EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Enhancing the reliability and accuracy of wireless sensor networks using a deep learning and blockchain approach with DV-HOP algorithm for DDoS mitigation and node localization

Bhupinder Kaur[1], Deepak Prashar[1,7], Leo Mrsic[2], Ahmad Almogren[3], Ateeq Ur Rehman[4*], Ayman Altameem[5] and Seada Hussen[6*]

*Correspondence: 202411144@gachon.ac.kr; seada.hussen@aastu.edu.et

[1] School of Computer Science Engineering, Lovely Professional University, Phagwara, Punjab, India
[2] Algebra University, Gradiscanska ulica 24, 10000 Zagreb, Croatia
[3] Department of Computer Science, College of Computer and Information Sciences, King Saud University, 11633 Riyadh, Saudi Arabia
[4] School of Computing, Gachon University, Seongnam-si 13120, Republic of Korea
[5] Department of Natural and Engineering Sciences, College of Applied Studies and Community Services, King Saud University, 11543 Riyadh, Saudi Arabia
[6] Department of Electrical Power, Adama Science and Technology University, 1888 Adama, Ethiopia
[7] Jadara University Research Center, Jadara University, Irbid, Jordan

Abstract

Wireless sensor networks (WSNs) are subject to distributed denial-of-service (DDoS) attacks that impact data dependability, mobility of nodes, and energy drain. The remedy to these challenges in this work is a solution based on deep learning integrated with a blockchain-aided distance-vector hop (DV-HOP) localization algorithm for reliable and secure node localization. Incorporating a blockchain ledger makes the network more trustworthy as it verifies usual and unusual system activities, whereas the DV-HOP algorithm mitigates localization inaccuracies and enhances node placement. The system is evaluated according to different performance measures like localization error, accuracy ratio, average localization error (ALE), probability of location, false positive rate (FPR), false negative rate (FNR), energy utilization, network stability, node failure rate, node recovery rate, and malicious node detection rate. Experimental results reveal improved security, accuracy, and efficiency with 17% FPR and 15% FNR, outperforming the conventional methods. This model enhances WSN performance in different environments via precise data transmission from the source to the destination. The results confirm that integrating deep learning with blockchain and DV-HOP increases network robustness, thus making WSNs more secure against security attacks while reducing energy consumption and localization accuracy. The proposed model presents a strong solution for real-world applications in wireless network environments.

Keywords: Wireless network devices, DV-HOP algorithm, Blockchain ledger, Reliable network devices

1 Introduction

Technology has dramatically been changing our daily lives, beginning with the smartness of tasks handling in shopping malls, agricultural fields, and even healthcare systems. Among the enabling technologies, wireless sensor networks (WSNs) have become a cornerstone for many applications, from environmental monitoring to smart cities.

WSNs consist of interconnected sensing nodes that detect events, collect data, and send it to a base station for processing. These networks play significant roles in the automation of systems, performing intelligent decision-making, and enhancing efficiency in several areas of activities [1].

A WSN is comprised of several sensor nodes that can either be fixed or mobile, terrestrial, multimedia, underwater, or underground [2]. These can be anchor nodes, which know their location with the help of technologies like GPS or can be unknown sensor nodes, whose localization is assumed to be taken care of by the anchor nodes. Localization forms a crucial step within WSNs that determines actual node positions, hence establishing that all data collected is actionable and meaningful. Localization accuracy impacts network performance, data integrity, and application functionality.

There are primarily five different categories of WSNs: mobile, multimedia, terrestrial, underwater, and underground [2]. Each type of sensor network has its advantages and disadvantages. The two main categories of WSN applications are tracking and monitoring.

1.1 Background

Initially used by the military, WSN has become integral to civilian systems. As shown in Fig. 1, a typical architecture uses multiple layers: Sensor nodes collect data, which is then transmitted via a communication network to the central base station. Early WSNs faced major energy efficiency, scalability, and fault tolerance challenges. Advances in hardware

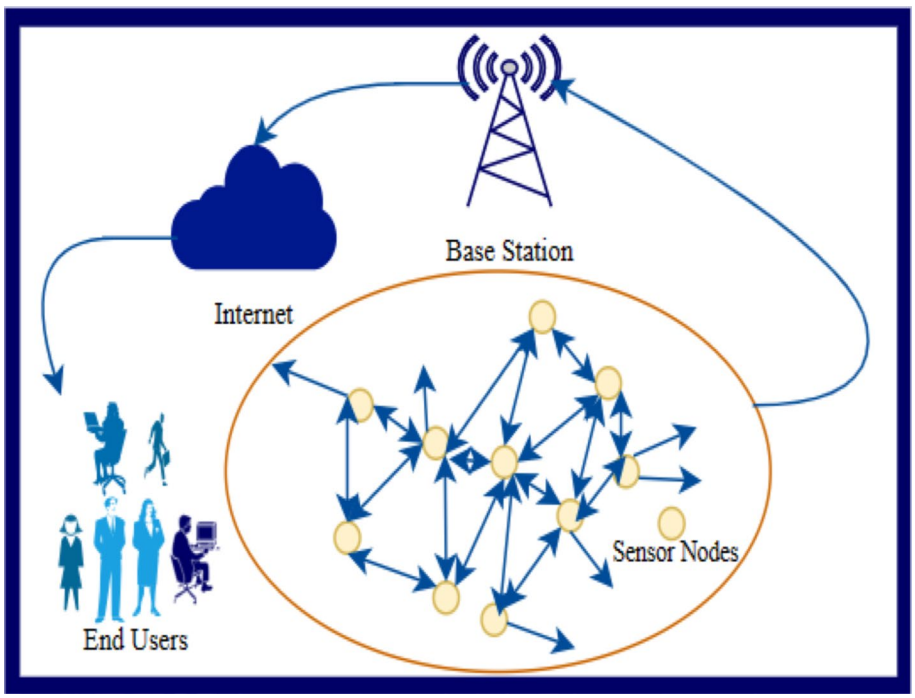

Fig. 1 Wireless sensor network (WSN) architecture. The architecture exemplifies a typical wireless sensor network (WSN) that consists of a base station, a sink node, and multiple sensor nodes. Data acquisition and communication are the responsibilities of sensor devices. The proposed DV-HOP algorithm is employed to efficiently localize data by routing it through intermediate nodes to the sink node. The sink node transmits aggregated data to the base station, where blockchain guarantees data integrity and security

and software have helped WSNs tackle some of these challenges, enabling exploration in environmental monitoring, health care, smart cities, and industrial automation.

Localization is crucial in WSNs because data must be tied to specific locations. Anchor-based and anchor-free localizations are the two primary localization methods: The former uses reference points, while the latter uses relative measurements. RSSI and ToA techniques enable distance measurement, and trilateration and triangulation algorithms pinpoint the location. Despite significant advancements, localization remains hampered by power consumption, interference issues, and hardware limitations.

1.2 Applications of WSN

Environmental Monitoring: WSNs track soil health, weather, water quality, and air quality. This data aids decisions on resource management, pollution control, and disaster prevention.

Health care: WSNs monitor medication use, vital signs, and changes in patient health. This technology helps medical professionals provide personalized care and reduce hospital readmissions. It is especially useful for remote patient monitoring.

Smart Cities: WSNs manage services such as parking, streetlights, traffic control, and waste disposal in smart cities. By collecting data from sensors, these systems make real-time decisions to improve citizens' quality of life. Agriculture: In agriculture, WSNs track crop growth, soil moisture, and weather conditions. This information boosts crop yields, saves water, and reduces pesticide and fertilizer use. Industrial Automation: WSNs track machinery to spot faults and optimize maintenance schedules. This technology cuts downtime, increases output, and enhances worker safety.

WSN localization challenges and methods impact homes, businesses, and industries [1, 2]. Key issues for sensor networks include energy, self-management, hardware–software problems, quality of service, information sharing, memory shortages, fault tolerance, positioning, and security [1, 3].

A WSN has many sensor nodes. These nodes fall into two types for localization: Beacon_Sensor/Anchor_Sensor, which knows its location, and Unknown_Sensor_Node/Dumb_Sensor_Node, which does not [4]. Beacon sensors connect to GPS, helping dumb nodes find their location. To locate a dumb node in 2D, at least three anchor sensors are needed; in 3D, at least four are required. While anchor sensors improve localization accuracy, they can raise network costs.

Unknown_sensor_nodes depend on anchors for their location within the network. For example, in a dense forest where manual deployment is hard, nodes may be dropped from an airplane. Once deployed, nodes sense phenomena and send data to the central base station. If the sensing node's location is unknown, that data becomes useless. Localization helps nodes find their position in the network after deployment [4, 5].

1.3 WSN localization processes involve three steps

1.3.1 Distance/angle determination

At the first step, calculate the distance/angle evaluation between two nodes, and the gathered information is used in localization [6]. Numerous techniques, including received signal strength indicator (RSSI), time of arrival (ToA), time difference of arrival

(TDoA), and angle of arrival (AoA), are for the distance/angle [5]. Every technique holds some benefits and drawbacks [6].

1.3.2 Locality determination

At this step, calculate the location of the dumb_node along with distance/angle and anchor node information. Trilateration, multilateration, and triangulation are three different types of calculations [7]. Trilateration: A method of calculating a node's location by estimating its distance from three other nodes. Multilateration, where information from more than three nodes, is required in estimating the location. In triangulation, the estimation of the node location is calculated by the cosines and sines.

1.3.3 Localization algorithm

The localization algorithm is required to locate other dumb nodes in the network. There are numerous algorithms available to determine where the dumb nodes are in the network [6–8].

1.4 Blockchain integration

Despite the progress, WSNs have to face issues such as data tampering, node impersonation, and malicious attacks. This proposal integrates blockchain technology into WSNs by providing decentralized, tamper-resistant ledger systems that can improve integrity, authentication, and trust among nodes in the network. Blockchain-based WSNs provide traceability that makes them quite resistant to attacks and loss of data. This paper presents a methodology on how blockchain can be integrated with advanced localization techniques to solve security issues and precision errors in WSN environments.

The key contributions of this work are:

- Our proposed methodology ensures integration of blockchain that supports security against distributed denial-of-service (DDoS) attacks along with enhanced data integrity as well as network reliability.
- Implementation of DV-HOP algorithm to lower localization errors, get an estimation for node location and hence enhance the system performance through limiting unnecessary errors.
- Demonstrated an advanced localization algorithm with metrics of localized error and average localization error (ALE) to illustrate better nodes and accuracy in positioning along the network.
- Performance measures developed are false positive rate (FPR), false negative rate (FNR), energy consumption, and accuracy rates, which have helped to measure and enhance effectiveness.
- For robust node detection and recovery, 17% FPR and 15% FNR were achieved, ensuring reliable true/false detection with proper differentiation between the normal and malicious nodes.
- The overall stability of the network, throughput, and resilience of topology are improved and make the network adaptive for different environments.

This paper focuses on integrating blockchain and advanced localization in WSNs with a focus on security issues, data integrity, and accuracy. The importance of WSNs, along with their challenges and difficulties, has been provided. This introduces blockchain as an improvement to increase the security, as well as accuracy aspects, in the related WSN environment. The proposed methodology, discuss how blockchain is applied to WSNs and advanced localization techniques. The design process describes the research design, simulation parameters, and analysis methods. The performance analysis compares results that indicate improvement over traditional WSNs, and the conclusion presents the key findings and future directions.

A 2D simulation was preferred because of computational restrictions and simplicity of implementation. Although a 3D world may offer better realism, the underlying premises of DV-HOP localization and blockchain-based security hold valid. Since 3D node connectivity and distance estimation would be more involved, one or more path loss models or altitude-dependent adjustments would be needed. So, for the current simulation's constraints, emphasis is placed on checking the 2D scenario first. The existing model is for static WSNs, which are usually mounted in applications such as environmental monitoring and industrial use. Mobile nodes imply extra complexities like frequent changes in topology, which are not considered in this study. DDoS attacks and compromised nodes were chosen because they represent major dangers for WSNs, particularly in resource-scrambled systems. Although the other threats, such as eavesdropping or node impersonation, apply to the domain under consideration, mitigating them would necessitate additional security requirements, so the focus is on DDOS attacks.

2 Related work

Recent works on the sparrow search algorithm (SSA) focused on its optimization ability in a multidisciplinary domain application, like feature selection and data classification. Inspired by the foraging and anti-predation behaviors of sparrows, SSA can be transferred to other problem domains. In [7], the authors presented a chaotic version called CSSA, which injects chaotic maps into the SSA to improve its searching ability and convergence in large-dimensional feature selection. The adaptations of SSA were reviewed by authors and included its potential for solving complex engineering, healthcare, and robotics problems while advancing further to cope with multiobjective optimization challenges [8].

To oversee the issues that come in networks, the present study introduced those simulated frameworks that combine a management system with a blockchain ledger along with advanced robust techniques. The management system of the network identifies the working of nodes, the record of the blockchain ledger, and the integrity of data. They also ensure that data transmitted in the network is correct or not. They also enhanced the reliability of the network system [9].

The DV-HOP algorithm is used in terms of localization that estimates the position of nodes from one end to another end. They also ensure the working of different nodes in different environments. To enhance the accuracy, further created a mayfly algorithm. The mayfly algorithm refines the position of nodes correctly to reduce error from the system [10]. This simulated framework also analyzes the behavior of wireless nodes to increase the optimization of a network system.

This has led to the integration of a blockchain ledger with WSNs' management system to solve several key challenges. These involve node mobility, energy constraints, and the presence of unauthorized nodes. Because the blockchain keeps every record of transactions, it ensures that there can be no unauthorized alterations; thus, the data integrity and security of the blockchain are guaranteed [11]. Through a decentralized approach, trust in the network can be enhanced through the provision of a transparent, immutable record of node activities and data transmissions [12, 13, 22].

The DV-HOP algorithm is utilized in localization within the WSN. These algorithms are applied to the estimation of node positions, which ensures that data is accurately transmitted over the network. To attain better precision in such estimates, the DV-HOP algorithm might not be able to realize an appreciable level of accuracy. The mayfly algorithm is added to fine-tune node positions, hence ensuring that the errors on localization are minimized. The mayfly algorithm, as proposed, emulates the behavior of natural mayflies for the optimization of node placement, a process inspired by natural selection and swarm intelligence, hence making the network more accurate and reliable.

WSNs have been used in various applications, including environmental determination, healthcare systems, and smart cities. The position of setting multiple nodes to build a connection between the nodes is a critical part of WSNs. Various advanced techniques and methods are used to improve the connectivity and accuracy of the network implemented in the system by use of simulation [14]. The robust techniques are used to face challenges created by malicious nodes. WSNs enhance the accuracy and efficiency of network systems.

Distinct types of work have been implemented using various advanced techniques in WSNs. The DV-HOP algorithm is used to estimate the position of nodes from one end to another end. A graph is structured within the phase. Within the graph, representations of nodes and edges are described. To improve the location accuracy of the three-dimensional DV-HOP technique, we have presented an improved algorithm in this study. For localization, the suggested technique simply makes use of nearby beacon nodes. Additionally, an ideal group of beacon nodes surrounding an unknown node is chosen using the coplanarity notion in order to estimate its location [15].

The impact of malicious nodes directly affects the model of WSNs. Localization error calculation is used to calculate the accuracy of the DV-HOP algorithm. The error is to be calculated by comparing the original position and the estimated position of nodes by the DV-HOP algorithm. This calculation is performed in both scenarios with and without interference from malicious nodes [16]. The accuracy can be assessed using malicious nodes. This phrase is used to understand the drawbacks of the DV-HOP algorithm in different environments. The overall approach is used to determine errors that occur within the model. In this paper, the authors provide two computationally effective 'range-free' 3D node localization algorithms that make use of biogeography-based optimization (BBO) and hybrid particle swarm optimization (HPSO). The suggested method takes into account node deployment in an anisotropic environment that is restricted within three-layer boundaries. The suggested algorithms' performance is contrasted with two range-free approaches that are currently in use: the weighted centroid method and the simple centroid method. The outcomes show that our strategy performs better in terms of accuracy and scalability than these conventional techniques [17].

The concept of blockchain ledger technology is used to determine the behavior of WSNs by multiple change interaction. The blockchain ledger initialization is used to track a change that occurs within the nodes. They also monitor the working of nodes in different environment situations. The blockchain starts with a block by a characterized proof of 1 and a previous proof of '0.' The blockchain parameter will record the transaction whenever a node's credibility changes and provides a secure record of changes. This parameter ensures the integrity and credibility of a network system which is important for sustaining a network.

Many optimal algorithms, including the genetic algorithm, ant colony algorithm, and mayfly algorithm, all enhance the accuracy of WSNs. These algorithms set an optimal position of nodes to contain a desired output [18]. The mayfly algorithm resolved the problem that occurs within the WSN when malicious DDOS attacks the network model. The algorithm passes through multiple cycles, which settle their velocity and reduce the error. The position can be updated using an equation with random factors. This factor is used to detect the error. The intensity of the algorithm represents the accuracy of every position of the node. This is also used to calculate the sum of errors between the estimated position and the actual position. Through this updated algorithm, the error is to be minimized and increase the accuracy of the system network [19].

In [20], the authors suggest a novel technique called N2-3D-DV-HOP (non-dominated sorting genetic algorithm II with 3D distance-vector hop), which expands on the 3D-DV-HOP algorithm by using multiobjective model and NSGA-I to increase the positioning accuracy of nodes in a three-dimensional environment [20–23]. The overall process analyzes the performance of networks in different conditions, including the presence of malicious nodes. The mechanism improves the accuracy and reliability of WSNs in multiple environments [24–27].

The framework proposed in this paper simulates and studies the behavior of wireless nodes in different environmental conditions—an analysis important for fine-tuning network performance and efficient node operation, even in changing and demanding environments [21]. In the proposed system, blockchain technology with advanced localization algorithms like DV-HOP and mayfly improves the overall reliability, security, and accuracy of WSNs [24]. It will make the application areas more robust and adaptive in environmental monitoring, health care, and smart cities. This all-rounded approach shall have WSNs meet effectively [27–29] the demanding modern network applications without a sacrificial diminution of high standards in the maintenance of data integrity and operational efficiency [30].

In [23, 24], the authors address energy-efficient communication strategies, crucial for sustaining WSN longevity [30, 31], particularly in resource-constrained scenarios like ours.

The integration of blockchain [32, 33] for secure and reliable data management is highlighted in studies by [25, 26]. These works provide insights into using blockchain for secure consensus, offloading mechanisms, and vehicular data sensing [34], which are relevant to our research in mitigating DDoS attacks [35–37] and securing WSN communication. In [27], the authors explore federated satellite-ground networks [38], offering perspectives on distributed intelligence and secure computation that can enhance our deep learning-driven approach to WSNs [39, 40].

Recent advancements in wireless sensor networks (WSNs) emphasize the need for robust security mechanisms and efficient resource management [41, 42] Researchers have explored various approaches to enhance data integrity, communication reliability, and energy efficiency in WSN deployments [43–46]. Among these, blockchain technology and deep learning have emerged as promising solutions for addressing security vulnerabilities and optimizing network operations [47, 48].

Additionally, [49] propose innovative frameworks for integrating blockchain with IoT and air-ground networks, underscoring the importance of decentralized security and computational efficiency [50]. These insights reinforce our model's focus on integrating deep learning and blockchain to improve node localization and threat mitigation in WSNs using the DV-HOP algorithm. In [51], the authors focus on optimizing resource allocation and routing in cloud-based and mobile edge computing environments, which directly relate to improving WSN performance under constrained resources.

The paper is structured to provide an overview of the proposed improvements on WSNs using blockchain and localization techniques. The introduction emphasizes the importance of WSNs and raises challenges such as security and localization. Related Work reviews the studies performed so far and identifies the gap in this research. The proposed methodology explains how blockchain can be integrated with WSNs and how the DV-HOP algorithm can be used. Design process describes the experimental design and collection process of data. Performance analysis reports and compares the results with those of earlier methods. Conclusion summarizes main findings and future work.

3 Methods

The flow of the proposed work as how it works is shown in the following parts: initialization phase, simulation phase, reputation and energy update phase, localization phase, optimization phase, simulation execution and visualization phase, and performance evaluation phase.

Figure 2 presents to minimize localization errors using blockchain technology. The method starts with the initialization phase, where parameters, sensor data, and blockchain nodes are set up to track accurately. This preliminary setup is supposed to set up all the elements of the localization system so that they are ready to work collectively with one another for accuracy. The next phase is the simulation phase, in which the system simulates realistic scenarios to test the localization accuracy of the network. Data collected from this phase is used to monitor the present localization error. After this, blockchain reputation and energy update phase comes, which employs blockchain toward achieving the trustworthiness as well as the integrity of the data. This blockchain-based system uses the powers of blockchain, ensures that data like node positions as well as reputation scores, calculated by the previous performance of the localization, and is nothing but tamper-proof and non-transactional. The reputation-based mechanism is used to filter out the unreliable data; otherwise, localization error gets increase. In the next localization phase, the calculated reputation data is combined with sensor inputs, to calculate the position of node accurately. This localization further refines itself into an optimization phase wherein algorithms make any optimizations on the sensor data and blockchain records with error reduction in mind. In the simulation execution and visualization phase, the simulation is performed with the refined localization system, and

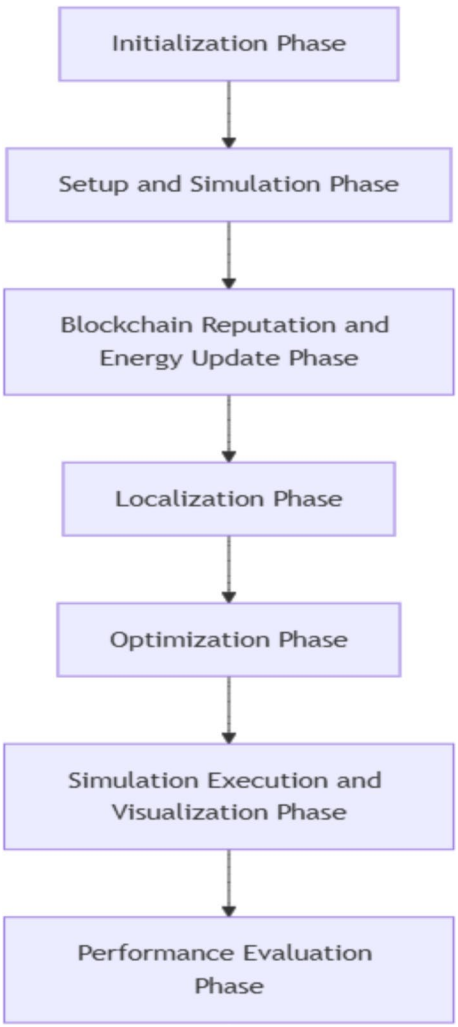

Fig. 2 Methodology of the proposed work. The figure represents minimizing localization errors using blockchain technology. The method starts with the initialization phase, where parameters, sensor data, and blockchain nodes are set up to track accurately. This preliminary setup is supposed to set up all the elements of the localization system so that they are ready to work in harmony with one another for accuracy

finally, the performance evaluation phase evaluates such improvement that the localization accuracy now shows—a methodology is efficiently making attempts to reduce error.

3.1 Initialization phase

3.1.1 Node deployment

The first step starts with the deployment of nodes. The nodes are deployed randomly in area, which are set to 800×600 square meters. Each node is allocated a desirable status, either 'normal' or 'malicious' which indicates a positive behavior with a combination of other nodes throughout the simulation framework.

3.1.2 Setting initial parameters

The next one communication range is set up to 150 m to communicate directly within a long distance. This parameter is crucial for creating a topology network. The term

topology means transmitting data from source to destination passing through a different parameter. Specification of simulation nodes also specified to run a model with 1000 rounds. This parameter is the foundation of simulation, to create a successful network.

3.1.3 Blockchain initialization

Blockchain ledger initialization is used to track a change that occurs within the nodes. They also monitor the working of nodes in different environment situations. The blockchain is initialized by an inaugural block differentiated through a proof value of 1 and an anterior hash value of '0.' The blockchain parameter will record the transaction whenever a node's credibility changes and provide a secure record of changes. This parameter ensures the integrity and credibility of the network system which is important for sustaining a network [50].

3.2 Simulation phase

3.2.1 Node movement

During this simulation phase, nodes remain static means nodes do not change the position. The different sensors are placed at different locations for monitoring purposes such as monitoring of environmental situations and health structure monitoring. This distribution will change with every round. This means nodes are randomly distributed per round [28]). The term static means that network topology is dependable. This parameter focused on this static approach describes the behavior of the WSN simulation model in different conditions.

3.2.2 Communication range visualization

The communication range of every node is visualized in circle form with a radius of 150 m. This circular structure helps to understand the communication linkage of nodes. When two nodes are linked with each other, then a line is drawn between them that indicates a connection between them. This communication range visualized the network topology between the nodes. The term topology means a network between the nodes to communicate with each other. This parameter is essential to analyze the performance of a network [29].

3.3 Reputation and energy update phase

3.3.1 Energy consumption

This step approximates the energy usage of every node since every node will spend 1 unit of energy every round. As soon as a node's energy reaches zero, its behavior can shift between regular and malicious behavior. Regular nodes are initially allocated a 100-unit energy buffer for continuous sensing and communication activities, while malicious nodes are allocated a smaller energy buffer. This distinction aims to simulate the restricted behavior of malicious nodes, which may attempt to disrupt network functionality.

Energy usage in WSNs is influenced by rate of data transmission, activity level of nodes, and environmental parameters. Data transmitting and receiving nodes at high rates consume energy rapidly, making efficient energy management methods necessary. An adaptive energy model allows simulation of real network trends, which ensures

robustness against passive and active security attacks [30]. This technique also focuses on the effect of energy supply on node performance and network stability.

3.3.2 Reputation management

A reputation system is used to monitor and rate the behavior of nodes during the simulation. The reputation score of each node is recorded and updated in the blockchain ledger, giving a transparent and tamper-evident history of its interactions. The reputation system considers deviations in node behavior, transaction time stamps, and rates of malicious behavior. The immutable nature of the blockchain ensures that any modifications to node credibility are safely stored, adding the reliability of the network. This system helps to identify and separate the nodes to enhance network reliability [31].

The mechanism of reputation is further reinforced through the application of solidity-based smart contracts. Node credibility is controlled by these contracts via an organized system that captures node energy levels and behavioral measures. Every node's Ethereum address is associated with a related reputation score, enabling monitoring in real time of trustworthiness. Malicious nodes can be marked within the system so that network administrators can isolate threats and ensure overall security.

By combining blockchain with reputation management, this system guarantees that only reliable nodes are involved in network operations, improving data integrity and deterring malicious behavior. This holistic solution leads to a more secure and efficient WSN environment, enabling applications where reliable sensor data is essential.

The contract includes three main functions:

registerNode: This function allows the registration of a node by associating its address with an initial energy value and a malicious status. This is typically done by the network's governing authority or an automated process.

$$\text{Node}_{\text{Ni}} = (Ai, E0, Mi) \tag{1}$$

where

- Ni is the ith node.
- Ai is the address of node Ni.
- E0 is the initial energy value assigned to the node.
- Mi is the malicious status, where Mi=1 if the node is malicious, and Mi=0 otherwise.

Update energy: This function updates the energy level of a node, enabling dynamic adjustment of its reputation. It ensures that only registered nodes can have their energy updated.

$$Ei = Ei + \Delta E \tag{2}$$

where *Ei* is the current energy of node Ni.

ΔE is the energy change for the node, which can be positive (reward) or negative (penalty).

This function only applies to registered nodes, ensuring that only nodes previously initialized with E0 can have their energy-adjusted.

isNodeMalicious and energy: These functions allow users to query the contract to check whether a node is malicious and to retrieve its energy level.

The functions check the malicious status Mi of a node Ni. If Mi=1, the node is classified as malicious; otherwise, it is not.

$$\text{Mi} = \begin{cases} 1 \text{ if node Ni is malicious} \\ 0 \text{ if node Ni is not malicious} \end{cases} \tag{3}$$

E0 is the initial energy of node Ni, ΔE_k is the kth energy update applied to node Ni, and n is the number of updates applied to the node.

The total energy Ei of node Ni at time t would then be:

$$Ei(t) = E_0 + \sum_{k=1}^{n} \Delta E_k \tag{4}$$

where Ei(t) is the current energy of node Ni at time t, and $\sum_{k=1}^{n} \Delta E_k$ is the sum of all energy changes (positive or negative) applied up to time t.

3.4 Localization phase

The DV-HOP algorithm is among the most popular localization algorithms in WSNs utilized to estimate the node positions. It operates via the utilization of hop counts as well as anchor nodes' distance estimates to the unknown nodes. The primary intent of DV-HOP is obtaining an efficient as well as economical node localization with no additional hardware installation, e.g., GPS. Instead, it applies the shortest path algorithm to determine the hop count between the nodes that are converted to physical distance using average hop length computation.

Localization precision is a very important challenge in WSNs, and DV-HOP is an important contribution toward minimizing positioning errors.

DV-HOP involves three major phases:

a. *DV-HOP estimation*: In the phase of estimating the distance, there is the formation of a graph structure whose nodes symbolize vertices while the edges symbolize the communication connections. A hop count between the nodes is established with a shortest path algorithm. This approach helps to estimate the positions of nodes [32]. This approach is crucial to determine the distance between the nodes to understand the network layers for further optimization.
b. *Localization error calculation*: In the phase localization error, a calculation of actual vs. estimated position difference facilitates accuracy assessment, particularly where malicious nodes exist. This calculation is performed in both scenarios with and without interference of malicious node. The accuracy can be assessed using malicious nodes. This phase is used to determine errors that occur within the model [34].
c. *Error correction*: In the DV-HOP algorithm, error correction comes from averaging hop distances so that a better estimation of localization is made. Such a computation calculates the average hop distance per node among all anchor nodes, and more reliable measurements can be computed based on varying topologies of networks. This computation further reduces the errors created from irregular distributions of nodes

along with inconsistent environmental settings using averaged distances for all the nodes

3.5 Optimization phase

3.5.1 Mayfly optimization

The mayfly optimization is used to filter the starting position estimated by the DV-HOP algorithm. The behavior of mayfly's optimization technique introduces the technique swarm-based optimization technique. This technique involves male and female mayflies that change their position based on personal and global environment. The algorithm passes through multiple cycles which may settle their velocity and reduce the error. The position can be updated using an equation with random factors. This factor is used to detect the error. The intensity of the algorithm represents the accuracy of every position of the node [35]. This is also used to calculate the sum of errors between the estimated position and the actual position. Through this updated algorithm, the error is to be minimized and the accuracy of the system network [33].

The mayfly optimization algorithm (MOA) was chosen in this study for its hybrid approach combining principles of swarm intelligence and evolutionary computation, making it particularly effective for complex optimization problems such as those in WSN. Unlike traditional algorithms, MOA mimics the behavior of mayflies to balance exploration and exploitation, which is critical in high-dimensional spaces where WSN nodes operate. The algorithm's adaptability allows it to quickly adjust to varying network conditions and counteract localization errors introduced by malicious nodes. Additionally, MOA optimizes node positioning with fewer iterations, which is beneficial for real-time WSN performance, conserving energy while maintaining accuracy and resilience to attacks.

MOA is a nature-inspired optimization algorithm based on the mating and flying behavior of mayflies. It depends on a swarm of 'male' and 'female' mayflies to explore a search space and improve solution precision, especially in scenarios with complex optimization processes like WSN. The algorithm strikes a balance between exploration (searching new regions) and exploitation (optimizing the existing solutions) by controlling the positions of the mayflies between their individual best positions and global best positions. Through iterative loops, the algorithm updates the velocities and positions of the mayflies to minimize localization errors to the lowest, which are very critical in WSN since the precise positioning of nodes is the core. The efficiency of MOA is pivotal in reducing computational cost and energy consumption while achieving high accuracy and robustness against threats like malicious attacks. Algorithm adaptability to fluctuating conditions renders it highly efficient for real-time optimization tasks for WSNs.

Table 1 describes how localization error varies with changes in the number of anchor nodes within a 100×100 area that contains a total of 100 nodes, and all nodes are working within a fixed communication range of 30. As the number of anchor nodes increases from 10 to 60, the DV-HOP error initially decreases (from 31.1035 to 28.5110) before rising again (up to 34.8248). In contrast, the mayfly error remains consistently lower than the DV-HOP error across all scenarios, indicating that mayfly is the more precise method. While having more anchor nodes initially enhances localization accuracy, there

Table 1 Average localization error for DV-HOP and mayfly optimization algorithm by changing anchor nodes

Area	Total nodes	Anchor nodes	Range	DV-HOP error	Mayfly optimization error
100*100	100	10	30	31.1035	25.6703
100*100	100	20	30	28.5110	24.1714
100*100	100	30	30	30.2875	24.4979
100*100	100	40	30	32.3154	24.9843
100*100	100	50	30	33.8520	25.4942
100*100	100	60	30	34.8248	26.0372

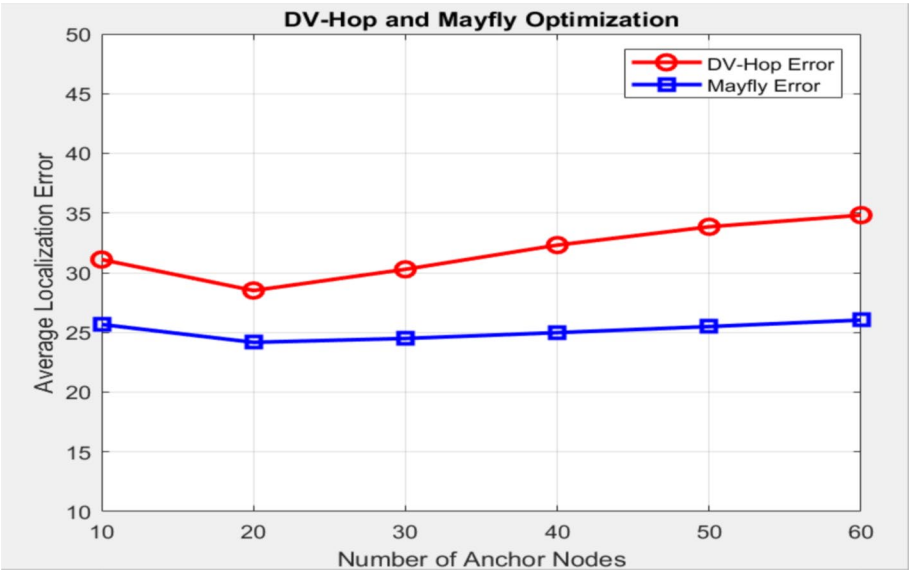

Fig. 3 Error as per the change in number of anchor nodes

is a threshold beyond which adding more anchors does not lead to significant improvements. The minimum error for DV-HOP is observed with 20 anchors (28.5110), while for mayfly, it is also at 20 anchors (24.1714). Overall, the mayfly method proves to be more dependable, consistently yielding lower localization errors. In Fig. 3 results of table are shown in the form of graph (Fig. 4).

Table 2 shows the variation in localization error as the total number of nodes increases in a 100×100 area, with the communication range maintained at 30 and the number of anchor nodes being adjusted. As the total number of nodes rises from 100 to 350, the DV-HOP error fluctuates between 28.3613 and 35.0477, while the error from the mayfly optimization method remains lower and more consistent. The minimum error for both techniques is noted at 150 total nodes and 20 anchor nodes. The mayfly optimization method demonstrates consistently superior performance compared to DV-HOP, indicating better localization accuracy. As additional nodes are introduced, the mayfly method shows greater adaptability, whereas DV-HOP encounters increased errors. The mayfly approach exhibits a more consistent error range, indicating its reliability for larger networks.

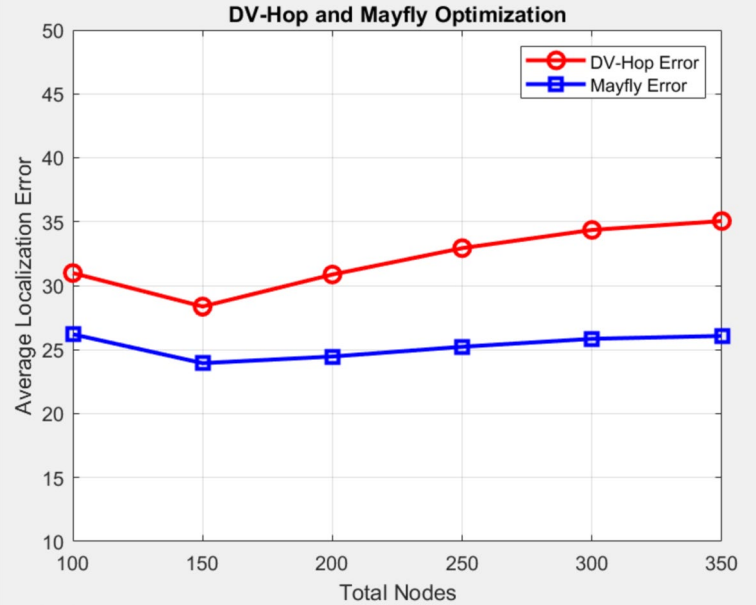

Fig. 4 Error as per the change in number of anchor nodes and total nodes

Table 2 Average localization error for DV-HOP and mayfly optimization algorithm by changing anchor nodes and total nodes

Area	Total nodes	Anchor nodes	Range	DV-HOP error	Mayfly optimization error
100*100	100	10	30	30.9797	26.2139
100*100	150	20	30	28.3613	23.9513
100*100	200	30	30	30.8647	24.4701
100*100	250	40	30	32.9288	25.2335
100*100	300	50	30	34.3512	25.8551
100*100	350	60	30	35.0477	26.0824

3.6 Simulation execution and visualization phase

3.6.1 Visualization

In this simulation phase, the node of the network is to be visualized on the screen highlight with distinct colors. The blue color shows normal nodes and the red color shows malicious nodes. The communication range represents circles and communication represents lines connecting with different nodes within the range. This visualization system understands network topology, the connection of nodes, and the interaction between the nodes. Changes in the position of nodes and energy levels are continuously updated providing a different condition of the network system over different time [34].

3.6.2 Simulation loop

In this phase, the simulation loop program adaptive rounds depend on the changes in the position of nodes and energy level of nodes. In every round, the movement of nodes,

communication range between the nodes, node visualization, energy consumption by nodes, and estimated position of nodes are executed optimistically. The error that occurs with normal nodes, as well as malicious nodes, is to be tracked and calculated by the simulation network. The overall process analyzes the performance of networks in different conditions including the presence of malicious nodes.

3.7 Performance evaluation phase

3.7.1 Localization error analysis

This phase examines the impact of malicious node behavior on system accuracy. Localization error is computed under both conditions—with and without the interference of malicious nodes. The error assessment is conducted across multiple rounds to evaluate the performance of the DV-HOP and mayfly optimized algorithms. Furthermore, this phase analyzes the influence of malicious nodes on network behavior.

3.7.2 Reputation system efficacy

The performance of the reputation system is measured as it is being watched in action on blockchain-logged transactions via simulation. The system is useful while monitoring network changes, especially against malicious node behavior. With improved blockchain ledger integrity and credibility, the reputation system secures the network and facilitates ideal node management. It validates the suggested model in sustaining network stability under different conditions [36].

This work contributes to developing a simulation platform to address critical challenges in wireless sensor networks (WSNs), including the interaction among energy usage, reputation management, and precision. The result of the model presented is likely to enhance efficiency and enable the development of more robust WSN networks in changing environments. By comparing the difference between normal nodes and the effect of attack nodes, overall network performance can be analyzed. The study also indicates the effectiveness of the system based on localization error and node location. The method proposed is designed to improve network performance under diverse conditions, even in the presence of a high number of malicious nodes.

To construct a deep framework for simulating a WSN with an efficient system, we can construct main three components: the network model, the attacked model, and the optimal model. Here each model is described as key formation and mathematical formulas.

3.8 Network model

The deep learning model with a gated recurrent unit is given in Fig. 5.

GRU-based secure and reliable WSN localization utilizes gated recurrent units (GRU) to enhance node localization accuracy and anomaly detection for WSNs. The model keeps track of sensor node data, network traffic, and blockchain activity logs against DDoS attacks and localization error reduction. It starts with feature extraction through min–max scaling or Z-score normalization and then proceeds with a stacked GRU layer for the detection of temporal dependencies and anomalies. Fully connected layers generalize the feature extraction and produce SoftMax-based classification to identify attacks. Classification is employed using binary cross-entropy, but estimation of localization error is performed with mean absolute error (MAE). Learning is assured by Adam optimizer, while performance is

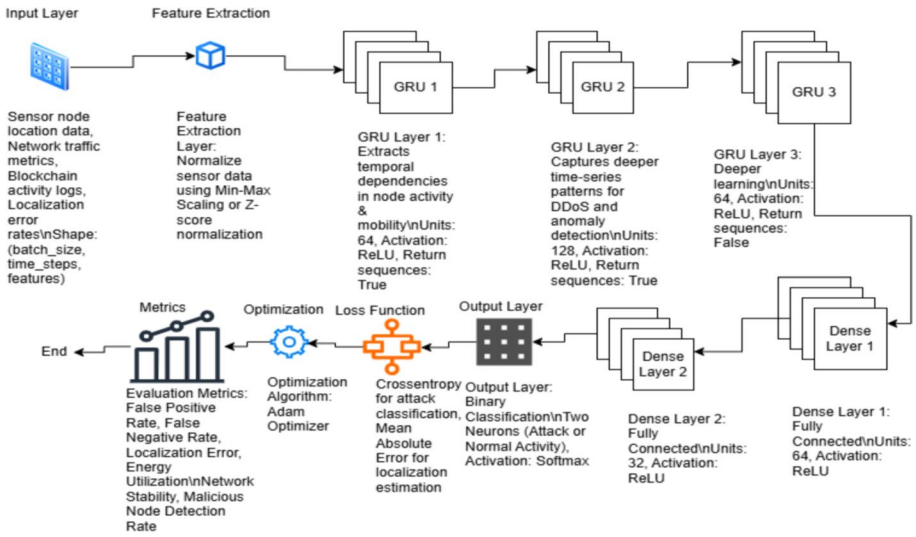

Fig. 5 Deep neural network model

monitored using metrics such as FPR, localization accuracy, and energy spent. The methodology increases network resilience, security, and energy efficiency, thus making WSNs less vulnerable to attacks while providing correct data transmission and localization.

The network model describes the structure and behavior of WSNs. The key formulation includes the position of nodes, a protocol for communication between nodes, and energy consumed by nodes [37].

3.8.1 Node deployment

- *Number of nodes* (N): Define a set of nodes $\{n_1,n_2,\ldots,n_N\}$.
- *Position of nodes* (p_i): Each node n_i has a position $pi=(x_i,y_i)$ in a 2D space, randomly initialized within the screen dimensions.

$$p_i = (x_i, y_i), x_i \in [0, \text{width}], y_i \in [0, \text{height}] \tag{5}$$

3.8.2 Communication range

Communication Range I: Nodes can communicate with each other if the Euclidean distance between them is less than or equal to R.

$$\text{if distance}(p_i, p_j) \leq R, \text{ then } n_i \text{ and } n_j \text{ are connected} \tag{6}$$

Distance calculation:

$$\text{Distance}(p_i, p) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{7}$$

3.8.3 Energy consumption

Energy level (E_i): Each node n_i has an energy level, initialized as normal or malicious energy based on its reputation.

$$E_i = \begin{cases} E_{\text{Normal}}, & \text{if Node is normal having energy} \leq 0 \\ E_{\text{malicious}}, & \text{if Node is malcious having energy} \leq 0 \end{cases} \tag{8}$$

3.8.4 Node evaluation

Evaluation (v): Nodes placed randomly with a speed of v, updating evaluation criteria at each time step.

$$p_i(t+1) = p_i(t) + v_i * \Delta t \tag{9}$$

where v_i is the normalized direction vector.

3.9 Attack model

The DDOS attack model simulates malicious behavior and its impact on the network, such as misreporting positions.

3.9.1 Reputation system

Reputation (r_i): Each node has a reputation status, either 'normal' or 'malicious.'

$$r_i = \begin{cases} \text{Normal, initially or when the node recovers} \\ \text{Malicious, is node energy is depeleted or node involvedin attack.} \end{cases} \tag{10}$$

Blockchain ledger: Records changes in reputation.

3.9.2 Localization error

Localization error (ϵ_i): The difference between actual and reported positions.

For normal nodes, the localization error is randomly assigned within the range of [−L, L], where L represents the predefined localization error limit. This ensures that the error distribution remains within a controlled boundary:

$$\in_i = \text{random}(-L, L) \tag{11}$$

For malicious nodes, the localization error is distributed within a broader range of [−2L, 2L], indicating a higher degree of deviation in estimated positions compared to normal nodes. This wider error distribution reflects the disruptive influence of malicious nodes on the network:

$$\in_i = \text{random}(-2L, 2L) \tag{12}$$

3.9.3 Localization and optimization model

This model involves estimating positions using DV-HOP and refining them using the mayfly algorithm.

3.9.4 DV-HOP estimation

- *Graph G(V,E)*): A graph where nodes are vertices V, and edges E represent communication links.

- *Hops calculation*: Use Dijkstra's algorithm to compute the shortest path (in hops) between nodes.

$$\text{hops}(n_i, n_j) = \text{Shortest path in terms of hops} \tag{13}$$

- *Position estimation*: Calculate estimated positions based on anchor nodes' positions and hop counts.

$$p_i = \frac{1}{|A|} \cdot \sum_{a \in A} p_a \tag{14}$$

where A is the set of anchor nodes.

3.9.5 Mayfly optimization algorithm

- *Initialization*: Define male and female mayflies' positions and velocities.
- *Light intensity calculation*: Based on Euclidean distance between estimated and actual positions.

$$I_i = \frac{1}{\left(1 + \sum (m_i - p_{\text{actual}})\right)^2} \tag{15}$$

- *Velocity update*: Update velocities based on personal and global best positions.

$$v_i(t+1) = v_i(t) + r_1(p_{\text{best } i} - m_i) + r_2\left(g_{\text{best}} - m_i\right) \tag{16}$$

- *Position update*: Update positions based on velocity.

$$m_i(t+1) = m_i(t) + v_i(t+1) \tag{17}$$

Table 3 presents the terminologies used within the framework.

4 Design process

The proposed methodology includes three key sections: determine the position of nodes, tracking of records by blockchain ledger, and mayfly optimization algorithm. The mayfly algorithm enhanced the accuracy of nodes within a wireless network system. The following practical setup will be shown as follows with the help of a table.

4.1 Experimental setup

Table 2 includes key parameters for the WSN simulation, the blockchain setup, the DV-HOP algorithm, and the mayfly optimization algorithm (Table 4).

4.2 Trust evaluation for beacon nodes

4.2.1 Objective

Evaluate and maintain the trust of beacon nodes (nodes with known positions) to ensure reliable localization and accurate reputation management.

Table 3 Terminology used within the framework

Variable	Meaning of Variable
N	Number of nodes in the network
N_i	With a node in the network
P_i	Position of node N_i in 2D space
X_i, Y_i	Coordinates of node N_i within the screen dimensions
R	Communication Range
Distance(p_i,p_j)	Euclidean distance between nodes N_i and N_j
E_i	The energy level of node
E_{Normal}	Energy level when a node is normal
$E_{\text{Malicious}}$	Energy level when a node is malicious
V	Speed of node movement
Δt	The time step for updating the position
R_i	Reputation status of node N_i
ϵi	Localization error of node n_i
L	Localization error range
$G(V,E)$	Graph where V are vertices (nodes), and E are edges (communication links)
Hops(n_i,nj)	The shortest path between nodes n_i and n_j in terms of hops
A	Set of anchor nodes
P_a	Position of anchor node a
I_i	The light intensity of male mayfly i
M_i	Position of male mayfly i
actual	Actual position of nodes
V_i	Velocity of male mayfly i
p_{besti}	Personal best position of male mayfly i
g_{best}	Global best position among all mayflies
R_1, R_2	Random coefficients for velocity update

Table 4 Parameters for the WSN simulation

Algorithm	Parameter	Value
WSN simulation	Number of nodes	20
	Communication range	150 m
	Number of rounds	1000
	Normal node energy	100 units
	Malicious node energy	50 units
	Localization error range	5 m
Blockchain	Initial proof	1
	Initial previous hash	'0'
DV-HOP estimation	Communication range	150 m
	Anchor nodes	Nodes with 'normal' reputation
Mayfly optimization	Number of iterations	100
	Number of mayflies	Equal to the number of nodes (20)
	Initial light intensity	calculated as $\frac{1}{1+\text{Sum of squared errors}}$
	Velocity update equation	$v_i = v_i + r_1 \times (p_{\text{best}} - x_i) + r_2 \times (g_{\text{best}} - x_i)$
	Position update equation	$x_i = x_i + v_i$
	Position clamping range	$[0,\ \text{width}]\,x\,[0,\ \text{height}]$

4.2.2 Process

4.2.2.1 Trust calculation Trust T_i of node i is determined based on its historical performance and reputation. For beacon nodes, trust is crucial for their role in localization.

$$\text{Define trust } T_i \text{ as}: \quad T_i = \frac{\text{Successful Transactions}}{\text{Total Transactions}} \tag{18}$$

where

- *Successful transactions* are the number of times the node has provided accurate and reliable data.
- *Total transactions* are the total number of interactions involving the node.

4.2.2.2 Trust update Trust is updated dynamically as nodes participate in network operations. For beacon nodes, trust is based on the accuracy of their reported positions. Any deviation from expected behavior impacts their trust level:

$$T_i^{\text{new}} = T_i^{\text{odd}} + \alpha \cdot \left(\text{Performance Metrics} - T_i^{\text{odd}}\right) \tag{19}$$

where

- *Performance metric* reflects the accuracy of the beacon node's position reports.
- α is a trust update factor ($0 < \alpha \leq 1$) controlling the rate of trust adjustment.

4.2.2.3 Beacon node selection Nodes with higher trust levels are chosen as anchors for localization to improve estimation accuracy.

4.3 Blockchain generation

4.3.1 Objective

Utilize blockchain technology to record and manage node reputations and transactions to ensure transparency and security.

4.3.2 Process

4.3.2.1 Blockchain structure The blockchain consists of a series of blocks, each containing:

$$\text{Block} = \left\{\text{index}, \text{time stamp}, \text{proof}, \text{previous}_{\text{hash}}, \text{Transaction}\right\}$$

where

Index is the position of the block in the chain.
Time stamp records the creation time of the block.
Proof is computational proof (e.g., PoW or PoS) ensuring block validity.

Previous Hash links to the hash of the previous block.
Transactions include reputation changes and other relevant data.

4.3.2.2 Transaction addition Transactions are added to the blockchain when node reputations change:

$$\text{Transaction} = \{\text{sender}, \text{receiver}, \text{amount}\}$$

where

Sender is the node whose reputation is being updated.
The receiver is typically a system or another node involved in the transaction.
Amount signifies the change in reputation or other relevant data.

4.3.2.3 Block creation New blocks are created and appended to the blockchain using the create_block method:

$$\text{New}_{\text{Block}} = \text{Blockchain.create}_{\text{block}}(\text{proof}, \text{previous}_{\text{hash}})$$

Proof and **previous_hash** ensure the block's integrity and link it to the previous chain.

In the proposed work, a new block is created when the create_block method is called. This typically occurs when a set of transactions has been collected, and the proof of work (PoW) has been completed. The create_block method constructs a new block by incorporating the current list of transactions, the proof obtained from solving the PoW puzzle, and the hash of the previous block.

4.3.3 Steps to create a new block

4.3.3.1 Transaction collection Transactions, which might include updates to nodes' energy levels or the registration of new nodes, are gathered into the current transactions list.

4.3.3.2 Proof of stake (PoS) The PoS mechanism ensures the validity of new blocks by selecting validators based on their stake rather than computational work. Unlike PoW, which relies on solving complex mathematical problems, PoS reduces energy consumption and enhances efficiency by allowing nodes with higher stakes or better reputation to validate transactions.

In this context, PoS can be influenced by the energy levels of participating nodes, dynamically adjusting the selection process based on reputation or energy metrics stored in the contract. This approach enhances security and reliability while maintaining network integrity in a more energy-efficient manner.

4.3.3.3 Block construction The new block is constructed and includes:

1. An index indicating its position in the blockchain.
2. A time stamp of its creation.

3. The proof of work.
4. The hash of the previous block.
5. Current transactions, such as updates to nodes' energy or malicious status.

4.3.3.4 Appending the block Once validated, the new block is appended to the blockchain. The current_transactions list is then reset for the next block.

4.3.3.5 Reputation influence In this, node energy levels and reputations stored in a smart contract become variables for block validation. Nodes with higher energy levels or reputations may have their transactions validated earlier or contribute more to the creation of new blocks. The smart contract is authenticated at certain time intervals or when some specific events are detected. It prevents unnecessary consumption of energy and helps in maintaining an updated network with fresh data. Nodes having excess energy or reputation can upgrade and authenticate more transactions in order to carry on safe and uninterrupted transactions. Normally, the system verifies the smart contract a few minutes at a time. During periods of high activity, such as when the system identifies suspicious behavior, it will verify more frequently. The dynamic approach keeps energy consumption smart yet block validation accurate and up to date.

4.3.4 Securing localization with blockchain

In wireless sensor networks (WSNs), precise localization is important for deciding node positions, which becomes a vital feature in environment monitoring and target tracking. Blockchain technology is used to keep a safe record that records all changes taking place within the nodes. This record enables tracking of node activity under various environmental conditions as well as promotes transparency in node actions [38]. The blockchain system updates its entries whenever a node's credibility status is changed, delivering a verifiable and secure history of changes. This ensures the reliability and integrity of the network that is fundamental in maintaining a stable and reliable system.

4.3.5 Energy and reputation management

Blockchain technology is used to track energy usage in WSNs. One energy unit is used by each node in one round of operation. The energy consumption model covers the expenses of sensor node operations, including communication. Once a node's energy supply depletes to zero, its activity can oscillate between 'normal' and 'malicious,' depending on the context. Normal nodes start with 100 units of energy, which makes the simulation realistic as nodes can fail or recover after some time [39]. In addition, blockchain also possesses a system of reputation management, which observes and evaluates the behavior of nodes. The system documents all the transactions, including node reputation adjustments, time stamps, and behavioral variations. By safely storing these variations in the blockchain ledger, the system is transparent and responsible. The system of reputation management can find and isolate malicious nodes, which will enhance the security and reliability of the network.

4.3.6 Consensus mechanism and block generation

A consensus protocol based on blockchain is used to authenticate transactions and ensure the integrity of the network ledger. A light consensus mechanism is used in WSNs because sensor nodes are resource-constrained. Proof of authority (PoA) is used to identify valid nodes that are tasked with authorizing transactions and creating new blocks. Block creation in this network is based on several parameters, including node energy levels, reputation values, and localization precision. Nodes having sufficient energy levels do not engage in unwanted interference, whereas reputation values are based on perceived data and consistency in behavior. Through the inclusion of these parameters, the network is secure and reliable [40]. The blockchain-based smart contract runs under different models of consensus, like proof of stake (PoS), instead of proof of work (PoW), which is more appropriate for public blockchains. PoS makes nodes with higher stakes or better reputation more influential in the validation of transactions, maximizing energy efficiency and security. This makes all the participating nodes come to a consensus about the validity of transactions, ensuring the stability and credibility of the blockchain network.

4.3.7 Reputation-influenced consensus

The contract tracks the reputation of nodes through the energy attribute and their behavior through the malicious flag. In a reputation-influenced consensus model, nodes with higher energy or better reputation may have a greater influence in validating transactions or generating blocks. For example, nodes with higher energy might be given priority in proposing or validating blocks, or malicious nodes could be penalized or excluded from participation.

To interfere the blockchain in WSNs, we created a system where data is to be secured through the energy level of nodes and records of the ledger. This block enhances the accuracy and reliability of network systems. This blockchain consensus is the decentralized approach of a network system. This approach helps to promote the credibility and integrity of network systems in different environments.

4.4 Mayfly optimization integration

4.4.1 Objective

Optimize node positions using the mayfly optimization algorithm to improve localization accuracy by iteratively refining estimates.

4.4.2 Process

4.4.2.1 Initialization Initialize mayflies' positions and velocities. Each mayfly represents a potential solution for the node positions:

$$\text{Position}_i = \text{current}_{\text{position}_i} + \text{velocity}_i^t \tag{21}$$

where Position_i^t is the position of the ith mayfly at iteration t. Velocity_i^t is the velocity of the ith mayfly at iteration t.

4.4.2.2 Light intensity calculation Calculate light intensity as a fitness measure based on proximity to the actual positions:

$$\text{Light}_{\text{intensity}} = \frac{1}{1 + \sum_j \left(\text{Position}_i - \text{Actual}_{\text{Position}_j}\right)^2} \tag{22}$$

where actual position$_j$ is the true position of the node j. Position$_i$ is the position of the ith mayfly.

4.4.2.3 Optimization process Update mayflies' velocities and positions based on personal and global best solutions:

$$\text{Velocity}_i^{t+1} = \text{Velocity}_i^t + r1 \cdot \left(P_{\text{Best}_i} - \text{Position}_i^t\right) + r_2 \cdot \left(G_{\text{Best}_i} - \text{Position}_i^t\right) \tag{23}$$

$$\text{Position}_i^{t+1} = \text{Position}_i^t + \text{Velocity}_i^{t+1} \tag{24}$$

where $r1$ and $r2$ are random coefficients between 0 and 1.

4.4.2.4 Final position update Use optimized positions for final localization estimation:

$$\text{Optimized}_{\text{position}_i} = \text{Position}_i^{\text{final}} \tag{25}$$

where $\text{Position}_i^{\text{final}}$ is the final optimized position of node iii after the algorithm converges.

By following this methodology as depicted in Fig. 6, the integration of blockchain with the mayfly optimization algorithm improves both the accuracy of localization and the management of node reputations within the network. This approach ensures

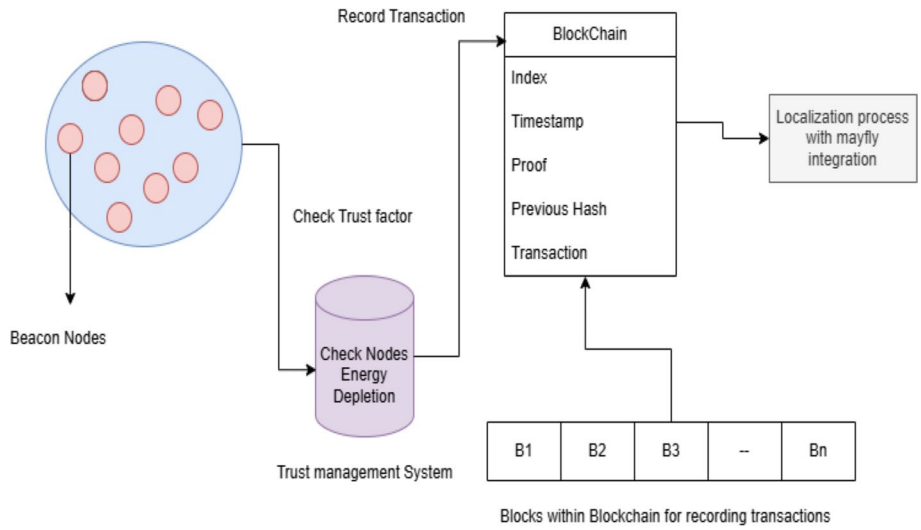

Fig. 6 Integration of blockchain with localization process. The image depicts the incorporation of blockchain technology into the localization process of wireless sensor networks (WSNs). By verifying transactions and keeping a decentralized ledger, blockchain provides safe and tamper-proof communication between nodes. The DV-HOP method is upgraded using deep learning techniques to assure exact node localization, while blockchain mechanisms safeguard the localization data and update the reputation ratings of nodes. This integration provides reliable network functioning even in the midst of possible security concerns, such as DDoS attacks, by boosting the accuracy and security of the localization process

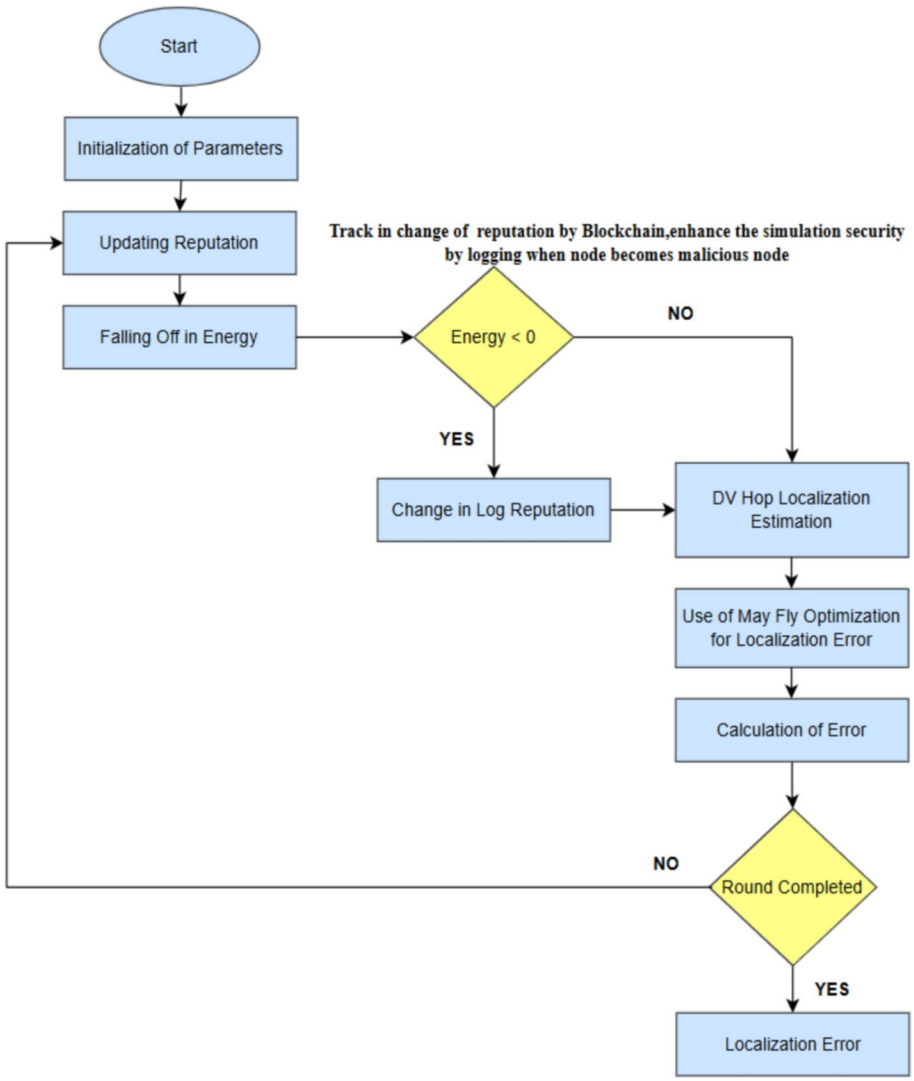

Fig. 7 Flowchart of the proposed work. The figure depicts the sequential processes involved in the suggested technique for upgrading wireless sensor networks (WSNs). The method begins with initializing network settings and building up the simulation environment. Blockchain is applied to provide secure communication by revising energy levels and reputation evaluations. The DV-HOP technique, coupled with deep learning, accomplishes precise node location, followed by optimization to increase network performance

secure, transparent, and effective node positioning and reputation management (Fig. 7).

The algorithms used for this work are given below.

Algorithm 1 DV-HOP estimation algorithm

```
1. Initialize network graph G with nodes and their positions.
2. for each node i in the network do
3.    Add node i to graph G.
4. end for
5. for each node i in the network do
6.    for each node j in the network do
7.       if i ≠ j and distance between i and j ≤ communication range then
8.          Add edge (i, j) to graph G.
9.       end if
10.    end for
11. end for
12. Initialize an empty dictionary for estimated positions.
13. for each node i in the network do
14.    if i is an anchor node then
15.       estimated_positions[i] = actual_position[i].
16.    else
17.       Calculate shortest path hops from node i to all other nodes.
18.       Select hops to anchor nodes.
19.       Calculate the average position of anchor nodes based on hops.
20.       estimated_positions[i] = (avg_x, avg_y).
21.    end if
22. end for
23. return estimated_positions.
```

Mayfly optimization algorithm

```
1. Initialize male and female mayfly populations with estimated positions.
2. Initialize velocities for male and female mayflies to zero.
3. Calculate the initial light intensity for male mayflies.
4. Set personal best positions for male mayflies to their initial positions.
5. Set the global best position to the position of the male mayfly with the highest light intensity.
6. for each iteration do
7.    for each male mayfly do
8.       Update velocity based on personal best and global best positions.
9.       Update the position of a male mayfly.
10.      Clip position to stay within boundaries.
11.      Calculate new light intensity for male mayfly.
12.      Update the personal best position if the new position has higher light intensity.
13.   end for
14.   Update the global best position if the new global best has higher light intensity.
15.   for each female mayfly do
16.      Update velocity based on the personal best of corresponding male and global best.
17.      Update the position of a female mayfly.
18.      Clip position to stay within boundaries.
19.   end for
20. end for
21. return optimized positions.
```

Simulation and evaluation

1. Initialize positions, reputations, and energy of nodes.
2. Initialize blockchain for reputation management.
3. while the simulation is running do
4. if the ratio of beacon nodes is being varied then
5. for each beacon ratio do
6. Select anchor nodes based on beacon ratio.
7. Perform DV-Hop estimation to get estimated positions.
8. Optimize estimated positions using Mayfly Optimization.
9. Calculate localization errors without attack.
10. Calculate localization error with attack.
11. Calculate the probability of finding true locations.
12. Store results.
13. end for
14. end if
15. if the ratio of malicious nodes is varied then
16. for each malicious ratio do
17. Update reputations of nodes based on a malicious ratio.
18. Select anchor nodes based on normal nodes.
19. Perform DV-Hop estimation to get estimated positions.
20. Optimize estimated positions using Mayfly Optimization.
21. Calculate the probability of finding true locations.
22. Store results.
23. end for
24. end if
25. Update node positions randomly within the movement speed limit.
26. Render nodes on screen.
27. Update screen.
28. end while
29. Plot results for localization error, probability of true locations, and comparative results.
30. Return Results

5 Results and discussion

In the proposed work, different several measures are created to calculate and compare the performance of the proposed localization and determine the detection of the algorithm between the existing methods. The different measures include localized error, ALE, accuracy rate, probability of location, and FPR. Each measure works on several aspects to increase the effectiveness of the algorithm. Localization error metric is focused on the behavior of malicious nodes on the accuracy of the system. Localization error is to be calculated in both situations with and without the interference of malicious nodes. The errors are to be determined in multiple rounds to execute the performance of DV-HOP and mayfly optimized algorithm. This approach analyzes how the malicious nodes affect the behavior of the network and resolves the problems that occur within the network. It specifically analyzes the location data such as mobile networks, sensor devices, and IoT applications. Localization ensures the accurate position of nodes and enhances the performance of the network system.

ALE means an error located over all the nodes in the network. The main objective of localization is to analyze the performance and accuracy of the algorithm. The ALE indicates that the position of nodes in the algorithm is specific. The ALE indicates the performance of the algorithm with the help of highlight lines or through the diagram.

The ALE determined the algorithm that which algorithm is used in which network environment to enhance the performance credibility. Practically we conduct that the ALE network maintains high efficiency and accuracy for different tasks including resource allocation, network connection, routing process, and maintaining a reliable network. The overall approach is to increase the performance and reliability of the network system as compared to [41–45].

Figure 8a shows the localized error is shown with or without evaluation of the trust model. With the evaluation of the trust model, the range of error is between 1 and 20 approximately, and without the evaluation of trust, the range of error is between 5 and 25. Localization error means an error located over all the nodes in the network. The main objective of localization is to analyze the performance and accuracy of algorithms. The LE Indicates whether the position of nodes in the algorithm is specific or not. Figure 8b shows the effect of beacon nodes on ALE in various terms. The lower ALE shows that the value of beacon nodes ranges between 5 and 10. Figure 8b demonstrates the impact of the number of beacon nodes on ALE for various methods. The proposed work shows that the value of lower ALE regularly ranging between beacon nodes is 5 to 10. In other highlighted methods, such as a [41–45] shows high ALE values ranging between 10 and 28, depending on the number of beacon nodes. This proposed supermodel maintains a low average localization error.

In Fig. 9, the credibility of finding out the true location of error by using the beacon nodes in the proposed work is high, value ranging between 0.85 and 0.98. Other method shows less credibility such as 0.7–0.85 for [41]) and 0.68–0.83 for [43]. This indicated that the proposed work is highly credible for finding the accurate location of errors. When the true location of the error is to be analyzed accurately then the proposed work is a further outcome to increase the performance of the system [41]. The proposed method maintains the probability of a range between 0.5 and 0.85 against the malicious

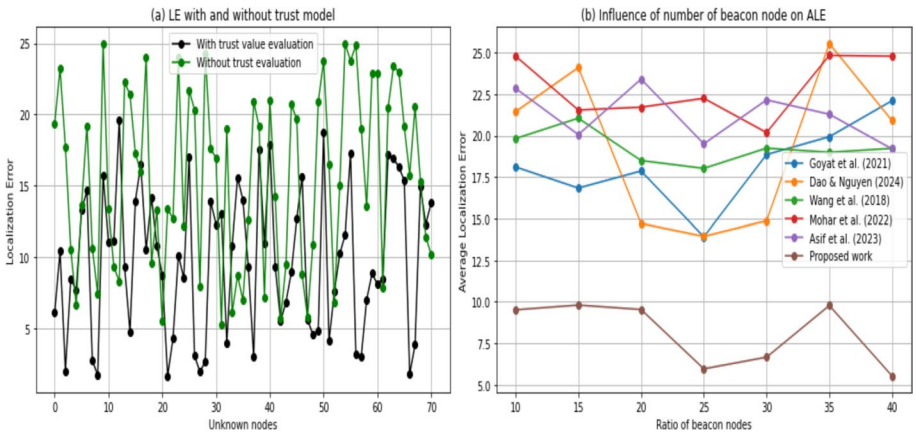

Fig. 8 Localization error with and without trust model, **b** impact of the number of beacons on average localization error (ALE). In the first diagram, **a** the localized error is shown with or without evaluation of the trust model. With evaluation of the trust model, the range of error is between 1 and 20 approximately, and without evaluation of trust, the range of error is between 5 and 25. Localization error means error located over all the nodes in the network. The main objective of localization is to analyze the performance and accuracy of algorithms. The LE indicates that the position of nodes in the algorithm is specific in nature or not. In the second diagram, **b** the effect of beacon nodes on ALE in various terms is shown. The lower ALE shows that the value of beacon nodes is ranging between 5 and 10. The second plot **b** demonstrates the impact of the number of beacon nodes on ALE for various methods

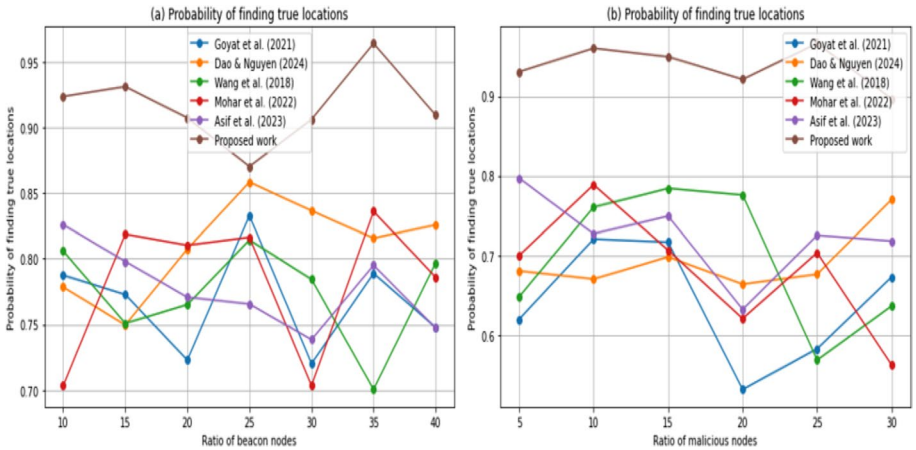

Fig. 9 Probability of finding true locations with beacon nodes. **b** Probability of finding true locations with malicious nodes. The credibility of finding out the true location of the error by using the beacon nodes in the proposed work is high, with a value ranging between 0.85 and 0.98. Other methods show less credibility, such as 0.7 to 0.85 for [41] and 0.68 to 0.83 for [43]. This indicated that proposed work is highly credible for finding the accurate location of errors. When the true location of the error is to be analyzed accurately, then proposed work is further outcome to increase the performance of the system [41]. The proposed method maintains the probability of a range between 0.5 and 0.85 against the malicious nodes. This shows the robustness of the proposed method against the malicious nodes

nodes. This shows the robustness of the proposed method against the malicious nodes (Table 5).

Table 5 shows the proposed work continuously to achieve an efficiently lower ALE compared with a localization algorithm indicating the high efficiency performance, localization accuracy, and the ratio of beacon nodes to malicious nodes.

Figure 10 shows that the determination of the accuracy of the proposed work is superior in nature range between 0.85 and 0.98, compared to the 0.49 to 0.89 range observed in other methods such as those by [41–45]. The accuracy under effectiveness of the proposed algorithm are high against the malicious nodes in the network system. This high detection accuracy underscores the effectiveness of the proposed algorithm in accurately identifying malicious nodes within a network.

The underlying mechanism shows the high accuracy detection in the model. The high accuracy is an integral part of the evaluated model. This model allocates specific values based on the behavior and work of nodes. The nodes work consistently containing a high performed value and the node works irregularly containing a low trust value. By this value, the accuracy and performance of the system are dependent. The consistent nodes easily tracked the unnecessary errors from the network. Further, the proposed work specifies robustness with the combination of machine learning techniques to analyze the behavior of nodes. This also analyzed the inconsistency of nodes which decreases the accuracy of the model. This includes various measures such as signal power, data efficiency, and timing of data transmission. This method is fast compared to a normal method to transmit the data from one end to another end. The algorithm is further ready to adapt to new threats to enhance the accuracy of the model. The overall approach indicates that the advanced analytical technique not only detects the malicious nodes but also minimizes the false activities on the network system. The advanced technique ensures the accuracy of the system model. The security is also enhanced using advanced

Table 5 Localization algorithms and % of beacon, malicious nodes along with average localization error

Localization algorithm	% of Beacon nodes	% of Malicious nodes	Average localization error (ALE)
Goyat et al., 2021 [41]	10	5	~24.5
	15	10	~21
	20	15	~23.5
	25	20	~16
	30	25	~20
	35	30	~21
	40	30	~21
Dao and Nguyen, 2024 [42]	10	5	~17
	15	10	~24
	20	15	~15
	25	20	~24
	30	25	~24
	35	30	~24
	40	30	~24
Wang et al., 2018 [43]	10	5	~19
	15	10	~19
	20	15	~19
	25	20	~19
	30	25	~19
	35	30	~19
	40	30	~19
Mohar et al., 2022 [44]	10	5	~23
	15	10	~24
	20	15	~24
	25	20	~18
	30	25	~21
	35	30	~21
	40	30	~21
Asif et al., 2023 [45]	10	5	~24
	15	10	~21
	20	15	~21
	25	20	~24
	30	25	~21
	35	30	~21
	40	30	~21
Proposed work	10	5	~8.5
	15	10	~9
	20	15	~9
	25	20	~8
	30	25	~8
	35	30	~8
	40	30	~8

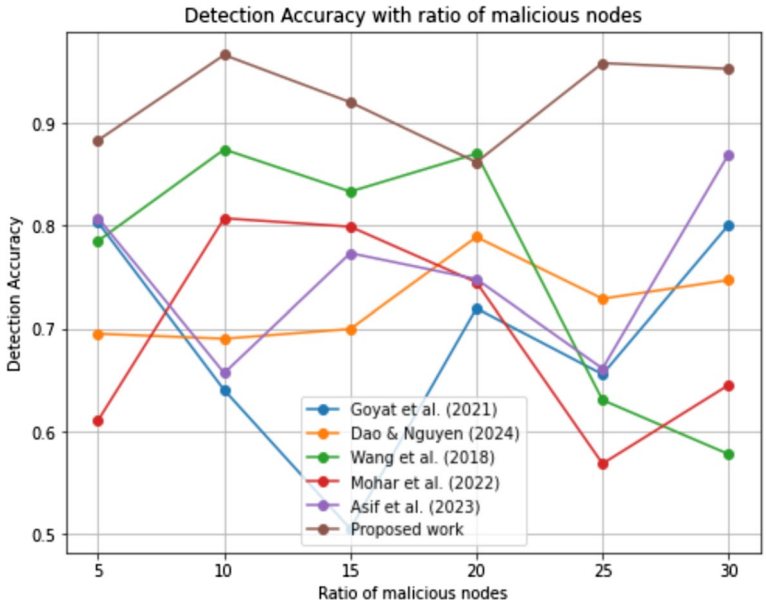

Fig. 10 Detection accuracy comparison. The determination of accuracy of the proposed work is superior in nature, with a range between 0.85 and 0.98, compared to the 0.49 to 0.89 range observed in other methods such as those by [41–45], The accuracy under the effectiveness of the proposed algorithm is high against the malicious nodes in the network system. This high detection accuracy underscores the effectiveness of the proposed algorithm in accurately identifying malicious nodes within a network

technique methods. This proposed work is highly reliable and ready to solve issues created by a malicious node.

Detection accuracy (DA): The proportion of true positive and true negative predictions out of all predictions.

$$\mathrm{DA} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{FP} + \mathrm{FN} + \mathrm{TP} + \mathrm{TN}} \times 100$$

where

- TP = true positives (correctly detected positive cases),
- TN = true negatives (correctly detected negative cases),
- FP = false positives (incorrectly detected positive cases),
- FN = false negatives (incorrectly detected negative cases).

False positive rate (FPR): The proportion of false positives out of all actual negatives.

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \times 100$$

False negative rate (FNR): The proportion of false negatives out of all actual positives.

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{TP} + \mathrm{FN}} \times 100$$

Average localization error (ALE): A metric that measures how far the detected object or region is from the actual object or region. ALE is typically measured in meters.

Scenario.

- Total number of objects: 100
- Actual positive cases (restricted objects): 50
- Actual negative cases (non-restricted objects): 50
- Metrics for the proposed work: DA = 91%, FPR = 17%, FNR = 15%

True positives (TP):

- Detection accuracy (DA) = 91%, meaning the system correctly identifies 91% of all cases.
- Thus, total correct predictions (true positives + true negatives) = 91% of 100 = 91 cases.
- We know that false positives (FP) and false negatives (FN) account for the remaining errors, which we will calculate next.

To start, calculate the false negative rate (FNR):

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{TP} + \mathrm{FN}} \times 100 = 15\%$$

Rearranging the equation to find FN:

$$\mathrm{FN} = \frac{\mathrm{FNR} \times (\mathrm{FN} + \mathrm{TP})}{100} = \frac{15 \times 50}{100} = 7.5 \approx 8$$

Therefore, FN = 8, meaning 8 actual positives were misclassified as negatives.
Thus, the number of *true positives (TP)* is:
TP = 50 − FN = 50 − 8 = 42.
False positives (FP):
The false positive rate (FPR) is 17%, which means 17% of the actual negative cases were classified as positive.

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \times 100$$

Rearranging to find FP:

$$\mathrm{FP} = \frac{\mathrm{FPR} \times (\mathrm{FP} + \mathrm{TN})}{100} = \frac{17 \times 5\big(\text{in percentage}\big)}{100} = 0.85 \approx 1$$

So, FP = 9, meaning 9 actual negatives were misclassified as positives.
Therefore, *true negatives (TN)* is:

$$\mathrm{TN} = 50 - \mathrm{FP} = 50 - 1 = 49$$

Detection accuracy (DA): Now that we have TP, TN, FP, and FN, we can verify the detection accuracy:

Table 6 ALE, average detection accuracy, false positive rates, and false negative rate comparison

Technique	ALE (m)	Average detection accuracy (DA) (%)	Average false positive rate (FPR) (%)	Average false negative rate (FNR) (%)
(Goyat et al., 2021[41])	~21	78	26	30
(Dao & Nguyen, 2024[42])	~20	81	28	27
(Wang et al., 2018[43])	~19	82	27	26
Mohar et al. (2022)	~20	80	29	28
(Asif et al.[45]., 2023)	~22	79	31	29
Proposed work	~8.5	91	17	15

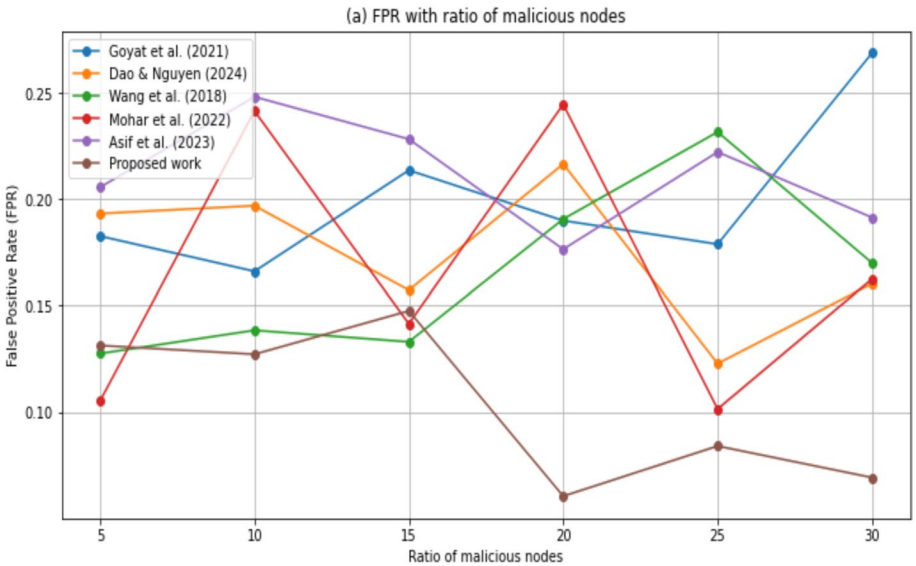

Fig. 11 Comparison of FPR. The false positive rate (FPR) of many methods for identifying malicious nodes in a network is shown in this figure. The suggested work outperforms other approaches, showing consistently low FPR over a range of harmful node ratios, with six experiments included. On the other hand, there are times when the FPR rises noticeably, especially when the ratio is 20. A ratio of 30 malicious nodes has the maximum FPR, while a more variable but still moderate FPR is shown. The graph highlights how effective the suggested effort is in reducing false positives

$$\mathrm{DA} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{FP} + \mathrm{FN} + \mathrm{TP} + \mathrm{TN}} \times 100$$

$$\mathrm{DA} = \frac{42 + 49}{42 + 41 + 9 + 8} \times 100 = 91\%$$

This comparative Table 6 shows the performance metrics of multiple localization techniques. The proposed work efficiently performs the terms of ALE with a value of approximately 8.5 m. It also achieves the highest average detection accuracy (91%) and the lowest average false positive rate (17%) and false negative rate (15%), defining the accuracy of localized nodes against the malicious nodes.

Figure 11 compares the FPR of various works in detecting malicious nodes in a network. Six studies are represented, with the proposed work showing consistently low FPR across different ratios of malicious nodes, outperforming other methods. In

contrast, experiences significant spikes in FPR at certain points, notably at a ratio of 20. The highest FPR at a ratio of 30 malicious nodes, while displaying more fluctuating but relatively moderate FPR. The graph highlights the effectiveness of the proposed work in minimizing false positives.

The graph shown in Fig. 12 presents the FNR with changes in ratios of malicious nodes in various aspects including [41–45] and the proposed work. The FNR calculated the proportion of actual malicious nodes incorrectly determined as non-malicious. The proposed work regularly shows a lower FNR, ranging from 0.1 to 0.25, showing optimal performance in identifying the malicious nodes in the correct order. Due to this variation, FNR value increases, peaking at 0.35. This indicates the proposed work's accuracy is higher and easy to detect malicious nodes.

The above-proposed approach results in WSN performance improvement in terms of several metrics are shown in Fig. 13. Packet transfer time is reduced by 10–15%; thus, data handling becomes faster. Clustering time is highly improved by 12–18% where the time to develop the network organization is faster. The first node death (FND) time increased by 8–12%. The last node death (LND) time is increased by 15–20%. Energy efficiency is also as much as 15–25% increased. So, the method is a highly desirable one for constrained environments in terms of resources. The packet loss rate is also lowered up to 10–15% with the system, which enhances the reliability of the data transmitted. These developments stand testimony to the efficacy of the proposed method in optimizing critical parameters of a WSN to approach a highly valued one toward the development of applications demanding efficient, long-lasting, and reliable networks. After all, the devised improvements together in energy management, data reliability, and network lifetime mark the superiority of the presented

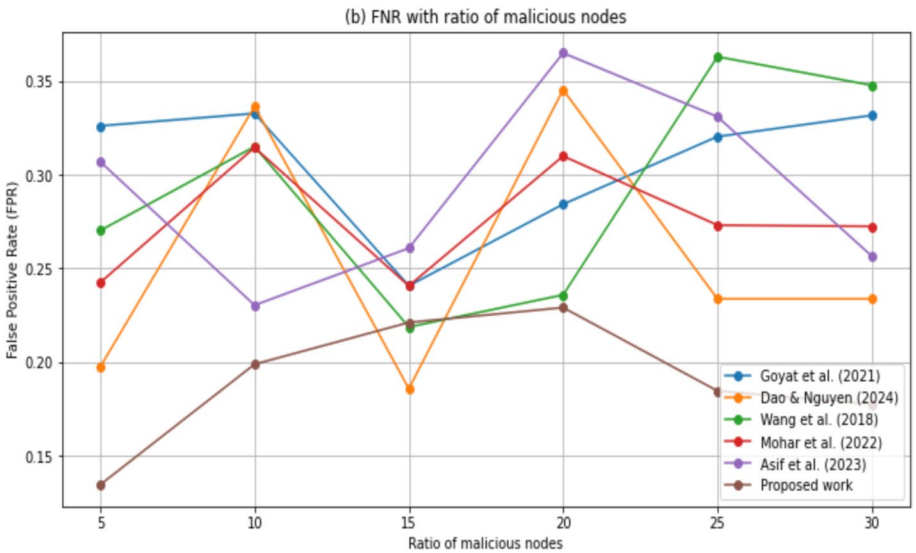

Fig. 12 Comparisons of FNR. The graph demonstrates the false negative rate (FNR) with varying ratios of malignant nodes in various aspects, including [41–45], and the proposed work. The FNR calculated the proportion of genuine malevolent nodes inaccurately designated as non-malicious. The proposed work routinely demonstrates a lower FNR, ranging from 0.1 to 0.25, demonstrating optimal performance to identify the malignant nodes in the correct order. Due to this variation, the FNR value is increasing, culminating at 0.35. This indicates the proposed work's accuracy is higher and straightforward to detect malicious nodes

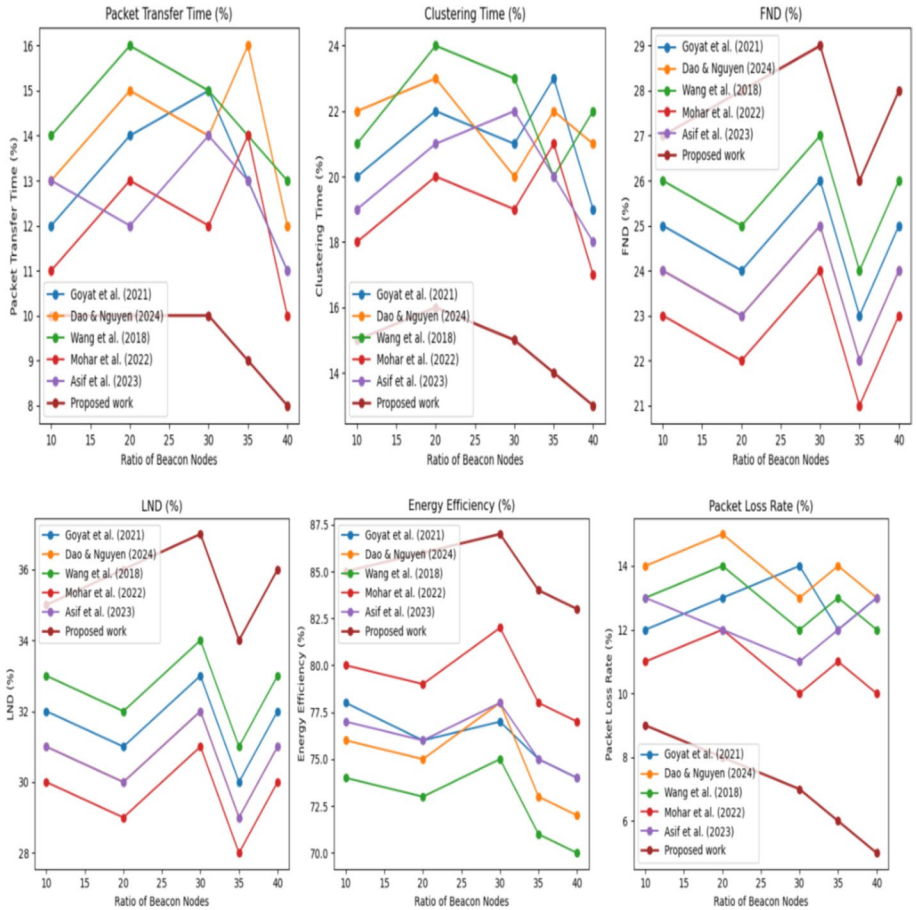

Fig. 13 Comparison of WSN performance metrics across techniques. The above-proposed approach results in WSN performance improvement in terms of several metrics, as shown in this figure. Packet transfer time is reduced by 10–15%; thus, data handling becomes faster. Clustering time is highly improved by 12–18% where the time to develop the network organization is faster. The FND time increased is by 8–12%. The LND time is increased by 15–20%. Energy efficiency is also as much as 15–25% increased. So the method is a highly desirable one for constrained environments in terms of resources. The packet loss rate is also lowered up to 10–15% with the system, which enhances the reliability of the data transmitted

approach compared with other techniques, making it an optimal solution for WSN real-world deployments.

6 Conclusion

The proposed method significantly enhances WSN performance values, primarily in the sense of enhancing localization precision, reducing localization error rates, and optimizing energy consumption. It reduces ALE by 8.5 m, compared to other techniques, in precise node positioning. It also enhances detection efficacy to 91%, lowering false positive and false negative rates to 17% and 15%, respectively. The very high accuracy level in malicious node discovery guarantees data integrity and secure communication across the network. This mechanism also increases energy efficiency and network longevity. Packet transfer time decreases by 10–15%, whereas the clustering time improves by 18%, leading to faster data exchange and better organization of the network. The enhanced FND and LND times also ensure a longer system

operating life, enhancing the dependability and solidity of the network. In addition, a 15% reduction in packet loss rates enhances the overall reliability and robustness of data over long-term WSN deployments.

In future, we can integrate GRU with CNN transformers for better spatiotemporal anomaly detection. Although no direct tests have been performed in 3D, the theoretical model is still scalable. Moreover, future research may also include the extension of the simulation to 3D space if more computational resources are available. Currently, mobility is not planned to be included because of complexity and increased computational overhead. Nevertheless, future versions may include mobility models if needed for certain applications. Since the emphasis was placed on static WSNs, algorithms such as DV-HOP were chosen. Mobility-based localization techniques, including Monte Carlo localization, were not explored in this research but might be a direction for future work. The system is only intended to monitor and counter unique threats. Multiple attacks target the system concurrently, the defense would be conditional on the success of blockchain-based reputation management. Anomaly detection could be implemented in future iterations to cover larger attacks.

Abbreviations

WSN	Wireless sensor network
DDOS	Distributed denial-of-service
DV-HOP	Distance-vector hop
FPR	False positive rate
FNR	False negative rate
GPS	Global positioning system
RSSI	Received signal strength indicator
ToA	Time of arrival
TDoA	Time difference of arrival
AoA	Angle of arrival
ALE	Average localization error
QoS	Quality of service
DA	Detection accuracy
TP	True positives
TN	True negatives
FP	False positives
FN	False negatives

Acknowledgements
This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number RSP2025R498.

Author contributions
Bhupinder Kaur was involved in conceptualization, data curation, formal analysis, methodology, writing—original draft, and software. Deepak Prashar was responsible for investigation, methodology, writing—original draft, and writing—reviewing and editing. Leo Mrsic took part in visualization, validation, and writing—reviewing and editing. Ahmad Almogren participated in writing—reviewing and editing, project administration, investigation, and methodology. Ateeq Ur Rehman assisted with writing—reviewing and editing, methodology, and conceptualization. Ayman Altameem helped with conceptualization, writing—reviewing and editing, and resources. Seada Hussen contributed to validation, investigation, and writing—reviewing and editing.

Funding
Not applicable.

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Competing interests
All authors do not have any financial and non-financial conflicts of interest.

Received: 30 November 2024 Accepted: 28 April 2025
Published online: 19 June 2025

References

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey. Comput. Networks **38**(4), 393–422 (2002)
2. J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)
3. O. Henry, Emerging issues in wireless sensor networks (2011).
4. J. Kuriakose, S. Joshi, R. Vikram Raju, A. Kilaru, A review on localization in wireless sensor networks. Adv. Intell. Syst. Comput. **264**, 599–610 (2014)
5. B. Kaur, D. Prashar, Localization in Wireless Sensor Network: Techniques, Algorithms Analysis and Challenges. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, (2021), pp. 1–7. https://doi.org/10.1109/ICRITO51393.2021.9596135.
6. S. Sivasakthiselvan, V. Nagarajan, "*Localization Techniques of Wireless Sensor Networks: A Review*," *Proc. 2020 IEEE Int. Conf. Commun. 799 Signal Process. ICCSP 2020*, (2020) pp. 1643–1648.
7. L.Y. Jia, T. Wang, A.G. Gad, A. Salem, A weighted-sum chaotic sparrow search algorithm for interdisciplinary feature selection and data classification. Sci. Rep. **13**(1), 1–28 (2023). https://doi.org/10.1038/s41598-023-38252-0
8. A. Saha, Application of sparrow search swarm intelligence optimization algorithm in identifying the critical surface in slope-stability. Discov. Geosci. **2**(1), 1–23 (2024). https://doi.org/10.1007/S44288-024-00070-W
9. N. Pan, L. Lv, R. Xiao, H. Wang, Z. Cui, A large-scale multi-objective firefly algorithm based on reward and punishment mechanisms and adaptive dimensional reorganization. Clust. Comput. (2024). https://doi.org/10.1007/S10586-024-04275-Z
10. Y. Zhao, C. Huang, M. Zhang, C. Lv, COLMA: a chaos-based mayfly algorithm with opposition-based learning and Levy flight for numerical optimization and engineering design. J. Supercomput. **79**(17), 19699–19745 (2023). https://doi.org/10.1007/S11227-023-05400-2
11. O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018). https://doi.org/10.1109/JIOT.2018.2812239
12. M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. **78**, 126–142 (2018). https://doi.org/10.1016/J.COSE.2018.06.004
13. C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, K.K.R. Choo, HomeChain: A blockchain-based secure mutual authentication system for smart homes. IEEE Internet Things J. **7**(2), 818–829 (2020). https://doi.org/10.1109/JIOT.2019.2944400
14 L. Zhao, K. Zhang, Y. Jia, An improved localization algorithm based on DV-Hop, in *Advances in Intelligent Systems and Interactive Applications: Proceedings of the 4th International Conference on Intelligent, Interactive Systems and Applications (IISA2019)*. ed. by F. Xhafa, S. Patnaik, M. Tavana (Springer International Publishing, Cham, 2020), pp.590–595. https://doi.org/10.1007/978-3-030-34387-3_72
15. A. Kaushik, D.K. Lobiyal, Enhanced three-dimensional DV-hop algorithm. Adv. Intell. Syst. Comput. **1270**, 269–278 (2021). https://doi.org/10.1007/978-981-15-8289-9_25
16. J. Yanfei, Z. Kexin, Z. Liquan, Improved DV-Hop location algorithm based on mobile anchor node and modified hop count for wireless sensor network. J. Electr. Comput. Eng. **2020**, 1–9 (2020). https://doi.org/10.1155/2020/9275603
17. A. Kumar, A. Khosla, J.S. Saini, S.S. Sidhu, Range-free 3D node localization in anisotropic wireless sensor networks. Appl. Soft Comput. J. **34**, 438–448 (2015). https://doi.org/10.1016/j.asoc.2015.05.025
18. A. Hadir, K. Zine-Dine, M. Bakhouya, J.E. Kafi, Novel localization algorithms in wireless sensor networks. Int. J. Wireless Mobile Comput. **16**(1), 80–96 (2019). https://doi.org/10.1504/ijwmc.2019.097439
19. G. Sharma, A. Kumar, Fuzzy logic based 3D localization in wireless sensor networks using invasive weed and bacterial foraging optimization. Telecommun. Syst. **67**(2), 149–162 (2018). https://doi.org/10.1007/s11235-017-0333-0
20. X. Cai, P. Wang, L. Du, Z. Cui, W. Zhang, J. Chen, Multi-objective three-dimensional DV-Hop localization algorithm with NSGA-II. IEEE Sens. J. **19**(21), 10003–10015 (2019). https://doi.org/10.1109/jsen.2019.2927733
21. N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, Secure IoT access at scale using blockchains and smart contracts. In *20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019*. (2019) https://doi.org/10.1109/WOWMOM.2019.8793047
22. B. Shala, U. Trick, A. Lehmann, B. Ghita, S. Shiaeles, Blockchain and trust for secure, end-user-based and decentralized IoT service provision. IEEE Access **8**, 119961–119979 (2020). https://doi.org/10.1109/ACCESS.2020.3005541
23. N. Gao, Y. Zeng, J. Wang, D. Wu, C. Zhang, Q. Song, S. Jin, Energy model for UAV communications: experimental validation and model generalization. China Commun. **18**(7), 253–264 (2021). https://doi.org/10.23919/JCC.2021.07.020
24. Y. Ma, T. Li, Y. Zhou, L. Yu, D. Jin, Mitigating energy consumption in heterogeneous mobile networks through data-driven optimization. IEEE Trans. Netw. Serv. Manage. **21**(4), 4369–4382 (2024). https://doi.org/10.1109/TNSM.2024.3416947
25. H. Luo, Q. Zhang, G. Sun, H. Yu, D. Niyato, Symbiotic blockchain consensus: cognitive backscatter communications-enabled wireless blockchain consensus. IEEE/ACM Trans. Netw. **32**(6), 5372–5387 (2024). https://doi.org/10.1109/TNET.2024.3462539
26. Y. Liu, Y. Zhao, A blockchain-enabled framework for vehicular data sensing: enhancing information freshness. IEEE Trans. Veh. Technol. **73**(11), 17416–17429 (2024). https://doi.org/10.1109/TVT.2024.3417689
27. Y. Gong, H. Yao, A. Nallanathan, Intelligent sensing, communication, computation and caching for satellite-ground integrated networks. IEEE Network **38**(4), 9–16 (2024). https://doi.org/10.1109/MNET.2024.3413543

28 D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Secure computation offloading in blockchain based IoT networks with deep reinforcement learning. IEEE Trans. Act. Netw. Sci. Eng. **8**(4), 3192–3208 (2021). https://doi.org/10.1109/TNSE.2021.3106956
29. S. Biswas, K. Sharif, F. Li, Z. Latif, S.S. Kanhere, S.P. Mohanty, Interoperability and synchronization management of blockchain-based decentralized e-health systems. IEEE Trans. Eng. Manage. **67**(4), 1363–1376 (2020). https://doi.org/10.1109/TEM.2020.2989779
30. R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund, V. Khetani, RDPC: Secure cloud storage with deduplication technique. *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, pp. 1280–1283 (2020). https://doi.org/10.1109/I-SMAC49090.2020.9243442
31. A.S.M. Sanwar Hosen, S. Singh, P.K. Sharma, U. Ghosh, J. Wang, I.H. Ra, G.H. Cho, Blockchain-based transaction validation protocol for a secure distributed IoT network. IEEE Access **8**, 117266 (2020)
32 A. Boukerche, H. Oliveira, E. Nakamura, A. Loureiro, *Localization systems for wireless sensor networks* (Wiley, Hoboken, 2008), pp.307–340
33. A. Boukerche, H.A.B.F. Oliveira, E.F. Nakamura, A.A.F. Loureiro, Localization systems for wireless sensor networks. Algorithms and Protocols for Wireless Sensor Netw 307–340 (2008a). https://doi.org/10.1002/9780470396360.CH11.
34. W.H. Cheng, J. Li, H. Li, An improved APIT location algorithm for wireless sensor networks, in *Advances in intelligent and soft computing 139 AISC*. (Springer, Cham, 2012), pp.113–119
35. B. Hofmann-Wellenhof, H. Lichtenegger, *Global positioning system: theory and practice* (Springer, Cham, 2012)
36 R. Goyat, M.K. Rai, G. Kumar, T.H. Kim, R. Saha, Energy efficient range-free localization algorithm for wireless sensor networks. Sensors **19**(16), 3603 (2019). https://doi.org/10.3390/s19163603
37. G. Han, H. Xu, T.Q. Duong, J. Jiang, T. Hara, Localization algorithms of wireless sensor networks: a survey. Telecommun. Syst. **52**(4), 2419–2436 (2013). https://doi.org/10.1007/s11235-011-9564-7
38. S. Yuan, B. Cao, M. Peng, Y. Sun, ChainSFL: Blockchain-driven federated learning from design to realization. In: *IEEE Wireless Communications and Networking Conference, WCNC*, *2021-March*. (2021) https://doi.org/10.1109/WCNC49053.2021.9417299
39. F. Yu, H. Lin, X. Wang, A. Yassine, M.S. Hossain, Blockchain-empowered secure federated learning system: architecture and applications. Comput. Commun. **196**, 55–65 (2022). https://doi.org/10.1016/J.COMCOM.2022.09.008
40. K. Toyoda, J. Zhao, A.N.S. Zhang, P.T. Mathiopoulos, Blockchain-enabled federated learning with mechanism design. IEEE Access **8**, 219744–219756 (2020). https://doi.org/10.1109/access.2020.3043037
41. R. Goyat, G. Kumar, M. Alazab, R. Saha, R. Thomas, M.K. Rai, A secure localization scheme based on trust assessment for WSNs using blockchain technology. Futur. Gener. Comput. Syst. **125**, 221–231 (2021). https://doi.org/10.1016/j.future.2021.06.039
42 T.-K. Dao, T.-T. Nguyen, An optimal node localization in WSN based on siege whale optimization algorithm. Comput. Model. Eng. Sci. **138**(3), 2201–2237 (2024). https://doi.org/10.32604/cmes.2023.029880
43. J. Wang, J. Cao, R.S. Sherratt, J.H. Park, An improved ant colony optimization-based approach with mobile sink for wireless sensor networks. J. Supercomput. **74**(12), 6633–6645 (2018). https://doi.org/10.1007/s11227-017-2115-6
44. S.S. Mohar, S.R. GoyalKaur, Localization of sensor nodes in wireless sensor networks using bat optimization algorithm with enhanced exploration and exploitation characteristics. J. Supercomput. **2022**(78), 11975–12023 (2022). https://doi.org/10.1007/s11227-022-04320-x
45. R. Asif, M. Farooq-i-Azam, M.H. Chaudary, A. Husen, S.R. Hassan, A distance vector hop-based secure and robust localization algorithm for wireless sensor networks. Electronics (Switzerland) **12**(10), 2237 (2023). https://doi.org/10.3390/electronics12102237
46. W. Zhao, F. Shao, S. Ye, W. Zheng, LSRR-LA: An anisotropy-tolerant localization algorithm based on least square regularized regression for multi-hop wireless sensor networks. Sensors **18**(11), 3974 (2018). https://doi.org/10.3390/s18113974
47. X. Chen, B. Zhang, 3D DV-hop localization scheme based on particle swarm optimization in wireless sensor networks. Int. J. Sensor Netw. **16**(2), 100–105 (2014). https://doi.org/10.1504/ijsnet.2014.065869
48. G. Sharma, A. Kumar, Improved range-free localization for three-dimensional wireless sensor networks using genetic algorithm. Comput. Electr. Eng. **72**, 808–827 (2018). https://doi.org/10.1016/j.compeleceng.2017.12.036
49. J. Yang, K. Yang, Z. Xiao, H. Jiang, S. Xu, S. Dustdar, Improving commute experience for private car users via blockchain-enabled multitask learning. IEEE Internet Things J. **10**(24), 21656–21669 (2023). https://doi.org/10.1109/JIOT.2023.3317639
50. S. Sun, S. Chen, R. Du, W. Li, D. Qi, Blockchain based fine-grained and scalable access control for IoT security and privacy. In: *Proceedings—2019 IEEE 4th International Conference on Data Science in Cyberspace, DSC 2019*, pp. 598–603 (2019). https://doi.org/10.1109/DSC.2019.00097
51. X. Zhang, D. Hou, Z. Xiong, Y. Liu, S. Wang, Y. Li, EALLR: Energy-aware low-latency routing data driven model in mobile edge computing. IEEE Trans. Consum. Electron. (2024). https://doi.org/10.1109/TCE.2024.3507158

Publisher's Note