasing the percentage of DoS nodes, the simulation provides insights into how the proposed model performs under escalating threat levels.

During the simulation, the proposed model was compared against both traditional RPL routing protocol and the protocol proposed by Dharini N et al. (2020). Various performance metrics, including packet delivery ratio, packet loss, end-to-end delay, detection accuracy, and routing overhead, were analyzed to evaluate the effectiveness of the proposed model in detecting and mitigating DoS attacks while ensuring efficient network operation.

Table 4. Simulation Parameters

Simulation Parameters	
Traffic type	Constant Bit Rate (CBR)
Propagation model	Nakagami Model
Mobility model	Random Waypoint
MAC type	802.11
Mode of channel	Wireless
Data payload	512 bytes/packet
Simulation area	1000mx1000m
Nodes’ speed	5-10 – 15 – 20-25 (m/s)
Data rate	10.4Mbps
Threshold	0.5

Packet Dropping Ratio Analysis

Figure 3 illustrates the impact of DoS on the packet dropping ratio within the WSN environment. It is evident from the graph that there exists a clear correlation between the number of DoS attacks and the packet dropping ratio, with a noticeable increase in the dropping ratio as the proportion of DoS attacks escalates over time. This trend persists consistently across regular intervals, highlighting the detrimental effect of DoS attacks on network performance.

The traditional DSR protocol, lacking a built-in security mechanism to detect and mitigate black hole attacks, demonstrates vulnerability to such malicious activities. Consequently, the absence of robust security measures within the DSR protocol contributes to the observed rise in the packet dropping ratio in the presence of DoS nodes. This visualization underscores the critical need for enhanced security mechanisms within WSN networks to counter the threat posed by DoS attacks. By implementing effective detection and mitigation strategies, WSN environments can alleviate the impact of DoS nodes and uphold optimal network performance and reliability.

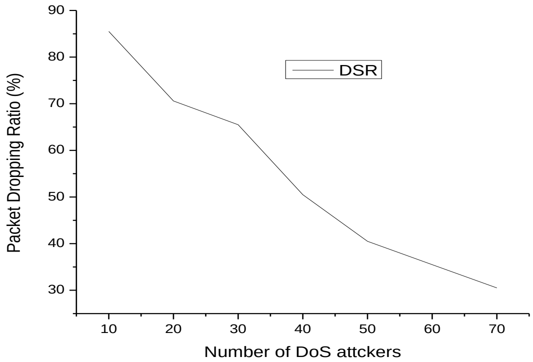


Figure 3. Influence of DoS attckers under normal DSR routing protocol

Packet delivery ratio analysis vs DoS attackers

Figure 4 illustrates the correlation between the packet delivery ratio and the occurrence of DoS attacks within the WSN environment. The analysis involves monitoring changes in the packet delivery ratio as the number of DoS nodes increases periodically. The depicted figure clearly demonstrates that the packet delivery ratio achieved by the proposed model surpasses that of the two existing models under consideration. Even as the quantity of DoS attacks escalates at regular intervals, the packet delivery ratio remains significantly higher when employing the proposed model compared to the traditional DSR routing protocol and the model proposed by Dharini et al. (2020).

This observation highlights the effectiveness of the proposed model in mitigating the impact of DoS on packet delivery within the WSN network. By incorporating advanced detection and mitigation techniques such as trust metrics and the Isolation Forest algorithm, the proposed model exhibits superior performance in maintaining a high packet delivery ratio despite the presence of DoS attacks.

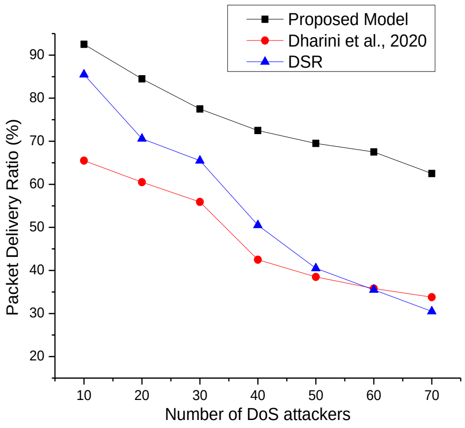


Figure 4. Packet Delivery Ratio vs % of DoS attackers

The proposed model integrates various Quality of Service (QoS) metrics, including Packet Delivery Ratio (PDR), Trust (T), Connectivity (CO), Contact Intimacy (CI), and Energy Efficiency (EE), to evaluate the reliability of participating devices within the WSN network. By utilizing Isolation Forest support, the model can identify and eliminate DoS devices, thus improving the overall packet delivery ratio. In contrast, the model proposed by Dharini et al. (2020) relies solely on packet count, energy, and Z-score as metrics to assess device trustworthiness. Due to this limited measurement approach, the delivery ratio achieved by the Dharini et al. (2020) model is lower compared to the proposed model but higher than that of the traditional DSR routing protocol. It is important to note that the traditional DSR protocol lacks inherent security mechanisms, resulting in a significantly lower packet delivery ratio compared to the other two models.

The incorporation of multiple QoS metrics and Isolation Forest support in the proposed model enables a more comprehensive evaluation of device reliability and facilitates the detection and mitigation of black hole devices. This holistic approach enhances the overall performance and security of the WSN network by effectively addressing various threats and vulnerabilities.

End to End delay analysis vs DoS attackers

Figure 5 illustrates the analysis of average delay versus the presence of DoS nodes within the WSN network. As the number of nodes increases, the proposed model demonstrates shorter delays compared to the other two models under consideration. This improvement in delay performance can be attributed to the inherent characteristics of the proposed model. By primarily consisting of trusted nodes and effectively removing DoS attacks through trust and Isolation Forest mechanisms, the proposed model ensures a network environment characterized by enhanced reliability and efficiency. The absence of DoS nodes significantly contributes to the reduction in delays experienced during packet transmission and routing processes. In contrast, the traditional DSR protocol lacks robust security mechanisms, rendering it susceptible to attacks, including DoS. Consequently, the presence of DoS within the DSR-based WSN network leads to increased delays, stemming from retransmissions and other network disruptions caused by malicious activities.

In the model proposed by Dharini et al. (2020), the weaker trust assessment methodology permits the possibility of DoS infiltrating the network. This results in longer delays compared to the proposed model but shorter delays compared to the DSR routing protocol. However, the delays observed in the Dharini et al. (2020) model are still inferior to those achieved by the proposed model due to its comprehensive trust assessment and mitigation strategies against DoS attacks. Overall, the analysis underscores the importance of robust security mechanisms in mitigating delays and ensuring efficient operation within WSN networks, emphasizing the effectiveness of the proposed model in achieving superior delay performance Through enhanced trust and security measures.

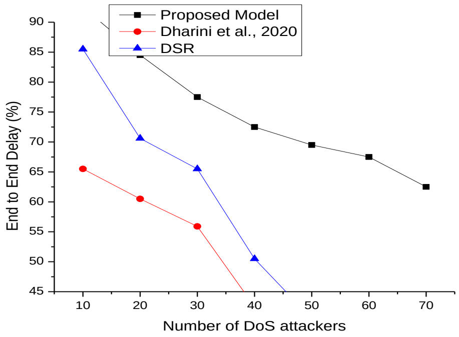


Figure 5. Average delay vs % DoS attacker

Routing overhead vs DoS attackers

Figure 6 illustrates the relationship between routing overhead and DoS attacks within the WSN network. It is evident from the figure that the routing overhead associated with the proposed model is lower compared to the other two models. This reduction in routing overhead can be attributed to the effective identification and elimination of DoS nodes facilitated by the proposed model. By employing robust trust evaluation mechanisms and Isolation Forest support, the proposed model ensures the smooth flow of routing-related information without encountering disruptions caused by DoS attacks. Consequently, the routing overhead is minimized in the suggested model, leading to more efficient network operation.

In contrast, in the model proposed by Dharini et al. (2020), where trust evaluation is weaker, the presence of DoS nodes results in routing issues such as packet dropping and retransmissions. These disruptions contribute to higher routing overhead compared to the proposed model. Similarly, in the DSR protocol, the lack of security measures also leads to routing-related issues, including packet drops and inefficient route discovery processes. Consequently, the routing overhead in the DSR protocol is higher compared to the proposed model. Overall, the reduction in routing overhead observed in the proposed model highlights the effectiveness of its security mechanisms in mitigating the impact of DoS attacks and ensuring efficient routing within the WSN network. By enhancing trust evaluation and incorporating advanced detection techniques, the proposed model achieves superior performance in terms of routing overhead compared to existing models.

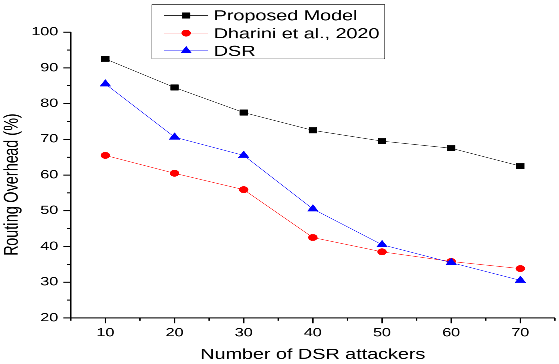


Figure 6. Routing overhead vs % of DoS attackers

Detection accuracy vs DoS attackers

Figure 7 illustrates the relationship between detection accuracy and the presence of DoS nodes within the WSN network. It is evident from the figure that the detection accuracy of the proposed model is notably high compared to the other two models. This superior detection accuracy in the proposed model can be attributed to the implementation of multiple trust evaluations combined with Isolation Forest techniques. These sophisticated mechanisms enable the accurate prediction of future behavior, allowing the proposed model to effectively identify and mitigate DoS attacks with a high degree of accuracy. In contrast, the lower detection accuracy observed in the model proposed by Dharini et al. (2020) can be attributed to its poor trust evaluation mechanism. The weaker trust assessment methodology employed in this model results in suboptimal detection capabilities, leading to lower accuracy in identifying black hole nodes.

Similarly, the traditional DSR protocol exhibits poor detection accuracy compared to the other two models due to the absence of dedicated detection features within the protocol itself. Without robust detection mechanisms, the DSR protocol lacks the capability to accurately identify and mitigate DoS attacks, resulting in lower detection accuracy compared to the proposed model and the Dharini et al. (2020) model. Overall, the high detection accuracy achieved by the proposed model underscores the effectiveness of its advanced trust evaluation and detection techniques in safeguarding the WSN network against DoS attacks. By leveraging these capabilities, the proposed model ensures superior performance in detecting and mitigating security threats compared to existing models.

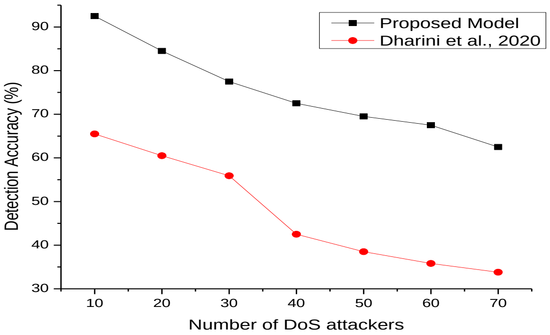


Figure 7. Detection Accuracy vs % of DoS attackers

7. CONCLUSION

In conclusion, this paper presents a novel approach utilizing the Isolation Forest algorithm for the classification of Denial of Service (DoS) attacks in Wireless Sensor Networks (WSNs). The distributed and resource-constrained nature of WSNs makes them vulnerable to security threats, necessitating effective detection and mitigation strategies for ensuring reliable operation. By leveraging trust metrics such as reliability, contact intimacy, cooperation, energy consumption, and throughput, our proposed method constructs datasets to analyze network behavior. The Isolation Forest algorithm effectively identifies anomalies indicative of DoS attacks by distinguishing normal network behavior from malicious activities. Experimental results demonstrate the efficacy of our approach in accurately detecting DoS attacks with minimal false positives, as evidenced by a mathematical model.

For future work, we intend to explore several avenues to further improve the proposed approach. Firstly, we plan to investigate the scalability of the Isolation Forest algorithm to handle larger WSNs with an increased number of nodes and more complex network topologies. Additionally, we aim to enhance the accuracy of DoS attack detection by incorporating additional trust metrics or exploring alternative machine learning algorithms. Furthermore, we will explore the integration of anomaly detection techniques with intrusion prevention mechanisms to provide real-time response capabilities to detected attacks. Finally, we will evaluate the proposed approach in real-world WSN deployments to assess its practical applicability and performance in diverse operating environments. Overall, these future directions aim to advance the state-of-the-art in WSN security and contribute to the development of robust and resilient sensor network systems.

REFERENCES

[1] Dharini, N., Duraipandian, N. & Katiravan, J. ELPC-Trust Framework for Wireless Sensor Networks. Wireless Pers Communication 113, 1709–1742(2020). https://doi.org/10.1007/s11277-020-07288-0

[2] Cao, ChunHua, et al. “IIBE: an improved identity-based encryption algorithm for WSN security.” Security and Communication Networks 2021 (2021): 1-8.

[3] Zhou, Hai, et al. “A security mechanism for cluster-based WSN against selective forwarding.” Sensors 16.9 (2016): 1537.

[4] Haseeb, Khalid, et al. “Secret sharing-based energy-aware and multi-hop routing protocol for WSN based WSNs.” IEEE Access 7 (2019): 79980-79988.

[5] Ourouss, Kaoutar, Najib Naja, and Abdellah Jamali. “Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol.” Wireless Personal Communications 116 (2021): 207-226.

[6] Majumder, Sayan, Debika Bhattacharyya, and Subhalaxmi Chakraborty. “Mitigation of Sybil Attack in Mobile Ad Hoc Network Using CRYPTO-DSR: A Novel Routing Protocol.” International Journal of Intelligent Systems and Applications in Engineering 11.4 (2023): 281-288.

[7] Ali, Shahwar, et al. “An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks.” International journal of distributed sensor networks 16.6 (2020): 1550147720925772.

[8] Anand, C., and N. Vasuki. “Trust based DoS attack detection in wireless sensor networks for reliable data transmission.” Wireless Personal Communications 121.4 (2021): 2911-2926.

[9] Jinhui, Xie, et al. “Intrusion detection system for hybrid DoS attacks using energy trust in wireless sensor networks.” Procedia computer science 131 (2018): 1188-1195.

[10] Kodali, Ravi Kishore, and SreeRamya Soratkal. “Trust model for WSN.” 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). IEEE, 2015.

[11] Pang, Baohe, et al. “A malicious node detection strategy based on fuzzy trust model and the abc algorithm in wireless sensor network.” IEEE wireless communications letters 10.8 (2021): 1613-1617.

[12] Awan, Saba, et al. “Blockchain based secure routing and trust management in wireless sensor networks.” Sensors 22.2 (2022): 411.

[13] Bangotra, Deep Kumar, et al. “A trust based secure intelligent opportunistic routing protocol for wireless sensor networks.” Wireless Personal Communications 127.2 (2022): 1045-1066.

[14] Das, Rahul, and Mona Dwivedi. “Cluster head selection and malicious node detection using large-scale energy-aware trust optimization algorithm for HWSN.” Journal of Reliable Intelligent Environments (2023): 1-17.

[15] Johnson, David B., and David A. “Maltz. Dynamic source routing in ad hoc wireless networks.” Mobile computing (1996): 153-181.

[16] Johnson, David B., David A. Maltz, and Josh Broch. “DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks.” Ad hoc networking 5.1 (2001): 139-172.

[17] Villalba, Luis Javier García, et al. “Routing protocols in wireless sensor networks.” Sensors 9.11 (2009): 8399-8421.

[18] Upadhyay, Raksha, Uma Rathore Bhatt, and Harendra Tripathi. “DDOS attack aware DSR routing protocol in WSN.” Procedia Computer Science 78 (2016): 68-74.

[19] Kashyap, Vikash Kumar, et al. “Comparative study of AODV and DSR routing protocols in wireless sensor network using NS-2 simulator.” 2017 international conference on computing, communication and automation (ICCCA). IEEE, 2017.

[20] Del-Valle-Soto, Carolina, et al. "On the MAC/Network/Energy performance evaluation of wireless sensor networks: Contrasting MPH, AODV, DSR and ZTR routing protocols." Sensors 14.12 (2014): 22811-22847.

[21] Rabeb, Faleh, et al. "An Extensive Comparison among DSDV, DSR and AODV Protocols in wireless sensor network." International Conference on Education and e-Learning Innovations. IEEE, 2012.

[22] Laghbi, Hassan, Saad Alateef, and Nigel Thomas. "The Impact of Resource DoS and Propagation Loss on VANET Routing." 39 th Annual UK Performance Engineering Workshop. 2023.

[23] Sultan, Mohamad T., Hesham El Sayed, and Manzoor Ahmed Khan. "Performance Analysis of the Impact of DDoS Attack on Routing Protocols in Infrastructure-less Mobile Networks." 2022 5th International Conference on Communications, Signal Processing, and their Applications (ICCSPA). IEEE, 2022.

[24] Abbas, Sohail, et al. "Survivability Analysis of MANET Routing Protocols under DOS Attacks." KSII Transactions on Internet and Information Systems (TIIS) 14.9 (2020): 3639-3662.

[25] Xu, Hongzuo, et al. "Deep isolation forest for anomaly detection." IEEE Transactions on Knowledge and Data Engineering (2023).

[26] Lesouple, Julien, et al. "Generalized isolation forest for anomaly detection." Pattern Recognition Letters 149 (2021): 109-119.

[27] Al Farizi, Wahid Salman, Indriana Hidayah, and Muhammad Nur Rizal. "Isolation forest based anomaly detection: A systematic literature review." 2021 8th International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE). IEEE, 2021.