Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

An Enhanced Source Location Privacy Protection Scheme for WSNS Using Multi-Phantom Differential Delay

R.Pitchandi 1 ,Dr. A. Swaminathan 2

1 Department of CSE, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai-600 117

2 Department of CSBS, Panimalar Engineering College, Chennai-600 123

Abstract

The Wireless Sensor Networks (WSNs) have been used in real time monitoring and data transmission in areas like surveillance, environmental monitoring and smart infrastructures and have become imperative in the industry. Nevertheless, the adversaries can easily track data packets to uncover the source node of an origin node because of their open communication lines and decentralized structure, making WSN highly susceptible to source location privacy attacks. To solve this critical problem, this study presents a new multi-layered privacy protection system that consists of four smart processes, including: Hybrid Energy Trust Node Estimation (HETNE) to select stable and trustworthy nodes using residual energy and behavioral reliability, Adaptive Fuzzy Privacy Clustering (AFPC) to create dynamic and privacy conscious clusters that consume minimum energy, Quantum Encryption Assisted Path Selection (QEAPS) to construct quantum secure and tamper free routing paths, and Multi-Phantom Differentiated Delay (MPDD) to create a series Combination of these techniques boosts anonymity, energy economy as well as routing security and greatly minimizes the probability of disclosure of source. Experimental analysis the given framework attains the best performance in energy consumption, a packet delivery ratio, network lifetime, safety period, and the range of privacy protection in comparison with the traditional approaches, which offer robust and privacy-sensitive communications in WSNs.

keywords: Wireless Sensor Networks, Source Location Privacy; Hybrid Energy Trust Node Estimation; Quantum Encryption; Phantom Nodes; Secure Routing; Privacy Protection.

1.Introduction

Wireless Sensor Networks (WSNs) comprise a network of distributed sensor nodes, which are used to measure physical or environmental conditions of temperature, motion, pressure or position. WSNs are an important part of different applications such as military surveillance, healthcare monitoring, and smart cities in the modern Internet of Things (IoT). Nevertheless, wireless communication is also broadcast by nature and WSNs are therefore very vulnerable to privacy violations, specifically the source location privacy (SLP) of

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

sensitive nodes [1]. To avoid tracing data packets to the origin node where important assets or confidential information can be revealed, the identity and location of the source node are important to protect. Within the scope of WSNs and the Internet of Things (IoT), source location security (source location privacy - SLP) is described as the ability to ensure that the physical location of a source node is not revealed to their enemies .The main aim of source location security is to ensure that an attacker cannot follow up and trace data packets to its source and then seize or destroy the object being tracked.

There are several location privacies of sources strategies proposed by researchers in WSNs. As an illustration, designed a privacy-saving mechanism of IoT-enabled WSNs that manage various assets, various location privacy-saving mechanisms of location-based services [2]. The Vector-Indistinguishability strategy, which guarantees privacy of the subsequent location data, and used Federated Learning in edge intelligence systems to secure smart healthcare systems. Also, suggested quantization-based privacy methods of stochastic optimization in a decentralized manner. Despite the fact that these approaches have enhanced privacy levels, it still has disadvantages including high energy usage, high overhead on communication, latency, and low scalability in a dynamic IoT setup. In order to beat these limitations, the suggested approach comes with an model, which combines smart node selection, adaptive routing, and lightweight encryption approaches [3].

The method retains the anonymity of source locations but does not affect the efficiency of the network. The system uses adaptive noise injection and node randomization techniques in order to deceive attackers are trying to follow data paths. Also, AI-based optimization will be incorporated to make sure that there will be a minimal amount of energy and delay during the transmission process [4]. The current proposal offers a powerful and scalable approach to ensuring privacy protection and energy and performance efficiency in IoT enabled WSNs to transmit data securely and therefore to greatly enhance the drawbacks of the current SLP mechanisms. The resolved the proposed method attackers are generally supposed to be well outfitted with such equipment as spectrum analyzers, capable of tracking network traffic, and employ Radio Frequency (RF) localization methods to track the strength of signal and angle of arrival of packets hop-by-hop through the network back to the source. The primary risk is contextual information (the pattern of traffic) and not the data packet content which may be encrypted. The packet is then sent to the base station by the phantom location either through a normal or secure route [5]. Effectiveness of source location security is generally defined in the terms of the safety period, which is the time period during which the source will be unnoticed by an adversary.

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

The primary value of the research is to:

- The smart WSN network that is privacy preserving and maintains its cost efficiency in communication by combining secure node selection, adaptive clustering, quantum-based protection of path security, and phantom-based privacy protection to enhance efficient data transmission.
- Dynamically estimate node reliability with respect to residual energy and level of trust HETNE to make sure that the participation of the node is optimal and secure.
- Determine a scheme of AFPC in order to create energy-efficient and privacy-sensitive clusters, which balance network load and enhance the stability of intra-cluster communication.
- Present an QEAPS protocol to define safe and hack-immune channels of communication based on quantum key encryption theories.
- Applies MPDD strategy to improve the privacy of source location through introducing multiple phantom nodes and variable delay transmission of the unpredictable routing paths.

The proposed WSN privacy model has been structured into five parts: Section 1 is the introduction, Section 2 is literature review, Section 3 is the proposed methodology, Section 4 discusses experimental results and performance measures whereby energy use, network lifetime, packet delivery ratio and source privacy were discussed, in addition to concluding the study with findings, limitations and future directions in Section 5.

2. Literature Survey

This proposed method involves the use of the Fuzzy and Distributed Autonomous Fashion Integration (IDAF- FIT) to cluster and in the meantime, the Cluster type of Head is selected as well [6]. The concept of routing is then initiated so as to pass the packet of the source to the target node by choosing the most appropriate route. ASLPP-RR, Routing, It is proposed to use an adaptive source location privacy preservation approach, and its more time complexity.

The existing scheme of location access control is inefficient as it does not ensure that the service providers that have been allowed access to location are not able to trace users. This essay is a proposal of a new privacy preservation location-based mobile application named MoveWithMe that is aimed at preserving privacy by spoofing queries whenever the user relies on location based mobile services [7]. Nevertheless, numerous mobile websites are gathering location data, and this is highly dangerous in terms of users being tracked down by mistake.

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

The effectiveness of shortest path protocol mechanism and soundness of the encryption are ensured, which enhances the location privacy and quality and safety of message delivery. Symmetric encryption and asymmetric encryption are the only major forms of a key management with varied methods of implementation [8]. This discusses the issues of ensuring security of sensor nodes through encryption methods and how we have beaten these problems with the aid of sophisticated technologies.

Sensor node location is among the most significant and essential information in the Wireless Sensor Networks (WSNs) because on which many location-based applications are primarily based [9]. This paper is a critical study of the specifics of the location privacy protection policies and explains the prominent processes within each policy. Nevertheless, the attackers can find the actual location of the source node with a lot of ease by deriving and examining the location information embedded within the data packets.

Table 1: Different Method in Source Location Privacy Protection Based on the WSN Technology

Author/Year	Techniques Used	Security Range	Limitations
Alrizq et al. (2024) [10]	Artificial Intelligence-based Node Location Optimization	Optimizes sensor node placement using AI to improve network coverage and connectivity	High computational complexity for large dynamic networks
Yuan et al. (2025) [11]	AI-Driven Optimization Algorithm	Enhances blockchain scalability and privacy using AI optimization	Complex AI-blockchain integration may increase latency
Mahmood et al. (2022) [12]	Reinforcement Learning Algorithm	Reinforcement learning-based fault detection for sensor reliability	Long training phase; environment-dependent performance
Lilhore et al. (2022) [13]	Depth-Controlled Energy-Efficient Routing Protocol (DEERP)	Energy-efficient routing protocol with depth control	Limited scalability and delay due to underwater signal attenuation
Kumar et al. (2022) [14]	Hybrid Competitive Swarm Optimization	Blockchain with lightweight secret sharing for secure medical data	Parameter tuning is complex; not suitable for highly mobile nodes

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

	(CSO) + Harmony Search Algorithm	exchange	
Li et al. (2023) [15]	Blockchain with Lightweight Secret Sharing Scheme	Hybrid swarm optimization for energy-efficient cluster head selection	High cryptographic computation load on low-power IoT devices
Singh et al. (2022) [16]	Federated Learning + Blockchain Framework	Privacy-preserving data sharing through federated learning and blockchain	Communication overhead and dependency on continuous connectivity.

Table 1: different method in source location privacy protection based on the WSN technology, including the techniques used, limitations, and security range.

Although the success has been achieved in data reliability, acoustic underwater communication channel is energy consuming in one node. A replacement and recharge of the battery of a submerged tip can be extremely costly [17]. To present a network architecture named Member Node Supported Cluster-Based Routing Protocol (MNS-CBRP) to provide a stable information transfer speed with the participation of the member nodes of the network, more energy consumption in run time performance.

The approach is an order of magnitude faster than traditional methods in terms of time complexity due to the use of a Generative Adversarial Network (GAN) generation methods. CEC information in the IoT systems is usually of high risk of privacy leakage because the data is large, strongly confidential, and highly secured, and cost range of the implementation process [18].

The suggest a strong architecture to anonymize spatiotemporal path datasets, termed as Machine Learning-Based Anonymization (MLA). In order to ensure the privacy of the highly sensitive datasets, a variation of the k-means algorithm has been suggested [19]. In the meantime, enhanced the alignment process by adding the multiple sequence alignment into the MLA workflow. All the algorithms and its framework were tested on the T-Drive, GeoLife and Gowalla location datasets, and more storge of the process in create the network issue.

Provides a solution to one of the location-based query problems. The location server would like to have a degree of control on its data, as the data is its property. To suggest a significant improvement on the earlier solution, which involves a two-stage solution where

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

the former stage is Oblivious Transfer and the latter step is Private Information Retrieval, to obtain a secure solution to both parties, high level of the signal issue in process [20].

3. Proposed Methodology

The proposed starts with HETNE that chooses the best and energy nodes using residual energy, trust level and stability of links to secure and balanced network performance. After identifying optimal nodes, AFPC clusters them into clusters fuzzy logic whereby each head of cluster is selected dynamically to ensure a balance of energy and privacy of the data. The QEAPS uses Quantum Encryption-Assisted Path Selection after clustering to create an unbreakable quantum key using Quantum Key Distribution (QKD) to ensure that data is not intercepted when being transmitted. Lastly, MPDD enhances source location privacy by channeling the data by the means of variable delay mechanisms and through a number of phantom nodes to form an immaterial transmission path. These synergistic approaches are a united intelligent workflow, which is more privacy protecting, energy saving, and resistant to tracking or eavesdropping attack in Wireless Sensor Networks.

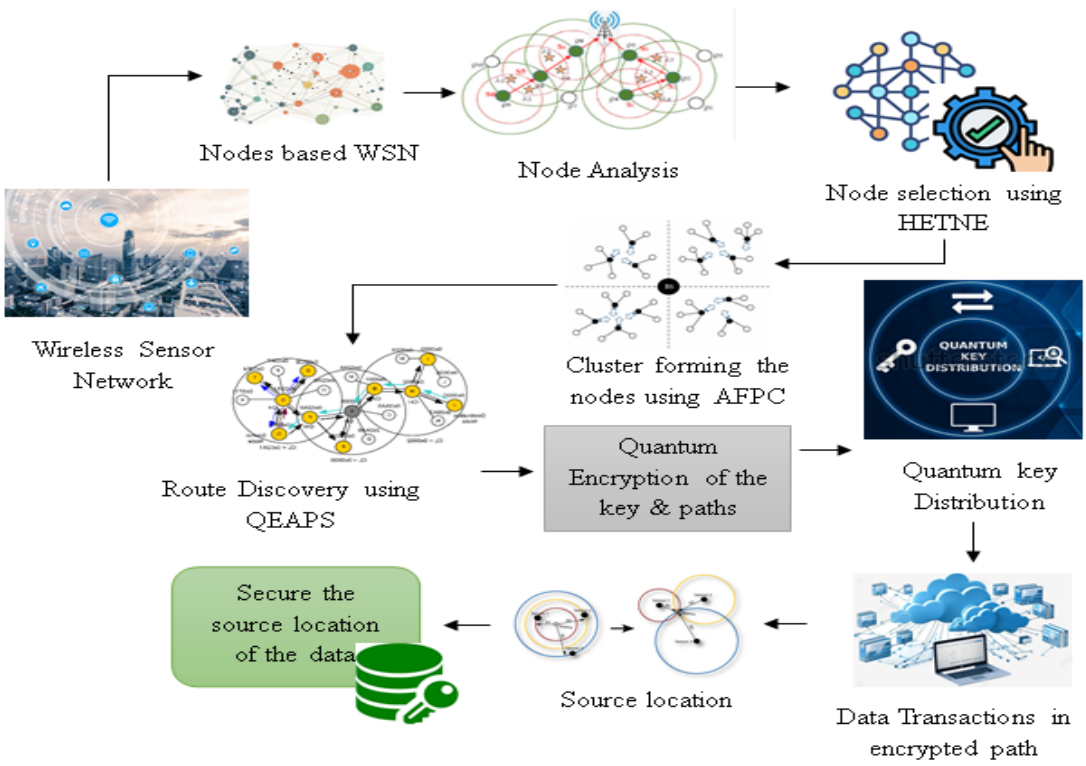

Figure 1: Architecture Diagram of Source Location Privacy Protection Scheme Using MPDD

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

Figure 1 show that the protecting source location privacy in wireless sensor networks is described in the workflow diagram. It involves an organized and intelligent multi-stage process. It begins with the wireless sensor networks where sensor nodes are used for monitoring and for collecting information. Through the node analysis, the HETNE finds the most trusted and energy-efficient nodes by looking at residual energy and trust parameters. The identified nodes are then clustered through AFPC. The AFPC algorithm employs fuzzy logic to form clusters of nodes that are energy-balanced and privacy-aware, in addition to allowing nodes to act as cluster heads dynamically. The next stage is known as QEAPS which protects the communication paths between the cluster heads and the sink by generating quantum-based encryption keys that actively ward off eavesdropping and tampering. At this stage, the data transactions are completed over these protected paths. The final stage is the protection of source location of the data in multi-phantom routing which introduces randomness and differential delay so that it is practically impossible for adversaries to determine the true source location of the data packet.

3.1 Hybrid Energy Trust Node Estimation (HETNE)

The node selection in the WSNs to the process of identifying and selecting the most appropriate sensor nodes to be involved in particular activities of the network like collection of data, routing, or forming a cluster. Because sensor nodes are generally energy constrained and deployed in large quantities, it is important to choose the appropriate nodes to ensure that the network is efficient, lasts long and is reliable. This is normally chosen using the critical parameters such as residual energy, communication range, the quality of the link, the level of trust and the stability of the node. The nodes that have more energy resources and high trust rates are favored to provide consistent performance and reduce the likelihood of failure or malicious actions. Proper node selection will ensure that the network is well balanced in terms of its energy consumption, will not experience congestion and will have a longer network life. The node selection process in an advanced WSN architecture is made adaptive, intelligent and privacy-sensitive with the help of fuzzy logic, swarm intelligence, and machine learning techniques.

The presented equation 1 that identifies the activation energy of a node, and all nodes N_i were rated by their residual energy E_i. Assuming that the power of a node is higher or at least equal to the threshold E_{th}, the node is considered active (N_i^{active}) and can be involved in network activities.

$$E_i \geq E_{th} \Rightarrow N_i^{active} \quad (1)$$

$$N_i^{active} \Rightarrow T_i = \frac{P_{succ,i}}{P_{total,i}} \quad (2)$$

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

After the equation 2 node is active, its trust value T_i is calculated as a ratio between successful packets transmission $P_{succ,i}$ and the total packets being processed $P_{total,i}$. This will make sure that only nodes which have a perfect track record of transmissions are eligible to further process.

$$T_i \Rightarrow F_i = \alpha E_i + \beta T_i + \gamma LQ_i + \delta S_i \quad (3)$$

The equation 3 calculation of the fitness score F_i is done by combining several parameters, including the residual energy E_i, trust value T_i, link quality LQ_i, and node stability S_i. The coefficients (α, β, γ) are used to balance the effects of each parameter based on the aims of the system.

$$F_i \geq F_{avg} \Rightarrow N_i^{selected} \quad (4)$$

Nodes with a fitness score F_i greater than the average fitness score F avg are referred to as selected nodes $N_i^{selected}$. The step will guarantee the selection of high-performing nodes, which have the best energy and trust values, and balance between performance and resource usage in equation 4.

$$N_i^{selected} + E_i \geq E_{th} \Rightarrow NS = \{N_i\} \quad (5)$$

Lastly, the nodes that are left to meet the energy threshold E_{th} are were put into the final node selection set NS. This makes sure that the nodes used in the subsequent steps such as clustering or routing are energy-efficient and reliable to offer a stable ground on the network in equation 5.

3.2 Adaptive Fuzzy Privacy Clustering (AFPC)

Once the node has been selected in WSN, cluster formation commences whereby, the selected nodes are grouped in terms of proximity, energy level and communication range to form effective communication zones. Every cluster is assigned a Cluster Head (CH) who is typically the node with the most residual energy and trust to handle the data aggregation and transmission to the base station. The other nodes will be member nodes where their sensed data is sent to the CH rather than the sink communicating with the sink. Such a process reduces the power usage and minimizes communication overhead. The CH periodically switches to high-energy nodes to ensure that there is a balance in the network and that the lifetime is extended. It is in this stage that nodes communicate with each other control messages to find the best grouping where the intra-cluster distance is the lowest possible and the grouping has good connectivity. In totality, the formation of clusters will increase the

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

efficiency of energy, scalability, and data security as the foundation of further actions such as safe routing and preserving privacy of source position in the WSN.

The membership strength $m_{i\to j}$ of node itoward candidate cluster head j is defined by this equation 6. It is a combination of three normalized parameters namely distance $d_{i,j}$ and residual energy E_j and link quality LQ_j. The 3-parameter weights $\omega_1, \omega_2, \omega_3$ modify the control of the effects of each parameter to trade off between energy efficiency and network reliability.

$$m_{i\to j} = \omega_1\left(1 - \frac{d_{i,j}}{d_{\max}}\right) + \omega_2 \frac{E_j}{E_{\max}} + \omega_3 LQ_j \tag{6}$$

$$CH_k = \arg\max_{j\in C_k} \Phi_j, \text{where} \Phi_j = \alpha E_j + \beta T_j + \gamma LQ_j \tag{7}$$

The equation 7 is used to choose a Cluster Head (CH) of each cluster C k according to the maximum utility score Φ_j. The score is the sum of residual energy E_j,trust factor T_j, and the link quality LQ_j of every node, weighted with 3 parameters.

$$\bar{D}_k = \frac{1}{|C_k|}\sum_{i\in C_k} d_{i,CH_k} \tag{8}$$

This equation 8 estimates the mean intra-cluster distance $\bar{D}_k$ the distance of member nodes to their Cluster Head. To reduce Dd in the process of establishing clusters making compact and energy-efficient clusters.

$$\bar{D}_k = \frac{1}{|C_k|}\sum_{i\in C_k} d_{i,CH_k} \tag{9}$$

$$E_k^{cluster} = \sum_{i\in C_k} E_{tx}(d_{i,CH_k}) + E_{agg} + E_{tx}(d_{CH_k,sink})$$

This equation 9 calculate the total energy consumption $E_k^{cluster}$in one cluster C_k. It has three terms (1) energy used by the member nodes to transmit data to the CH denoted by $E_{tx}(d_{i,CH_k})$; (2) energy used in data aggregation at the CH denoted by E_{agg}; and (3) energy used by the CH in sending the aggregated data to sink node denoted by $E_{tx}(d_{CH_k,sink})$. The system compares it to direct-to-sink transmission energy to establish that cluster-based routing is actually power-saving and network lifetime is enhanced.

$$(E_{CH_k} \le E_{th\_rot}) \Rightarrow CH_k \leftarrow \arg\max_{j\in C_k\setminus\{CH_k\}} \Phi_j \tag{10}$$

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

Once the energy of the current E_{CH_k} drops below a predetermined threshold E_{th_rot}, the system will automatically choose the new CH_k a member of the rest of the cluster with the same utility score Φ_j. This active rotation system allows balancing the energy consumption of the network since no node is overloaded in equation 10.

3.3 Quantum Encryption assisted Path Selection (QEAPS)

The section explained that data transmission in the WSNs once the clusters are formed, Quantum Key Distribution (QKD) is used to create encryption keys that cannot be broken by any person between cluster heads and the base station so that communication paths cannot be compromised by eavesdropping and tampering. After creating clusters, the system compares various routing paths, on the basis of energy usage, trustworthiness and stability of links. Quantum-assisted encryption is used to select the optimal path in dynamically balancing load and ensuring data privacy. The packets that are sent along the chosen path are coded using quantum-generated keys and it is impossible to intercept or alter the information without the notice of the attacker. This pathing mechanism using quantum security helps not only in attacking routing-based attacks but also provides an improved level of data integrity, privacy, and power consumption, which builds upon the privacy of location of sources framework in the WSN.

The equation 11 depicts the QKD procedure between the Cluster Head CH and the Sink node. A secure and unbreakable encryption key, $K_{CH,sink}$, is created using quantum cryptography, allowing data communication to be safe from interception or alteration. This key serves as the basis for secure routing and encryption in the next phases for data transmitting.

$$K_{CH,sink} = QKD(CH, sink) \tag{11}$$

$$C(p) = \sum_{(i,j)\in p} \left[\omega_1 E_{tx}(d_{i,j}) + \omega_2(1 - T_{i,j}) + \omega_3(1 - LQ_{i,j})\right] \tag{12}$$

This equation 12 specifies the path cost function with each link (i, j) in the path p evaluated in aspects of energy consumption E_{tx}, trustworthiness $T_{i,j}$, and link quality $LQ_{i,j}$, and the weight coefficients enforce importance of each aspect.

The best routing path p^* is chosen from all possible paths p, based on the lowest cost value $C(p)$. The construction ensures that only paths that are secured with current quantum keys $K_{i,j}$ are deemed valid in equation 13.

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

$$p^* = \arg\min_{p \in \mathcal{P}} C(p) \text{ subject to } \forall (i,j) \in p: K_{i,j} \quad (13)$$

$$K_{path} = Derive(\{K_{i,j} \mid (i,j) \in p^*\}) \Rightarrow C_{text} = Enc_{K_{path}}(\text{payload}) \quad (14)$$

This equation 14 incorporates both the derivation of path keys and the encryption of data. After the optimal routing path p^* is selected, the quantum keys along the path $K_{i,j}$ are combined using a key derivation function to produce a single session key referred to as K_{path}. This unified key is then used to encrypt the data payload into the ciphertext referred to as C_{text}, such that only authorized nodes along the quantum-secured route can decrypt.

$$\text{Verify}_{K_{path}}(C_{text}) = \begin{cases} \text{TRUE} & \Rightarrow \text{deliver to sink} \\ \text{FALSE} & \Rightarrow \text{raise alert, } p' = \arg\min_{p \in \mathcal{P} \setminus \{p^*\}} C(p) \end{cases} \quad (15)$$

The verifies the authenticity of the data being sent while detecting potential attacks, and the received ciphertext $C_{text}$is verified using the same session key K_{path}. If this verification is successful TRUE, then the packet is sent to the sink node in equation 15. If the verification was not successful TRUE, this indicates either data tampering or eavesdropping, and the system will generate an alert and reselect a different secure path p'. This action preserves the authenticity of the data, protects against replay or man-in-the-middle attacks, and maintains secure communication despite any adversarial conditions.

3.4 Multi-Phantom Differential Delay (MPDD)

The section enhances the privacy of source localization, which is introduced by unpredictability of the transmission pathways in the data. Once the safe route has been established using QEAPS, MPDD creates several phantom nodes, virtual or randomly chosen intermediate nodes that are used to represent the decoy sources and hide the actual origin of the data. The source node sends packets to one or more phantom nodes vaguely selected on energy efficiency and network topology instead of sending data to the sink. These phantom nodes then send the data on randomized paths via a differential delay mechanism, in which the packets are sent out at different times, and are sent on alternate paths. This measure greatly disorients attackers who are trying to establish the connection of the source of communication. MPDD guarantees robust source location privacy protection in the wireless sensor networks by combining phantom routing and adaptive delay management to ensure a high level of anonymity, route randomness, and high resilience to location-based attack.

The presented equation 16 role detects possible phantom nodes P_{ph} based on three parameters namely residual energyE_i, distance to sink $D_{i,sink}$ and trust T_i. These nodes

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

possessing a high energy, adequate distance and trust values are the best kind of nodes that can be selected to act as decoy nodes in confusing the attackers.

$$P_{ph} = f(E_i, D_{i,sink}, T_i) \tag{16}$$

The equation 17 determined potential phantom nodes P_{ph}, a random set of n nodes N_{ph} is sampled. This random selection provides an element of randomness such that the data origin cannot be identified, even if the attackers observe the communication pattern.

$$N_{ph} = \text{RandSelect}(P_{ph}, n) \tag{17}$$

The equation 18 produces multiple alternate pathsR_{alt} from phantom nodes to sink based on the network topology Topo_{WSN}. This function produces a number of paths that are both randomized and energy-efficient to achieve route diversity and obfuscate the true source.

$$R_{alt} = \text{RouteGen}(N_{ph}, \text{Topo}_{WSN}) \tag{18}$$

The differential delay mechanism implements a time delay in the transmission of each packet Δt where αis a scale factor and T_{max} the maximal allowed delay.

$$\Delta t = \alpha \times \text{Rand}(0, T_{max}) \tag{19}$$

By randomizing the packets transmission time, this enhances the anonymity and diminishes the ability of an attacker to draw temporal traffic correlation in equation 19.

$$\text{SLP}_{MPDD} = \sum_{i=1}^{N_{ph}} [\eta \cdot R_{alt_i} + \beta \cdot \Delta t_i] \tag{20}$$

This equation 20 represents the overall Source Location Privacy (SLP) level achieved by MPDD. It represents the combination of the route randomness R_{alt_i} multiplied by η and the differential delay Δt_i multiplied by β. A higher SLP value indicates that the true source location is better protected against tracing and eavesdropping.

4. Result and Discussion

The performance evaluation of the MPDD method against other techniques such as GAN, MLA, and MNS-CBRP indicates an improvement in performance metrics. The safety window increases because the MPDD technique dynamically weakens the likelihood of nodes being compromised early. The energy consumption per packet is significantly decreased due to the balanced nature of data transmissions, and the adaptive delay control that prevents particular nodes from being overused. Consequently, the increased lifetime for

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

the sensor network allows for prolonged periods of connectivity and session existence since the data collected can be transmitted at a later time. The packet delivery ratio is very high meaning reliable transmission of packets without continuous interruptions, and without regard to the malicious adversary. The probability of source disclosure is minimized since the adversary is misled by using random paths in place of nearby phantom paths—thereby enforcing a stronger location privacy. The privacy range is also enhanced due to the routing that has a multipath structure coupled with the delay, which increases anonymity overall. Overall, the MPDD is a better technique for privacy, efficiency, and transmission reliability over existing techniques.

Table 2: simulation Parameter

Parameter	value
Number of nodes	250
Language Name	Python
Network size	3500m*3500m
Sink Location	Centre
Package transmission interval	1s
Length of message	1024 bits
Length package head	34 bits

In the table 2 demonstrate the simulation incorporates 250 nodes set within a 3500m × 3500m field, with the sink located in the center of the field for balanced communication. The simulation is programmed in Python, and each node transmits a 1024-bit message every 1 second to allow for continuous monitoring. Each packet includes a 34-bit header, with control and routing information, for effective and safe delivery of information.

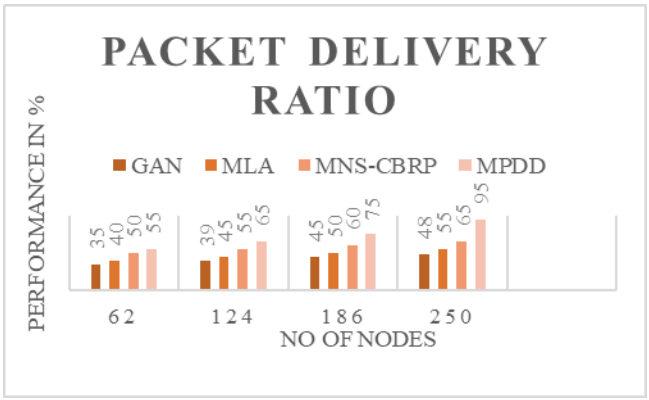

Figure 2: Analysis of packet Delivery Ratio

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

Figure 2 shows an enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 77%, 82%, and 87% the proposed method GAT prediction packet delivery ratio in 95%, respectively. The proposed system has a better PDR than the traditional WSN technique because it uses QEAPS to discover routes in a secure and efficient manner. Consistent encryption of paths makes packets fail to get lost through ill intent interceptions. This will guarantee that a higher percentage of packets are received at the target destinations.

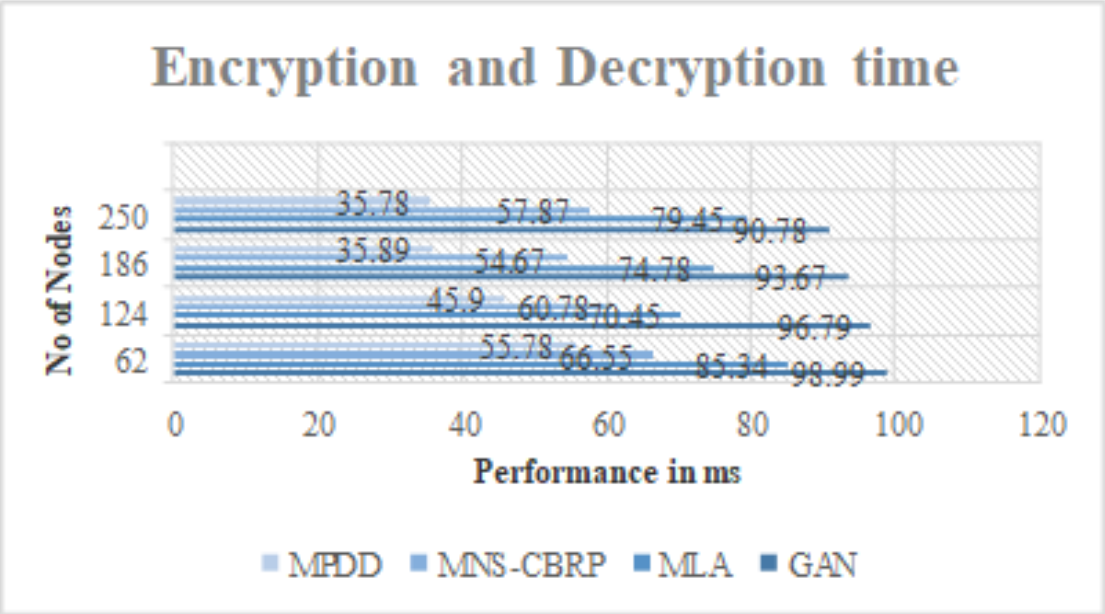

Figure 3: Analysis of Encryption and Decryption time

Figure 3 shows enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 57.67ms, 62.56 ms, and 77.56 ms the proposed method MPDD prediction encryption and decryption time in 22 ms, respectively. Encryption and decryption delays are also very minimal and the security of data confidentiality is guaranteed with quantum-based encryption. The proposed system is more effective in protecting data as compared to the traditional cryptographic models. This improves security and efficiency of communication.

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

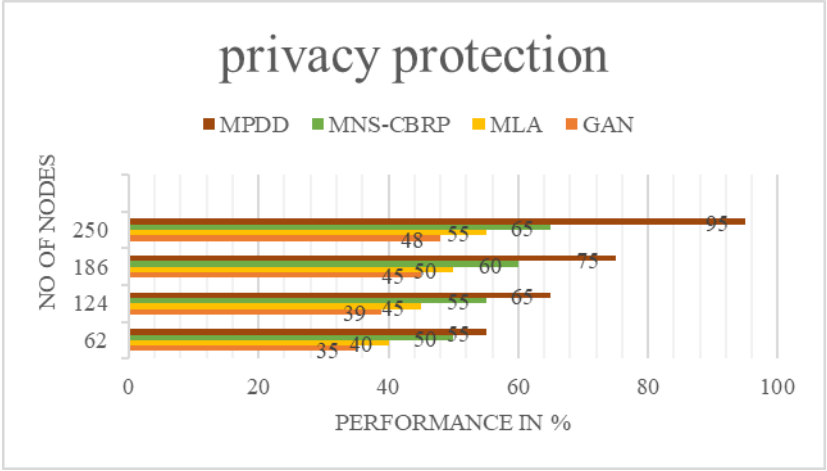

Figure 4: Analysis of privacy protection

Figure 4 shows enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 77.78%, 82.90%, and 87.67% the proposed method MPDD prediction privacy protection range in 95.45%, respectively. The system increases the privacy protection range by moving dynamically phantom nodes and delay patterns. This is such that the location of the source will be concealed even in distances. It, therefore, offers a greater protection of privacy than the method of the past WSNs.

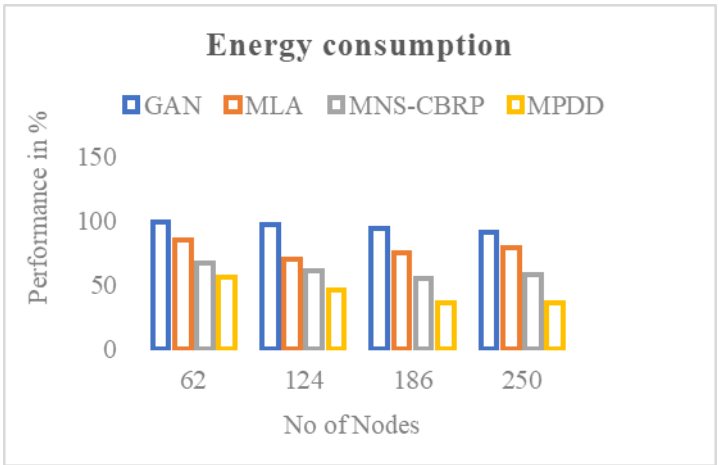

Figure 5: Analysis of Energy consumption

Figure 5 shows enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 77.78%, 82.90%, and 87.67% the proposed method MPDD prediction energy consumption in 35.45%, respectively. The

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

WSN model proposed based on MPDD is very economical as it minimizes the energy use by optimizing the selection of nodes and the route of data using HETNE and AFPC. Efficient cluster formation also reduces unnecessary use of energy in comparison to current models which have redundant transmissions. Consequently, there are longer operational efficiency and reduced energy drain of network nodes.

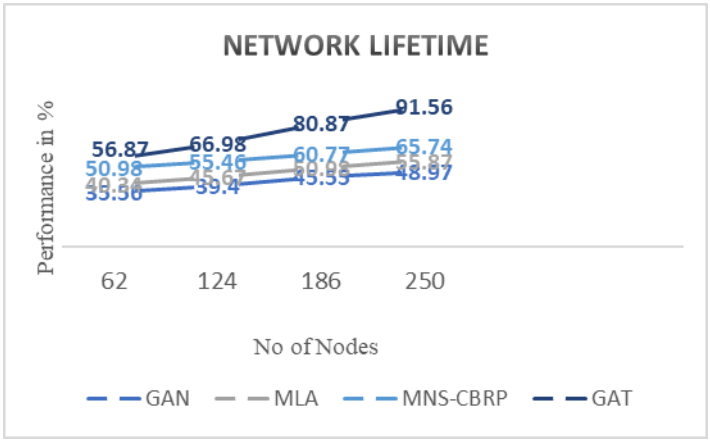

Figure 6: Analysis of Network Lifetime

Figure 6 shows enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 77%, 82%, and 87% the proposed method MPDD prediction network lifetime in 91.56%, respectively. The adaptive cluster formation and selected balanced node is beneficial to the distribution of loads among the nodes. This minimizes early node failures, increasing the system node life. As a result, the given solution shows a greater network lifetime as compared to the current WSN systems.

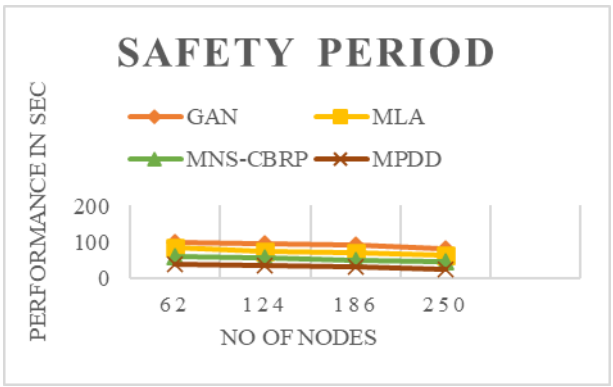

Figure 7: Analysis of safety period

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

Figure 7 shows enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 77 sec 82 sec, and 87sec the proposed method MPDD prediction safety period in 39 sec, respectively. Multi-phantom differentiated delay mechanism is a useful method of confusing the attackers due to randomization of the message paths. This extends the time of safety of the source node till it can be traced. Therefore, the suggested approach makes the networks resilient to tracking attacks compared to traditional models.

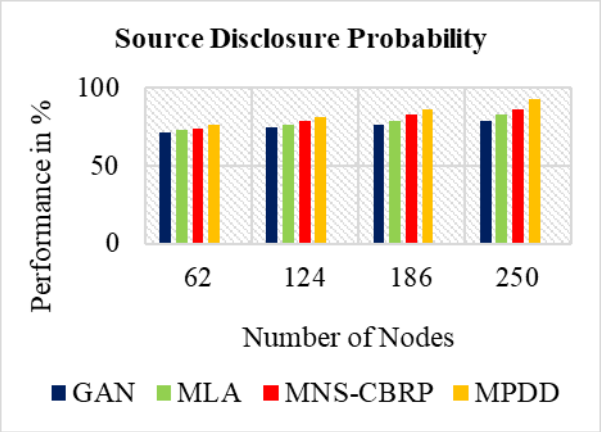

Figure 8 Analysis of Source Disclosure Probability

Figure 8 shows enhanced source location privacy protection scheme for WSNs using multi-phantom differential delay. The suggested WSN Technology approach outperformed well-known methods, such as GAN, MLA, MNS-CBRP with 77.56%, 82.23%, and 87.56% the proposed method MPDD prediction source disclosure probability in 45.22%, respectively. The MPDD scheme reduces the chances of disclosing the source by inserting various delays as well as multi-phantom paths. It is able to generate unpredictable data traces unlike other previous methods, which were static. As a result, chances of a hacker establishing the actual source are minimal.

4.1 Discussion

The section explained that WSN privacy protection approaches such as existing method have their drawbacks in maintaining balanced energy usage, a steady route, and strong location privacy. Traditional WSN privacy protection approaches tend to consume more energy, operate with a shorter network life, have a higher probability of source disclosure, and due to predictable data routes and static node communication, exhibit the clock in exposing historical traffic patterns. The proposed MPDD-based framework proactively responds to these weaknesses using its adaptive and intelligent design. The

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

proposed protection method uses QEAPS and MPDD which works well to increase privacy through the use of dynamic phantom nodes and differential delay routing, to obscure the original data source. The adaptive delay provides a well-balanced transmission load and reduces the possibility of traffic pattern detection, while increasing safety period and privacy protection range. Improvements to energy use, packet delivery ratio, and network life span were observed; this clearly shows increased performance with safe and efficient WSN communication.

5. Conclusion

In conclusion, Source Location Privacy Protection Framework for WSNs enhances data confidentiality, routing security, and node anonymity using a four-stage intelligent based on HETNE, AFPC, QEAPS, and MPDD. This integrated framework also allows for efficient node selection, adaptive-privacy clustering, secure data routing through quantum encryption, and unpredictable data packet forwarding using multiple phantom nodes. These processes together minimize energy use, improve network lifetime, and increase resilience against source-tracing and eavesdropping attacks. However, the system has some limitations, including computational overhead associated with quantum encryption, routing latency that can occur with multipath delays, and scalability concerns related to dense deployments. Future research will focus on adding lightweight post-quantum cryptographic schemes, machine learning-based adaptive routing, and blockchain-enabled trust validation, with the intention of improving efficiency, scalability, and real time performance in subsequent IoT and large scale WSN applications. The Performance metrics achieved is a source disclosure probability in 45.22%, safety period in 0.39 sec, network lifetime in 91.56%, energy consumption in 35.45%, privacy protection range in 95.45%, encryption and decryption time in 22 sec, packet delivery ratio in 95%of the process.

Reference

1. Manjula, R., Tejodbhav Koduru, and Raja Datta. "Protecting source location privacy in IoT-Enabled wireless sensor networks: the case of multiple Assets." *IEEE Internet of Things Journal* 9.13 (2021): 10807-10820.
2. Jiang, Hongbo, et al. "Location privacy-preserving mechanisms in location-based services: A comprehensive survey." *ACM Computing Surveys (CSUR)* 54.1 (2021): 1-36.
3. Zhao, Ying, and Jinjun Chen. "Vector-indistinguishability: location dependency based privacy protection for successive location data." *IEEE Transactions on Computers* 73.4 (2023): 970-979.

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

4. Akter, Mahmuda, et al. "Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems." *IEEE Journal of Biomedical and Health Informatics* 26.12 (2022): 5805-5816.
5. Wang, Yongqiang, and Tamer Başar. "Quantization enabled privacy protection in decentralized stochastic optimization." *IEEE Transactions on Automatic Control* 68.7 (2022): 4038-4052.
6. Babu, M. Vasim, et al. "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network." *Mobile Networks and Applications* 26.3 (2021): 1059-1067.
7. J. Kang, D. Steiert, D. Lin, and Y. Fu, “MoveWithMe: Location privacy preservation for smartphone users,” IEEE Trans. Inf. Forensics Secur.,vol. 15, pp. 711–724, 2020.
8. A. Alzaabi, A. Aldoobi, L. Alserkal, D. Alnuaimi, M. Alsuwaidi and N. Ababneh, "Enhancing Source-Location Privacy in IoT Wireless Sensor Networks Routing," *2021 IEEE 4th International Conference on Computer and Communication Engineering Technology (CCET)*, Beijing, China, 2021, pp. 376-381, doi: 10.1109/CCET52649.2021.9544401.
9. Jiang, J., Han, G., Wang, H., & Guizani, M. (2018). A survey on location privacy protection in Wireless Sensor Networks. *Journal of Network and Computer Applications*, *125*, 93-114. https://doi.org/10.1016/j.jnca.2018.10.008
10. Alrizq, Mesfer, et al. "Optimization of sensor node location utilizing artificial intelligence for mobile wireless sensor network." *Wireless Networks* 30.7 (2024): 6619-6631.
11. Yuan, Fujiang, et al. "AI-driven optimization of blockchain scalability, security, and privacy protection." *Algorithms* 18.5 (2025): 263.
12. Mahmood, Tariq, et al. "An intelligent fault detection approach based on reinforcement learning system in wireless sensor network." *The Journal of Supercomputing* 78.3 (2022): 3646-3675.
13. Lilhore, Umesh Kumar, et al. "A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks." *International Journal of Distributed Sensor Networks* 18.9 (2022): 15501329221117118.
14. Kumar, Anil, et al. "Optimal cluster head selection for energy efficient wireless sensor network using hybrid competitive swarm optimization and harmony search algorithm." *Sustainable Energy Technologies and Assessments* 52 (2022): 102243.
15. Li, Chaoyang, et al. "Efficient privacy preserving in IoMT with blockchain and lightweight secret sharing." *IEEE Internet of Things Journal* 10.24 (2023): 22051-22064.

Power System Technology
ISSN:1000-3673

Received: 16-06-2025 Revised: 05-07-2025 Accepted: 20-08-2025

16. Singh, Saurabh, et al. "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology." *Future Generation Computer Systems* 129 (2022): 380-388.
17. Sathish, Kaveripakam, et al. "Reliable data transmission in underwater wireless sensor networks using a cluster-based routing protocol endorsed by member nodes." *Electronics* 12.6 (2023): 1287.
18. Zhang, Peiying, et al. "A security-and privacy-preserving approach based on data disturbance for collaborative edge computing in social IoT systems." *IEEE Transactions on Computational Social Systems* 9.1 (2021): 97-108.
19. S. Shaham, M. Ding, B. Liu, S. Dang, Z. Lin and J. Li, "Privacy Preserving Location Data Publishing: A Machine Learning Approach," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 9, pp. 3270-3283, 1 Sept. 2021, doi: 10.1109/TKDE.2020.2964658
20. R. Paulet, M. G. Kaosar, X. Yi and E. Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1200-1210, May 2014, doi: 10.1109/TKDE.2013.87.