RESEARCH PAPER

Revolutionizing Data Communication: A Secure and Efficient Inter-Channel Framework with Multi-Regional Detection Approach

Sushma P. Pawale[1*] and Dr. Poornima G Patil[2]

[1*]*Research Scholar, Department of CSE, Visvesvaraya Technological University, Belagavi-590018, Karnataka, India*
[2]*Assistant Professor, Department of CSE, Visvesvaraya Technological University, Belagavi-590018, Karnataka, India*
[*]***Corresponding Author:*** *sushmap9feb@gmail.com*

Received: 24th April, 2026; Revised: 20th May 2026; Accepted: 30th June, 2026; Available Online: 10th July, 2026

ABSTRACT
Wireless sensor networks (WSN) pose significant security risks, as they are vulnerable to attacks at every network layer, making them crucial for network protection. The constrained resources of sensor nodes pose significant challenges, necessitating the development of energy-efficient and secure communication protocols. Localization technology is crucial in WSNs, but advancements have led to increasing security issues, such as Sinkhole attacks, selective forwarding attacks, wormhole attacks, malicious attacks, etc. This paper addresses the critical issue of achieving both energy efficiency and security in WSNs. The proposed framework ensures the confidentiality, integrity, and authenticity of data while minimizing energy consumption. To create a safe network environment, the suggested framework makes use of a novel Inter-Channel Data Communication Algorithm and a fault-tolerant data transfer mechanism. To ensure high separation, the algorithm chooses non-sequential cluster heads based on the Davies-Bouldin function and mean frequency. Initiating communication among nodes involves taking into account the cluster heads' level of trust, which is estimated by utilizing the beta distribution and signal arrival time. The process is streamlined and the load of trust checks for all nodes is lessened because the mean trust value barrier is met. The probable malicious nodes are identified using circular concentric frequency mapping and clone authentication in a multi-region detection approach. To look for suspicious activity in non-collinear neighborly nodes, an adaptive threshold function based on reputation is employed.

Keywords: Wireless sensor networks; Security; Clustering; Trust; Cluster Head Selection; circular concentric frequency mapping.

How to cite this article: Pawale SP, Patil PG, Revolutionizing Data Communication: A Secure and Efficient Inter-Channel Framework with Multi-Regional Detection Approach. Int J Drug Deliv Technol. 2026;16(7):603-631. DOI: 10.25258/ijddt.16.7.65
Source of support: Nil.
Conflict of interest: None

1. INTRODUCTION

WSNs are extremely useful in a different platforms, comprising environmental monitoring, target tracking, health monitoring, as well as different maintenance tasks [1]. Security is crucial when using WSNs for a variety of uses [2]. However, in wireless sensor networks, both prevention and identification of malicious attacks may be high or poor [3]. Numerous attacks, including wormholes [4], sinkholes [5], Sybil [6], sleep [7], and selective forward assaults [8], have been seen in Sensor Network. Numerous academics have acknowledged their infrastructure, which consists of movable devices used in various trade activities using decentralized and scalable methods.

WSNs are subject to errors and malicious attacks due to their limited resources and use in hostile situations. The base station may get inaccurate or misleading data from the damaged or impacted sensor nodes. To lower system performance, hostile nodes in the network will maliciously delete packets, alter their contents, and delay data transfer [9]. These kinds of attacks shorten the lifespan of the network, cast doubt on the veracity of the data, cause the fault-tolerant routing system to malfunction, and lower energy levels [10]. Serious attacks against routing protocols could include injecting malicious or incorrect routing information into a network, which would result in packet losses or delays from routing disputes. Numerous strategies, including information correlation across numerous nodes and encryption, have been put forth to prevent routing attacks [11]. The term "faulty nodes" refers to nodes that malfunction or malfunction-related abnormalities in operation. The term "malicious nodes" refers to the opposite category, which consists of compromised nodes. Among these threats include distributed denial of service (DDoS), challenge collapsar, fake data injection (FDI), and witch assaults [12]. Designing an effective and energy-efficient malicious node detection approach is crucial since the detection and defence of malicious nodes are severely limited by factors like the environment and energy usage [13]. Therefore, in order to guarantee that the networks operate dependably, it is essential to precisely and quickly identify malicious and malfunctioning nodes.

In general, there is no unified master node in the social and defense networks to oversee communication among network nodes. According to peer-to-peer

**Author for Correspondence: sushmap9feb@gmail.com*

network research, these networks display virtual networks coventry existence or network logical functionalities, i.e., networks constructed on top of other networks, similar to the Internet [14]. The structure of a network node is often determined by its logical ID. The majority of wireless sensor networks are made up of smaller infrastructure or non-infrastructure networks. WSN nodes are not part of static infrastructure, which can include base stations, gateways, access points, single-hop, and multi-hop communication [15]. The majority of recent research has been on encryption and RSSI methods as safeguards against malicious attacks and the remaining answers accounted for artificial intelligence and encryption hybrid techniques, however there exists issues related to security and fault tolerance in malicious attacked network. Hence there is a need to develop a secured environment to defend the network from malicious attacks. The key contribution of the suggested work is given as follows:

- To ensure a high point of isolation among cluster heads, a novel Inter-Channel Data Communication Algorithm is utilized within a secure network framework.
- By taking into account the signals' arrival time and assessing the degree of the trust relationship, trust is built.
- To ensure clone authentication in the network, suspicious malicious nodes are identified using a multi-region detection approach.
- Back propagation routing is used to find the nodal communication line, which isolates the attack source from the rest of the system.
- With this method, frequency hopping and data transfer caused by malicious nodes are eliminated, along with the requirement to inspect every node for malicious activity.

The remaining section of this article is structured as follows. The related work on security management in WSNs is compiled in Section 2. The suggested Security Design Scheme for Concentric Mapping-Based Malicious Attacks in Clustered WSN is presented in Section 3. The model setting and the performance estimation findings are covered in Section 4. Section 5 provides a conclusion and a few points of view for the paper.

2. LITERATURE SURVEY

Jlassi et al [16] in their paper proposed an active and precise technique for Sybil attack recognition and prevention. The suggested technique creates a routing table with deployed node data within it. The node's keys that will be used for communication and data transmission among them are confirmed by the base station. As soon as nodes receive the signal from the base station, data transmission takes place among them. The message authentication technique will enhance data transfer in the network and boost performance when compared to RPC. Future research should employ a revolutionary technique that ensures the network's energy usage while identifying malicious assaults.

Muruganandam et al [17] in their work employed Passive Ad Hoc Identity Technique and Key Distribution by utilizing Neighbor Discover Distance Process. The cooperative message authentication protocol operates under the supposition that every safety message contains the sender vehicle's location data, which can be produced by a global positioning system. Throughput, delivery ratio, delay time, and energy-efficient parameters are examples of factors that can be used to enhance the total efficacy of safe data transmission over wireless sensor networks and to distinguish between outcomes. However, future work can propose a new Sybil attack for defense mechanisms.

Dong et al [18] in their work presented a recognition and security process beside Sybil attacks based on the distance vector-hop (DV-Hop) technique. According to experimental results, the approach may increase the security of the node location in WSN. Compared to the conventional DV-Hop, the suggested technique decreased the average localization error by 3% when there were 50 beacon nodes. Future work must be done to boost location coverage in WSN and enhance the accuracy of DV Hop-based security localization.

Abbas [19] in his work proposed a recognition system that discovers both direct and indirect Sybil identities by means of one-time localization without causing overhead in the form of period localization data distribution. The examination of our approach reveals that the overhead of communication, storage, and computing is greatly reduced. Nonetheless, to implement the suggested plan, methods that are appropriate for scenarios in which users might not alter their wireless transmit capabilities must be used.

Huan et al [20] suggested a new node identification system namely node identification against Spoofing attack (NISA). To accomplish simultaneous node recognition and assault detection, it makes use of the reverse time synchronization system, which evaluates the clock skews of sensor nodes at the head of a wireless sensor network (WSN), as well as spatially correlated radio link data. Additionally, they offer distributed and centralized NISA for handling single-hop and multi-hop situations, the prior of which makes use of a convolutional neural network with one input and numerous outputs. Conversely, by using more sophisticated thresholding and parameter fusion approaches, distributed NISA might be enhanced.

From the survey, for [16] detecting malicious attacks with an assurance of energy consumption of the network is required, [17] Defense mechanisms for attacks at network layer has to be developed, [18] to increase location coverage in WSN and enhance the

accuracy of DV Hop-based security localisation [19], it is essential to implement suitable techniques for scenarios in which users might not alter their wireless transmit powers. These techniques could be enhanced by implementing more sophisticated thresholding and parameter fusion methods [20]. Hence to overcome the above mentioned issues a novel technique has to be adopted.

3. PROPOSED METHODOLOGY

WSNs are open networks where anyone can identify and capture messages among sensor nodes. Attackers can use illicit techniques to connect with powerful workstations or information sources, resulting in potential security vulnerabilities. Network security has turn out to be a serious problem for WSNs. Previous research has focused on rerouting data due to malicious attacks, which can cause impaired modulation quality and low system data rates. To identify suspicious malicious nodes in routing attacks, previous works have focused on collecting nearby data using all nodes in WSNs via internode communication, which rises the communication problem and reduces network lifetime. A novel technique is needed to overcome these issues.

A framework for the secure network is adopted in which initially the fault-tolerant data transfer is employed by a novel Inter-Channel Data Communication Algorithm in which initially non-sequential cluster heads are selected in the network which utilizes mean frequency and Davies-Bouldin function to maintain high separation between the cluster heads. The communication between the nodes is initiated by considering a degree of trust to the cluster heads which is identified using the time of arrival of signals to the cluster heads considering beta distribution to describe the trust value cluster head region in the network space and evaluate the trust relation degree to carryout communication between nodes which satisfy the threshold of mean trust value thereby establishing a secured data transfer, thereby eliminating the need to check the trust of all the nodes in the network which in turn reduces burden. In case of suspicious maliciousness, the node is identified by adopting a novel Multi Regional Detection Approach in which the monitoring node are chosen with initial trust degree which checks for clone authentication in the network nodes with circular concentric frequency mapping in which the detective communication channel is initially progressed in non-collinear neighborly nodes of the monitoring node by reputation adaptive threshold function, creating a threshold considering packet transfer and power density of nodes and the check progresses until the suspicious node is recognized by which the monitoring node concentric region is checked thereby the malicious node in the particular concentric space is identified and the nodal communication path to the node is identified by back propagation routing which performs a neighboring cluster head data transmission search in the bounded concentric space is done through which the source of the attack is identified and is isolated from the system and hence the frequency hopping and the need for checking all nodes for maliciousness is avoided thereby the transmission of data in the network due malicious node is eliminated. Thus the adopted framework provides a secure environment for the wireless sensor network.

3.1 Multi-Regional Detection Approach

The term "Multi-Regional Detection Approach" suggests a method or strategy for detecting and identifying malicious activities or entities in a network that spans multiple regions or areas. This approach is often employed in the context of wireless sensor networks (WSNs) or similar distributed systems where security is a significant concern.

Here's a general explanation of a Multi-Regional Detection Approach:

- Detection Across Multiple Regions:

In a network, especially a wireless sensor network, regions can be defined based on geographic or logical criteria. The Multi-Regional Detection Approach involves monitoring and analyzing activities or behaviors across these different regions.

- Monitoring Nodes:

The approach typically involves deploying special nodes, known as monitoring nodes, strategically across the network. These nodes are responsible for observing and analyzing the behavior of other nodes within their respective regions.

- Initial Trust Degree:

Monitoring nodes may be assigned an initial trust degree, indicating a level of reliability or credibility. This trust degree serves as a starting point for evaluating the trustworthiness of neighboring nodes.

- Clone Authentication and Concentric Frequency Mapping:

The approach may incorporate techniques such as clone authentication, which helps in detecting malicious nodes. Concentric frequency mapping involves organizing nodes based on their communication frequencies in concentric circles, facilitating the analysis of their interactions as shown in Figure 1.

- Reputation Adaptive Threshold Function:

To identify suspicious activities, a reputation adaptive threshold function may be employed. This function dynamically adjusts detection thresholds based on the reputation or historical behavior of nodes. Nodes exceeding these thresholds are flagged as potential threats.

- Progressive Check of Neighborly Nodes:

The approach involves a systematic and progressive check of nodes in the vicinity of the monitoring node. The reputation adaptive threshold function is applied to non-collinear neighborly nodes to identify anomalies or signs of malicious behavior.

- Back Propagation Routing:

If a suspicious node is identified, a mechanism like back propagation routing may be used to trace the communication path to the node. This can involve identifying neighboring cluster heads or determining the path through which the malicious activity entered the network.

In summary, a Multi-Regional Detection Approach is a security strategy that encompasses monitoring, analyzing, and adapting to potential threats across different regions in a network. It leverages a combination of techniques such as clone authentication, concentric frequency mapping, reputation-based thresholds, and back propagation routing to enhance the recognition and division of malicious nodes or activities.

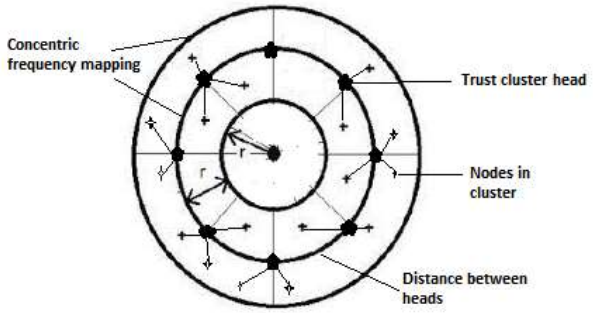

Figure 1: Architecture Diagram

3.2 Inter-Cluster Data Communication Algorithm

This section introduces a novel inter-cluster data communication algorithm that functions at both intra- and inter-cluster levels. For evaluating trust, every one of those two tiers employs a distributed and centralized methodology. According to a predetermined trust threshold, each cluster member (cluster-head) in the distributed approach evaluated the unique trust values for each of its neighboring nodes in the cluster (or, in a WSN, separately), in order to determine whether or not they were trustworthy. Regarding the centralized method, a base station (or cluster-head) constructs feedback for every member (or cluster-head) according to the recommendation values (i.e., previously computed on the dispersed method) that are obtained from other members (or other cluster-heads).

3.2.1 Network topology and assumptions

In the hierarchical WSNs architecture, a node can be in two ways a cluster leader or a cluster member, as shown in Fig. 2. A member of a cluster can communicate with its cluster leader directly or over many hops. A cluster head sends the aggregated data to the base station directly or through additional cluster heads.

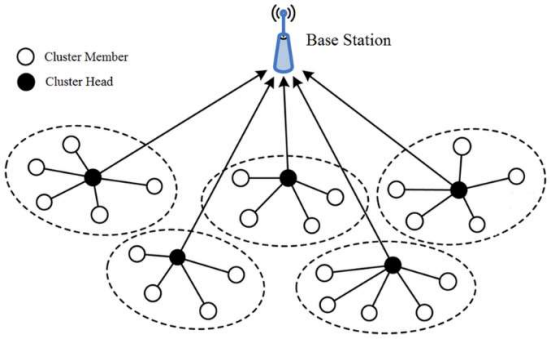

Figure 2: Network topology

Equivalent to the considerations presented in [21], we adopt the subsequent presumptions:

- The choice of a reliable node to serve as the cluster head is one of the most crucial specifications for clustered WSNs. Interesting techniques for choosing reliable cluster heads were proposed in;
- To protect trust values, we presume an encrypted communication channel, which may be constructed with any key management system;
- Since the trust value is an integer among 0 and 10, it takes up 4 bits of memory space, which is 50% less than that of a Group-based Trust Management Scheme (GTMS), which uses 1 byte, and 87.5% less than that of other protocols that treat the trust value as a real number, which uses 4 bytes;

- We use a timing window with several time units, as described in, to count the number of successful Si j and unsuccessful Ui j connections among nodes i and j. Every operation that takes place within a time unit is documented. The temporal window adds fresh experiences while also forgetting older ones.

3.2.2 Intra-cluster trust management

The works claims that regardless of the application's need for fault tolerance, the majority of trust management techniques employ a static function to assess node cooperation. The number of successful connections in GTMS is inversely related to the severity or punishment coefficient. The punishment coefficient in the Lightweight and Dependable Trust System (LDTS) is based on how many interactions fail.

$$T_{ij}^{c} = \lceil 10 \times P^{(1-P)\propto} \rceil \quad (1)$$

Where $\lceil . \rceil$ is the nearest integer value. A parameter, $\alpha \geq 2$ controls the severity of the trust function and P is the percentage of effective communications over the time window $\triangle t$ defined by:

$$P = \frac{S_{ij}^{c}(\Delta t)}{S_{ij}^{c}(\Delta t) + U_{ij}^{c}(\Delta t)} \quad (2)$$

Here $S_{ij}^{c}(\Delta t)$and $U_{ij}^{c}(\Delta t)$ are the number of times that the transmitter node i and the receiver node j successfully and unsuccessfully communicated over a period of time △t, accordingly. The successful percentage is not a linear function of this concept of trust communication.

The trust function presented in this study has an additional intriguing feature in that it increases the difference among the trust values provided to trustworthy and untrustworthy nodes, hence reducing decision-making difficulty when choosing a relay node.

Without using a severity coefficient, a lot of alternative trust protocols calculate the proportion of successful contacts. Using an integer parameter α, we describe an adaptive trust function in the suggested approach that may be adjusted based on the application's severity requirements.

3.2.2.1 Communication trust calculation

Certain attacks, such as the blackhole and greyhole attacks, involve a malicious node tricking other nodes into forwarding their packets over it in order to discard the targeted packets and sever connectivity. In order to counter such assaults, we use the following equation to describe the communication trust T_{ij}^{c} of node j maintained at node i:

It is true that this function treats non-cooperative nodes badly and rewards those that perform as predicted.

3.2.2.2 Data trust calculation

The focus of this research is on WSNs with high deployment densities where the data recorded has a spatial correlation, meaning that the values recorded on the same phenomena by neighbouring nodes are basically identical. Similar to communication trust, T_{ij}^{d} is defined as the data trust that member node i maintains with its neighbour j inside the same cluster, as determined by the equation that follows:

$$T_{ij}^{d} = \lceil 10 \times P^{(1-P)\propto} \rceil \quad (3)$$

where P is the fraction of effective recorded data for the period of $\triangle t$. This fraction is defined by:

$$P = \frac{S_{ij}^{d}(\Delta t)}{S_{ij}^{d}(\Delta t) + U_{ij}^{d}(\Delta t)} \quad (4)$$

Corresponding to its neighbour node i, $S_{ij}^{d}(\Delta t)$ represents the number of effective data reports submitted by node j over a period $\triangle t$, and $U_{ij}^{d}(\Delta t)$ represents the number of unsuccessful recorded data by node j over a period $\triangle t$. Taking into account that the recorded values of node i and its neighbour j in the cluster at time t are $r_i(t)$ and $r_j(t)$, accordingly. When $|r_i(t) - r_j(t))| \leq \varepsilon$, the neighbour i considers $r_j(t)$ as a successful report. The error tolerance ε, may vary depending on the node's sensing unit error variance and network spatial correlation. If ε is greater than or equal to ε, the report is deemed failed.

It should be noted that all nearby nodes of the data source listen to its broadcasts in order to assess the data trust. The goal is to maximise the number of votes on the sensor node, which will reduce the impact of any potentially poor suggestions in the cluster head's overall evaluation.

The communication is impacted by the detected data's correctness. In fact, the source may also believe that i is unwilling to assist in forwarding its data if a cluster member i chosen as a relay by the source j believes the latter's reported data are inaccurate and should be rejected. It is unclear which of the two nodes is correct. The subsequent trust values that the cluster head has received from its members will be added together to settle this issue.

Assume that every cluster has n members, and that every cluster-head,ch, broadcasts a request packet to its members on a regular basis. Each member will reply by sending ch their report on trust values for the cluster's neighbouring nodes. Ch in the two matrix will uphold these trust principles. As seen below, the first matrix D preserves data trust values, while the second matrix C saves communication trust values that are provided by its members:

$$D = \begin{pmatrix} X & T_{12}^{d} & \cdots & T_{1n}^{d} \\ T_{21}^{d} & X & \cdots & T_{2n}^{d} \\ \vdots & \vdots & \vdots & \vdots \\ T_{n1}^{d} & T_{n2}^{d} & \cdots & X \end{pmatrix} \quad (5)$$

$$C = \begin{pmatrix} X & T_{12}^{c} & \cdots & T_{1n}^{c} \\ T_{21}^{c} & X & \cdots & T_{2n}^{c} \\ \vdots & \vdots & \vdots & \vdots \\ T_{n1}^{c} & T_{n2}^{c} & \cdots & X \end{pmatrix} \quad (6)$$

Li et al. [21] derived inspiration from the beta feedback system [22], which computes the trust feedback $(T_{ch,1}, T_{ch,2}, \cdots, T_{ch,n})$ for cluster members using statistical theory. For the binary event (α, β), the beta distribution function is expressed as follows:

$$P(x) = Beta(\alpha, \beta) = \int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}\, d\theta \quad (7)$$

where α > 0 and β > 0, and the equivalent probability density function is denoted by the gamma function Γ as follows:

$$f(p|\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1} 1 - p^{\beta-1} \quad (8)$$

Here 0 ≤ p ≤ 1 and α, β ≥0. The probability expectation value for beta density function is determined as:

$$E\big(f(p|\alpha, \beta)\big) = \frac{\alpha}{\alpha+\beta} \quad (9)$$

We estimate the feedback using the beta probability density function because of the method's simplicity and versatility ($(T_{ch,j})$j=1..2. Thus, the data trust feedback $(T_{ch,j}^{d}$)j=1..2 for a given member is calculated as following way:

$$T_{ch,j}^{d} = \left\lceil 10 \times E\left(f\left(p\middle|v_j^d + 1, v_j^d + 1\right)\right)\right\rceil \quad (10)$$

$$T_{ch,j} = \left\lceil 10 \times \frac{v_j^d + 1}{v_j^d + v_j^d + 2}\right\rceil \quad (11)$$

The closest integer function is represented by ⌈.⌉; the total number of positive data trust suggestions ($T_{ij}^{d} \geq 5$) is represented by v_j^d; the the amount of negative data trust suggestions ($T_{ij}^{d} < 5$) is indicated by v_j^d, which is determined from the matrix D for member j; the subsequent likelihoods of binary events (v_j^d, v_j^d) are indicated by $f\left(p\middle|v_j^d + 1, v_j^d + 1\right)$. Prior to determining communication trust feedback $(T_{ch,j}^{c})$j=1..2, the cluster-head estimates the data trust feedback of its members and declines communication trust suggestions of members absorbing a low data trust feedback from the matrix C. This is due to the suggestions are likely to be untrustworthy, as we previously explained above. Similar to data trust feedback, feedback on communication trust is defined as follows:

$$T_{ch,j}^{c} = \left\lceil 10 \times E\left(f\left(p\middle|v_j^c + 1, v_j^c + 1\right)\right)\right\rceil \quad (12)$$

$$v_j^d, v_j^d = \left\lceil 10 \times \frac{v_j^c + 1}{v_j^c + v_j^c + 2}\right\rceil \quad (13)$$

Where⌈.⌉ is the nearby integer function; v_j^c represents the total amount of negative communication trust references (i.e., $T_{ij}^{c} < 5$) determined from the matrix C for member j, and v_j^c corresponds to the amount of positive communication trust references (i.e., $T_{ij}^{c} \geq 5$); $f\left(p\middle|v_j^c + 1, v_j^c + 1\right)$ represents the posterior probabilities of binary events (v_j^c, v_j^cc). Thus, a cluster-member j is theoretical communication trusted if $T_{ch,j}^{c} \geq 5$, else it is indicated as communication untrusted.

Now, based on two vectors $(T_{ch,j}^{d})_{j=1..2}$ and$(T_{ch,j}^{c})_{j=1..2}$, we describe the global trust feedback (Tch,j)j=1..2 for every cluster-member as follows:

$$T_j = \left\lceil 10 \times \frac{T_j^d \times T_j^c}{T_j^d \times T_j^d + (10 - {}^{d}_{j}) \times (10 - T_j^c)}\right\rceil \quad (14)$$

According to this concept of feedback, a sensor node that reports inaccurate measurements is probable to be distrusted in communications since it believes that data recorded by nodes nearby is unreliable and should be rejected if it is chosen to serve as a relay.

3.3 Davies–Bouldin Index (DBI)

This index uses both clusters and means to represent class separability as the proportion of within-cluster scattering to between-cluster isolation. Since scatter matrices depend on the cluster geometry, this index has a geometrical as well as statistical rationale. The comparison of every pair of clusters that represents the degree of difference between the two clusters must be

calculated to obtain the DB index. Data samples that have been labeled for a particular activity in feature-channel space form clusters. The definition of two clusters, i and j, being similar is

$$R_{ij} = \frac{S_i + S_j}{M_{ij}} \qquad (15)$$

where S_i and S_j are the diffusions of i^{th} and j^{th} clusters, correspondingly and attained by

$$S_i = \left\{ \frac{1}{|X_i|} \sum_{x \in X_i} \|x - m_i\|_2^q \right\}^{1/q} \qquad (16)$$

The Xi and mi are the number of points and mean point of cluster i th, correspondingly.

$$m_i = \frac{1}{|X_i|} \sum_{x \in X_i} x \qquad x, m_i \epsilon \Re^L \quad L = L_f \cdot L_c \qquad (17)$$

M_{ij} is the inter-cluster distance and specified by

$$M_{ij} = \left\{ \sum_{k=1}^{C} |m_i - m_j|^p \right\}^{1/p} \qquad (18)$$

We have chosen to use the Euclidean distance as a metric among the points in the cluster and the mean point, assuming p=q=2. DB index is described as

$$DBI = \frac{max}{i \epsilon C} \frac{1}{C} \sum_{j=1}^{C} R_{ij} \qquad (19)$$

Where C represents the quantity of clusters. Finding clusters with the least amount of scatter within the cluster and the greatest amount of separation across classes is geometrically feasible. The DB index is predicted to drop monotonically for clusters that are well-separated, therefore reducing the DB index may be a trustworthy objective function that helps identify the optimal selection of the cluster head.

3.4 Clone Authentication:

In a network, a single node can sometimes attempt to impersonate multiple legitimate nodes, leading to a clone attack (also known as a malicious attack). This is especially common in wireless sensor networks or other distributed systems. Clone authentication is the process of identifying and removing these fraudulent nodes to maintain the network's integrity.

To achieve this, each node in the network is uniquely identified through a combination of features such as its unique identifier, cryptographic keys, or physical properties. During the initialization phase, security measures are implemented to ensure that each node is initialized uniquely and securely.

Clone authentication mechanisms use various techniques to detect nodes that try to create multiple identities. This may include monitoring communication patterns, analyzing cryptographic signatures, or using physical attributes of the nodes. When a potential clone is identified, the network can take action to isolate or eliminate the suspicious node. This may involve revoking cryptographic keys, blocking communication from the identified clone, or informing neighboring nodes about the potential threat.

3.5 Concentric Frequency Mapping:

Concentric frequency mapping is a strategy commonly used in networks, especially in wireless sensor networks. It involves organizing nodes based on their communication frequencies into concentric circles or regions. This helps to facilitate efficient communication, minimize interference, and provide a structured approach to monitoring and managing network activities.

The process of concentric frequency mapping includes assigning specific communication frequencies to nodes based on a mapping strategy. Nodes with similar or adjacent frequencies are then organized into concentric circles. These circles represent different communication zones or regions within the network. Nodes within the same circle or region share a similar frequency or communication channel.

Concentric frequency mapping helps to reduce interference between nodes that operate on different frequencies, making it easier to analyze interactions between nodes within the same or neighboring circles. It enables efficient use of the available spectrum and enhances overall communication reliability and performance. Additionally, this mapping structure can be particularly useful in detecting abnormal patterns of communication that may indicate malicious activities or deviations from expected behavior.

This approach enhances wireless communication security by organizing nodes based on communication frequencies and implementing measures against clone attacks, resulting in a more robust and efficient communication environment.

3.6 Reputation Adaptive Threshold Function:

A Reputation Adaptive Threshold Function is a mechanism used in security systems, particularly in the context of intrusion detection or anomaly detection in networks. This function helps identify abnormal activities in networks while minimizing false positives. It dynamically adjusts detection thresholds based on the historical behaviour or reputation of entities within the network to enhance the accuracy and effectiveness of identifying abnormal activities.

There are key components and aspects of a Reputation Adaptive Threshold Function. Nodes or entities within the network are assigned reputation scores based on their past behaviour and interactions. Reputation can be established through a variety of metrics, including successful transactions, adherence to security protocols, or feedback from other nodes in the network. Initially, the system sets detection thresholds based on a default or predefined value. These thresholds represent the acceptable limits for normal behaviour and activities within the network.

As the system operates and collects more data about the behaviour of nodes, the Reputation Adaptive Threshold Function continuously updates the detection thresholds based on the evolving reputation scores. If a node's reputation is consistently high, the threshold for deeming its behaviour as anomalous may be raised. Conversely, if a node's reputation deteriorates, the threshold for flagging anomalous behaviour may be lowered.

The function evaluates real-time events or activities against the dynamically adjusted thresholds. If an entity's behaviour surpasses the threshold, it may be flagged as potentially malicious or suspicious. By adapting thresholds based on reputation, the system aims to reduce false positives. Nodes with a positive reputation are less likely to trigger alarms, even if their behaviour slightly deviates from the norm.

This adaptive approach helps maintain a balance between sensitivity to anomalies and the avoidance of unnecessary alerts. The function incorporates machine learning or statistical methods to continuously learn and adapt to changes in the network environment. This adaptability allows the system to respond to evolving threats and ensures that the thresholds remain relevant over time.

Reputation adaptive thresholding adds a level of context-awareness to security measures. The system considers the historical context of entities' behaviour, making it more resilient to adaptive or sophisticated attacks. This approach is particularly valuable in dynamic environments where the characteristics of normal behaviour may change over time. By dynamically adjusting thresholds based on reputation, the Reputation Adaptive Threshold Function contributes to a more resilient and effective security system in networks, improving the overall accuracy of anomaly detection.

3.7 Progressive Check of Neighbourly Nodes:

"Progressive Check of Neighbourly Nodes" refers to a process of systematically examining neighbouring nodes in a network. This is typically done in the context of WSNs or further distributed systems. The examination process involves progressively assessing the behaviour, interactions, or attributes of nearby nodes to identify any anomalies, potential threats, or deviations from expected norms.

The approach involves a step-by-step assessment of nodes that are in proximity or neighbours to a reference node. Each node in the neighborhood is subject to a progressive check to analyse its behaviour and activities. This evaluation process may incorporate adaptive threshold mechanisms to dynamically adjust the thresholds based on factors such as the historical behaviour of the nodes, their reputation scores, or statistical metrics. Adaptive thresholds can help in distinguishing normal variations from potentially malicious activities.

Reputation scores of neighbouring nodes may also be considered during the progressive check. Nodes with positive reputations are less likely to trigger alarms, while those with declining reputations may undergo more scrutiny. The evaluation includes an analysis of the behaviour exhibited by neighbourly nodes. This may involve assessing communication patterns, data transfer rates, energy consumption, or other relevant metrics depending on the specific context of the network.

The primary objective of the progressive check is to detect any anomalies or deviations from the expected behaviour of neighbouring nodes. Anomalies may indicate potential security threats, such as malicious activities or compromised nodes. The progressive check is often an iterative process that can be repeated periodically or triggered by specific events. This iterative nature ensures that the security system continuously monitors and adapts to changes in the network environment.

In some cases, collaborative detection mechanisms may be employed. Neighbouring nodes may share information about their own observations and contribute to the overall assessment of the network's security. If a node is identified as potentially malicious or exhibiting anomalous behaviour, immediate response mechanisms, such as isolation or alert generation, may be triggered to mitigate the impact of the threat.

The progressive check of neighbourly nodes is often integrated into broader security protocols within the network. It aligns with the overall security strategy and contributes to maintaining the integrity of the network.

3.8 Back Propagation Routing:

Back Propagation Routing is a technique used in network communication, specifically in WSNs, to trace and identify the source of detected anomalies or security threats. The term "back propagation" is borrowed from artificial neural networks. In the context of routing, it involves moving backward through the network iteratively, retracing the communication path from the point of detection back to its source. This routing strategy is typically employed when a monitoring node or security mechanism identifies potential security threats or malicious activities within the network.

Once a threat is detected, the back propagation routing algorithm works by progressively backtracking through the nodes that relayed the suspicious information, moving towards the original source. The process involves analyzing communication logs, routing tables, or other relevant data to pinpoint the exact path through which the malicious data or activity entered the network. By identifying the source of the threat, network administrators can take targeted action, such as isolating the compromised node, strengthening security measures, or conducting further investigations.

Back propagation routing is instrumental in enhancing the resilience and security of wireless sensor networks by enabling a focused response to security incidents and efficiently mitigating potential risks. Key features and steps involved in Back Propagation Routing include: iterative backtracking through the network, analyzing communication logs and routing tables, pinpointing the exact path of the malicious data or activity and taking targeted action to mitigate the threat.

Before starting the back propagation routing process, there is usually a trigger event that alerts the network to malicious activity, anomalies, or security threats. Intrusion detection systems, anomaly detection algorithms, or other security mechanisms can help identify such events. Once a suspicious activity is detected, the goal is to trace back and identify the source of the event. Back propagation routing helps locate the origin of the communication or security incident.

Back propagation routing involves a trace-back mechanism that reverses the path of data transmission. Instead of moving forward through the network toward the destination, the system traces backward from the affected or monitored node. During the back propagation, the routing mechanism identifies the intermediate nodes or hops that the data packet traversed. This information is crucial for understanding the route taken by the communication event.

In the context of wireless sensor networks, particularly those organized into clusters, back propagation may involve searching for neighbouring cluster heads. This step helps narrow down the potential source of the event. The search for the source of the event is often conducted within a bounded concentric space. This space may be defined depend on the closeness to the affected node or the region where the suspicious activity occurred.

Once the source node is identified through back propagation routing, appropriate measures are taken to isolate the node from the network. This may involve revoking its access privileges, blocking its communication, or taking other security actions. The ultimate goal of back propagation routing is to eliminate the security threat or address anomalous behavior, as isolating the source node can prevent the propagation of malicious activities and maintain network integrity.

4. RESULT AND DISCUSSION

The simulation setting and evaluation metrics are covered in this segment. We talk about how the quantity of fake nodes affects the accuracy of localization. We test the effectiveness of our suggested algorithm, the DV-HOP scheme with malicious attack, and the DV-HOP scheme without malicious attack in this research.

4.1 Simulation Settings

A detailed description of our simulation setup is presented in this section. For periodic monitoring, a target area measuring 100 m x 100 m has 100 sensor nodes organized in total. The base station, or sink node, is situated in the middle of the area. The same network simulation parameters are used throughout the simulation, which are included in Table 1 below. To simulate, the suggested strategy, we used MATLAB. Every simulation is run on a system equipped with a 16GB DDR3 1600MHz RAM and an Intel (R) Core (TM) i5-3230M CPU running at 2.60GHz. The MATLAB R2021a was utilized.

Table 1: Simulation parameters

Parameters	Values
Number of nodes	100
MAC protocol	802.11
Transmission Radius	200 m
% of fake nodes	10-50
Coverage area	100 m*100 m
Radio propagation model	Two ray ground
Number of malicious nodes	5–35

In our simulations, the CHs' distribution according to the proposed algorithm is identical to that in Fig 3. As shown in Fig 3, the network has been divided into 16 clusters in this simulation, and each cluster has selected a CH and an IN.

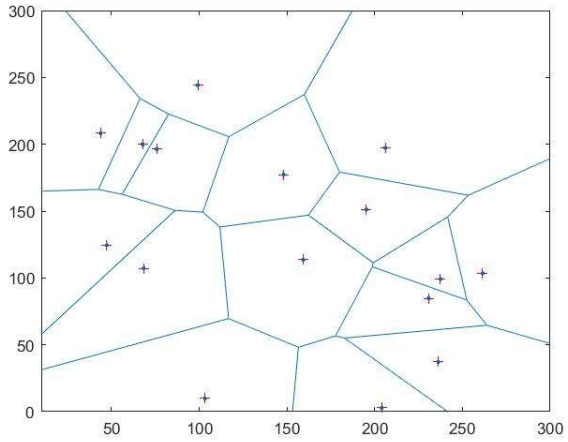

Figure 3: Network nodes distribution

4.2 Evaluation Metrics

1. Network Lifetime

The network lifetime refers to the duration between the deployment of the nodes and the point when the network stops functioning. The interpretation of this duration varies based on the application area. For example, it can be measured as the number of communication rounds until the first node fails, or the rounds until a certain percentage of nodes fail. Additionally, it can also be measured as the rounds until the last node exhausts its energy reserves in the network.

- Number of live nodes: the number of live nodes per round. (N−dead).
- Number of malicious nodes: the number of malicious nodes in a round. (malicious = dead).

2. Throughput

The total number of successfully transferred bits to the destination during a given amount of time is referred to as throughput. The efficiency of the network capacity is determined by the throughput. This formula can be used to calculate the network throughput.

$$Throughput = \frac{NR}{NS} \quad (20)$$

Where NS is the total number of packets transmitted by the source, and NR is the total number of packets received by the destination.

3. Average Residual Energy

Residual energy (RE) is another name for remaining energy. The residual energy indicates the protocol's capacity to utilize network energy as effectively as feasible. Calculating the average residual energy requires using equation (34)

$$RE = \frac{E_0 - CE}{E_0} \quad (21)$$

where CE is the average energy consumption and E_0 is the average starting energy.

4. Average Localization Error (ALE)

Furthermore, we use the average localization error and coverage as assessment measures in this research. The following formula is used to get the average localization error, or ALE for short:

$$Average\ Localization\ Error\ (ALE) = \frac{\sum_{i=1}^{n}\sqrt{(x_i' - x_i)^2 + (y_i' - y_i)^2}}{nr} \quad (22)$$

Where n is the number of unknown nodes, r is the network communication radius, and (x_i', y_i') and (x_i, y_i) are the indefinite node's actual and estimated coordinates, respectively.

Figures 4 and 5 indicate the network lifespan performance in terms of the number of live nodes and malicious nodes. It is abundantly clear from the results that the suggested approach performs better with regard to network lifetime. The rationale is that by minimizing the use of nodes with high traffic rates for sensing and transmission duties, the suggested strategy takes traffic variability into account. In order to mitigate the early mortality of high traffic nodes which mainly involves the avoidance of picking nodes with high traffic for CH roles this is accomplished by employing an energy and traffic aware distributed and centralized approach. It was shown that by utilizing a distributed and centralized method, the number of live nodes, as shown in Fig. 4, may extend the lifespan of the network.

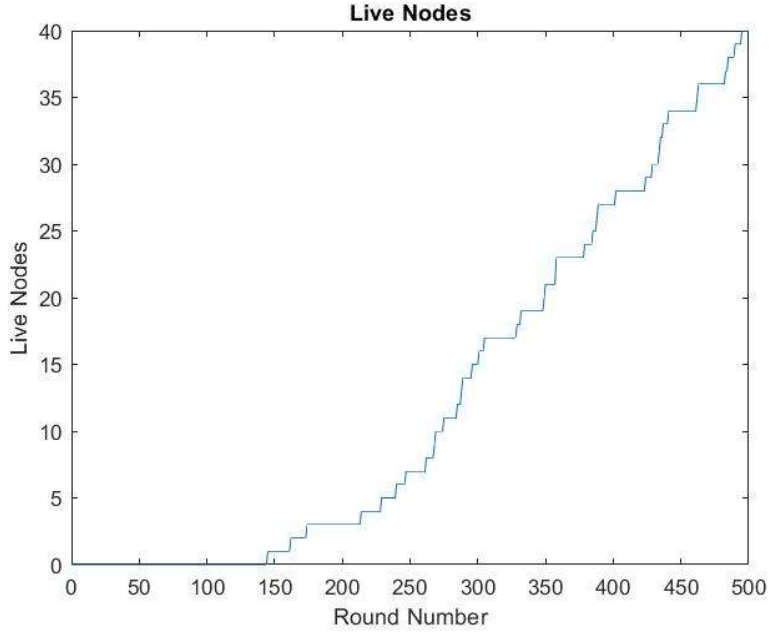

Figure 4: Number of live nodes.

Fig 5 represents the number of malicious nodes per round which displays that the number of malicious nodes in proposed method is deferred unlike in existing methods which display fast growth in the number of malicious nodes.

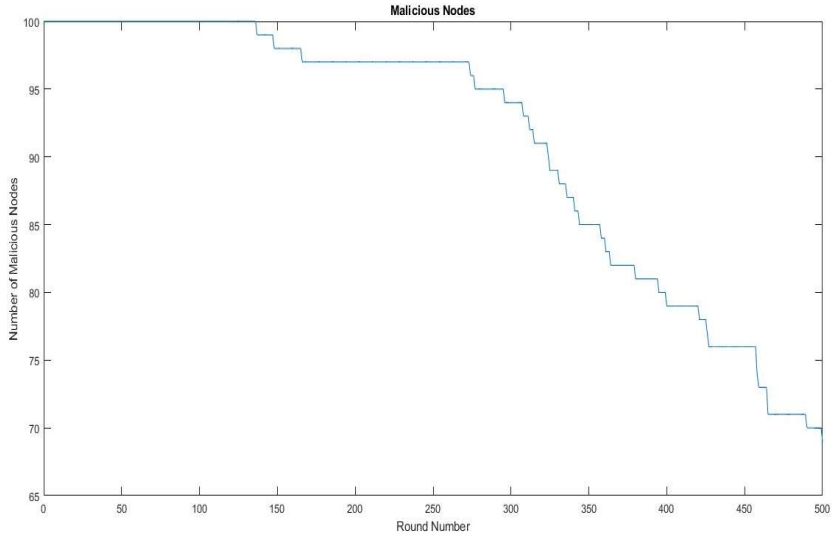

Figure 5: Number of malicious nodes.

4.3 Throughput

The total number of bits transferred to the target in a certain amount period is referred to as throughput. Although using a dispersed and centralized approach across the network nodes, the suggested strategy offers somewhat higher throughput, as seen in Fig. 6 below. As the number of communication rounds increases, the suggested approach protocol has demonstrated an increase in throughput to BS. This is explained by the suggested technique's extended network lifetime.

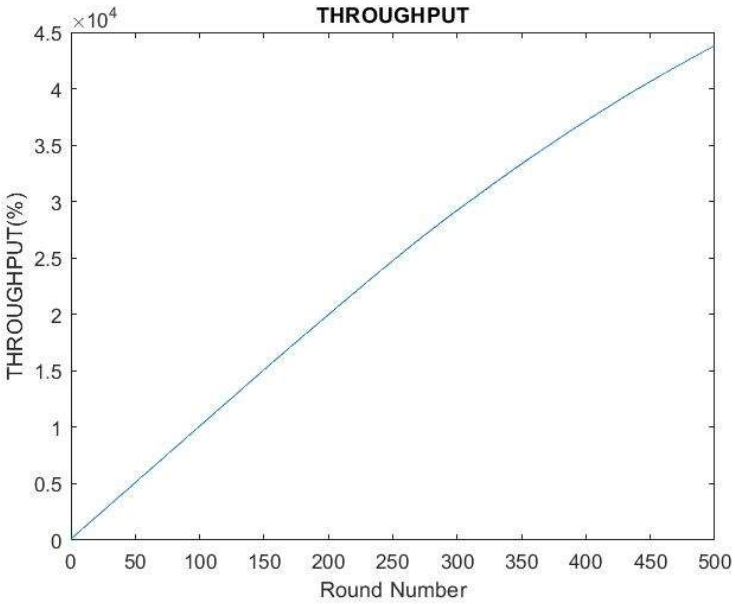

Figure 6: Throughput

4.4 Average Residual Energy

The suggested method has more residual energy than the current methods, as Fig. 7 illustrates. This is the outcome of energy-saving techniques used in the suggested approach, such as CH selection, the application of a decentralized and distributed technique, and the reduction of energy loss from idle listening in the steady state. Since choosing a node with a high number of couples in this framework prevents the choice of isolated nodes for CH roles, the CH selection approach utilised in the suggested approach improves load balancing. As a result, as shown in Fig. 7, eliminating redundant data transmission between pair nodes by adding distributed and centralized approach and appropriately selecting CH in the framework should have an important effect on decreasing network energy consumption. This is accurate because only one node among the pairs sends data to CH during each communication round, and that node has high energy and low data rate. Furthermore, a significant contribution to reducing node energy usage was made by employing efficient TDMA time allocation between paired groups and unpaired nodes. As a result, the framework has demonstrated significant network average residual energy when compared to the current approaches, as illustrated in Fig 7.

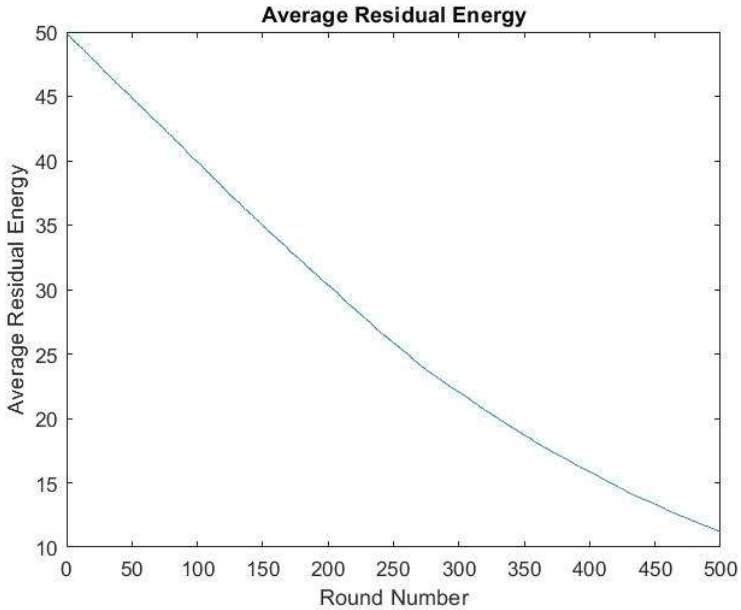

Figure 7: Average residual energy

The accuracy of the security localization approach depend on the DV-HOP technique can be affected in the real-world situation by the number of malicious nodes. Thus, we test our proposed algorithm's performance with different numbers of malicious nodes and discover that our technique performs superior even as the number of fake nodes increases.

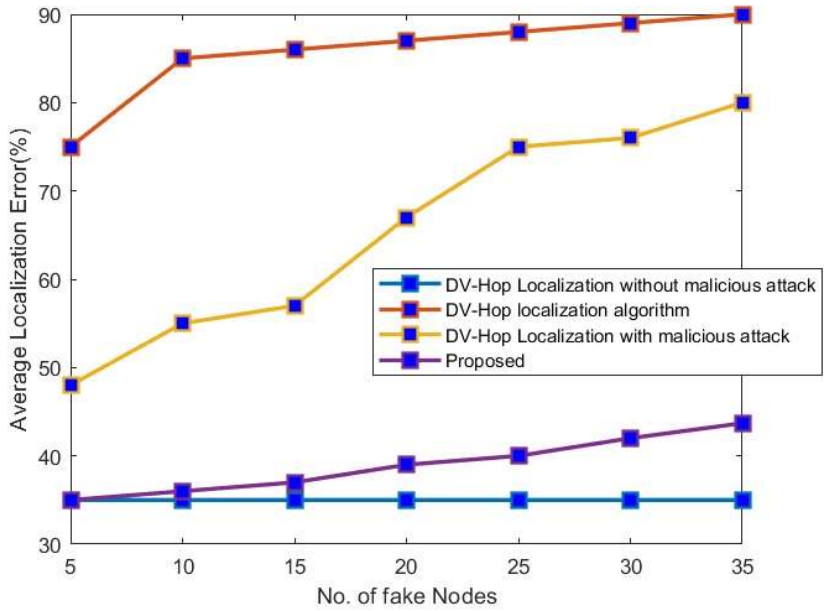

Figure 8: Average location error against the number of malicious nodes

We select the quantity of fake nodes from the following set: {5, 10, 15, 20, 25, 30, 35}. We assess and contrast our suggested algorithm's performance with those of the other two approaches (DV-Hop with and without malicious attack). The model outcomes are displayed in Figs. 8 and 9, in that order. Figure 8 shows that while DV-Hop localization without malicious attack stays constant, the localization error for both our suggested technique and DV-Hop localization with malicious attack increases as the number of malicious nodes rises. This is owing to the possibility of an increase in the mistake rate of recurrence and the quantity of malicious nodes that, in WSN, depict the erroneous location.

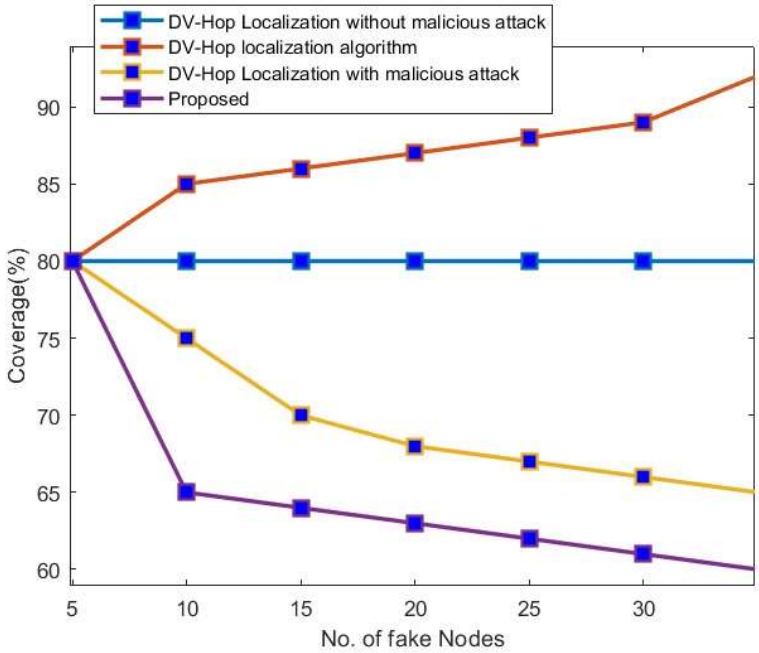

Figure 9: Coverage percentage in relation to the quantity of malicious nodes

As can be seen in Fig. 8, the fault grows with the quantity of malicious nodes. By employing the hop difference and the neighbor list to alter the two-step security localization technique depend on DV-HOP, our algorithm reduces the localization error. We discover that as the quantity of malicious nodes rises, our process's coverage falls. This is indicated by the coverage metric. Nevertheless, as Fig. 9 illustrates, the coverage in DV-Hop Localization with malicious attacks rises whereas the coverage in DV-Hop Localization without malicious attacks stays unchanged. The rationale is that to rise the accuracy of the security localization, our system uses the merging method to further limit the number of malicious nodes. As the number of malicious nodes reduces, the overall coverage lowers. As seen, in the case of a malicious attack in WSN, our technique performs better than the DV-Hop algorithm.

5. CONCLUSION

In conclusion, addressing the security issues in WSNs, particularly the threat of malicious network layer attacks, is imperative for ensuring the integrity of the network. The proposed framework offers a comprehensive solution by incorporating a novel Inter-Channel Data Communication Algorithm and a fault-tolerant data transfer mechanism. The algorithm's selection of non-sequential cluster heads, guided by the Davies-Bouldin function and mean frequency, ensures effective separation and organization within the network. The incorporation of trust levels in communication, determined through the beta distribution and signal arrival time, not only enhances security but also optimizes the process by setting a mean trust value threshold. The multi-region detection approach, featuring circular concentric frequency mapping and clone authentication, proves effective in identifying potential malicious nodes. The adaptive threshold function, based on reputation, further refines the process by scrutinizing non-collinear neighborly nodes for suspicious activity. Altogether, this framework establishes a robust security foundation for WSNs, mitigating the risks associated with malicious attacks and providing a safer and more reliable wireless sensor network environment.

REFERENCES

[1] Muduli, Lalatendu, Devi Prasad Mishra, and Prasanta Jana, K. (2018). Application of wireless sensor network for environmental monitoring in underground coal mines: A systematic review. *Journal of Network and Computer Applications*, *106*, 48-67.

[2] Mohamed, E. Reem, et al. (2018). Survey on wireless sensor network applications and energy efficient routing protocols. *Wireless Personal Communications*, *101*(2), 1019-1055.

[3] Sinha, Somnath, and Aditi Paul. (2020). Neuro-fuzzy based intrusion detection system for wireless sensor network. *Wireless Personal Communications, 114*(1), 835-851.

[4] Luo, Xiao, et al. (2019). CREDND: A novel secure neighbor discovery algorithm for wormhole attack. *IEEE Access*, *7*, 18194-18205.

[5] Ali, Haibat, and Jae-ho Choi. (2019). A review of underground pipeline leakage and sinkhole monitoring methods based on wireless sensor networking. *Sustainability*, *11*(15), 4007.

[6] Shagari, Nura Modi, et al. (2020). Heterogeneous energy and traffic aware sleep-awake cluster-based routing protocol for wireless sensor network. *IEEE Access*, *8,* 12232-12252.

[7] Yuan, Yali, et al. (2018). Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks. *IEEE Access*, *6*, 27629-27636.

[8] Ioannou, Christiana, and VasosVassiliou. (2019). Classifying security attacks in IoT networks using supervised learning. *2019 15th International conference on distributed computing in sensor systems (DCOSS). IEEE*.

[9] M. Sahu, N. Sethi, & S. K. Das. (2022). A Survey on Detection of Malicious Nodes in Wireless Sensor Networks. *In 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI),* 710-715.

[10] Angappan, Arthanareeswaran, et al. (2021). Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN. *Journal of Ambient Intelligence and Humanized Computing, 12*(6), 6567-6578.

[11] Hussein, Safwan Mawlood, Juan Antonio López Ramos, and Abubakar Muhammad Ashir. (2022). A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks. *Electronics, 11*(17), 2721.

[12] Lai, Yingxu, Liyao Tong, Jing Liu, Yipeng Wang, Tong Tang, Zijian Zhao, and Hua Qin. (2022). Identifying malicious nodes in wireless sensor networks based on correlation detection. *computers & security*, *113*, 102540.

[13] Zhang, Junlin. (2023). WSN Network Node Malicious Intrusion Detection Method Based on Reputation Score. *Journal of Cyber Security and Mobility,* 55-76.

[14] Al-Azez, T. Zaineb, et al. (2019). Energy efficient IoT virtualization framework with peer to peer networking and processing. *IEEE Access*, *7,* 50697-50709.

[15] Faris, Kadhim, et al. (2021). Survey of Wireless Sensor Network based on Power Consumption and Data Aggregation. *International Journal of Progressive Research in Science and Engineering*, *2*(9), 22-32.

[16] Jlassi, Wadii, et al. (2021). A Novel Dynamic Authentication Method for Sybil Attack Detection and Prevention in Wireless Sensor Networks. *International Conference on Advanced Information Networking and Applications*. Springer, Cham.

[17] A. Muruganandam, and R. Anitha. Passive Adhoc Identity for Sybil Attack Detection Using NDD Algorithm. *International Conference on Computing and Intelligence Systems*, 4.

[18] Dong, Shi, Xin-gang Zhang, and Wen-gang Zhou. (2020). A security localization algorithm based on DV-hop against sybil attack in wireless sensor networks. *Journal of Electrical Engineering & Technology*, *15*(2), 919-926.

[19] Abbas, Sohail. (2019). An efficient sybil attack detection for internet of things. *World Conference on Information Systems and Technologies. Springer, Cham*.

[20] Huan, Xintao, Kyeong Soo Kim, and Junqing Zhang. (2021). NISA: Node identification and spoofing attack detection based on clock features and radio information for wireless sensor networks. *IEEE Transactions on Communications*, *69*(7), 4691-4703.

[21] X. Li, F. Zhou, & J. Du. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE Transaction on Information Forensics and Security, 8*(6), 924–935.

[22] A. Whitby, A. Josang, & J. Indulska. (2007). Filtering out unfair ratings in bayesian reputation systems. *In The autonomous agents and multi agent systems. New York.*