Secure Power Management in Wireless Sensor Networks for Power Monitoring Using Deep Reinforcement Learning

Jin Du[1], Xiaodong Wang2, Hao Zhang[2], Hao Zhang[2]
[1]State Grid Jibei Information & Telecommunication Company. Beijing 100054, China.
[2]State Grid Jibei Electric Power Company Limited, Beijing 100054, China.
E-mail: JinDu12@outlook.com, Linazheng123@outlook.com, yizhou89@outlook.com

Keywords: deep reinforcement learning, energy efficiency, secure power management, secure routing, wireless sensor networks

Received: September 10, 2024

Wireless Sensor Networks (WSNs), widely used in healthcare, environmental monitoring, and military applications, rely on battery-powered sensors with limited energy reserves. Extending the operational lifetime of these networks is a critical challenge, particularly under both external and internal security threats. This paper introduces a novel Secure Power Management (SPM) framework that integrates Deep Reinforcement Learning (DRL) with a token-based Elliptic Curve Cryptography (ECC) policy to optimize energy efficiency and ensure secure communication. The SPM system dynamically transitions sensor nodes between active and sleep modes based on network activity, significantly reducing energy consumption. It remains effective even in the presence of malicious attacks, maintaining robust performance across various threat scenarios. Simulation results demonstrate that the proposed method reduces power consumption by up to 20.01% compared to conventional schemes, while improving energy efficiency by 15%, enhancing packet delivery reliability, and prolonging network lifespan. These findings highlight the potential of DRL-based secure power management for resilient and energy-aware WSN operations.

Povzetek: Razvili so varen sistem upravljanja z energijo za brezžična senzorska omrežja (WSN) z uporabo globokega okrepljenega učenja in ECC za podaljšanje življenjske dobe.

1 Introduction

The previous several decades have seen a transformation in our lifestyles brought about by interactive settings. In the process of reworking our day-to-day lives to make them more comfortable, sensing plays a crucial part. The transformation of our houses into smart homes may be attributed, for example, to the presence of networked sensors that possess the ability to make deductions. Within the scope of such an application, household security, household medical care, family processing of information, family entertainment, and family business are all included. If wired sensing systems need a separate twisted shielded pair wire connection, then wireless sensor networks (WSNs) are more advantageous from an economic standpoint than wired sensing systems. As a result, the latter has considerable expenses associated with its implementation (Kaushik, J. (2021), Swati, et.al, (2022)). On the other hand, in order to properly accomplish its specific goal and achieve cost minimization, a WSN has to operate for a considerable amount of time continuously. Importantly, there is a trade-off between the life expectancy of a WSN and the amount of power that is used by the different functions of the network. In addition, reducing the amount of energy that is used is a primary priority owing to the various components involved. One of the main focuses of research on wireless sensor networks is the appropriate management of network nodes within the constraints of the WSN's limited resources in order to regulate the networks' energy properly. Another difficulty stemming from the sensor's intended use—data collection—is the restricted resources available to the WSN node. As a consequence, bringing down the price of these gadgets to meet consumer demands is crucial, but doing so poses security risks due to their inability to provide even the most basic degree of protection. To be compatible to other network management activities, security administration in WSNs should not rely heavily on connections, processing, or storage (Prajapati, S., et.al, (2023), Cao, C., et.al, (2021)).

As a vital component of the energy sector, electricity affects people's daily lives and the economy as a whole, making the safe and reliable functioning of the power delivery and distribution system a top priority (Sinha, S., et.al, (2022), Thangamuthu, A.P. et.al, (2021)). This paper proposes an application system for the monitoring, examination, security, and interactive aid of layered power distribution and transmission systems using WSN technology and combined with the operating and monitoring requirements of these systems (Srividhya, G., et.al, (2021), Jaiswal, S.K., et.al, (2023)). An insider attack or other hostile assault may be effectively mitigated with secure power management. Afterwards, it intelligently

puts the nodes of the wireless sensor network into sleep mode when they're not in use and wakes them up when needed. With the goal of delivering reliable and safe power management for WSNs (Wang, S., et.al, (2021), R., S.K., et.al, (2021)).

We suggested a method for WSN power management that is both efficient and secure. By combining an effective routing strategy with well-managed security, this method efficiently transmits data throughout the network. The primary goal of this study is to enhance the current systems' power management and routing efficiency while simultaneously discovering and providing robust secure power management in WSNs. On the other hand, reducing the total power consumption of the network is more important owing to the intricacy of the issue that has been presented; this is still a promising field for study. Consequently, this article discusses the primary methods that have been discovered for reducing the amount of electricity that is used (Kaushik, I. et.al, (2020), Bharanidharan, R. (2020), Qamar, S., et.al, (2020)).

Here is how the remainder of the work is structured. The paper's power management models are introduced in Section 2. Section 3 introduces the SPM in WSN that makes use of DRL. In Section 4, we provide and analyze the findings of the simulation. In Section 5, we draw a conclusion and lay forth the groundwork for our future research.

1.1 Power-management and control in WSN

Power consumption model

The ability to perceive, process, and send data is inherent to every node. A WSN relies on sensor nodes, which are often battery-operated and have limited computing and storage capacities, and uses a wireless means for communication. One of the most important resources in WSNs is energy, and these networks use a variety of communication protocols that aim to save it. The sending and receiving of data are also components of communication (G, M., A., et.al, (2023), Roja, P., et.al, (2022), Khan, T.A., et.al, (2022)). Here, we provide a model for the power consumption of communication (P_c) as:

$$P_c = N_T[P_T(T_{ON} + T_{ST}) + P_{OUT}(T_{ON})] + N_R[P_R(R_{ON} + R_{ST})] \quad (1)$$

Where N_T is the typical pulse rate at which the transmitter is activated, N_R is the typical frequency of the receiver's operation in milliseconds, P_T is the amount of power that the transmitter uses, and P_R is the amount of power that the receiver uses. T_{ON} is the transceiver's startup time, and is the transmitter on time P_{OuT} is the output transmitting power, R_{ON} stands for the receiver's start-up time, and R_ST for its on-time performance.

When a system is not in use, it may be put into a low-power state—also called "sleeping mode"—or its power can be "gated"—that is, turned off—a control strategy. This is a low-power design approach that works, but it adds additional power consumption and operational latency whenever the machine sleeps or wakes up. Negative power savings occurs when the structure's sleeping period is small and the additional power usage is more than while the system is operating. A positive power savings may be achieved by using the power monitoring system, and its break-even point has been described. Additionally, it guarantees that the machine remains in sleep mode for just the correct amount of successive clock cycles before being awakened up (Nandal, V., et.al, (2021), Yuvaraja, M., et.al, (2024), Almansoori, M.N., et.al, (2022)). Negative power saving, or increased power consumption, will occur if the system's sleep duration is insufficient to meet the break-even threshold. The additional regulating activities caused by power management turning on and off a system result in excess energy E_"overhed," as demonstrated in Eq. (2).

$$E_{\text{overhead}} = 2\frac{W_H}{a}E_{cyc}^{s} \quad (2)$$

Where W_H represents the active dimension of the goal system, α is the ratio of the overall route area to the area of the gated structure, and E_{cyc}^{s} is the amount of energy needed to turn the functional units on and off. Even though the system continues to utilize power when switching on and off, the voltage is unstable throughout this time, rendering it useless for typical tasks. Using Equation (2), we can express the overall energy savings achieved by the framework all over the N clock cycles of gating.

$$E_{\text{saved}} = E_{cyc}^{L}\frac{DIBL}{mV_t} \times \frac{N^2}{2} \times \frac{aLV_{\text{dd}}}{2\left(\frac{V_2}{2} + \frac{C_D}{C_s}\right)} \quad (3)$$

Three variables: supply voltage, subthreshold slope factor (m), and drain-induce barrier reducing factor (DIBL) (V_{dd}), temperature voltage (V_t), and leakage factor (L) are all variables in this context $= E_{cyc}^{L}/E_{cyc}^{s}$, and C_D and C_S standing for switching capacitance and decoupling capacitance, correspondingly. When $E_{\text{saved}} = E_{\text{overhead}}$, To get the break-even point, N, use the following formula.

$$N = 2\frac{1}{L\alpha}\sqrt{\frac{mV_tW_H}{V_{dd} * DIBL}\left(1 + 2\frac{C_D}{C_s}\right)} \quad (4)$$

Power management techniques

There are typically two states of operation for a sensor node: active and idle. In active mode, the node acquires data from sensors and communicates wirelessly. In idle mode, it does nothing. Since the power consumption during the active phase is necessary to carry out the sensor node's fundamental function, it is considered acceptable. In contrast, superfluous subsystems should be disabled

entirely as any power used while inactive is a waste of resources. The sensor node may still have a power leak that gradually depletes the battery. When deployed in large numbers (50-100), the power-hungry sensors still need to have their batteries changed often, even with advanced battery technology (Hassan, K., et.al, (2023), N.P., et.al, (2020), Sharma, A., et.al, (2023), Ahmad, R., et.al, (2022)). This is why these systems use power-management strategies, some of which will be covered in more detail below.

- **Power gating:** Since the node receiver only turns on when a message is waiting for it, the wake-up technique is also one of the most energy-efficient ways to handle idle mode. A typical transceiver uses a lot of power, whereas this kind of receiver only a fraction of that. As a rule, latency is greater, sensitivity is lesser, and data rate is lower. Since this method only activates the intended nodes, it also lessens the likelihood of overhearing. When turned on, wake-up receivers also drain power supplies, thus they need to be very power efficient if they want to reap the benefits of energy gain.

- **Dynamic voltage frequency scaling:** Here, we may dynamically lower the voltage and frequency selectively, allowing the block to merely satisfy its present job deadlines. This method is similar to power gating in that it runs slower blocks at lower frequencies while providing voltage without entirely cutting off the supply. In order to calculate the necessary decrease whilst the system is running, this method needs sufficient information about the application's power consumption. Maximizing power savings also entails controlling voltage and frequency using hardware and software.

- **Energy harvesting from surrounding:** The sensor nodes' reliance on a battery for electricity puts a cap on the network's lifespan because of the battery's limited capacity to store energy. An appealing alternative for systems that rely only on batteries is energy-harvesting devices in conjunction with rechargeable batteries. In order to greatly extend the life and functionality of the sensor nodes, these systems are able to collect energy from their environment. Solar, thermoelectric, electrostatic, electromagnetic waves, and piezoelectric methods are all used to collect energy. But the environment isn't always predictable, thus it's possible that a certain harvester won't ensure the node can run safely. As a result, hybrid harvesters are being utilized, which include two or more ecological harvesters.

2 Related works

Ghosh, R., et.al, (2021) presented an innovative, smart controller to sustain mobility in wireless sensor networks (WSNs). Principally, the focal point is dependent on the arrangement of fuzzy input variables (i.e., remaining battery power [RBP], mobility, and centrality solution) to crucial usages, similar to personnel safety in an industrialized atmosphere. A mobility controller dependent upon type-1 fuzzy logic (T1FL) is planned to support sensor mobile nodes (MN). Here, a role model cluster head (RMCH) is picked out among the cluster heads (CHs) that may simply convey the message to the mobile base station (BS) by determining the appropriate type-1 fuzzy (T1F) descriptors such as RBP, mobility of the sink, and the centrality of the clusters. Type-1 fuzzy inference system (Mamdani's rule) is utilized to opt for the possibility to be RMCH. The validity of the introduced model is carried out by means of multiple linear regressions.

Gudhekar, G.S., et.al, (2021) The design and development of an intelligent monitoring and controlling system for home appliances in a real time system is presented in this project. This system principally monitors the electrical parameters such as voltage and current and subsequently calculates the power consumption of the home appliances that are need to be monitored. The innovation of this system is controlling mechanism implementation in Iot based by server. The user can control the home appliances by mobile app using server data. The developed system is a low-cost and flexible in operation and thus can save electricity expense of the consumers. Also, the proposed system is an economical and easily operable. Due to these intelligent characteristics, it becomes an electricity expense reducer and people friendly. Adopting WSNs for power management provides great advantages over traditional wired system. By using WSN technology data can be collected through sensing unit and transferred wirelessly to a control system for operation and management.

Nandini, G., et.al, (2020) Power utilization is the significant worry in our daily life. It is assessed that normal power utilization of family apparatuses is 90 units (kWh) per month in India. All gadgets are worked by taking power. It has to shrewd screen power and diminish the measure of utilization. Brilliant screen which computes the electrical boundaries, for example, voltage and power at that point therefore power devoured by the devices. So, it can get away from of the gadgets taken a tremendous part in power utilization. WSN senses and records the physical changes in environment. The essential idea of WSN is the devices are not associated truly. The gathered data is given to the devices which are kept to certain territory. In this paper IOT is utilized alongside WSN with the goal that the framework can get to the devices from any place. A smart energy management system can contribute towards reducing the expenses and still satisfy the demands. This framework additionally gives adaptability in activity and consequently we can spare the power.

Das, S. (2023) main challenge of power management in WSNs is to maximize the network lifespan by scheduling the monitoring activities and optimizing the data transfer rate. Therefore, various power control methods were

proposed to reduce energy consumption and extend the network lifetime. This article provides an overview of the power management techniques used to reduce energy consumption in WSNs. Specifically, this article explains various scheduling, routing and sleeping techniques that are used to manage the power drain in WSNs.

Bengheni, A. (2024) presented Relay node selection scheme and Deep sleep period for power management in Energy Harvesting Wireless Sensor Networks (RD-EHWSN), a new energy-saving scheme founded on asynchronous duty cycling. RD-EHWSN reduces sensor node energy consumption and guarantees equilibrium energy use between sensor nodes in WSN with the energy harvesting capacity by adjusting these sensor nodes duty cycles more drastically and deeply by according to the estimated value of its residual energy on the basis of future-presented harvested energy, and this is done through the use of a new proposed energy threshold policy. RD-EHWSN also grips the benefit of transmitter initiated using the low power listening (LPL) technique with short preamble messages and uses a new relay node selection procedure to achieve the load balancing in WSN. We implemented RD-EHWSN by using OMNeT++/MiXiM. For evaluation, we compared it with PS-EHWSN, under multiple concurrent multihop traffic flows scenarios and scenarios in which nodes can harvest different energy harvesting rate. In all experiments, RD-EHWSN significantly outperformed the PS-EHWSN scheme; the results of simulation demonstrate that our scheme enhances the general yielding of WSN thru lessening the energy consumption and the mean latency, as well as raising the packet delivery ratio and the throughput.

Table 1 shows related works.

Table 1: Summary of related works

Studies	Methodologies	Results
Ghosh, R., et.al, (2021)	For sensor mobile nodes, a type-1 fuzzy logic (T1FL) mobility controller is envisioned. The role model cluster head (RMCH) is chosen between the cluster heads (CHs) to send the message to the mobile base station (BS) using type-1 fuzzy (T1F) characteristics such RBP, sink mobility, and cluster centrality.	High PDR and Delay
Gudhekar, G.S., et.al, (2021)	This system monitors voltage and current to compute household appliance power usage. The server-based IoT controlling mechanism is this system's novelty. Mobile app users may manage home appliances using server data. With its cheap cost and flexibility, the system may save users money on power.	Higher mobility causes high PLR
Nandini, G., et.al, (2020)	The gathered data is given to the devices which are kept to certain territory. In this paper IOT is utilized alongside WSN with the goal that the framework can get to the devices from any place. A smart energy management system can contribute towards reducing the expenses and still satisfy the demands. This framework additionally gives adaptability in activity and consequently we can spare the power.	Gathered data consumes more energy and causes delay
Das, S. (2023)	Various power control methods were proposed to reduce energy consumption and extend the network lifetime.	Predicted the performance for network lifetime and energy consumption
Bengheni, A. (2024)	Relay node selection scheme and Deep sleep period for power management in Energy Harvesting	High energy consumption for large scale environment

2.1 Existing gaps and challenges

There are several obstacles to overcome while deploying and operating WSNs, the most significant of which is striking a balance between energy efficiency and strong security measures. Suboptimal network performance is typically the result of traditional methodologies that treat

these concerns independently. Important obstacles include of the following:

- Energy savings: The fundamental problem is finding ways to prolong the lifetime of the network without compromising its operational performance, considering the restricted authority resources of the sensor nodes.
- Safety: Various security risks, such as data breaches and node manipulation, might affect WSNs due to the open character of wireless communication; hence, thorough security solutions are required.
- Ability to adjust: Conventional static approaches are inadequate in the face of constantly changing threat environments and dynamic network circumstances, necessitating flexible tactics.

To tackle these issues holistically, our suggested SPM approach makes use of DRL. In contrast to more static approaches, SPM continuously optimizes power and security by responding to evolving network circumstances and potential security risks. Not only does this method address the shortcomings of current methods, but it also provides a versatile and extensible framework for managing WSNs in their entirety.

3 Materials and methods

The experimental setup for the suggested SPM, which makes use of DRL and an improved LEACH algorithm, is detailed in this section. We will also discuss the results of the suggested techniques, which include LEACH improvement to reduce power consumption and increase the lifetime of the network and lightweight cryptography to prevent third parties from joining the group of sensors.

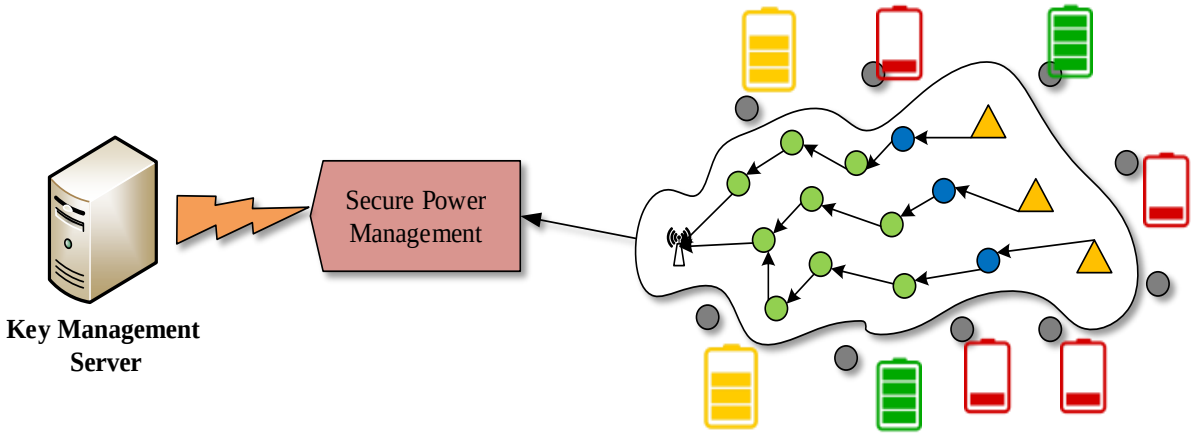

Figure 1: System model using SPM with DRL

3.1 Power optimization using DRL

The idea behind the suggested SPM method is to provide a single solution that uses DRL to optimize network operations in real-time, which would increase energy effectiveness and safety equally. Accurately modeling the communication quality between nodes is of utmost importance in our suggested technique. Our energy savings and safety measures, as well as the improvement of the network's general performance, are built around this paradigm.

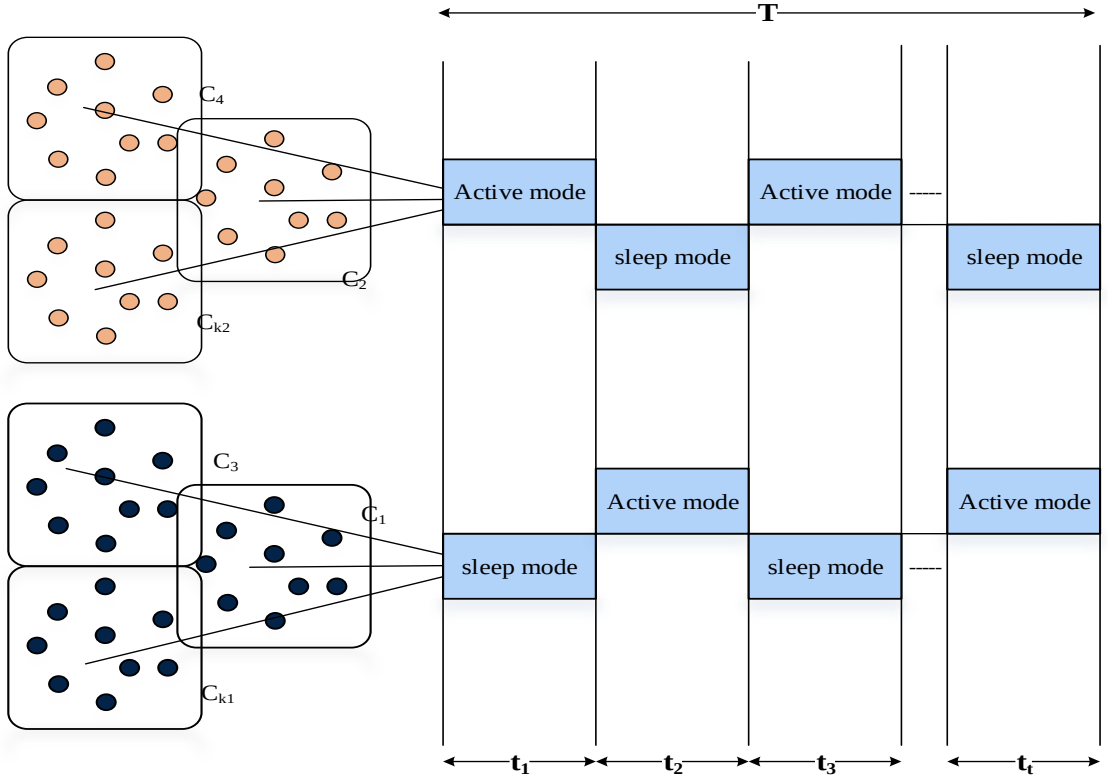

Figure 2: Power Management in WSNs

The quality of the connection between nodes i and j may be described in terms of the wireless communication features of WSNs by

$$Q_{ij} = \frac{P_{tx} \times G_{tx} \times G_{rx}}{L(d_{ij}) \times V} \quad (5)$$

where P_{tz} is the transmission power and G_{tz} and G_{rz} is the gain of the receiving antenna and the broadcasting antenna, respectively. $L(d_{ij})$ denotes the function for path loss, while V stands for the power of noise. We establish a security index that takes into account the potential dangers to WSN and the amount of energy used by each node:

$$E_{eff}(i) = \frac{D_i}{E_i} \quad (6)$$

$$S_{\text{risk}}(i) = \frac{A_i}{T} \quad (7)$$

Where D_i E_i, where is the energy consumption of node i and can be determined using (4), is the data throughput of node i. A_i counts the assaults that node i endured during the time interval T.

$$E_i = P_{tx} \times t_{tx} + P_{rx} \times t_{rx} + P_{\text{idle}} \times t_{\text{idle}} \quad (8)$$

WhereP_{tz}, P_{rz}, and P_{idle} indicate the node's power while it is transmitting, receiving, and idle, correspondingly. At the same time, t_{tx}, t_{r_x}, and t_{dlle} the amount of time that the node spent in each of these stages, separately. The following is a definition of the optimization issue that aims to optimize energy efficiency while minimizing the overall network security risk:

$$\max_p \sum_{i=1}^{N} E_{\text{eff}}(i) = \max_p \frac{D_i}{E_i} \quad (9)$$

$$\min_p \sum_{i=1}^{N} S_{\text{risk}}(i) = \max_p \frac{A_i}{T} \quad (10)$$

In this case, p denotes the network policy, which includes the encryption level and transmission power of every node.

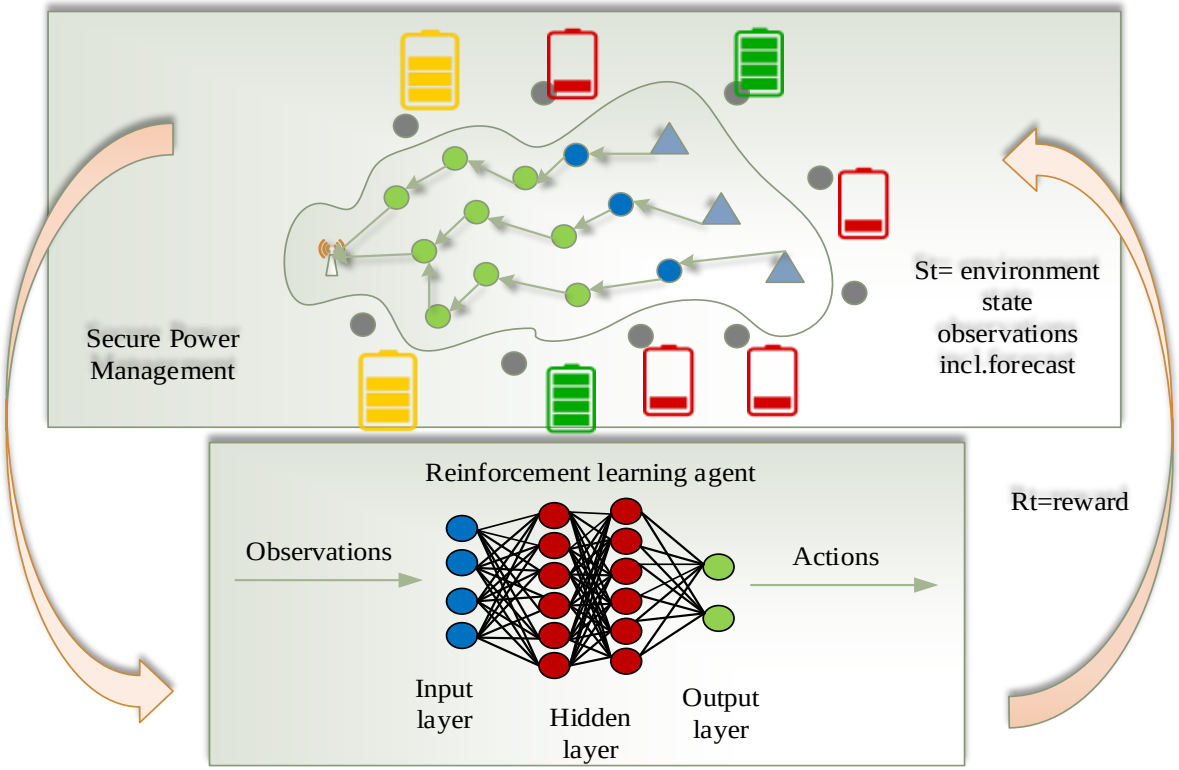

Figure 3 (a): SPM using DRL

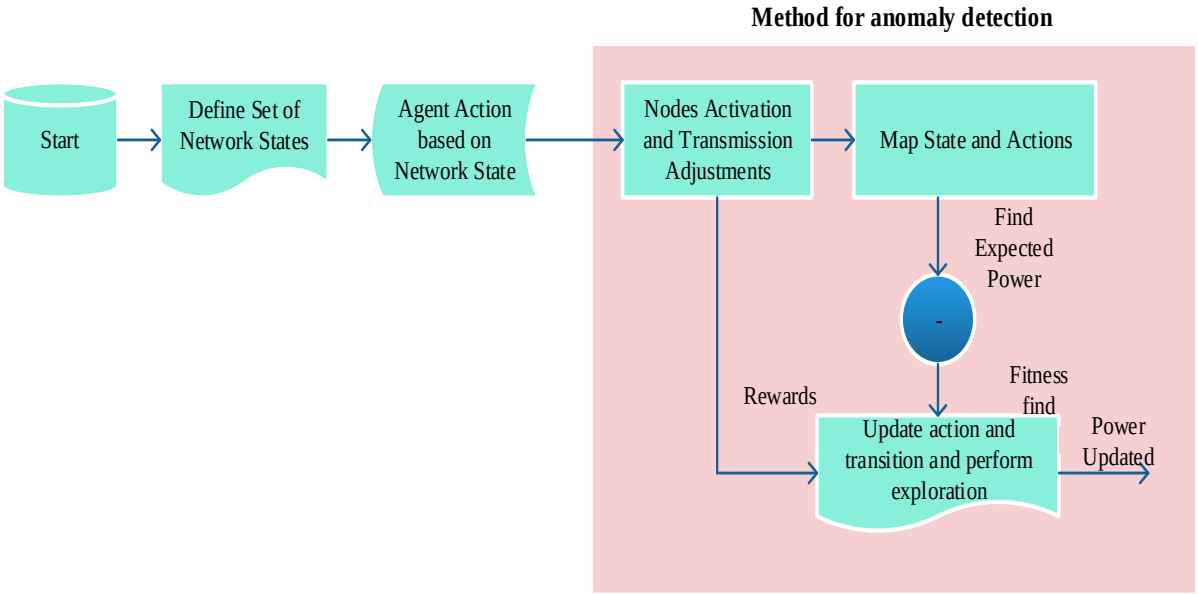

Figure 3 (b): DRL flowchart

We begin by defining an MDP, which is a quintuple array, so that we may utilize DRL for optimizing the WSN approach. (S, A, P, R, γ). S is the state space. A lies the domain of action. The probability of transferring states is abbreviated as P. $P(s' \mid s, a)$. R is the reward function, well-defined as $R(s, a, s')$. γ represents the discount percentage. In order to maximize the network's performance while simultaneously addressing energy efficiency and security, we use DRL to discover a plan. We introduce a novel composite reward function:

$$R(s,a) = \alpha \times \sum_{i=1}^{N} E_{eff}(i) - \beta \times \sum_{i=1}^{N} S_{\text{risk}}(i) \quad (11)$$

in which the weighting parameters are denoted by α and β. Reinforcement learning aims to maximize the network's predicted reward. This idea might be stated as

$$J(\pi) = E_{\pi}(R_1 + \gamma R_2 + \gamma^2 R_3 + \cdots] \quad (12)$$

where R_t is the payoff if time t is met. We use Bellman's the greatest efficiency principle for mathematical proof [34] to show that our suggested DRL-based neural network design is the best technique, instead of Q-value. This Bellman equation is satisfied by the Q-value function that the neural network generates:

$$Q(s,a) = R(s,a) + \gamma \times E\left[\max_{a'} Q(s',a')\right] \quad (13)$$

in where γ stands for the discount element, $s'$for the next state, and $a'$for the next action.
Finding the policy π that optimizes the Q-value function is the objective of strategy optimization. The resulting optimization issue looks like this:

$$\max_{\pi} E[Q(s,a)] \quad (14)$$

We may get the policy's gradient using the policy gradient approach, which is as

$$\nabla J(\pi) = E[\nabla \log \pi(a \mid s)(Q(s,a) - V(s))] \quad (15)$$

where the value function of state s is denoted as V(s). We can find the best policy by repeatedly changing the policy parameters.
It is important to mention that our suggested method is to develop a WSN strategy optimization process that is more resilient and successful than deep Q-learning. This will guarantee that SPM can manage the complexities and difficulties that are unique to WSNs. Some examples of this include the ever-changing threat environment for network security, the varied and flexible nature of network structures, and the changeable energy profile of sensor nodes. In particular, our optimization approach exhibits the traits listed below:

- Our state space representation has been enhanced. To better capture the intricate dynamics of WSNs, SPM's state space has been expanded to include a wider range of network properties.

- Function for personalized rewards. Although most deep Q-learning systems do not aim to maximize energy efficiency and ensure network security, we use a tailored reward function that is specifically designed to do just that.

- We optimize policies for WSNs. Node energy restrictions and the necessity for quick reaction to security threats are two examples of operational limitations and performance objectives that our methodology tailors the policy optimization method to meet in WSNs.

- High-tech system for reliving past experiences. To improve upon the standard deep Q-learning method, we have integrated a state-of-the-art experience replay process that is more suited to the spatial and temporal heterogeneity in WSNs.

- The incorporation of procedures tailored to WSNs. By integrating SPM with protocols designed for WSNs, we can easily translate learned techniques into policies that can be put into practice in a real-world system setting.

3.2 Secure path selection for power aware routing

We have used a private key that is produced using a random integer within a particular range of the curve's field size in our suggested technique. The four steps of the scheme are as follows: determining the total number of clusters, verifying each node, determining who is the cluster head, distributing keys among all members of the group, creating a routing table using the routing protocol, and finally, rekeying in the event that any changes occur within the group.
All the nodes in the network must have the same traits and be at the same authority level for the scheme to function. In each case, the protocol specifies a mechanism that each node with data to transmit follows in order to determine where to send it. It is possible for every node in the network to construct or calculate its private key inside the ECC. These keys are integers ranging from 1 to 256 bits, which is the field size of the curve.
The secp256k1 curve and the elliptic curve digital signing technique (ECDSA), which are often used in cryptocurrency systems, are utilized in this research. The unique non-random construction of secp256k1 makes it possible to do very efficient computations. A well-optimized secp256k1 implementation often outperforms other known EC curves by 30% or more. On a curve ($\mathbb{F}p$), the six domain parameters of secp256k1, also called the Koblitz curve, are defined as a sextuple T = (P, a, b, G, n, and h).
With generator point G, the elliptic curve, with r_i as the private key for node i, the computational cost of the cyclic ECC key creation and distribution in the method one table can be estimated for n the amount of nodes in the sensor network. Scalar multiplication, as shown in Equation (10) is required to get a shared key for a node.

$$P_t = (r_1 \cdot r_2 \cdot r_3 \cdot r_4 \ldots\ldots\ldots \cdot r_n) \cdot G \quad (16)$$

EC scalar multiplication is where the "operator" comes in. A total complexity may be determined for n nodes by using Equation (11).

$$O\left(n(r^n \cdot G)\right) \tag{17}$$

By analyzing the SPM data, a unique random key may be generated. The one who distributes the secret key is

$$\text{Skey}\ (n) = \text{Rand}\ () \times \text{Dist}\ (n, n+1) \times \text{EfM}\ (n) \tag{18}$$

$$\text{SKey}\ (n) = \text{Rand}\ () \times \text{Dist}\ \left(n, n\frac{1}{LR(n)} + \frac{1}{\text{DR}\ (n)}\right) \tag{19}$$

A significant drawback of this protocol is that it chooses an additional cluster head only after a full round has passed, and it doesn't take the node's leftover energy into account at all. In the event that a cluster header is selected during the course of a round and subsequently dies, all aggregate data associated with that cluster header will be erased, and subsequent rounds will not be able to receive or send data successfully. One other issue with LEACH is that cluster heads are selected at random or by looking at the energy of the highest energy cluster. However, this selection process doesn't account for the distance to the sink or the size of the package, which are factors that determine the energy needed to transmit the message. The node that is farthest from the base station, even if it has the greatest energy, may not be the best candidate. To summarize, in most cases, the parameters that determine if the CH desires to be replaced have to do with the amount of energy required to collect all the packets sent by the light nodes, sensor nodes, or leave nodes and get them ready to submit the information via regular links, taking into account the power consumption. The identification of an Advanced Persistent Threat (APT) impacting the CH is another factor that might initiate a request for replacement.

In response to these issues, we suggested the following two changes to the initial LEACH protocol: The cluster header calculates the energy needed to transport a packet before sending it, E_{tx}. If the amount of power needed to send a packet, E_{tx}, is less than or equal to the residual energy ($E_{rs\ \text{sidual}}$) of the node (i.e., $E_{tx} \leq E_{\text{rosidual}}$), Afterwards, the cluster header will be demoted and a replacement will be selected. The previous cluster header should have its aggregated data moved to the new one. You may calculate the necessary transmit energy for a packet of length PacketLength by applying Equations (6) and (7).

$$E_{LX} = S_{EIx} \times \text{ PacketLength } + S_{Eys} \times d^2 \tag{20}$$

$$E_{EX} = S_{EEx} \times \text{ PacketLength } + S_{Emp} \times d^4 \tag{21}$$

where S_{Etx} is the energy parameter for the transmitter at the base station and S_{Emp} and S_{Efs} and in the free space model, they represent the energy characteristics for the kind of radio transmitter, respectively. In this context, "d" refers to the distance in kilometers among the node and network hub S. To find the distance among node i and base station S, we may use the formula (8), which takes into account the ephemeral nature of distances.

$$d_t = \sqrt[2]{(x_t - x_s)^2 + (y_t - y_s)^2} \tag{23}$$

Where x, in any dimension, denotes the node's or base station's two-dimensional coordinates. The energy-factor for distance is used to choose the cluster header F_{cd}, calculated by use of Equation (2). The highest-ranking node F_{ed} is consistently selected as the cluster's parent node. In contrast to the LEACH protocol's reliance on nodes with the greatest energy levels or random selection techniques, this method takes the distance among the node and the base station into account during the selection process.

$$E_{at} = E_{\text{rsstual}} - E_{tx} \times \frac{1}{d^2} \tag{24}$$

In addition, nodes are only considered for the role of cluster leader if they guarantee that their residual energy $E_{r\ \text{rsidual}}$ is greater than transit energy E_{tx} may be a good choice for cluster headers.

For an RREQ message delivered by the source node, the next hop in SPM decides the RSS (0<RSS$_{f_0}$(n)<100) and then floods the sent message. Receiving nodes estimate the source's power utilization metric (PfM) using Eq., and the destination node's RREP message conveys this information together with the node's critical routing metrics, including receive-rate, loss-rate, and delay-rate,

$$\text{PFM}\ (n) = \text{RR}\ (n) + \frac{1}{\text{LR}\ (n)} + \frac{1}{\text{DR}\ (n)} \tag{25}$$

where

RR(n) → receive-rate of the node n

LR(n) → loss-rate of the node

n DR(n) → delay-rate of the node n.

3.3 Transmission power adjustment

The distance between nodes in the route determines how the nodes' transmission power is changed. It lessens energy waste. It will be necessary to use less transmission power for the nearby node. More energy is wasted since the transmission power is set higher for the closest node. Until the packet reaches its destination, the transmission power of each node in the route is modified according to the distance between them. The two-ray ground reflection simulation will be used to modify the transmission power.

$$P_r = P_t G_t G_r h_t^2 h_r^2 / d^4 L \quad (26)$$
$$P_t = P_r d^4 L / G_t G_r h_t^2 h_r^2$$

where G_r and G_t stands for the receiving antenna gain and the transmitting antenna gain, with P_r representing the received signal power (in Watt) and P_t the transmitted signal power. In this case, L stands for system loss and d for the distance between the transmitter and receiver. The antenna heights for transmitting and receiving signals are denoted by ht and hr, respectively. In wireless sensor networks, transmission range levels might be used. Neither too many nor too few transmission range levels are acceptable. Power loss for the range level shift will be greater when there are an excessive number of range levels.

4 Results

Using NS3.27, a simulation was run to include the DRL algorithm into the node controlling power of the WSN. NS3 is a simulator that models network protocols primarily using discrete event time. In the virtual setting, the nodes are dispersed. need NS3's node-config command to be set up as mobile nodes. You can find a description of the parameters used to simulate the SPM system in Table 2. Each node We have a data source at (0,0) and a target node sink at (150,150) in our 500m × 500m square area simulation, with 100 sensor nodes randomly dispersed throughout. Our parameters for the communication set-up are a 30m radius, 500mV for the node's transmission power, and 250mV for its reception power. The given method has the following parameters: α = 0.5, β = 1, ρ = 0.2, and Δ = τ ij 0.02. when shown in Figure 2, the communication linkages among the nodes re-establish themselves when the power consumption decreases, once the whole network finishes routing at the rated power. Thus, although the total number of nodes required to finish data transfer grows in relation to the number of hops between them, the energy usage of those nodes actually decreases. At last, the network's viability is enhanced and its service life is prolonged. The outcomes of the simulation are displayed in Figure 4.

Table 2: Parameters used for proposed SPM model

Definition	Average Value
Size of testbed (number of nodes)	50,100 homogenous
Number of base stations (Bs)	1
Initial energy for each sensor	0.005 j
Radio circuitry energy dissipation, Eelec	50 nj/bit
Energy dissipation of amplifier in free-space, Efs	10 pj/bit
Energy dissipation of amplifier in multipath, Emp	0.0013 pj/bit
Energy consumption for data aggregation, Eda	5 nj/bit
Global testbed area	$n \times n$
Local area (cluster size)	n/nc
Time	10 rounds
Packet size	400-bits
Message size	328-bits
Encryption key length	256-bits

First, a 50 nodes situation is used to conduct the simulation study for the SPM scheme. The packet delivery ratio measures how many data packets made it from the source node to all of their destinations as a percentage. Equation 3.4 is used to measure PDR.

$$PDR = \sum_{0}^{n} \text{packet Received / Time} \quad (27)$$

Packet Loss Rate (PLR)—As shown in Figure 4 and Equation 3.5, the PLR is the rate at which data packets are lost in a network as a function of time.

$$\text{PLR} = \sum_{0}^{n} (\text{Sent Pkts} - \text{Revd Pkts}) / \text{Time} \quad (28)$$

The average delay is the time that has elapsed between the most recent and most prior packets received. Here, n=50, and it is measured using Eq. 3.6, where n is the total amount of nodes.

$$\text{Average Delay Time} = \sum_{0}^{n} \frac{\text{packetreceivedtime} - \text{packetsenttime}}{n} \quad (29)$$

We begin by implementing the power control strategy separately in our testbed experiment. Using power control, we gather data for a set destination node location several times and compare it to the regular situation. According to our findings, node power consumption is highest while in the transmission condition. Figure 4a. In the figure, we display the average power value. Afterwards, we proceed to independently execute the power management system. In this section, we quantify electricity use in various states. In this case, we see that the sensor node's power consumption is lowest while it is in the SLEEP state.

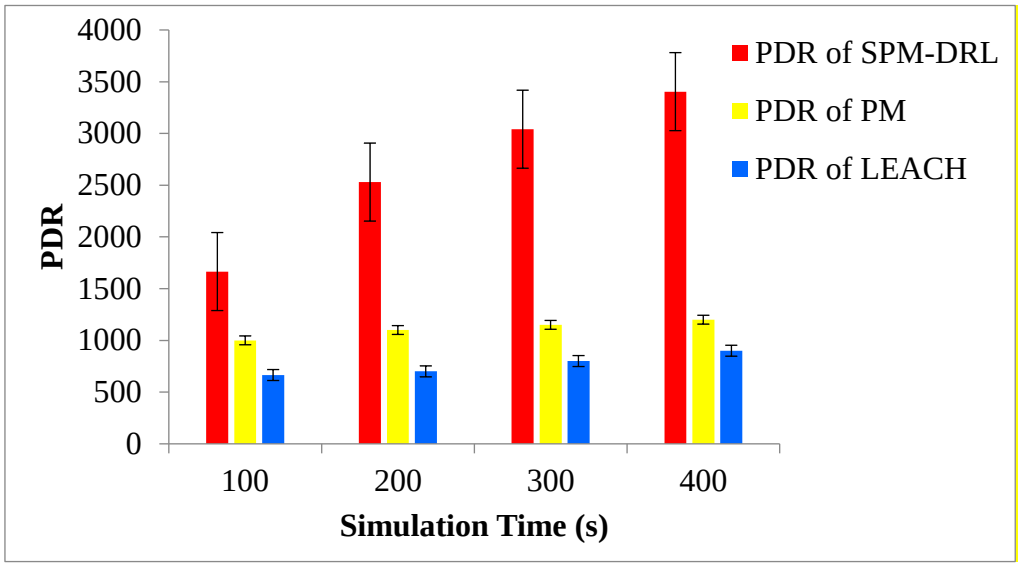

Figure 4(a): PDR vs. simulation time

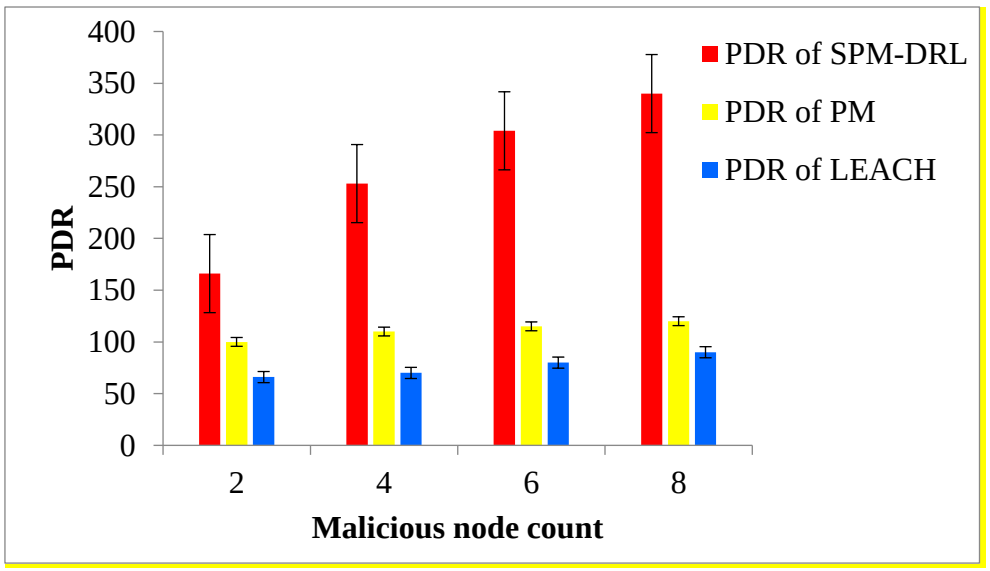

Figure 4(b): PDR vs. malicious node count

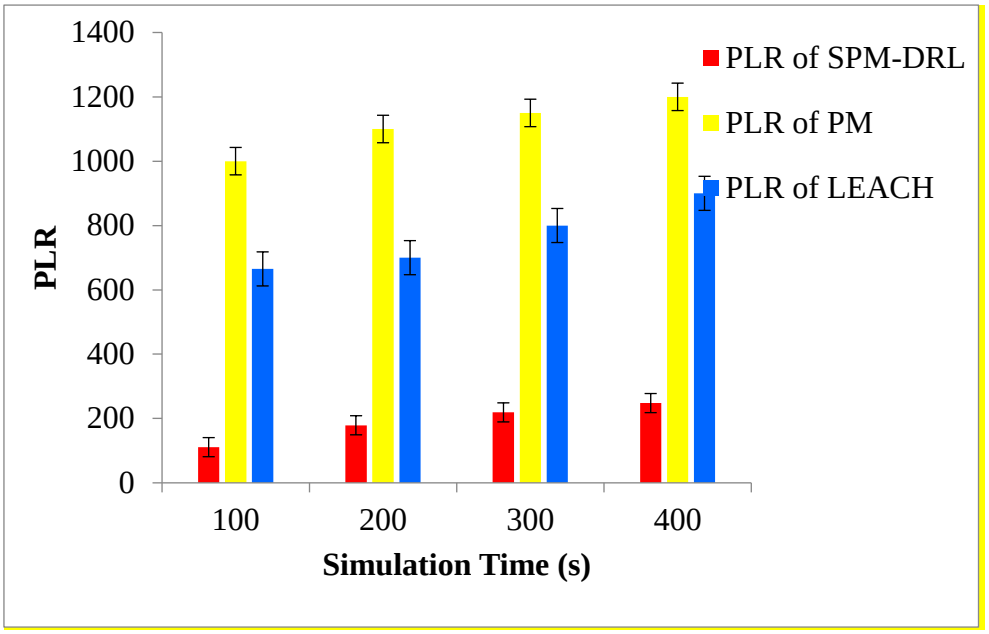

Figure 5(a): PLR vs. simulation time

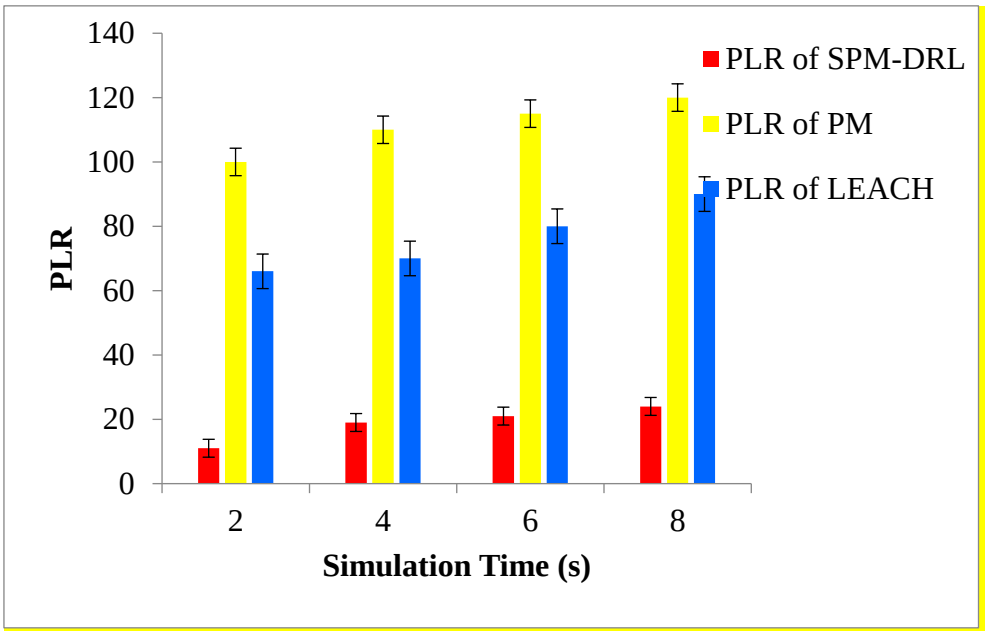

Figure 5(b): PLR vs. malicious node count

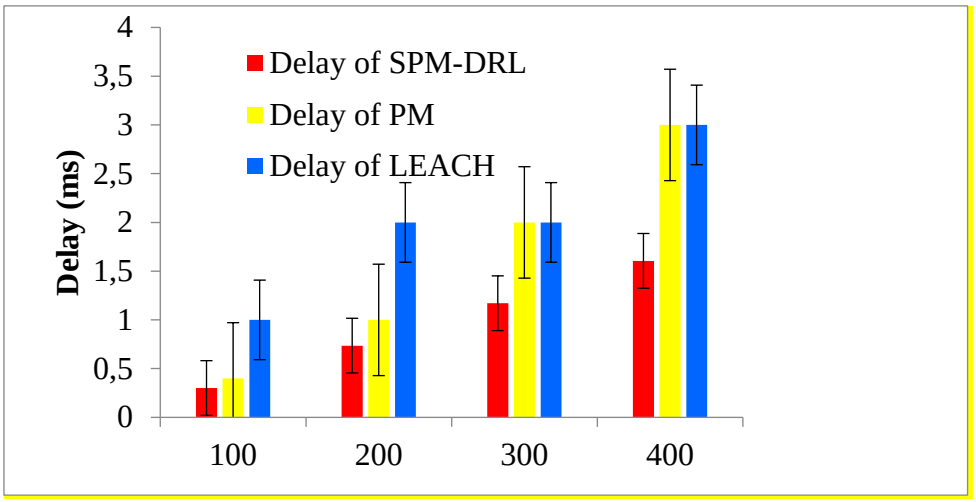

Figure 6(a): Delay vs. simulation time

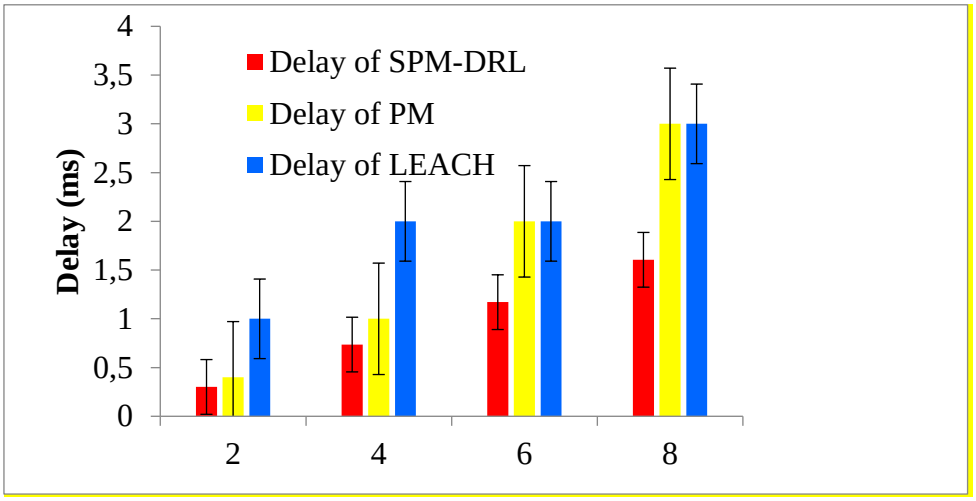

Figure 6(b): Delay vs. malicious node count

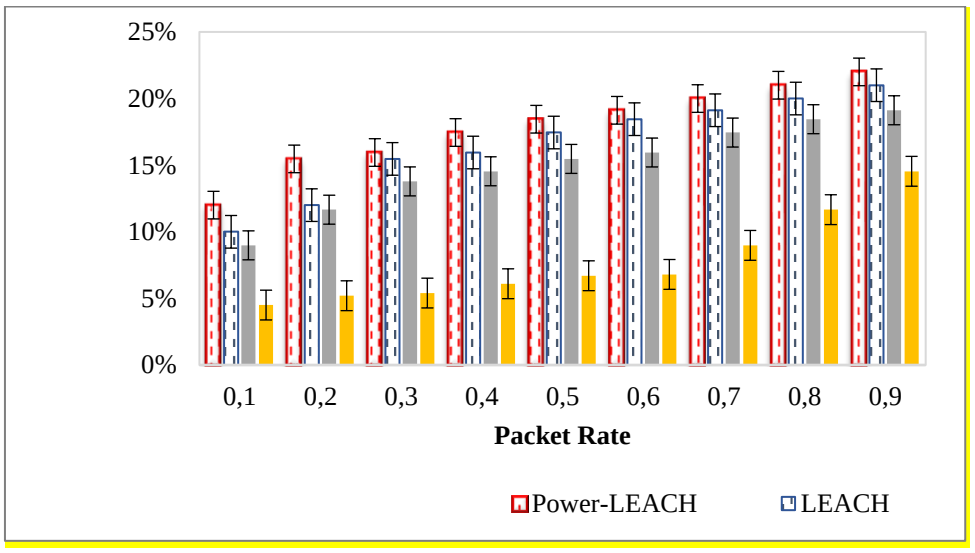

Figure 7(a): Packet rate vs. power saving performance

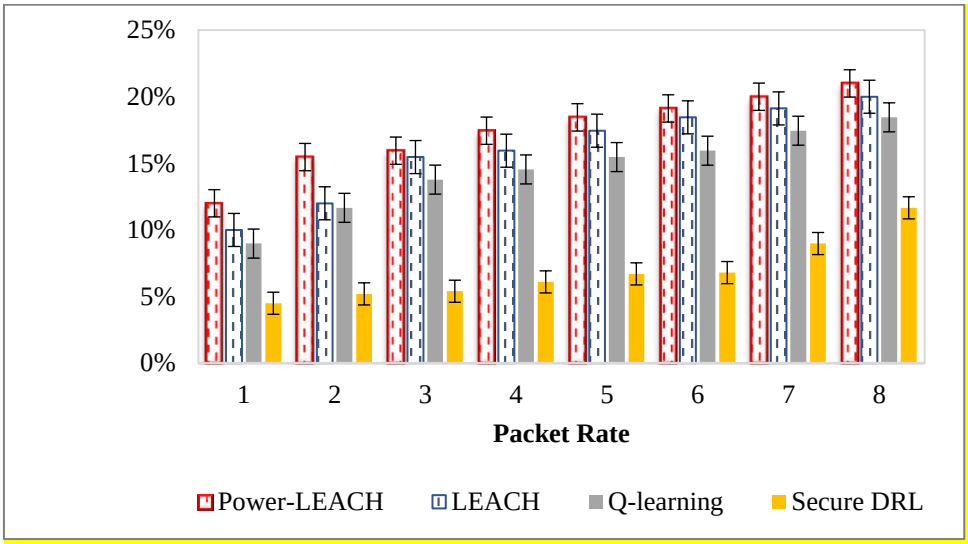

Figure 7 (a): Packet rate vs. malicious node count

5 Discussion

fig 4 illustrates the performance of pdr whereas fig 5 depicts the plr for different packet rates. fig 6 and fig 7 depicts the delay and power saving performance. based on the results thare plotted in the graphs, the proposed approach is described in detail. efficiency in power consumption by nodes, reliability in packet transmission and network longevity, and security of communication between nodes are key metrics that define the effect of our concept. this study was originally intended for an agricultural setting, where sensors might be powered by a single battery or assisted with solar power charging cycles; hence, power consumption is an important consideration. due to the unique nature of this setting, the nodes are not uniformly dispersed across a flat surface. there may be a set of nodes for every plot or region that has been designated for the purpose of deploying sensors to gather data about the crop and the environment. nodes from other farmers, communication shadow zones caused by bad weather, the need to readjust any sensor node's calibration because of unfavorable deployment circumstances, and so on are all potential issues with farm distribution. in a nutshell, these are the kinds of situations that call into question the wisdom of a head-end (ch) node's dynamic re-election in general, not only when its power is completely depleted. along with the decreased power usage and the potential for collisions between nodes from other plots, the suggested cryptographic approach should be used to prevent data contamination.

in terms of power, we measured how the algorithm's power drain changes over time. table 1 defines the criteria and fixes the transmissions from node to node. the field-based sensor nodes are designed to collect data and even combine it into an array for synthesis. in addition, both the transmission rate and the packet size are constant. power consumption during packet transmission is proportional to both the routing scheme and the size of the packet. one method involves clustering nodes using a modified version of leach with a ch that is elected dynamically. another method involves dividing nodes into two layers: one layer where sensor nodes act as light nodes as well as the ch is responsible for keeping the ch log. the second layer groups all the chs into separate chs, creating a second layer of trust at which every log are shared and smart contracts execute to ensure reliable packet transmission. in terms of the network's lifespan, we may say that it has ended when the ch node has used up all of its power to send data packets or even receive tiny control packets. we still consider it power squandered if the operating threshold (oth) is not reached, even if it still has some power. keep in mind that the aforementioned simulation only works in two-dimensional space, with flat surfaces used for node placement. an uneven terrain with obstacles may have been adequately represented by a three-model.

it is significant to determine how often a packet does not reach its intended node or is not recognized at its destination is a measure of the dependability of its transmission via the network. problems with packet loss in an internet of things transmission may arise from a variety of sources, including as agricultural equipment operating in the 2.4 ghz band close to the nodes or denial-of-service attacks that prevent the nodes from transmitting data to the chs. node power consumption is affected by packet loss in every scenario. since power is raised in the event of a connection loss, as is the case for every radio transmission. the ch is simple to target in the event of a node assault since it receives all signals from nearby nodes. an attacker may then attempt to shut down the network by assembling it. one strength of our protocol is that it promptly selects a new node before the current one goes down. this helps with power savings by preventing packet injection and making chs quickly identify which ones not to process. another strength is that it stops attackers from salvaging useful information

from transmissions. with the use of distributed ledger technology (dlt), the proposal's extension may detect when a node goes down or is compromised (due to smart contracts), which would then disable all nodes until the attacker's identity or pattern is determined.

6 Conclusions

This research was conducted to develop and evaluate dynamic secure power management methods for use in wireless sensor networks. Node power consumption administration in WSNs is best handled by DRL approaches because to its multi-path, dynamic, and self-organizing properties. This article presents the DRL algorithm. Wireless sensor networks may drastically cut their energy usage due to an algorithm that allows nodes to discover alternative routes and connections to finish communications even when their communication power is low. Furthermore, we may enhance the overall network's information transmission quality by suitably modifying the track reward amounts and adjustable weights. The model assumes that the sensors are positioned on a flat surface, which may not be the case in situations when the surface is uneven, even if the results achieved using the suggested technique are stunning and promising. Another drawback is that it only takes into account a homogeneous context, where all sensors are identical, there could be heterogeneity and various kinds of sensors used to track different kinds of physical occurrences. The next future step is a 3D implementation and an experimental evaluation of the suggested solution in more intricate WSN systems to determine the method's resistance to various assaults.

In future, the proposed SPM method with multi-agent DRL is deployed for large scale environment and also compared for different number of scenarios such as Varying Environmental Conditions and Node Density, and Malicious Nodes count, which shows how the proposed method are implemented.

Acknowledgments

This work is supported by the Science and Technology Project of State Grid Corporation of China. (No.: 5108-202114038A-0-0-00).

Conflict of interest

The authors declare no conflict of interest.

References

[1] Kaushik, J. (2021). Security Techniques Against Power Exhausting Attacks in WSN: A Fundamental Study. 377- 391. https://turcomat.org/index.php/turkbilmat/article/view/4189

[2] Swati, & Arora, M. (2022). Several Categories of Energy-Efficient Routing Protocols, Features, and Security Necessities in WSN: A Review. 1-6. https://doi.org/10.1109/icict55121.2022.10064506

[3] Prajapati, S., & Desai, M. (2023). Selection of Secure Cluster Head with Trust Management Based Routing Protocol for WSN. https://doi.org/10.1109/indiscon58499.2023.10269951

[4] Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. (2021). IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. Secur. *Commun. Networks*, 2021, 8527068:1-8527068:8. https://doi.org/10.1155/2021/8527068

[5] Sinha, S., & Aggarwal, S. (2022). Cryptographic Algorithms for Security in Wireless Sensor Networks. *2022 3rd International Conference on Intelligent Engineering and Management* (ICIEM), 111-117. https://doi.org/10.1155/2021/8527068

[6] Thangamuthu, A.P. (2021). Security in Wireless Sensor Networks: Issues and Challenges. *Shanlax International Journal of Arts, Science and Humanities*, 8, 120-128. https://doi.org/10.1109/icact.2006.206151

[7] Alghamdi, A., Shahrani, A.M., Alyami, S., Khan, I.R., Sri, P.S., Dutta, P., Rizwan, A., & Venkatareddy, P. (2023). Security and energy efficient cyber-physical systems using predictive modeling approaches in wireless sensor network. *Wireless Networks,* 1-16. https://doi.org/10.1007/s11276-023-03345-1

[8] Narrative: Alghamdi, A., et.al, (2023) Srividhya, G., Nagarajan, R., & Kannadhasan, S. (2021). *Enhancement of Clustering Techniques Efficiency for WSN using LEACH Algorithm. Journal of Physics: Conference Series*, 1921. https://doi.org/10.1088/1742-6596/1921/1/012013

[9] Jaiswal, S.K., & Dwivedi, A.K. (2023). A Security and Application of Wireless Sensor Network: A Comprehensive Study. 2023 *International Conference on IoT, Communication and Automation Technology* (ICICAT), 1-5. https://doi.org/10.1109/icicat57735.2023.10263644

[10] Wang, S., & Chen, Y. (2021). Optimization of Wireless Sensor Network Architecture with Security System. *J. Sensors,* 1-11. https://doi.org/10.1155/2021/7886639

[11] R., S.K., K, L., M, A.P., & K, S. (2021). Security Techniques in Wireless Sensor Networks - A Comprehensive Survey. 2021 Smart Technologies, *Communication and Robotics* (STCR), 1-6. https://doi.org/10.1109/stcr51658.2021.9588872

[12] Kaushik, I., & Sharma, N. (2020). Black Hole Attack and Its Security Measure in Wireless Sensors Networks. 401- 416 https://doi.org/10.1007/978-3-030-40305-8_20

[13] Bharanidharan, R. (2020). A Novel Blockchain Approach for Improve the Performance of Network

Security Using Polynomial Ephemeral Blockchain-Based Secure Routing in Wireless Sensor Network. *Journal of Computational and Theoretical Nanoscience,* 17, 5598-5604. https://doi.org/10.1166/jctn.2020.9458

[14] Qamar, S., Khan, N., Ahmad, N., Hussain, M.R., Naim, A., Quadri, N.N., Israil, M., Arafath, M.S., & Rahman, A.A. (2020). Fault Analysis for Lightweight Block Cipher and Security Analysis in Wireless Sensor Network for Internet of Things. 3-11 https://doi.org/10.1007/978-981-15-3172-9_1

[15] N.P., S., & D, B. (2020). REVIEW ON DYNAMIC KEY SECURITY PROTOCOLS IN WIRELESS SENSOR NETWORK USING PSEUDORANDOM NUMBER GENERATOR. *International Journal of Technical Research & Science.* 16-20 https://doi.org/10.30780/specialissue-icrdet-2019/003

[16] Sharma, A., Babbar, H., Rani, S., Sah, D.K., Sehar, S., & Gianini, G. (2023). MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT. *Energies.*4198, https://doi.org/10.3390/en16104198

[17] Ahmad, R., Wazirali, R., Abu-Ain, T., & Almohamad, T.A. (2022). Adaptive Trust-Based Framework for Securing and Reducing Cost in Low-Cost 6LoWPAN Wireless Sensor Networks. *Applied Sciences*. 8605, https://doi.org/10.3390/app12178605

[18] G, M., A., A., R, R., K, K., & Clement Singh C., J. (2023). Trust And Energy-Aware Routing Protocol for Wireless Sensor Networks Based on Secure Routing. *International journal of electrical and computer engineering systems*.1015-1025, https://doi.org/10.32985/ijeces.14.9.6

[19] Roja, P., & Misbha, D. (2022). Lightweight Secure Key Distribution Protocol (LSKDP) for Wireless Sensor Networks. *ECS Transactions*. 107, https://doi.org/10.1149/10701.8239ecst

[20] Khan, T.A., Singh, K., Gupta, S., & Manjul, M. (2022). Multi Trust-based Secure Trust Model for WSNs. https://doi.org/10.21203/rs.3.rs-2566539/v1

[21] Nandal, V., & Dahiya, S. (2021). IoT Based Energy-Efficient Data Aggregation Wireless Sensor Network in Agriculture: A Review. 58(1): 2985-3007. https://doi.org/10.17762/pae.v58i1.1194

[22] Yuvaraja, M., Sureshkumar, S., James, S.J., Thillaikkarasi, S., & Castillo-González, D.W. (2024). An Energy-Efficient Cluster Head Selection and Secure Data Transmission in WSN using Spider Monkey Optimized Algorithm and Hybrid Cryptographic with Security. *Salud, Ciencia y Tecnología - Serie de Conferencias*.650, https://doi.org/10.56294/sctconf2024650

[23] Almansoori, M.N., Elshamy, A.A., & Mustafa, A.A. (2022). Secure Z-MAC Protocol as a Proposed Solution for Improving Security in WSNs. Inf., 13, 105. https://doi.org/10.3390/info13030105

[24] Hassan, K., Madkour, M., & Nouh, S.A. (2023). A REVIEW OF SECURITY CHALLENGES AND SOLUTIONS IN WIRELESS SENSOR NETWORKS. Journal of Al-Azhar University Engineering Sector. 10.21608/AUEJ.2023.217015.1380

[25] Ghosh, R., Mohanty, S., Pattnaik, P.K., & Pramanik, S. (2021). A Novel Approach Towards Selection of Role Model Cluster Head for Power Management in WSN. https://doi.org/10.4018/978-1-7998-3624-7.ch015

[26] Gudhekar, G.S., S. Ingle, A.K., & Guide (2021). Wsn-Based Smart Sensors and Actuator for Power Management in Intelligent Buildings. https://doi.org/10.1109/tmech.2014.2301716

[27] Nandini, G., & Srinivas, D.R. (2020). Power Management in Smart Buildings by Using Wsn and Iot. *Solid State Technology*, 4606-4618.

[28] Das, S. (2023). A Specific Power Management Protocol for Minimizing and Managing the Power Drain of the WSN. *World Conference on Communication & Computing* (WCONF), 1-6. https://doi.org/10.1109/wconf58270.2023.10235254

[29] Bengheni, A. (2024). Relay node selection scheme and deep sleep period for power management in energy-harvesting wireless sensor networks. *International Journal of Communication Systems*, 37. https://doi.org/10.1002/dac.5742