EURASIP Journal on Information Security

RESEARCH

Open Access

# DQ-NN and phantom routing for enhanced source location privacy for IoT under multiple source and destination

Arpitha T.[1], Dharamendra Chouhan[1] and Shreyas J.[2*]

**Abstract**

The Internet of Things (IoT) is now an essential component of our day-to-day lives. In any case, the association of various devices presents numerous security challenges in IoT. In some cases, ubiquitous data or traffic may be collected by certain smart devices which threatens the privacy of a source node location. To address this issue, a hybrid DL technique named Deep Q Learning Neural network (DQ-NN) is proposed for the Source Location Privacy (SLP) in IoT networks based on phantom routing. Here, an IoT network with multiple sources and destinations is considered first, and then the phantom node is chosen by analyzing neighbor list, energy, distance, and trust heterogeneity parameters. After that, multiple routes are created from the source node to the sink node via the phantom node. Finally, path selection is performed by the proposed DQ-NN. Moreover, DQ-NN is obtained by merging the Deep Q Learning Network (DQN) and Deep Neural Network (DNN). A simulation environment consisting of 150 nodes is created to study the effectiveness of performance and scalability. The proposed novel DQ-NN outperforms other existing algorithms, by recording a high network lifetime is 111.912, a safety period of 664970.7 m, an energy is 0.034 J, and a distance is 56.594 m.

**Keywords** Internet of things, Source location privacy, Deep Q learning network, Phantom routing, Deep Q learning neural network

## 1 Introduction

The IoT is an assorted network, which contains a number of interconnected devices with computing power from minimal to average. These devices persist to pervade deeper in our private platform and industrial and commercial fields, through processing, storing, and sensing whole types of data [2]. The key component of IoT is huge deployments of wireless sensor networks (WSNs), which are used for various purposes, such as tracking and observing [7, 15]. In addition, the information aggregated through the structure of IoT is utilized by a number of providers to maximize the rate of application or services offered. Consequently, numerous IoT-based applications are utilizing the position data tailoring its features to the position of a user or object it concerns.

However, there are a number of barriers that the delay next to evolution and promotion of the IoT, named as processes like user acceptance, security, and privacy. Having been incorporated into their everyday process and being able to gather and allocate huge volumes of data, IoT has concerned the interest of malevolent attackers that repeatedly attack IoT structures to obtain potentially important data [11]. The SLP is significant because the initiating node position of the message forwarded by the sourcenode in the IoT sensor network

*Correspondence:
Shreyas J.
shreyas.j@manipal.edu
[1] Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru 560001, Karnataka, India
[2] Department of Information Technology, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, Karnataka, India

includes private data that is required to be saved from various kinds of adversaries, like network loop methods, directed random paths, and undirected random paths. The data-oriented technique motivates the privacy of data [27] gathered by the sensor nodes and queries located in a network. Context-oriented privacy can be characterized as uncertainties with regard to contextual information, similar to the position and timings of network hubs [20, 27].

Phantom routing has been devised to guard SLP by changing a flooding routing process to contain the primary directed random walk continued by the flooding [10, 13]. However, based on random techniques can keep SLP in theory, it encounters the problem of failure link, and messages cannot be effectively received to a sink. The scheme of the fake sources utilizes the sensor nodes in a network as the fake resources to broadcast fake messages, in such a way that the challenger cannot detect which resource is actual. This technique has been effective in protecting the SLP; however, it results in higher energy usage of sensor nodes. Another scheme appropriate in the delay-tolerant networks alters the message delay algorithm to attain near-ideal SLP but at a high cost of receiving latency [5, 13]. Despite these frameworks, only a few studies have been performed with the purpose of fake source schemes in networks with various sources and destinations. Moreover, there are several applications, which require to analyze the position privacy of communicating nodes [10]. The necessity to conserve the source position of various assets can be handled before the utilization of WSNs can become prevalent in screening purposes, not least because a single benefit scene can occasionally substantiate the significant expense of deploying large-scale WSNs [14, 16, 17]. Here Angle-based Dynamic Routing Scheme (ADRS) is devised in [6], which utilizes the notion of visible region and defines the path by the visible region during the phantom routing, named as failure path.

The protocol of credit routing has ensured the source of location privacy, but it did not take the power of a visible region. Phantom routing with a locational angle (PRLA) role measures the self-assured probability by an offset angle of a sensor node to minimize the probability of routing by visible region. Considering the disadvantages of the PRLA method, two schemes utilizing phantom nodes were devised to protect the SLP. Through utilizing imperfect flooding, nodes away from the source are chosen as phantom nodes that importantly enlarged the position diversity of phantom nodes in SLP Preservation Protocol in the WSN Utilizing Source-Based Restricted Flooding (PUSBRF). Here, in comparison to the PUSBRF protocol, the Enhanced SLP Preservation Protocol Using Source-based Restricted Flooding (EPUSBRF) avoids the visible region in a routing operation, and network security time is increased.

The SLP protection routing technique under a random virtual ring (PRVR) was devised for extending the routing way to virtualize the range of a source node, making it complex for adversaries to apply effective reverse tracking. Moreover, the techniques [9, 10] utilize directed random walks to protect the SLP. In these methods, the phantom resources are so long from source node. When the forwarding node transfers the packets, it gradually chooses a obtaining node from the set of parent or child nodes to transfer packets to the sink node. Moreover, phantom nodes accumulated by a directed routing scheme will collect in several fixed areas that cannot attain the use of the geographical diversity of the phantom nodes and difficult routes in transmission [9, 22].

The challenges faced by existing techniques that are collected based on SLP in IoT under multiple sources and destinations are described as follows.

1. In [15], the Hybrid phantom scheme ensured SLP and generated more accurate query responses with minimum communication costs. However, packets' overhead was not decreased because of the absence of a timing technique.
2. SLPRR was developed in [27] for SLP protection in IoT. This method improved the safety time without affecting the network lifetime, but it failed to reduce the necessary time to transfer fake packets and actual packets to more powerful adversaries such as global adversary.
3. In [28], HASHA was developed to protect location privacy in IoT, and this algorithm performed well in real-world applications; it failed to investigate the times' of each node participating in the routing owing to the overlapping issue.
4. The EBBT model [29] had a better performance even in real-world applications. However, this method was not generalized for other datasets and caused ineffective routing.
5. SLP process is an emerging research area in IoT because source position can provide attackers with valuable data about the target being observed and tracked. However, it is still challenging to solve problems such as accurate paths between the nodes, improving the centralized distribution of the phantom nodes near source nodes, and reducing network communication overhead.

The emerging IoT has become an essential component of the daily activities. In any case, the association of various devices presents numerous security challenges in IoT. So, several traditional route selection papers are analyzed with their benefits and shortcomings, which implement better path selection and conquer the issues of existing techniques.

The primary aim of this paper is better path selection based on the phantom routing protocol in IoT with multiple sources and destinations, which is done by DQ-NN. Here, IoT network is simulated initially with multiple sources and destinations, and then phantom node selection is processed under the energy, neighbor list, distance, and trust heterogeneity parameters. Then, the multiple routes are created from source node to the sink node by the phantom node. At last, path selection is performed by the proposed DQ-NN, which is obtained by merging DQN and DNN.

The key contribution of this article is listed below.

- Proposed DQ-NN for path selection: Here, a DQ-NN model is proposed for selecting an ideal path for transmission based on the phantom routing protocol in IoT. The selection of the path is done by DQ-NN, which is obtained by merging DQN and DNN.

The remnant sections of this work include the following: part 2 indicates the review of the existing route selection schemes along with their shortcomings. Part 3 illustrates the path selection using the proposed DQ-NN. Part 4 discusses the effectiveness of DQ-NN in contrast to the traditional techniques, and part 5 gives the conclusion of this research.

## 2 Related work

Hussain et al. [15] devised a Hybrid phantom method for improving SLP in IoT. This technique had improved privacy, but sensor operation in an open platform was a major problem for prediction and classification. Wang et al. [27] devised a SLP protection scheme under ring loop routing (SLPRR) for IoT. This technique resulted in minimum energy consumption, but it required more time for transmitting the data packets.

Zhang and Zhang [28] developed a HASHA for protecting location privacy in IoT WSNs, and it offered the best location privacy with minimum communication overheads, although HASHA consumed more power than phantom routing since the hash operation was required for both the transmitter and receiver. Zhou et al. [29] developed an energy-efficient SLP protection scheme (EBBT) for path selection and achieved a very low delay in delivering the packets. However, it was unable to process a data privacy protection technique for protecting the position of the source node.

Mutalemwa and Shin [21] devised a new relay ring routing (ReRR) protocol for achieving the reliability of WSN communications. Here, the routing path in this model had high path diversity, but energy distribution was not balanced in this model. Chen et al. [9] developed a Privacy Protection Scheme Based on Sector Phantom Routing (PSSPR) for addressing the SLP problems. The communication overhead of the technique was low, although the network had a much higher security time.

Gu et al. [13] leverages silent nodes that become periodically silent and do not participate in data transmission. The silent periods as assigned on a random basis to the nodes. Even though this technique enhances SLP by confusing the adversary, additional energy is consumed to keep the random activation and deactivation and deactivation of nodes.

Shukla et al. [25] devised random rings and a limited hop fake packet routing scheme (SLP-RRFPR) for SLP, and the source node's safety period was high, but it failed to perform well in network typologies such as elliptical and circular. Gu et al. [13] introduced a routing scheme based on silent nodes for selecting an optimal path for proving SLP. A high level of privacy was achieved at the expense of negligible overhead, but it addressed the SLP problem in different network configurations.

George et al. [12] presented an innovative approach that combines the foraging behavior of coot birds with shepherd's herding behavior during the initialization process to optimize the network boundary. SS-COOT algorithm improves the diversification phase and avoids premature convergence. Although there are significant performance improvements, the computational cost is high.

Arunachalaperumal et al. [3] introduced a unique technique to improve SLP in WSN. This approach creates a false packet-forwarding scheme (FPFS) by combining a sequential assignment routing (SAR) strategy with an improved reptile search algorithm (IRSA). Although there is an improvement in PDR and throughput, energy consumption is more due to the introduction of dual routing of dummy packets, and since it is for the WSN network, it may not scale well for IoT considerations.

Table 1 presents each approach's routing techniques, objectives, metrics, and limitations.

Following an extensive literature survey on SLP in IoT exists many advanced methods, like hybrid optimization, metaheuristic-based routing, federated learning, and proxy node selection that are intended to enhance privacy, efficiency, and energy conservation. Although these techniques have demonstrated advances in terms of improving energy usage, privacy, and efficiency, they frequently concentrate on certain cases or have drawbacks in terms of computing overhead, adaptability to various IoT contexts, or defense against sophisticated adversaries. The lack of a more robust, flexible, and effective method to fully handle SLP in IoT with low computational costs, good network performance, and balanced energy consumption is the research gap. Therefore, our novel proposed work comprehensively addresses SLP in IoT combining phantom routing to resist adversaries by generating multiple paths

**Table 1** Summary of related existing works

| Reference | Strategy | Objectives | Merits | Limitations |
|---|---|---|---|---|
| Chenet al. [9] | PSSPR | Better Safety time that existing | Safety time, communication overhead | High energy dissipation |
| Arunachalaperumalet al. [3] | MSAR-FPFS | Better SLP using dual routing and SAR technique | Optimal route selection, prevents adversary detection | High computation cost while optimization |
| Hussainet al. [15] | Hybrid phantom method | Low energy consumption | Safety period, energy consumption, network lifetime | High packet overhead |
| Li et al. [18] | Proxy source node selection + shortest path routing | SLP protection and improve efficiency | Reduced network overhead | May not be suited for IoT scenarios |
| Georgeet al. [12] | SS COOT Optimization | Enhance SLP routing | Improved throughput, PDR and energy efficient | May not be suited for vast IoT scenarios |
| Saguet al. [24] | Metaheuristic optimization with CNN+DBN and Bi-LSTM+GRU | Optimized DL models for IoT security | Better accuracy, diverse dataset | High computational complexity |
| Almuqrenet al. [1] | Modified Firefly Optimization + Hybrid CNN-QRNN | Botnet threat detection and classification for cloud-based IoT | High detection precision, better feature selection | Limited to botnet detection |
| Mutalemwaand Shin [22] | Proxy node routing | Generation of random routes for each packet | Energy consumption, safety period, attack success rate | More packet delivery cost, high energy dissipation |
| Mutalemwaand Shin [21] | ReRR protocol | Diversified routing path | Energy consumption, network lifetime | Unbalanced energy distribution, high end to end delay |
| Zhouet al. [29] | EBBT | Low delay in packet delivery | Average hops, energy consumption, security period | Absence of data privacy protection method |
| Chenet al. [9] | PSSPR | Better Safety time that existing | Safety time, communication overhead | More energy consumption |

from source to destination and DQNN approach to optimize path selection based on dynamic network conditions among multiple paths generated.

## 3 System model

The IoT [15] model used in this work is elucidated using the system model. The IoT encompasses various nodes, such as source node, phantom node, and sink node as shown in Fig. 1. The attacker in a model has higher computing power and minimum storage space. It can choose the position of the source node and regularly creates encrypted packets about panda and transfers it to the sink hop-by-hop in a reverse angle, and it consists of the following conditions:

- Sensor nodes are positioned uniformly in a network to consequently see the activities and positions of character of a source node, where every node is allocated resources and has minimum computation of the capacity and energy.
- All the sensor nodes are linked, and every node has data about its neighborhood node, the position of the sink node, and its equivalent position in the network.
- The relative position information is broadcast to keep an updated network.

### 3.1 Phantom node

It is utilized to generate the operation of a source node with the aim of confusing adversary. Here, the source node transmits the data in a random manner to the phantom node, which in turn receives the data to sink node utilizing the shortest path technique. Here, the packets will be delivered to a phantom node that is randomly found, and from phantom node, the data is transferred to sink node by selecting a random path based on certain criteria. While data is transmitted in this manner, the adversary finds it difficult to track the source location, thereby ensuring SLP. The rate of privacy is directly associated with the length of random walk and the lengthier the random walk, the higher the rate of privacy preservation. Figure 1 displays the system model of IoT.

## 4 Proposed DQ-NN for location privacy in IoT with multiple sources and destinations

The major aim of this paper is to develop a proposed DQ-NN for protecting location privacy in IoT with multiple sources and destinations. IoT network is simulated at first with multiple sources and destinations, and then the phantom node is chosen by considering the neighbor list, energy, distance, and trust heterogeneity parameters. Then, multiple routes are created from source node to phantom node. Consequently, multiple routes are

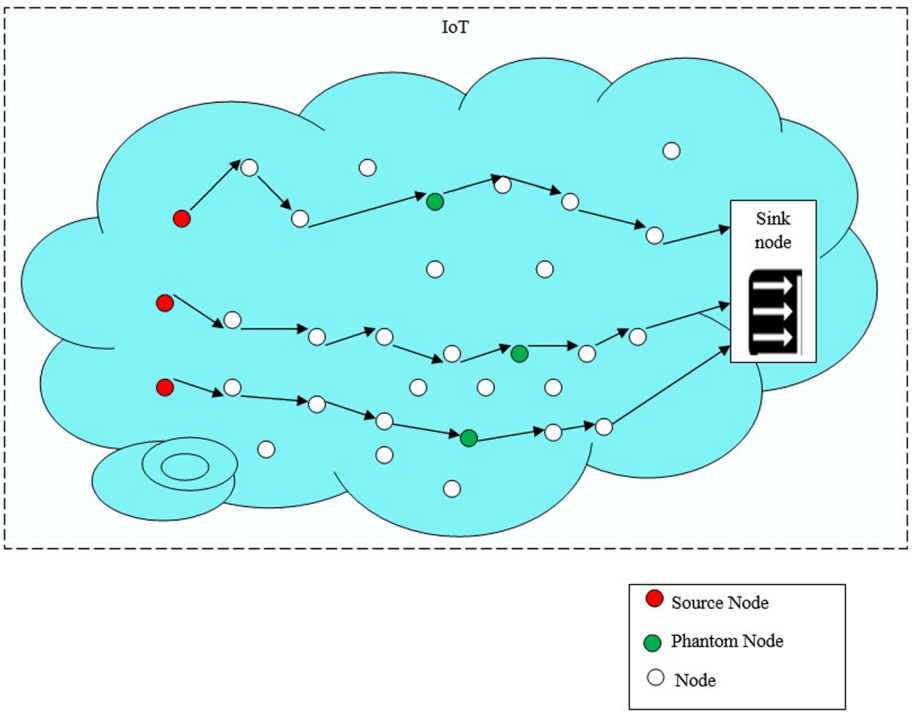



**Fig. 1** System model of IoT with multiple source and destinations

generated from phantom node to sink node. Finally, path selection is processed by DQ-NN. In addition, DQ-NN is formed by incorporating DQN [19] and DNN [26]. Here, Fig. 2 represents a structure of DQ-NN for location privacy in IoT with multiple sources and destinations.

### 4.1 Phantom node selection

A selection process of a phantom node is performed with respect to elements such as energy, distance, trust, neighbor list, and the heterogeneity. During the communication among nodes, new phantom nodes are selected randomly and consider the above parameters. The fitness solution for each node is estimated.

#### *4.1.1 Energy model*

Energy consumption plays an essential role in estimating the performance of the routing method. It records the statistical output in every simulation [27]. The following expression is utilized to measure energy consumption.

$$C_B(D,f) = \begin{cases} D * C_{\text{elec}} + D * \alpha_{fs} * f^2 & \text{if } f \le f_0 \\ D * C_{\text{elec}} + D * \alpha_{\text{amp}} * f^4 & \text{if } f > f_0 \end{cases} \quad (1)$$

where $C_{\text{elec}}$ indicates the transmitting circuit loss, $f$ represents the distance of nodes, $C_B$ represents the transmitted energy, $D$ indicates the packet length and illustrates the two modes of two system parameters, and $f_O$ indicates the distance threshold.

$$f_0 = \sqrt{\frac{\alpha_{fs}}{\alpha_{amp}}} \quad (2)$$

$$C_r = D * C_{elec} \quad (3)$$

$C_r$ indicates receiving energy.

#### *4.1.2 Distance*

The distance is calculated based on the distance between the panda node and sink node and is expressed as,

$$G(a,b) = \|f(a) - f(b)\| \quad (4)$$

where $F_a$ denotes the source node $a$ , and $F_b$ indicates the sink node $b$.

#### *4.1.3 Heterogeneity*

IoT networks may be structured in a heterogeneous form, so the source node needs to know the heterogeneity of a node during the phantom node selection. The source node is considered the heterogeneous node for selecting the phantom node or if it does how much the node is dependable with trust, mobility, energy, and so on. The value of heterogeneity is denoted as $L$.

#### *4.1.4 Neighbor identification list*

It contains various data, such as neighbored sensor nodes, and node IDs. The more amount of neighbors in

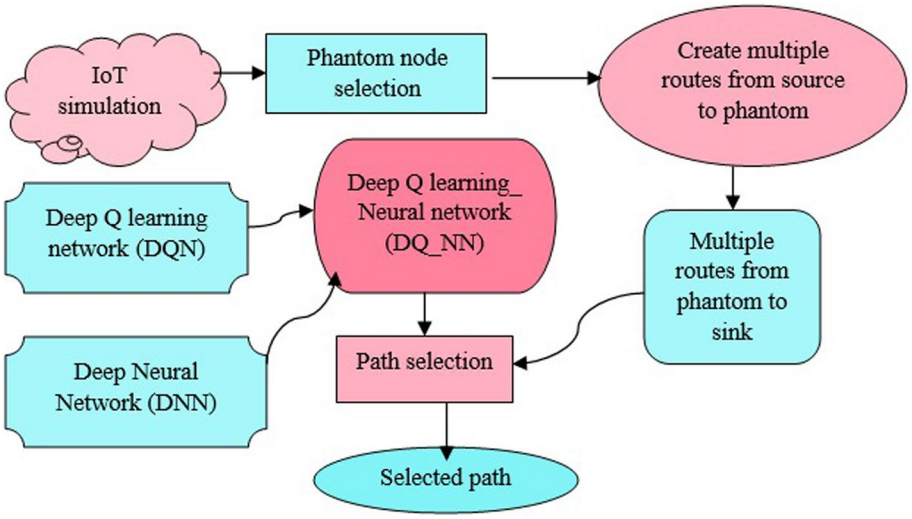



**Fig. 2** Structure of DQ_NN for location privacy in IoT with multiple sources and destinations

the list decreases the probability for a challenger to backtrack the source node and the neighbor identification list is indicated as $M$.

#### 4.1.5 Trust factor

The trust factor [8] refers to the trust of a node in another while transmitting data, and the various kinds of trust considered are direct trust, indirect trust, and historical trust, defined as,

$$E_{c,d} = -\frac{1}{3}\left[E^{D}_{c,d}(t) + E_{c,d}I^{D}(t) + E^{H}_{c,d}(t)\right] \tag{5}$$

where $E^{D}_{c,d}(t)$ represents the direct trust at time $t$, $E^{I}_{c,d}D(t)$ indicates the indirect trust at time $t$, and $E^{H}_{c,d}(t)$ denotes the historical trust at time $t$. Here, $c$ indicates the agent and $d$ signifies the upon agent.

i) Direct trust. Direct also called local trust indicates the part of a trust, where the agent calculates the trust from their own experience with a target agent.

$$E^{D}_{c,d}(t) = Sat_n(c,d) \tag{6}$$

where $Sat$ indicates the satisfaction value. $n$ represents the number of transactions.

ii) Indirect trust. The calculation of indirect trust is based on the analysis of the direct trust elements and neighborhood for obtaining the trust rate of a trustee, and the trustee gets the trust value data through a recommender. The indirect trust measures also vary under the node as a direct trust measurement is utilized as an element.

$$E^{ID}_{(c,d)}(t) = f_t\left(E^{D}_{(c,d)}(t), E^{D}_{(c,d)}(t)\right) \tag{7}$$

where $E^{ID}_{(c,e)}(t)$ indicates the indirect trust between a node and $c$ , $e$, $f_t(.)$ is estimated based on the network needs.

iii) Histological trust. The historical trust is constructed from the last experience, which is reflected in the long-term behavior of the pattern [16]. Although it measures the length between the source and destination beyond the one hop, the packet might be felt by intermediate nodes owing to unexpected processes, and is expressed as,

$$E^{H}_{(c,d)}(t) = \frac{\eta E^{H}_{(n-1)(c,d)}(t) E^{RT}_{(n-1)(c,d)}(t)}{2} \tag{8}$$

where $E^{RT}_{(n-1)(c,d)}$ indicates the recent factor, and $\eta$ denotes the forgetting factor. The path parameters are split into two and are given by,

$$I_1 = \{C_r, E_{(c,d)}\} \tag{9}$$

$$I_2 = \{G_{(a,b)}, M, L\} \tag{10}$$

The calculation of fitness is defined as,

$$F_{\text{itt}} = \left[(1 - C_r) + G_{(a,b)} + M + (1 - E_{(c,d)})\right] \tag{11}$$

The process of phantom node selection is detailed in Algorithm 1. Phantom node selected dynamic based on the network conditions. Once the hello packet is broadcasted, network parameters like energy, distance, heterogeneity, trust, and neighbor are updated. The node with high fitness is selected as phantom node.

**Algorithm 1** Phantom node selection algorithm

**Initialize** nodes and a threshold $thres$
All nodes broadcast a hello packet
Determine the energy, distance, heterogeneity, neighbor identification list, and trust of all nodes
Measure the fitness $F_{\text{itt}} = [(1 - C_r) + G_{(a,b)} + M + (1 - E_{(c,d)})]$ for all nodes
If $F_{\text{itt}} < thres$, Node is selected as the phantom node

### 4.2 Multiple path creation

Once the phantom node is selected, and phantom nodes obtain the message, it sends a message to the destination through multiple random pathways, thereby preventing the adversary from identifying the position of the source node. The creation of multiple paths [15] is processed under the following conditions:

1. Generate the multiple routes from a source node to a phantom node
2. Generate multiple routes from the phantom to the sink node

Multiple route creation from the source to phantom node and phantom node to sink node is performed depending on parameters like energy, heterogeneity, distance, trust, and neighbor identification list, and is elaborated in Algorithm 2. The best path is selected according to DQ_NN routing.

**Algorithm 2** Route selection algorithm

**Initiating the route selection** from the source to the phantom node
The source node sends a route request
Receive the route request in an intermediate node
Update parameters like energy, heterogeneity, distance, trust, and neighbor identification list
Select the phantom node utilizing the parameters
Generate multiple routes from a source node to a phantom node
Generate multiple routes from the phantom node to the sink node
Select routes from the phantom node to the sink node
Generate a greater number of routes from the phantom node to the sink
Uniformly select multiple routes from the phantom to the sink
Forward the received message from phantom to the next hop

### 4.3 Path selection

Here, path selection is based on the phantom routing protocol in IoT under multiple sources and destinations, which is done by DQ_NN that is formed by combining DQN [26] and DNN [19]. The DQ_NN employs three sections: DQN, DQ_NN layer, and DNN. At first, the DQN technique is applied, where the selected parameter $I_1$ acts as input, and its output is denoted as $\varpi_1$. In the DQ_NN layer, the merging of DQN output $\varpi_1$ and selected path parameter output $I_2$ is accomplished by regression modeling. To develop the regression modeling, the fractional calculus (FC) [4] concept is used as it effectively preserves the information. The DQ_NN layer's output is represented as $\varpi_2$. The output of the DQ_NN layer $\varpi_2$ is fed to the DNN, and its output is denoted as $\varpi_3$, and Fig. 3 signifies the structure of DQ_NN for path selection.

#### *4.3.1 DQN model*

The input of DQN [19] is the selected parameter $I_1$, and the process of path selection is elaborated as follows. The DQN is a feed-forward network based on Q-learning, which is a kind of Deep Reinforcement Learning (RL) [23], and it depends on the action-value function to generate the cumulative output. The maximum capacity to

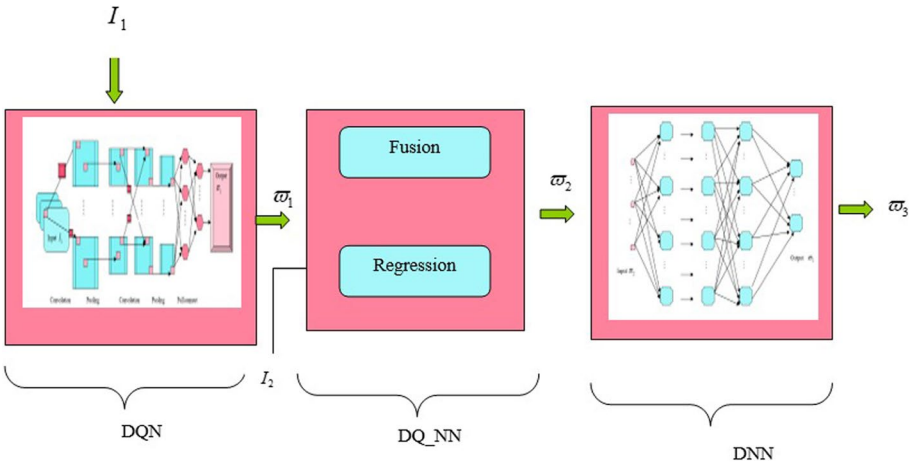



**Fig. 3** Structure of DQ_NN for path selection

process the high-dimensional inputs makes the DQN an appealing option for real-world problems. This technique also performs better in large-scale inputs. The Reinforcement Learning (RL)-based value of action function is defined as,

$$A_j^{\pi}(g_j, h_j) = \mathbb{E}\left[\sum_{l=0}^{\infty} \phi^l i_{(j+l)} \mid g_j = g, h_j = h; \pi\right] \quad (12)$$

where $\mathbb{E}$ indicates the expectation, the ideal action-value function is expressed as $A^*(g,h) = \max_{\pi}(g,h)$, $\phi$ indicates the discount factor, $i$ signifies the state, $g$ represents the action selection, $h$ signifies the action function, and it is verified the Bellman ideal equation,

$$A^*(g_t, h_t) = \mathbb{E}\left[i + \phi \max_h A^*(g_{(j+1)}, h) \mid g_j, h_j\right] \quad (13)$$

The RL technique is to select an ideal policy $\pi^*(g) = \arg\max A^*(g,h)$, which increases the ideal action-value functions $\max_h A^*(g,h)$.

One of the popular RL techniques is Q-learning which evaluates the ideal action value function by the upgraded iteration value, and its rule is defined as,

$$A_{j+1}(g_j, h_{j_t}) = A_j(g_j, h_t) + \Omega_j(g_j, h_j)(i_j + \phi \max_h A_{jt}(g_{(jt+1)}, h) - A_j(g_j, h_j)) \quad (14)$$

where $\Omega_j(g_j, h_j)$ denotes the learning rate.

Q-learning employs a table to save whole performance values that perform well on RL issues with small-scale action space and discrete state space. Meanwhile, more practical problems are on a high scale and continuous, and a tabular format is not effective in this case. Thus, the operation of approximation parameterized through $\theta$ is utilized to evaluate the action value function. Commonly, value $\theta$ can be optimized by minimizing the given loss function

$$H_j(\theta_j) = \mathbb{E}\left[(J_j - A(g_{jt}, h_j; \theta_j))^2\right] \quad (15)$$

where $J_j$ is the objective function. Then, the rule $\theta$ is upgraded through gradient descent and is expressed as,

$$\theta_{j+1} = \theta_j + \Omega_j(J_j - A(g_j, h_t; \theta_j))\nabla_{\theta_t} A(g_j, h_j; \theta_j) \quad (16)$$

DNN is used to approximate the action value function for DQN. In DQN, two different networks are used: the online network and the target network, which is used for supplying the objective solution. The element $\theta_t$ of an online network is upgraded in every step, while parameter $\theta_j^-$ is copied from an online network in each step, which is the target network. The DQN's objective function is expressed as

$$J_j^{\mathrm{DQN}} = i_j + \phi \max_h A\left(g_{j+1}, h; \theta_j^-\right) \quad (17)$$

Moreover, the above Eq. (17) is transformed into

$$\varpi_1 = i_j + \phi A\left(k_j, \arg\max_h A(g_{j+1}, h; \theta_j^-); \theta_j^-\right) \quad (18)$$

where $\varpi_1$ indicates the output of DQN, and Fig. 4 represents the overview of DQN.

#### 4.3.2 DQ_NN layer

The DQN's output $\varpi_1$ and selected parameter $I_2$ are fed to the DQ_NN layer, where integration of $\varpi_1$, $I_2$ is employed by fusion, and fusion is performed by the regression modeling. For developing the regression modeling, FC [4] is added to attain better performance. The functioning of the DQ_NN layer is described below.

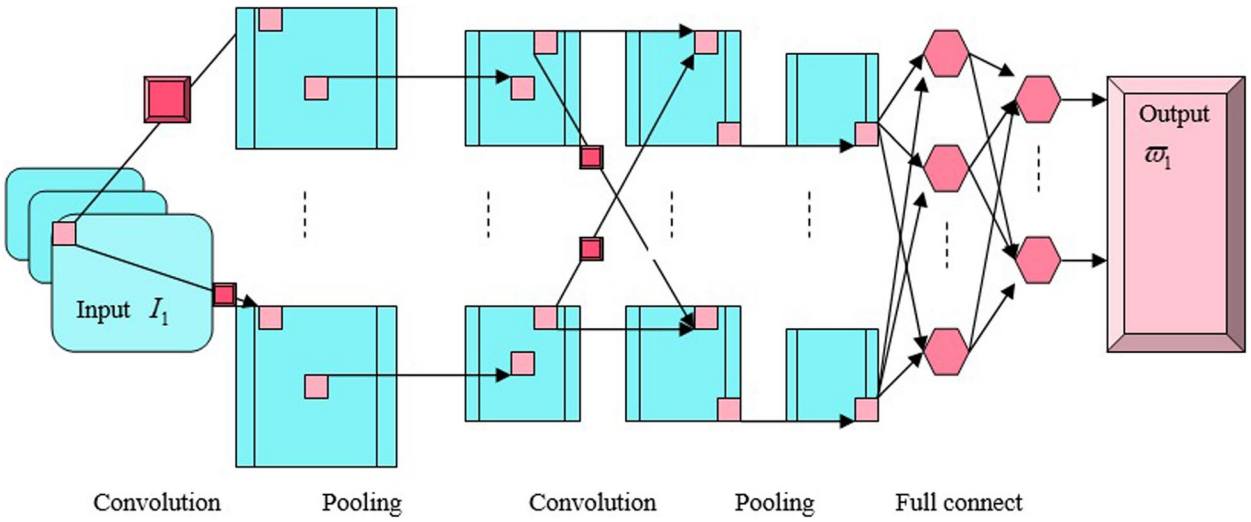



**Fig. 4** Framework of DQN

Considering the time interval $t$, the output is modeled based on the selected path parameter $I_2$ as

$$m = \sum_{o=1}^{n} I_{2o} \cdot K_o \tag{19}$$

FC [8] is employed for improving the performance of DQ_NN, and from FC,

$$m(t+1) = \beta m(t) + \frac{1}{2}\beta m(t-1) \tag{20}$$

Then, the equation changes to

$$\varpi_2 = \beta \cdot m + \frac{1}{2}\beta \cdot \varpi_1 \tag{21}$$

Here, $m$ represents the output from the $t$-th interval, $m_1$ indicates the output from the $(t-1)$-th interval, and applying equation is expressed as

$$\varpi_2 = \beta \cdot \sum_{o=1}^{n} I_{2o} \cdot K_o + \frac{1}{2}\beta \cdot \varpi_1 \tag{22}$$

where $\beta$ indicates the constant, and weight is indicated as $K$. $\varpi_2$ is the output of the DQ_NN layer which is applied to the DNN model for path selection.

#### *4.3.3 DNN model*

The output of DQ_NN $\varpi_2$ is subjected to the DNN [26], which is a composition of a number of layers of nodes that obtains the input from the other layers and generate an output until an exceptional output is obtained. The network is called so because there is a similarity between this programming method and the way the brain processes. This scheme is processed better in complex methods, and is expressed as

$$O = (P, N, \psi) \tag{23}$$

where $P$ is the group of layers, $N$ indicates the group of connections between the layers, and $\psi$ denotes the group of functions. DNN has an input layer, output layer, and hidden layers. Every layer contains a number of nodes. Here, two values are recorded, and its value before and after an activation function correspondingly. The rectified linear unit (ReLU) is the most famous activation employed in DNN, and the activation value of each node in the hidden layer is expressed as

$$\mathrm{ReLU}(p_{q,r}) = \begin{cases} p_{q,r} & \text{if } p_{q,r} \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

where the output node is associated with a variable $p_{q,r}$ for $1 < q < Q$ and $1 \leq r \leq t_q$, $Q$ indicates the layers, and $t_q$ represents the node. Other than the input node, each node is linked to nodes in the consequent layer by the pre-trained elements in such a way that for all $q$ and $r$ with $2 \leq q \leq Q$ and $1 \leq r \leq t_q$, which is expressed as,

$$p_{q,r} = s_{q,r} + \sum_{1 \leq u \leq t_{q-1}} v_{q-1,u,r} \cdot x_{q-1,u} \tag{25}$$

where $v_{q-1,u,r}$ indicates the weight for connection between $n_{q-1,u}$ and $n_{q,r}$, $n_{q-1,u}$ is the $u$-th node of layer $q-1$, $n_{q,r}$ denotes the $r$-th node of layer $q$, and $s_{q,r}$ indicates the bias for node $n_{q,r}$. Due to the utilization of ReLU in expression (25), the character of a NN is greatly non-linear. Finally, for each input, DNN allocates a label,

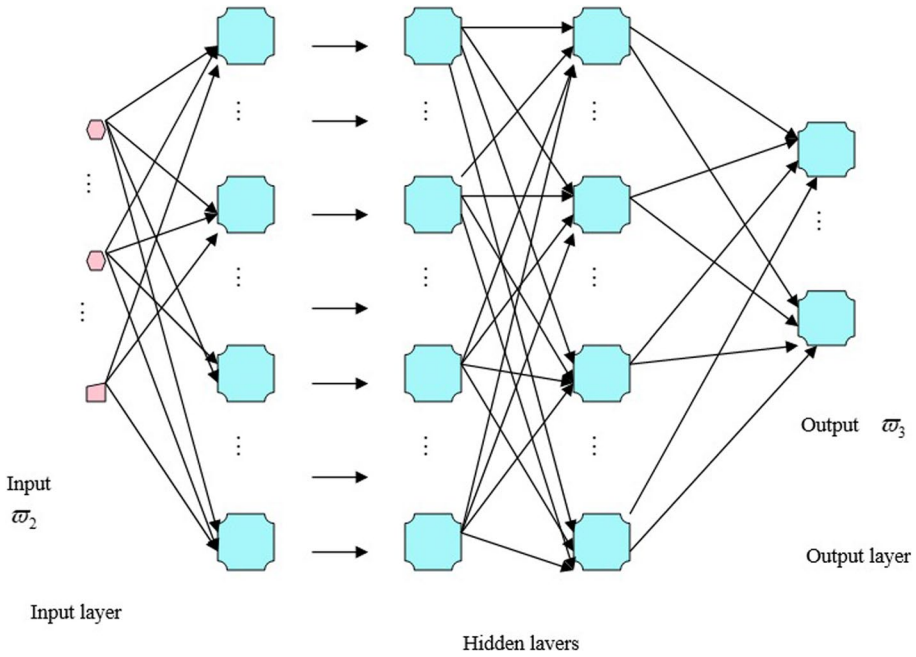



**Fig. 5** Structure of DNN with its input as $\varpi_2$ and output as $\varpi_3$

which is the index of an output layer with the maximum value, and Fig. 5 demonstrates the DNN structure.

$$\varpi_3 = \arg \max_{1 \le l \le t_q} p_{q,r} \tag{26}$$

Here $p_{q,r} = \varpi_2$, the output of the DNN can be expressed as,

$$\varpi_3 = \arg \max_{1 \le r \le t_q} \varpi_2 \tag{27}$$

Here, $\varpi_3$ is an output of DQ-NN and is selected as the new path for routing. Figure 5 portrays the structure of the DNN.

## 5 Results and discussion

The experimental result obtained by DQ-NN for path selection based on the phantom routing protocol in IoT under multiple sources and destinations is briefly elaborated below.

### 5.1 Experimental set-up

The devised DQ-NN method for path selection based on the phantom routing protocol in IoT is implemented using MATLAB tool with network simulation. The system is evaluated for three cases: using 50 nodes, 100 nodes, and 150 nodes. These scenarios help to provide reasonable and diverse points to analyze the system's performance and scalability.

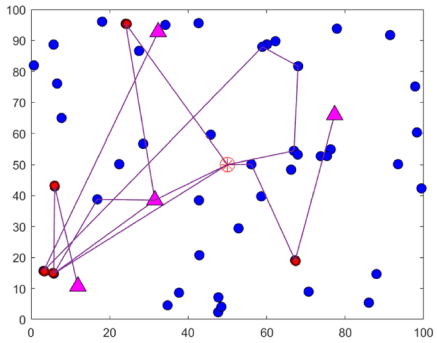
### 5.2 Evaluation measures

The devised DQ-NN technique's performance is measured utilizing several performance indicators, which are detailed below.

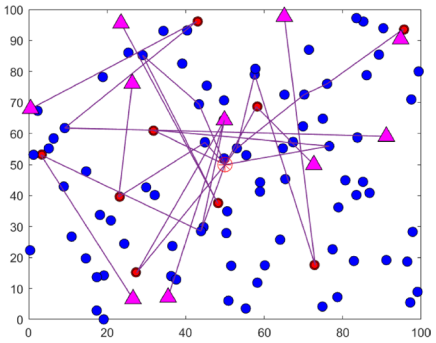
- Distance: Equation (4) is used for discovering the minimum distance between the nodes.
- Energy: Equation (1) is used for measuring the total amount of energy received by this DQ-NN method.
- Network lifetime: The time required for transferring the amount of packets in the IoT before the first node is dead is the network lifetime.
- Safety period: It is a time period that permits the attackers to discover the source. The safety period is calculated by the amount of effectively transmitted packets, which are transferred from the source node to the sink node.

### 5.3 Experimental simulation result

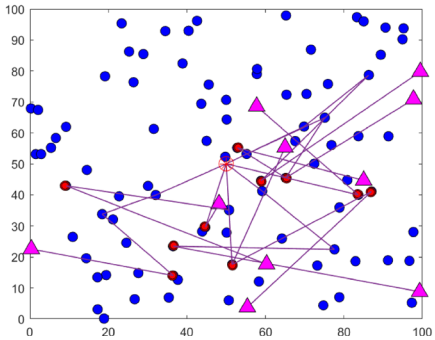
Figure 6 represents the simulation result of the DQ-NN method under varying nodes. Figure 6a displays the simulation result with 50 nodes, Fig. 6b reveals simulation output with 100 nodes, and Fig. 6c indicates the simulation output with 150 nodes.



(a) Results under varying 50 nodes



(b) Results under varying 100 nodes



(c) Results under varying 150 nodes

**Fig. 6** Simulation result of DQ-NN method under varying nodes. **a** Simulation result under varying 50 nodes. **b** Simulation result under varying 100 nodes. **c** Simulation result under varying 150 nodes

### 5.4 Comparative techniques

The conventional techniques, such as the Hybrid phantom method [15], SLPRR [7], HASHA [11], and EBBT [27], are compared with the designed DQ-NN model to analyze the effectiveness of the devised approach.

### 5.5 Comparative assessment

The superiority assessment of DQ-NN during the routing for selecting the best path between the nodes is done by varying amounts of nodes as 50, 100, and 150 and is elaborated below.

#### *5.5.1 Varying 50 nodes*

Figure 7 represents a comparative investigation of DQ-NN based on the routing in terms of various metrics and the number of rounds. Figure 7 indicates the assessment of DQ-NN with distance. While considering the number of rounds as 1000, the distance of DQ-NN is 57.795 m, and the value attained by other conventional methods Hybrid phantom method, SLPRR, HASHA, and EBBT is 83.911 m, 67.994 m, 60.685 m, and 61.899 m, respectively.

The energy-based comparative evaluation of DQ-NN is displayed in Fig. 8. The energy of various techniques Hybrid phantom method, SLPRR, HASHA, EBBT, and the proposed DQ-NN is 0.006 J, 0.011 J, 0.013 J, 0.012 J, and 0.013, respectively, with the number of rounds being 800. Figure 9 displays the assessment of DQ-NN concerning the network lifetime.

The network lifetime of the various existing schemes Hybrid phantom method, SLPRR, HASHA, and EBBT is 99.512, 100.317, 99.792, and 97, respectively. The network lifetime of DQ-NN is 101.828 with the number of rounds being 1000. Figure 10 demonstrates the safety period-based comparative evaluation of DQ-NN. Taking the number of rounds as 800, the safety period of DQ-NN is 664,970.7 m, and the conventional method's safety period of the Hybrid phantom method, SLPRR, HASHA, and EBBT is 212,688 m, 554,640 m, 302,537.1 m, and 425,376 m, respectively.

#### *5.5.2 Varying 100 nodes*

Figure 11 indicates analysis of DQ-NN for 100 nodes by various rounds utilizing the various metrics. The

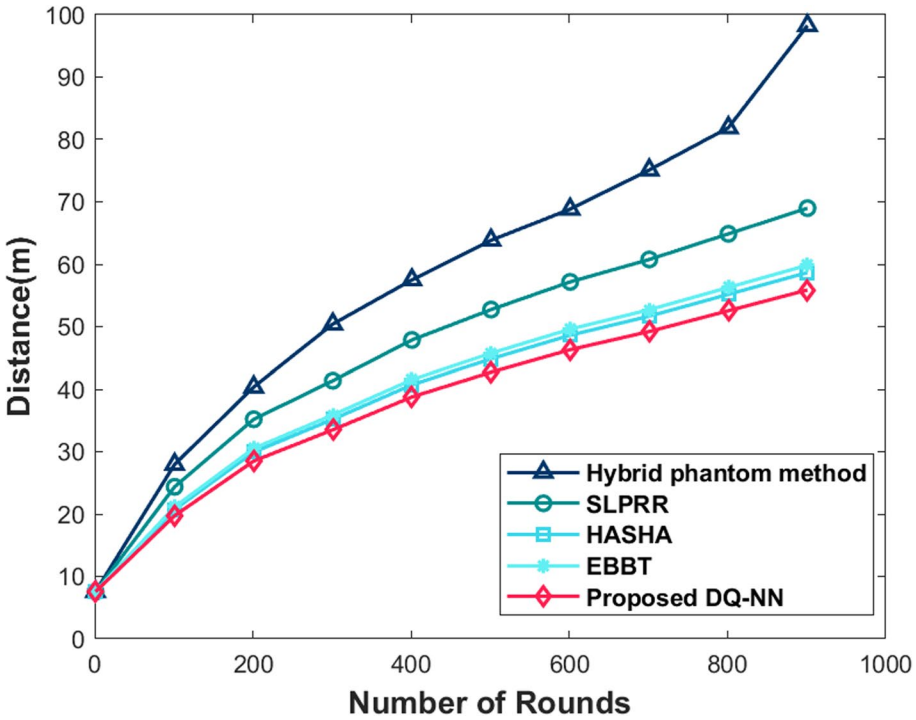



**Fig. 7** Comparative assessment of DQ_NN model based on distance for varying 50 nodes

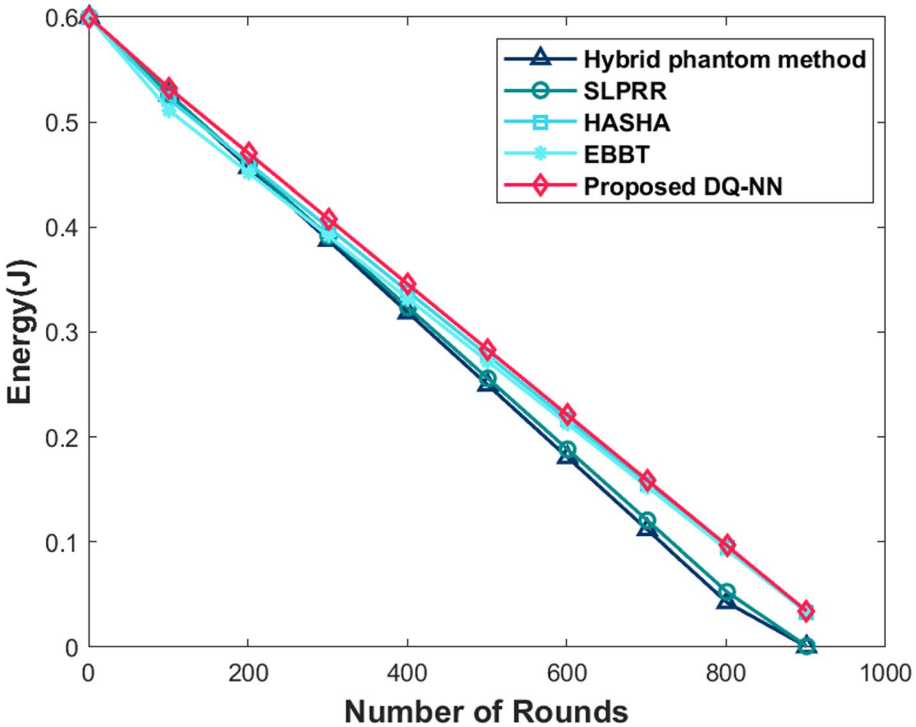



**Fig. 8** Comparative assessment of DQ_NN model based on energy for varying 50 nodes

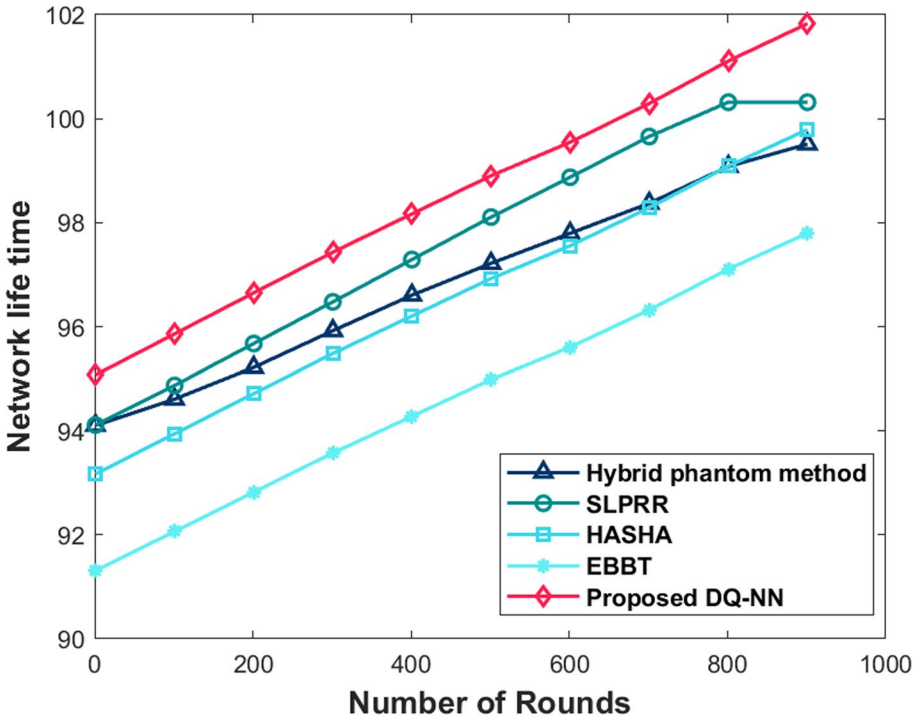



**Fig. 9** Comparative assessment of DQ_NN model based on network lifetime for varying 50 nodes

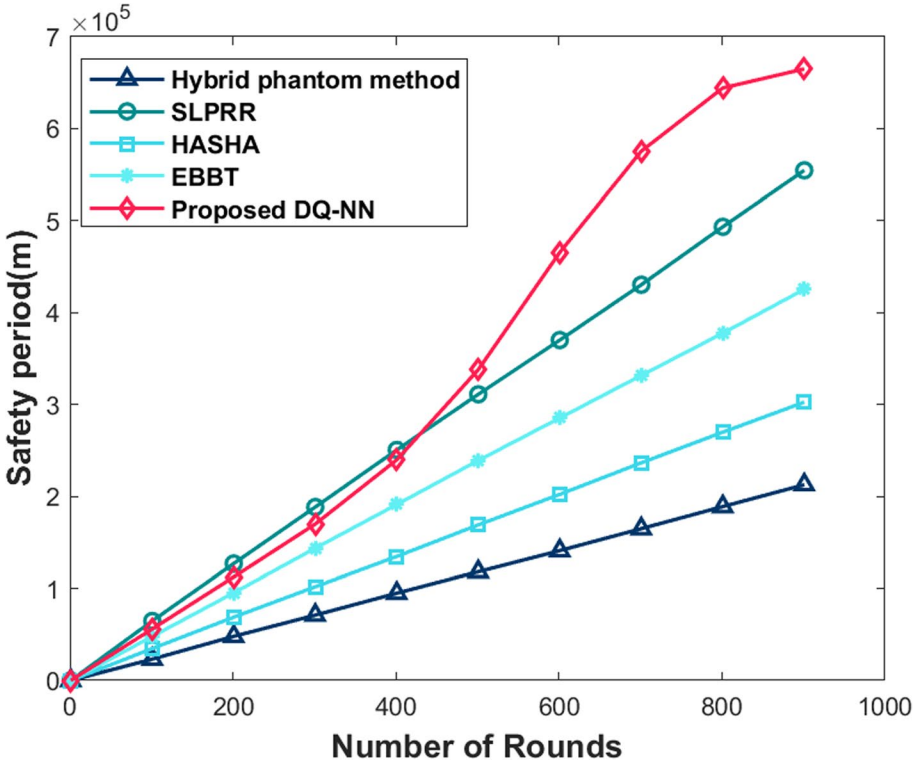



**Fig. 10** Comparative assessment of DQ_NN model based on safety period for varying 50 nodes

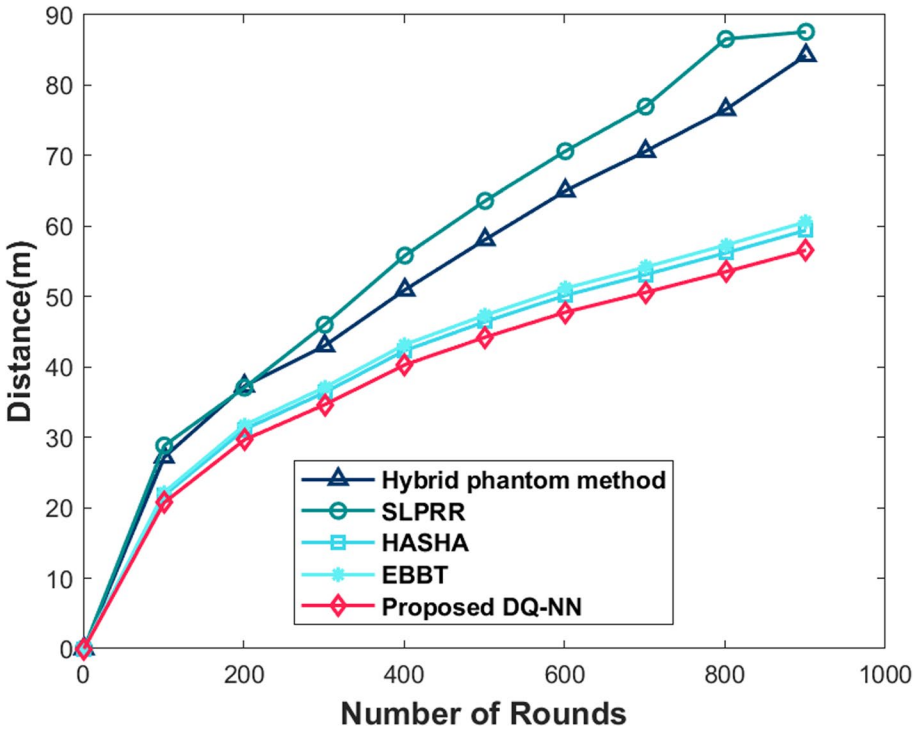



**Fig. 11** Comparative assessment of DQ_NN model based on distance for varying 100 nodes

analysis under various techniques utilizing distance is exhibited in Fig. 11. The value of distance obtained by the routing models Hybrid phantom method, SLPRR, HASHA, EBBT, and the proposed DQ-NN is 84.236 m, 87.587 m, 59.424 m, 60.612 m, and 56.594 m, respectively, for 1000 rounds. The analysis of DQ-NN shows that it has achieved minimum distance compared to the other schemes.

The analysis concerning the energy of DQ-NN is portrayed in Fig. 12. The obtained energy of DQ-NN is 0.096 J for 800 rounds, and the energy of the conventional routing techniques Hybrid phantom method, SLPRR, HASHA, and EBBT is 0.044 J, 0.001 J, 0.094 J, and 0.096 J, respectively. Here, compared to other existing techniques, DQ-NN achieved better energy. The evaluation of routing schemes in terms of network lifetime is represented in Fig. 13. For analyzing 1000 rounds, the network lifetime of various techniques Hybrid phantom method, SLPRR, HASHA, EBBT, and DQ-NN is 106.146, 105.589, 106.209, 104.085, and 108.377, respectively. Figure 14 displays the assessment of various routing methods in terms of safety time. The value recorded by the safety time of various techniques Hybrid phantom method, SLPRR, HASHA, EBBT, and devised DQ-NN is 160,596.000 m, 255,429.474 m, 192,765.600 m, 184,450.286 m, and 366,349.567 m, for 1000 rounds.

#### *5.5.3 Varying 150 nodes*

Figure 15 signifies the analysis of DQ-NN utilizing the various metrics when the number of nodes is 150. The assessment of DQ-NN based on distance measurement is revealed in Fig. 15. Here, considering the number of rounds as 1000, the distance of multiple techniques Hybrid phantom method, SLPRR, HASHA, EBBT, and proposed DQ-NN is 83.911 m, 67.994 m, 60.685 m, 61.899 m, and 57.795 m, respectively.

Figure 16 displays DQ-NN assessment with energy using various routing algorithms. Here, energy gained by conventional routing methods Hybrid phantom method, SLPRR, HASHA, and EBBT with the number of rounds of 800 is 0.006 J, 0.011 J, 0.013 J, and 0.012 J, respectively. The devised DQ-NN attained an energy value of 0.013J. Figure 17 represents the assessment of DQ-NN in terms of network lifetime. The network lifetime obtained by varying routing schemes Hybrid phantom method, SLPRR, HASHA, EBBT, and the proposed DQ-NN is 105.790, 107.047, 109.674, 107.481, and 111.912, for taking 1000 rounds. Figure 18 shows the safety period-based analysis of various methods. When considering 800 rounds, the safety period of DQ-NN is 331,497.564 m, and the safety period of the other conventional methods Hybrid phantom method, SLPRR, HASHA, and EBBT is 143,888.400 m, 207,442.286 m, 242,196.000 m, and 193,665.600 m, respectively.

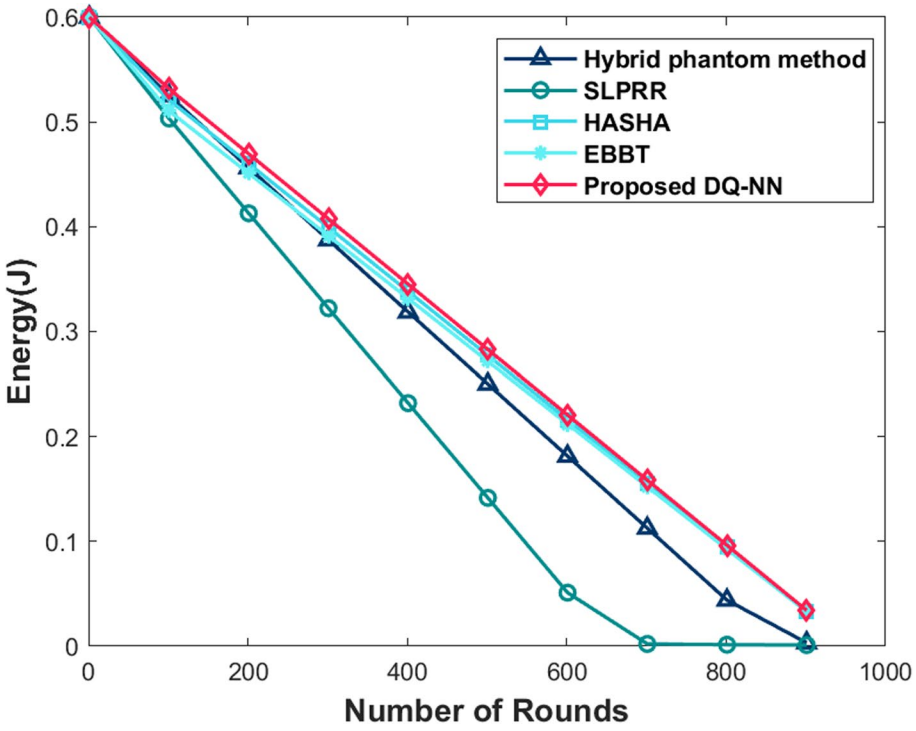



**Fig. 12** Comparative assessment of DQ_NN model based on energy for varying 100 nodes

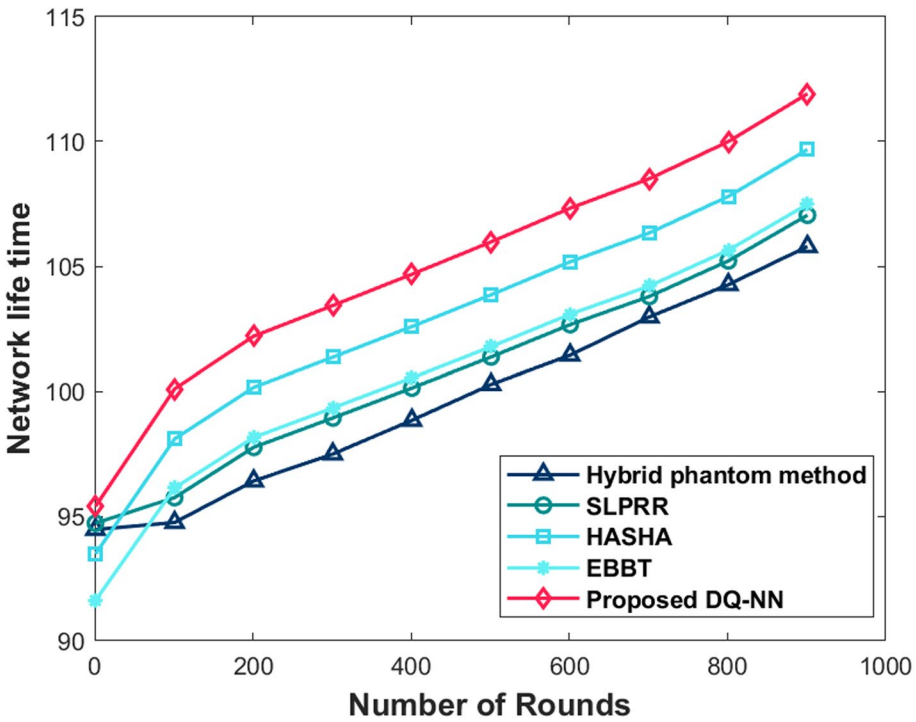



**Fig. 13** Comparative assessment of DQ_NN model based on network lifetime for varying 100 nodes

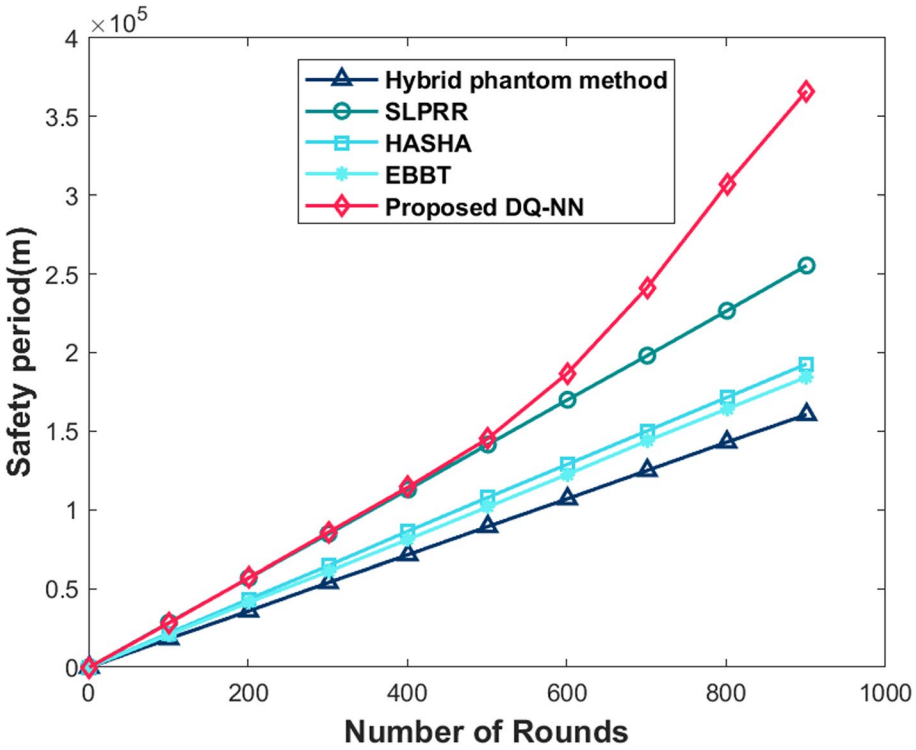



**Fig. 14** Comparative assessment of DQ_NN model based on safety period for varying 100 nodes

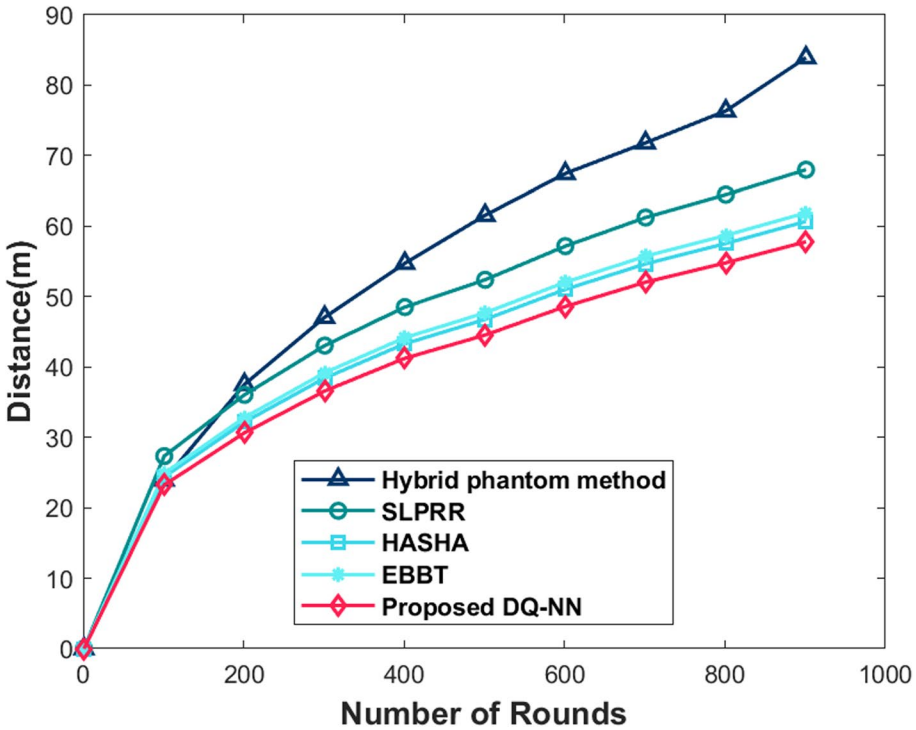



**Fig. 15** Comparative assessment of DQ_NN model based on distance for varying 150 nodes

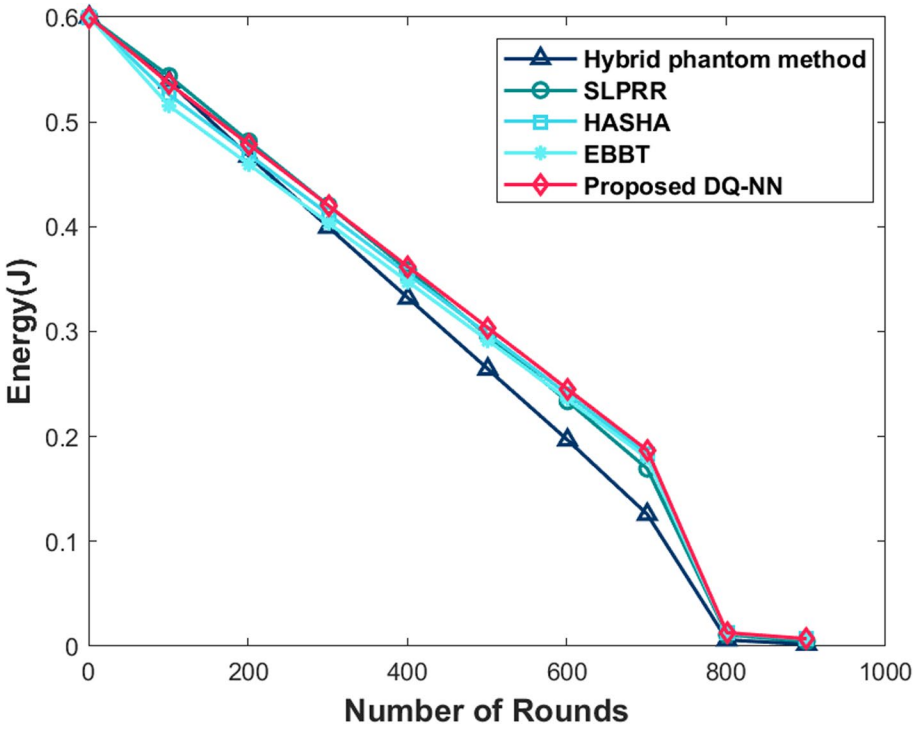



**Fig. 16** Comparative assessment of DQ_NN model based on energy for varying 150 nodes

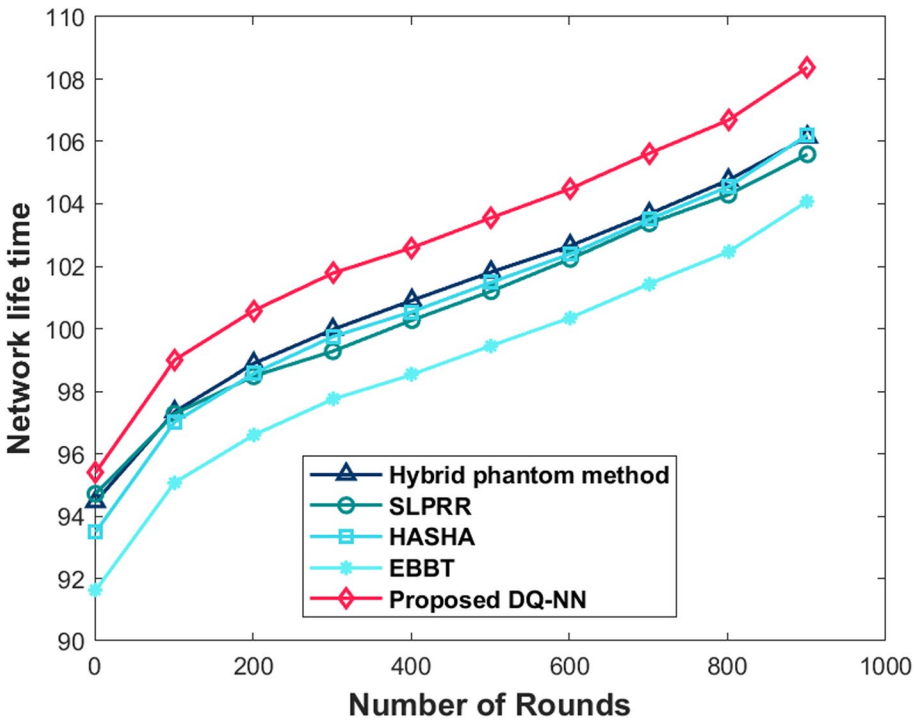



**Fig. 17** Comparative assessment of DQ_NN model based on network lifetime for varying 150 nodes

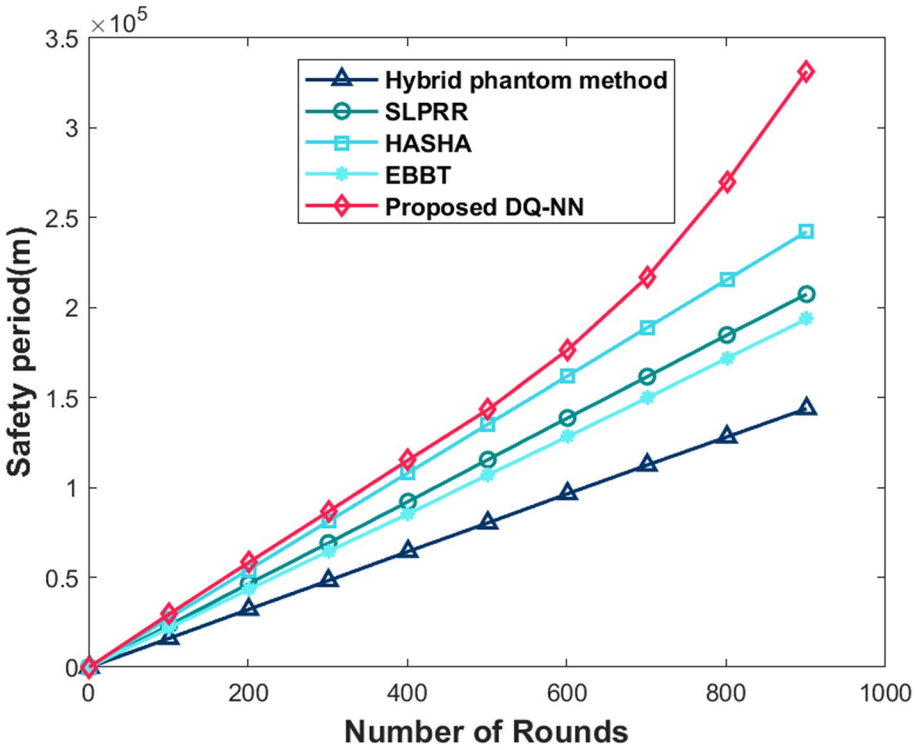



**Fig. 18** Comparative assessment of DQ_NN model based on safety period for varying 150 nodes

**Table 2** Comparative discussion

| No. of nodes | Evaluation parameters | Hybrid phantom method | SLPRR | HASHA | EBBT | Proposed DQ_NN |
|---|---|---|---|---|---|---|
| 50 | Distance (m) | 83.911 | 67.994 | 60.685 | 61.899 | 57.795 |
| | Energy (J) | 0.002 | 0.005 | 0.007 | 0.007 | 0.007 |
| | Network lifetime (sec) | 99.512 | 100.317 | 99.792 | 97.796 | 101.828 |
| | Safety period (m) | 212688 | 554640 | 302537.1 | 425376 | **664970.7** |
| 100 | Distance (m) | 84.236 | 87.587 | 59.424 | 60.612 | **56.594** |
| | Energy (J) | 0.003 | 0.001 | 0.033 | 0.033 | **0.034** |
| | Network lifetime (s) | 106.146 | 105.589 | 106.209 | 104.085 | 108.377 |
| | Safety period (m) | 160596.000 | 255429.474 | 192765.600 | 184450.286 | 366349.567 |
| 150 | Distance (m) | 83.911 | 67.994 | 60.685 | 61.899 | 57.795 |
| | Energy (J) | 0.002 | 0.005 | 0.007 | 0.007 | 0.007 |
| | Network lifetime (sec) | 105.790 | 107.047 | 109.674 | 107.481 | **111.912** |
| | Safety period (m) | 143888.400 | 207442.286 | 242196.000 | 193665.600 | **331497.564** |

### 5.6 Comparative discussion

Table 2 presents the results obtained by the proposed DQ-NN for path selection based on phantom routing protocol in IoT. Here, the devised DQ-NN method evaluated better results when compared with other conventional techniques with a minimum distance of 56.594 m, higher energy of 0.034J, greater network lifetime of 111.912, and higher safety period 664970.7 m with a number of rounds of 1000. The other conventional methods Hybrid phantom method, SLPRR, HASHA, and EBBT gained a distance of 84.236 m, 87.587 m, 59.424 m, and 60.612 m, respectively. The energy obtained by Hybrid phantom method, SLPRR, HASHA, and EBBT is 0.003 J, 0.001 J, 0.033 J, and 0.033 J, respectively. The network lifetime is recorded to be 105.790 for Hybrid phantom method, 107.047 for SLPRR, 109.674 for HASHA, and 107.481 for EBBT. The safety

period of Hybrid phantom method, SLPRR, HASH, and EBBT is 212,688 m, 554,640 m, 302,537.1 m, and 425,376 m, respectively. Moreover, the fusion of DQN and DNN achieved higher convergence speed, thereby enabling the DQ-NN to attain a better performance while selecting a path using phantom routing.

## 6 Conclusion

The research work significantly enhances location privacy and reduces consumption of energy in IoT. A novel hybrid DQ-NN is proposed for SLP in IoT with multiple source and destination nodes. Initially, IoT nodes are simulated with multiple sources and destinations, and then the phantom node is chosen dynamically based on several parameters. After that, multiple routes are created from the source node to the phantom node. Then, multiple routes are generated from the phantom node to the sink node. Finally, path selection is performed by the proposed DQ-NN. Using DQ-NN model for dynamic adjustment of network parameters improved optimization efficiency. Moreover, DQ-NN is obtained by merging DQN and DNN. Moreover, the effectiveness of the DQ-NN model in selecting a path is measured, and the DQ-NN model achieved the minimum distance of 56.594 m, higher energy of 0.034 J, maximum network lifetime of 111.912, and higher safety period of 664,970.7 m.

The work's limitation is that just backtracking is taken into consideration; more attacks may be considered. In the future dimension, we intend to add more metrics like task value, for analyzing the effectiveness of the DQ_NN technique in the IoT environment.

### Abbreviations

| | |
|---|---|
| IoT | Internet of Things |
| SLP | Source Location Privacy |
| PR | Phantom routing |
| PSSPR | Privacy Protection Scheme on Sector PR |
| SLPRR | SLP protection under ring loop routing |
| EBBT | Energy Balanced Branch Tree |
| SLP-RRFPR | SLP random rings and a limited hop fake packet routing |
| ReRR | Relay ring routing |
| MSAR-FPFS | Metaheuristics with sequential assignment routing based false packet forwarding scheme |
| DNN | Deep Neural Network |
| DQN | Deep Q Learning Network |
| DQ_NN | Deep Q Learning Neural Network |

### Acknowledgements

The authors thank the editor and reviewers for their insightful comments to improve the manuscript.

### Authors' contributions

Arpitha T: conception and design of the study, implementation, acquisition of data, analysis, and/or interpretation of data, writing-original draft. Dharamendra Chouhan: guidance and reviewing of the paper. Shreyas J* (corresponding author): reviewing the paper.

### Funding

Open access funding provided by Manipal Academy of Higher Education, Manipal No funding is available for this research.

### 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

The authors declare no competing interests.

Received: 22 May 2024 Accepted: 14 August 2024
Published online: 05 September 2024

### References

1. L. Almuqren, H. Alqahtani, S.S. Aljameel, A.S. Salama, I. Yaseen, A.A. Alneil, Hybrid metaheuristics with machine learning based botnet detection in cloud assisted internet of things environment. Int. J. Comput. Netw. Appl. (2023). https://doi.org/10.1109/ACCESS.2023.3322369
2. T. Arpitha, D. Chouhan, J. Shreyas, Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications. J. Eng. Appl. Sci. **71**, 8 (2024). https://doi.org/10.1186/s44147-023-00342-1
3. C. Arunachalaperumal, E. Mary Anita et al., Improved reptile search algorithm with sequential assignment routing based false packet forwarding scheme for source location privacy protection on wireless sensor networks. J. Intell. Fuzzy Syst. (Preprint) **47**, 1–12 (2024)
4. P.R. Bhaladhare, D.C. Jinwala, A clustering approach for the l-diversity model in privacy preserving data mining using fractional calculus-bacterial foraging optimization algorithm. Adv. Comput. Eng. **2014**(1), 396529 (2014). https://doi.org/10.1155/2014/396529
5. M. Bradbury, A. Jhumka, *in 2017 IEEE Trustcom/BigDataSE/ICESS, A near-optimal source location privacy scheme for wireless sensor networks* (IEEE, Sydney, 2017), pp.409–416
6. M. Bradbury, A. Jhumka, M. Leeke, Hybrid online protocols for source location privacy in wireless sensor networks. J. Parallel Distrib. Comput. **115**, 67–81 (2018). https://doi.org/10.1016/j.jpdc.2018.01.006
7. M. Bradbury, A. Jhumka, C. Maple, A spatial source location privacy-aware duty cycle for internet of things sensor networks. ACM Trans. Internet Things. **2**, 1–32 (2021). https://doi.org/10.1145/3430379
8. Z. Chen, M. He, W. Liang, K. Chen, Trust-aware and low energy consumption security topology protocol of wireless sensor network. J. Sensors. **2015**(1), 716468 (2015). https://doi.org/10.1155/2015/716468
9. Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, H. Zhou, PSSPR: a source location privacy protection scheme based on sector phantom routing in WSNs. Int. J. Intell. Syst. **123**, 1204–1221 (2022). https://doi.org/10.1002/int.22666
10. M. Conti, J. Willemsen, B. Crispo, Providing source location privacy in wireless sensor networks: A survey. IEEE Commun. Surv. Tutor. **15**(3), 1238–1280 (2013). https://doi.org/10.1109/SURV.2013.011413.00118
11. K. Dimitriou, I. Roussaki, Location privacy protection in distributed iot environments based on dynamic sensor node clustering. Sensors. **19**(13), 3022 (2019). https://doi.org/10.3390/s19133022
12. C.M. George, K. Gayathri, S. Reeja, Hybrid optimization enabled routing protocol for enhancing source location privacy in wireless sensor networks. Int. J. Comput. Netw. Appl. **10**(1), 51–67 (2023). https://doi.org/10.22247/ijcna/2023/218511
13. C. Gu, A. Jhumka, C. Maple, Silence is golden: A source location privacy scheme for wireless sensor networks based on silent nodes. Secur. Commun. Netw. **2022**(1), 5026,549 (2022). https://doi.org/10.1155/2022/5026549
14. M. Guo, X. Jin, N. Pissinou, S. Zanlongo, B. Carbunar, S.S. Iyengar, In-network trajectory privacy preservation. ACM Comput. Surv. **48**(2), 1–29 (2015). https://doi.org/10.1145/2818183
15. T. Hussain, B. Yang, H.U. Rahman, A. Iqbal, F. Ali, et al., Improving source location privacy in social Internet of Things using a hybrid phantom routing technique. Comput. Secur. **123**, 102917 (2022). https://doi.org/10.1016/j.cose.2022.102917

16. C. Lachner, T. Rausch, S. Dustdar, *in 2019 IEEE Global Communications Conference (GLOBECOM), Oriot: A source location privacy system for resource constrained iot devices* (Hawaii, IEEE, 2019), pp.1–6
17. J.F. Laikin, M. Bradbury, C. Gu, M. Leeke, in *2016 IEEE international conference on communication systems (ICCS)*, Towards fake sources for source location privacy in wireless sensor networks with multiple sources (IEEE, Shenzen, 2016), pp. 1–6
18. F. Li, P. Ren, G. Yang, Y. Sun, Y. Wang, Y. Wang, S. Li, H. Zhou, An efficient anonymous communication scheme to protect the privacy of the source node location in the Internet of Things. Secur. Commun. Netw. **2021**(1), 6670847 (2021)
19. P. Lv, X. Wang, Y. Cheng, Z. Duan, Stochastic double deep Q-network. IEEE. Access. **7**, 79446–79454 (2019). https://doi.org/10.1109/ACCESS.2019.2922706
20. R. Manjula, T. Koduru, R. Datta, Protecting source location privacy in iot-enabled wireless sensor networks: The case of multiple assets. IEEE Internet Things J. **9**(13), 10807–10820 (2021)
21. L.C. Mutalemwa, S. Shin, Protecting source location privacy in iot-enabled wireless sensor networks: The case of multiple assets. IEEE Access. **9**, 104820–104836 (2021)
22. L.C. Mutalemwa, S. Shin, Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing. Sensors. **19**, 1037 (2019). https://doi.org/10.3390/s19051037
23. T. Naumowicz, R. Freeman, H. Kirk, B. Dean, M. Calsyn, A. Liers, A. Braendle, T. Guilford, J. Schiller, *in IEEE Local Computer Network Conference, IEEE local computer network conference* (IEEE, Washington, 2010), pp.882–889
24. A. Sagu, N.S. Gill, P. Gulia, P.K. Singh, W.C. Hong, Design of metaheuristic optimization algorithms for deep learning model for secure iot environment. Sustainability. **15**(3), 2204 (2023)
25. A. Shukla, D. Singh, M. Sajwan, M. Kumar, D. Kumari, A. Kumar, M. Panthi, SLP-RRFPR: A source location privacy protection scheme based on random ring and limited hop fake packet routing for wireless sensor networks. Multimed. Tools Appl. **81**(8), 11145–11185 (2022)
26. Y. Sun, X. Huang, D. Kroening, J. Sharp, M. Hill, R. Ashmore, Testing deep neural networks. (2018). https://doi.org/10.48550/arXiv.1803.04792. arXiv preprint arXiv:1803.04792
27. H. Wang, G. Han, L. Zhou, J.A. Ansere, W. Zhang, A source location privacy protection scheme based on ring-loop routing for the IoT. Comput. Netw. **148**, 142–150 (2019). https://doi.org/10.1016/j.comnet.2018.11.005
28. Q. Zhang, K. Zhang, Protecting location privacy in IoT wireless sensor networks through addresses anonymity. Secur. Commun. Netw. **2022**(1), 2440313 (2022). https://doi.org/10.1155/2022/2440313
29. J. Zhou, X. Zhang, Z. Jiang, Recognition of imbalanced epileptic EEG signals by a graph-based extreme learning machine. Wirel. Commun. Mob. Comput. **2021**, 1–12 (2021). https://doi.org/10.1155/2021/5871684

## Publisher's Note