https://doi.org/10.48047/AFJBS.6.5.2024. 9549-9597

AfricanJournalofBiological Sciences

CTSR-DL: Cluster based trusted secure aware routing for WSN Assisted IoT using deep learning technique

[1]Abhishek Srivastava,[2] Dr. Rajeev Paulus
[1]Department of Electronic & Communication Engineering,
SHUATS, Prayag Raj, India.
abhishek200959@gmail.com
[2]Assistant Professor
Department of Electronic & Communication Engineering,
SHUATS, Prayag Raj, India.
rajeev.paulus@shiats.edu.in

Article History
Volume 6, Issue 5, 2024
Received: 22 May 2024
Accepted: 03Jun 2024
doi:*10.48047/AFJBS.6.5.2024. 9549-9597*

Abstract:
In this era of rapid technological progress, wireless technology has demonstrated immense potential, particularly in data transmission. One promising domain for harnessing the power of wireless technologies is traffic control. IoT (Internet of Things) has garnered significant attention, as it encourages devices to collaborate and share services and data. Wireless Sensor Networks (WSNs) play a crucial role within the IoT framework by facilitating data transmission. Routing, a fundamental strategy, involves establishing routes and transmitting data packets to destination from source within the networks. As IoT networks continue to expand, the challenge of maintaining security grows increasingly complex. Secure routing mechanisms must adapt to accommodate the growing number of devices and potential security threats. In this research, we introduce the concept of cluster-based trusted secure aware routing for WSN-Assisted IoT using a deep learning technique (CTSR-DL). Our approach involves the development of the enhanced chaos game optimization (ECGO) algorithm, which efficiently balances the load by clustering nodes within the network. The trust level of nodes is calculated using various metrics, including mobility, received signal strength (RSS), and congestion rate. Furthermore, we employ the convolutional neural network-bagged decision tree (CNN-BDT) for optimal path selection between sources and destinations. For assessing our proposed CTSR-DL approach performance, we conducted various simulation scenarios. The results clearly demonstrate the effectiveness of our approach when compared with existing routing methods.

Keywords: clustering, trust degree, secure routing, wireless sensor network, Inter of things (IoT), optimal path finder

1. Introduction

WSN consists of a multitude of spatially distributed sensor node, each equipped to collect data from its environment, which can range from temperature and humidity to motion and light [1]. These networks excel in applications where real-time data collection is imperative, providing the raw sensory information. IoT is a broader framework that interconnects everyday objects, devices, and systems to the internet [2]. It empowers these devices to become "smart" and capable of seamless communication with one another, central servers, and cloud platforms. The IoT transcends domains, finding applications in smart homes, smart cities, industrial automation, healthcare, and more [3]. WSN Assisted IoT creates a symbiotic relationship by integrating the sensing capabilities of WSNs into the broader IoT ecosystem. In this context, sensor nodes act as the vital data collection points within the IoT network. They communicate with each other and, in some cases, with other IoT devices or gateways [4]. These sensor nodes are pivotal in providing real-time, granular data. The information gathered by these sensor devices is subsequently transferred to centralized servers or cloud platforms where they undergo analysis and processing. The combined data is then made accessible to various IoT devices, including smartphones, computers, or actuators, enabling real-time monitoring, informed decision-making, and responsive actions based on changing environment [5][6]. WSN Assisted IoT is particularly impactful in applications where detailed, up-to-the-minute data is crucial. For instance, it is integral to environmental monitoring, where factors like air quality, temperature, and humidity require constant tracking. In smart agriculture, it ensures crops receive the optimal conditions for growth, and in industrial automation, it contributes to efficient and real-time control of manufacturing processes [7].

Secure routing in the WSN-IoT is of utmost significance for a multitude of critical reasons. First and foremost, it ensures the confidentiality of data transmitted within IoT networks [8][9]. Given that IoT devices frequently handle sensitive information, secure routing mechanisms

protect against unauthorized access, assuring that data remains confidential. Additionally, secure routing plays a pivotal role in safeguarding data integrity. It verifies that data collected from IoT devices remains accurate and unaltered during transmission, which is fundamental for reliable decision-making [10]. Authentication is another crucial aspect addressed by secure routing. It validates the identity of devices before granting them access to the network, thus preventing unauthorized entities from infiltrating or influencing the data flow. Furthermore, secure routing contributes to the availability of data. In IoT applications, it's imperative that data is accessible when needed. By protecting against various network attacks, secure routing ensures the continuous availability of data [11]. Energy efficiency is paramount in WSNs and IoT devices, many of which operate under resource constraints, particularly regarding energy. Secure routing protocols [12]-[15] are thoughtfully designed to minimize energy consumption while upholding a high standard of security. By expanding the operational lifecycle of IoT networks, this design decision effectively mitigates the need for frequent battery replacements. Defending against a spectrum of potential threats is a vital function of secure routing, encompassing protection against eavesdropping, denial-of-service attacks, and data injection attacks [16]. These mechanisms guarantee the network's continued operation and the protection of data. Compliance with legal and regulatory requirements is a necessity in various industries, and secure routing facilitates adherence to these stipulations, averting potential legal ramifications [17]. Privacy protection in applications involving personal information surveillance is paramount. As IoT networks expand, the complexity of maintaining security increases. Secure routing mechanisms scale effectively to accommodate the growing number of devices and address evolving threats [18], reflecting the dynamism inherent to IoT environments. The secure routing in WSN-IoT is instrumental in addressing security and privacy concerns, sustaining data integrity, and upholding the reliable operation of these networks [19][20]. It is a linchpin in fostering trust and confidence within the IoT ecosystem.

1. Our contributions

The proposed cluster-based trusted secure aware routing for WSN Assisted IoT, implemented through deep learning techniques and referred to as CTSR-DL, offers several noteworthy contributions to the field. These contributions can be summarized as follows:

1. Firstly, our approach introduces an enhanced chaos game optimization (ECGO) algorithm, specifically designed to achieve efficient load-balanced clustering within the network. This is a critical step in organizing the nodes within the network effectively, ensuring that data transmission and processing are optimized. Moreover, our approach goes beyond mere clustering; it calculates the trust level of nodes based on multiple design measures. These measures encompass factors such as node mobility, received signal strength (RSS), and congestion rate. This multi-faceted trust calculation is instrumental in enhancing the security and reliability of data transmission within the network.
2. Secondly, the convolutional neural network–bagged decision tree (CNN-BDT) is employed to determine the optimal path selection between the data source and destination. This is a crucial component in routing decisions, as it ensures that data is transmitted along the most efficient and reliable routes within the network. The use of deep learning, specifically CNN-BDT, enhances the accuracy of path selection and ultimately leads to improved network performance.
3. Finally, our approach is thoroughly validated through series of comprehensive simulation scenarios. These simulations evaluate the impact of nodes, including their positioning and behavior, on the network's performance. Additionally, we assess the network's resilience against various types of attacks. This validation process is crucial in demonstrating the

effectiveness of CTSR-DL approach under different real-world conditions and security threats.

1.3 Paper Organization

The paper's remaining sections are structured as follows: In Sect 2, the extensive survey of prior research in the domain of WSN-IoT networks is conducted. Section 3 outlines the primary research challenges and provides a detailed explanation of the proposed CTSR-DL approach, which includes novel algorithms. Moving on to Section 4, the CTSR-DL approach is subjected to experimental evaluation, and the obtained results are juxtaposed with findings from previous studies. Lastly, in Section 5, the paper draws conclusions and highlights the contributions made in this research endeavor.

2. Related Work

This section conducts a thorough survey of prior researches efforts focusing on security-aware routing within the WSN-IoT environment. Through this comprehensive review, we pinpoint the existing gaps in the body of research, thereby identifying areas that warrant further investigation.

2.1 State-of-art works on routing in WSN-IoT

Deebak et al. [21] have introduced a protocol for secure routing and monitoring within a global sensor network. They employ a Two-Fish (TF) symmetric key approach, which utilizes multi-variant tuples to detect and thwart potential adversaries in the network. Their approach is rooted in the ATE (Authentication and Encryption Model). By employing an EWF (eligibility weight function), the protocol identifies sensor guard node, which is further obscured through the application of a complex symmetric key mechanism. To enhance security and routing efficiency, the authors opt for a secure hybrid routing protocol, which amalgamates key features from both

the OLSR and AOMDV protocols. The outcome of this approach demonstrates notable increase in monitoring nodes when compared to other routing schemes, underscoring effectiveness in bolstering network security and reliability.

Ullah et al. [22] have introduced an innovative scheme that leverages FoG to aggregate healthcare data securely and efficiently. This technique allows for secure peer-to-peer communication between healthcare sensing equipment and wearables, allowing for the collection and transmission of sensitive data to a central hub. The information gathered by this node can then be sent on to a FoG server. An aggregator can share encrypted data with a neighboring aggregator if it is located too far from the FoG server to send data directly. The data is added to the dataset already being aggregated by the intermediary aggregator, and then sent on to the FoG server. In response, the FoG server determines what values are needed and stores them in a local repository that may be synced with cloud repositories at a later time. The results of this approach demonstrate noticeable improvements in various aspects, including storage efficiency, communication effectiveness, transmission ratios, energy conservation, and system resilience.

Path bridging is the basis for new cooperative multipath routing methods described by Kim et al. [23], which improve inter-path communication. Specific bridge nodes are responsible for tracking and storing data packets as they move around the network. These cached packets can be subsequently relayed in cases where transmission failures or delays occur along any one of the paths. The utilization of bridge nodes for inter-path communication effectively meets the requirements for packet delivery ratios and time constraints, while also contributing to reduced energy consumption. Notably, this approach optimizes the network by constructing a smaller number of paths, streamlining the communication process. Through comprehensive simulations, this scheme has demonstrated its ability to achieve lower energy consumption levels, low-delay packet delivery & high-reliability.

The goal of the energy-efficient geographic (EEG) routing protocol proposed by Hameed et al. [24] is to maximize network throughput while minimizing drain on sensor node power. The mean square error algorithm is used by the protocol to help with the difficulty of sensor localization, resulting in more accurate sensor location. By requiring nodes to just keep track of a single neighbor, the protocol significantly reduces routing overhead. This protocol's main success lies in its ability to close the energy gap between sensor nodes and the rest of the network. Extensive simulations show that compared to a leading state-of-the-art geographic routing protocol, this scheme significantly outperforms it in terms of energy management and packet delivery ratio.

The LSDAR (light-weight structure-based data aggregation routing) protocol was presented by Haseeb et al. [25]. With the goals of improving energy routing performance and securing node-level data from potential harmful attacks, this protocol was developed with IoT-WSN in mind. The protocol takes a clustering method, partitioning nodes into autonomous groups with different radiuses. Energy imbalances and potential "energy holes" close to the base station are efficiently mitigated by this method. The A-star heuristics algorithm quickly establishes routing pathways, ensuring reliable, resource-conserving data transfer with no transmission loops. A mathematically unbreakable one-time pad encryption algorithm is used to protect communication channels between nodes in the network from being exploited by malicious actors.

Coverage defects in the network can be minimized thanks to Jain's [26] coverage hole-healing algorithm (CHHA). The CHHA method is implemented to identify these coverage gaps, and it leverages the concept of virtual forces to determine the optimal movement of mobile sensor nodes. This movement is crucial in rectifying and healing the identified coverage holes. The process initiates with clustering using the k-means clustering technique, followed by the selection of the coverage hole with careful consideration of several critical network constraints. They employ the MO-EPO (multi-objective emperor penguin optimization) algorithm to select the

most favorable routing paths. The outcome of this comprehensive approach is a noteworthy improvement in terms of accuracy, energy efficiency, network longevity, a higher number of active nodes, and an increased packet delivery ratio.

An energy-efficient routing protocol for WSN-based IoT has been suggested by Tan et al. [27]. The protocol then chooses a CHN based on a number of factors, including the energy left over after each round and the distance between the sink and the nodes in each cell. The protocol uses the Kruskal method to create a minimum spanning tree (MST) between nodes and their corresponding CHNs in order to establish effective data delivery channels within each cell while consuming as little energy as possible. To further lessen the load on the network's power supply, an ant colony algorithm is used to plot the most efficient routes for sending data packets from the CHNs to the centralized sink. The importance of effective data routing for enhanced network sustainability is shown by this energy-efficient protocol's contribution to the continued operation of WSN-based IoT.

To extend the life of IoT-WSN systems used for forest fire warning, Pedditi et al. [28] have suggested an energy-efficient routing protocol (EERP). To further conserve energy and network resources, EERP only permits sensor nodes in close proximity to an event to report the event. The protocol also includes a technique to prevent low-power sensor nodes from being appointed as cluster chiefs, extending their useful lifetime. When transmitting data, EERP uses many hops between the source nodes and the Base Station. The performance of the protocol is measured against that of comparable MAC protocols in a number of different settings. The findings underline the value and use of EERP in extending the life of Internet of Things (IoT)-based wireless sensor network (WSN) systems used to detect forest fires.

The meta-heuristic-based secure and energy-efficient routing (MHSEER) protocol was developed specifically for WSN-IIoT by Sharma et al. [29]. To protect sensitive information during transmission, the MHSEER protocol uses counter-encryption mode (CEM) encryption. The

protocol makes use of meta-heuristics to promote trustworthy knowledge acquisition and choice making. In addition to using CEM, which is both computationally easy and random, we employ a heuristics method to improve data routing for dependability and security. The results of the MHSEER protocol are promising, with a throughput improvement of 95.81% and decreases of 5.12% in packet drop ratio, 0.10 ms in packet delay, 0.0102 mJ in energy usage, and 6.51% in faulty paths.

For efficient data distribution in hierarchically structured IoT-WSNs, Altowaijri [30] presents the efficient multi-hop routing protocol (EMRP). By considering the query area, EMRP enables coordinated query distribution and data aggregation across all participating nodes. However, there are certain difficulties with this strategy. It causes batteries to die out and nodes to become inoperable more quickly, which might be a problem if the node in question has recently acquired or received crucial data. Also, when enormous amounts of data are being transferred from the real world to cyberspace, this method can cause a sensory bottleneck in both worlds.

2.2 Research problem

The amalgamation of WSN-IoT greatly enhances the capabilities of IoT by facilitating efficient and dependable data collection, optimizing energy efficiency, and enabling real-time monitoring. This synergy makes WSN-IoT a robust and versatile solution with applications spanning diverse domains, including smart cities, agriculture, healthcare, and industrial automation. In prior work [31], we explored the use of multi-objective optimization to develop a cluster-based routing strategy for WSN-IoT that takes into account both energy and lifetime constraints. To ensure overall energy efficiency inside the WSN-IoT system, we developed a routing strategy called Energy and Lifetime Aware Cluster (ELR-C) that uses the Multi-Objective Chaotic Slime Mold (MCSM) algorithm to achieve optimal clustering. Using trust-degree assessments as a guide, we

used different design metrics to determine which nodes in a cluster would serve as Cluster Heads (CH). The Improved Butterfly Optimization (IBO) technique was used to achieve this optimization for these metrics. For multi-hop routing between CHs and sink nodes, we integrated a Cat Hunting algorithm with a feed-forward neural network (CH-FFNN) to further improve energy efficiency and network longevity. An appropriate secure deep learning (SecDL) strategy for dynamic cluster-based WSN-IoT has been proposed by Sujanthi et al. [32]. This method, based on a network structure of Bi-concentric hexagons and enhanced by movable sink technology, was developed to maximize energy efficiency. Within the Bi-Hex network, dynamic clusters were established, and ideal CHs were picked by the quality prediction phenomenon (QP2), guaranteeing both QoS and energy efficiency. Within each cluster, data aggregation was enabled and maintained with a method of data reduction and removal that worked in both directions. Using OT-PRESENT cryptography, we were able to provide the highest level of safety for the combined data. The ciphertext was sent to the mobile sink via the most efficient path, guaranteeing excellent quality of service. Safeguarding the sensing data from illegal access by IoT users necessitated the selection of the ideal route to IoT-user security, which was facilitated by a well-fitted deep neural network known as Co-Futon.

The literature review reveals several notable research gaps, underscoring the critical importance of prioritizing security within the WSN-IoT. The sensitivity of the data processed and transmitted within WSN-IoT is not overstated. It encompasses personal information, industrial data, and environmental data, necessitating the utmost for maintaining data confidentiality, integrity, and availability to safeguard individuals, organizations, and critical infrastructure. The rapid proliferation of IoT devices introduces an equally rapid increase in potential vulnerabilities, making security measures a paramount concern. WSNs-IoT devices often operate in uncontrolled or hostile environments, compounding their susceptibility to physical and cyber attacks. This vulnerability is further accentuated by the distributed and wireless nature of these networks.

Furthermore, the diverse landscape of IoT applications, including industrial automation, healthcare and smart cities necessitates adaptable and industry-standard compliant security measures. Resource constraints within many IoT devices, characterized by limited processing power, memory, and energy resources, pose a formidable challenge. Ensuring robust security within these resource-constrained environments is vital to avert exploitation. Data privacy is emerging as a critical issue, particularly in IoT applications tracking user behaviors and preferences.

Security breaches not only have economic ramifications, including revenue loss and data breach costs, but also harm an organization's reputation. In critical infrastructure and military sectors, the security of IoT and WSNs holds direct national security implications, necessitating a robust defense against cyber attacks. The constantly evolving threat landscape introduces novel vulnerabilities and attack techniques regularly, demanding ongoing security efforts, updates, and proactive countermeasures. Given these multifaceted considerations, an unwavering focus on security in the realm of WSN-IoT is indispensable to protect individuals, organizations, and the integrity and functionality of IoT-WSN systems. The challenge lies in simultaneously achieving Quality of Service (QoS), security provisioning, and energy efficiency, as these objectives are often at odds with each other due to issues such as high time complexity, energy consumption, and suboptimal algorithm design. Consequently, the design of a trusted secure aware routing solution for the WSN-IoT becomes crucial imperative. To tackle the aforementioned challenges, we present a novel solution called the cluster-based trusted secure aware routing approach for WSN-IoT utilizing deep learning technique (CTSR-DL). Our proposed CTSR-DL approach is guided by the following key objectives:

- Our primary goal is to devise a cluster-based routing strategy that guarantees the QoS (Quality of Service) for data transmission in the WSN-IoT environment.

- We aim to calculate the trust degree for each node based on crucial design constraints, a critical step to ensure efficient data aggregation within the network.
- We leverage deep learning techniques to develop an optimal path finder. This path finder is instrumental in computing the best and most secure routing path, bolstering the security of data transmission.

These objectives collectively form the foundation of our CTSR-DL approach. It aims to improve the reliability, security and efficiency of data transmission in WSN-IoT settings.

3. Proposed methodology

Fig.1 shows the network model of our proposed CTSR-DL approach, which involves a series of essential processes, including cluster formation, trust degree computation, and optimal path selection. In this network model, we consider a configuration consisting of a total of 'n' IoT sensor nodes, a base station (BS), and a computing system for data analysis. The sensor nodes are dispersed at will over the network, with only the base station (BS) remaining in one location. To begin, we initiate the clustering of each node within the WSN-IoT environment, and this is accomplished using an enhanced chaos game optimization (ECGO) algorithm. This clustering is essential for organizing and optimizing the data flow within the network. The trustworthiness of each node is a critical factor in securing the network. To ascertain trust levels, various metrics are employed, including mobility, RSS, and congestion rate. These metrics collectively help in evaluating the reliability and credibility of each node in the network. Energy consumption in routing processes can vary, particularly when different routing paths, both small and large, are utilized. It's essential to consider this variability and optimize energy efficiency in routing processes. Within this system model, we introduce a hierarchy-based energy-efficient routing approach, where highly trusted nodes act as collector nodes responsible for receiving data from

member nodes. This hierarchy helps in efficiently aggregating data from various sources in the network.

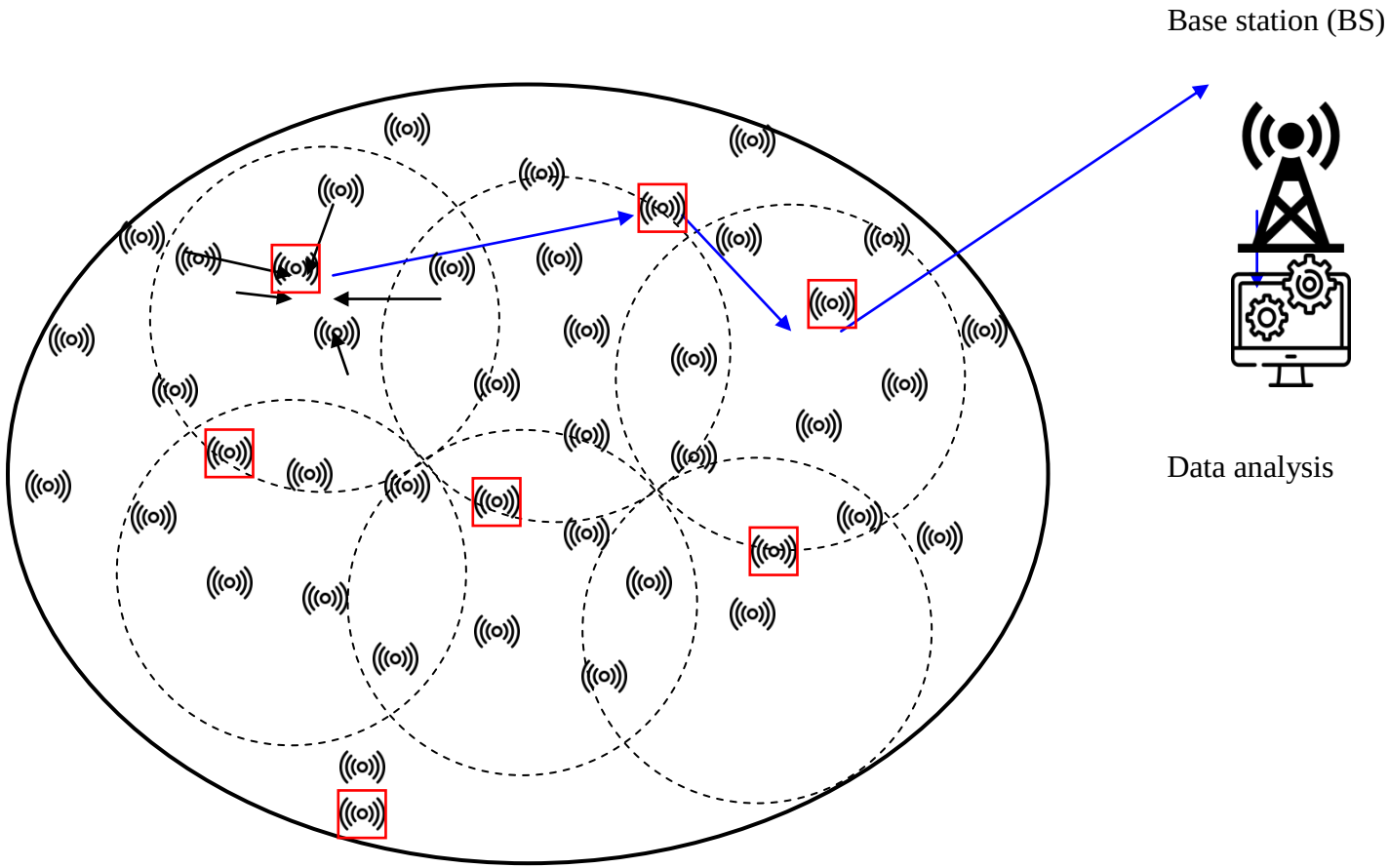

Fig. 1 Overall network design of proposed CNN-BDT approach

We implement the convolutional neural network-bagged decision tree (CNN-BDT) in path selection optimally between the source and destination nodes. This selection process ensures that data is routed along the efficient and secure path, further enhancing network performance. Additionally, the model takes into account a number of nodes that have reached the end of their operational life, as shown in Fig. 1. These "expired" nodes play a role in energy management within the network. As nodes continue to transmit and receive data packets at various distances, their energy levels decrease at varying rates over time, which can impact network longevity and efficiency.

3.1 Clustering using enhanced chaos game optimization (ECGO) algorithm

Cluster formation, as implemented in the CTSR-DL approach, is a fundamental process for structuring and optimizing the flow of data within the WSN-IoT environment. Initially, all IoT sensor nodes are treated as a single unstructured group, dispersed randomly over the network. Objective of cluster formation is to create a more organized and efficient network architecture. To achieve this, the enhanced chaos game optimization (ECGO) algorithm is employed. ECGO excels in identifying nodes that are in close spatial proximity and well-suited for forming clusters. It takes into account factors such as communication patterns, spatial relationships, and trust levels of nodes. One of the primary goals of cluster formation is load balancing. ECGO ensures that the load is evenly distributed among clusters, preventing any single cluster from becoming overwhelmed with data transmission and processing tasks. The ECGO algorithm is a nature-inspired optimization technique that draws its inspiration from the chaotic behavior of certain dynamic systems. It is a variant of the chaos game optimization (CGO) algorithm, enhanced to improve its performance and convergence speed. ECGO is primarily used for solving optimization problems, particularly those involving search and exploration in multi-dimensional

solution spaces. By iteratively updating the candidate points using chaotic maps, the algorithm can converge towards the actual boundary with a high level of precision. Each decision candidate (S_u) in the ECGO algorithm is made up of decision variables (s_j^u), which indicate where these suitable seeds are in the search space. These aspects can be represented mathematically as follows:

$$S = \begin{bmatrix} S_1 \\ S_2 \\ ? \\ S_u \\ ? \\ S_w \end{bmatrix} = \begin{bmatrix} s_1^1 & s_1^2 & ? & s_1^l & ? & s_1^F \\ s_2^1 & s_2^2 & ? & s_2^l & ? & s_2^F \\ ? & ? & ? & ? & ? & ? \\ s_u^1 & s_u^2 & ? & s_u^l & ? & s_h^f \\ ? & ? & ? & ? & ? & ? \\ s_o^1 & s_o^2 & ? & s_o^j & ? & s_o^f \end{bmatrix}, \begin{cases} i = 1,2,....O. \\ i = 1,2,....F. \end{cases} \quad (1)$$

where d is the seed's dimension and W is the number of suitable seeds in the search space. These suitable seeds' initial positions in the search space are chosen at random:

$$s_u^j(0) = s_{u,Min}^j + Rand.\left(s_{u,Max}^j - s_{u,Min}^l\right) \begin{cases} u = 1,2,....O. \\ h = 1,2,....F. \end{cases} \quad (2)$$

where $s_U^j(0)$ determines the eligible seeds' initial position; $s_{U,Min}^j$ and $s_{u,Max}^j$ are the u-th decision candidate's L-th decision variable's minimum and maximum allowable values; The random number rand falls within the range [0,1]. The following is the mathematical representation of this process:

$$seed_u^1 = S_U + \varepsilon_U \times (\chi_U \times GU - \gamma_U \times OG_U), \quad U = 1,2,...,O \quad (3)$$

where S_U is a potential U-th solution, GU is the global best that has been found so far, and OG_U is the mean values of a few selected seeds that are eligible. ε_U is the factorial that is

generated at random for the purpose of modeling the seeds' movement limitations while each of the χ_U and γ_U represent a 0 or 1 random number to simulate the possibility of rolling a die.

$$seed_U^2 = GU + \varepsilon_U \times (\chi_U \times -S_U - \gamma_U \times OG_U), \;\; U = 1,2,...,O \tag{4}$$

where ε_U is a factorial that is generated at random to model restrictions on seed movement when each of χ_U and γ_U represents a 0 or 1 random number to resemble the rolling of a die. The ECGO approach is then presented and analyzed for solving time-varying linear inequalities in the following subsections.

$$\underset{n(a)\in e^u}{Min}\, D(N(A), A) \in T, \;\; A \in [0, +\infty) \tag{5}$$

We define the gradient of a solution in order to get it online.

$$G(N(A), A) = \partial D(N(A),\ A) / \partial N(A) \tag{6}$$

which is unquestionably a nonlinear mapping function that can be distinguished from $\partial D(N^*(A)$. In addition, the time-varying set of capture points is defined as.

$$\Omega^*(A) = \{(A, n^*(A)) \,|\, \partial D(N^*(A), A) / \partial N^*(A) = 0\} \tag{7}$$

for time instant r ∈ [0, +∞). The first seed's described additional parameters are included. This look is created with the help of a random integer generator function that selects between blue and green faces by generating just two integers, 0 and 1. It is important to note that the seed has the ability to move in the direction of the connected lines the S_u and the HU, as well. Some random factorials are also utilized to fulfill this aim, as:

$$seed_U^3 = OG_U + \varepsilon_U \times (\varepsilon_U \times -A_U - \gamma_U \times GU), \;\; U = 1,2,...,O \tag{8}$$

Another method is utilized to generate the fourth seed in order to incorporate the mutation phase into the positional updates of the appropriate seeds in the search space. Changes in the decision variables chosen at random serve as the basis for any revisions to this initial position.

$$seed_U^4 = S_U(S_U^h = S_U^h + e), \quad l = [1,2,....,F] \tag{9}$$

where Here, J is some irrational number between [1,f] and E is a uniformly distributed random number. in the range [0, 1]. Four distinct formulas that control the restrictions on seed movement are presented in order to control and adjust the speed of exploration and utilization of the ECGO algorithm.

$$\varepsilon_U = \begin{cases} rand \\ 2 \times rand \\ (\gamma \times rand) + 1 \\ (\eta \times rand) + (\sim \eta) \end{cases} \tag{10}$$

where is a random integer with a uniform distribution in the [0,1] interval, and random numbers. Algorithm 1 shows the working steps involved in the cluster formation.

Algorithm 1 Cluster formation using ECGO

Input	: Node position, location and number of population
Output	: Cluster formation
1	Initialization parameters
2	Compute the search space $a_I^k(0) = a_{I,Min}^k + Rand.(a_{I,Max}^k - a_{I,Min}^K) \begin{cases} i = 1,2,....P. \\ i = 1,2,....D. \end{cases}$
3	If a=0, and b=1

4 Define its gradient for each fitness $H(M(S),S) = \partial F(M(S), S)/\partial M(S)$

5 While Do

6 Define time-varying set $\Omega^*(S) = \{(S, m^*(S)) \mid \partial F(M^*(S), S)/\partial M^*(S) = 0\}$

7 Compute movement limitations of the seeds $\alpha_I = \begin{cases} rand \\ 2 \times rand \\ (\delta \times rand) + 1 \\ (\varepsilon \times rand) + (\sim \varepsilon) \end{cases}$

8 Find the best output solution

9 End if

10 End

Trust degree computation is used to evaluate the reliability and trustworthiness of individual network nodes. The trust degree is a measure that reflects a node's ability to efficiently perform network-related tasks while adhering to specific criteria. This computation is carried out by assessing various metrics and data gathered from the network. These metrics often encompass factors like mobility, which gauges how frequently a node changes location, Received Signal Strength (RSS) to assess communication link quality, and congestion rate to measure the extent of network traffic congestion. Once these metrics are collected and analyzed, a trust computation algorithm is employed to calculate the trust degree for each node. This algorithm assigns scores or values to nodes based on their performance in these metrics. The result is a measure of the trustworthiness of each node, allowing the network to identify which nodes are the most reliable

and dependable. In a network, the node with the highest trust degree is the most reliable one, signifying its superior reliability and performance. This node plays a critical role within the network, such as being selected as the cluster head in cluster-based network architectures. Cluster heads are central to tasks like coordinating data aggregation, routing, and security management within the cluster. The highest trusted node may also handle data aggregation, security management, and serve as a reliable backup in case of node failures.

3.2 Optimal path finder using convolutional neural network-bagged decision tree (CNN-BDT)

In the CTSR-DL approach, the optimal path finder employs deep learning techniques to make this determination. When it comes to analyzing and processing data, deep learning is a subfield of machine learning that makes use of neural networks with numerous layers. These neural networks can analyze enormous datasets to learn complicated patterns and draw accurate conclusions. A dataset containing the network's structure, historical data on node behavior, and numerous network metrics is used to train the deep learning model. This training allows the model to learn the relationships between different factors that influence path selection. Once the deep learning model is trained, it can evaluate potential routes within the network based on specific objectives. These objectives may include minimizing energy consumption, network lifetime, ensuring secure data transmission, or optimizing QoS. The optimal path finder also focuses on security aspects, ensuring that the chosen path is resistant to potential threats or attacks. The deep learning model can adapt to changing network conditions and requirements. It can dynamically select the best path based on real-time data, making it suitable for dynamic and evolving network like WSN-IoT. The convolutional neural network-bagged decision tree (CNN-BDT) is a hybrid machine learning model that combines elements of both CNNs and BDTs to improve the accuracy &

efficiency of classification & prediction tasks. CNNs are a class of deep neural networks commonly used for data and signal processing tasks. They are particularly well-suited for tasks that involve analyzing grid-like data. CNNs use a hierarchical model to process data through multiple layers of convolutional and pooling operations. These layers automatically learn relevant features from the input data, making them powerful for tasks like data recognition. BDT often referred to as ensemble learning, involve combining multiple decision tree models for improving overall predictive performance. The data used to train each decision tree variesl and the results are aggregated to produce a more accurate and robust model. Bagging helps reduce overfitting and increases the model's generalization ability. The combination of CNNs and BDTs, as in CNN-BDT, leverages the strengths of both approaches. In practical terms, it may involve using a CNN for feature extraction and encoding, followed by a bagging ensemble of decision trees for classification or prediction. We call the class variable C and its values (d1,..., dj). With Bagging, m different classifiers are created. Each one is provided with a replicated training set based on bootstrapping: A total of N instances are picked at random with replacement. Although BDT is the most common classification algorithm used in the Bagging scheme, there are many more. When a new instance needs to be categorized, the number of classifiers that predict a particular class value for the instance, also known as the number of votes, is tallied for each possible state of the class variable. The most popular choice among voters will be the one used to represent the occurrence. Consider the dataset C to contain Q examples. We pretend that A is an attribute, and that the values for it are a1, a2, etc. The CNN-BDT predicts that there is a good chance that the variable A will take the value $1 \leq i \leq t$

$$i_I = \left\{ \left[\frac{q(a_I)}{Q+t}, \frac{q(a_I)+t}{Q+t} \right] \right\} \tag{11}$$

where n(xi) is the number of data points where X = xi, i = 1, 2, •••,t, and s > 0 for a specific model hyperparameter. We demonstrated that the intervals defined by the CNN-BDT are also expressible in terms of a belief function, and that the entire set of probability intervals is within reach. The resulting fitness set is based on the given intervals.

$$J^{C}(A)=\left\{m\mid\sum_{I=1}^{s}m(a_{I})=1,\frac{q(a_{I})}{Q+t}\leq m(a_{I})\leq\frac{q(a_{I})+t}{Q+t}\right\} \tag{12}$$

The choice of the hyperparameter s is an intriguing open problem. It's obvious that the gaps get bigger as s gets bigger. As new information becomes available, the convergence of the lower and upper probability is affected by the s hyperparameter. Let's pretend c1,.., ck are the values of a class variable called C. Let X be a variable with the range [x1,..., xt]. Let's call the optimal set for the class variable in partition D KD(C).

$$J^{C}(D)=\left\{m\mid\sum_{I=1}^{s}m(d_{I})=1,\frac{q(d_{I})}{Q+t}\leq m(d_{I})\leq\frac{q(d_{I})+t}{Q+t}\right\} \tag{13}$$

The greatest Shannon Entropy in this fitness set is taken into account by the ICDT split criterion:

$$H^{*}(J^{C}(d))=MAX\{G(m)\mid m\in J^{C}(d)\} \tag{14}$$

Where the Shannon entropy is H^{*}, as stated by Shannon (1948):

$$G(m)=-\sum_{I=1}^{j}m(d_{j})\log\ m(d_{j}) \tag{15}$$

It is the algorithm that maximizes that obtains the probability distribution. The discounted accuracy measure (DACC) is an attempt at a worldwide assessment of a less-than-perfect classifier.

$$dacc=\frac{1}{Q_{test}}\sum_{I=1}^{Q_{test}}\frac{(corrrect)_{I}}{|u_{I}|} \tag{16}$$

If the prediction for an instance is right, MIC adds a value which depends on $|u_I|$. where N Test is the size of the test set, $|u_I|$is the set of non-dominated states for the ith instance, and (correct)i is one if the true class value is in $|u_I|$and zero otherwise. MIC increases a value based on if the prediction for an instance is accurate.

When an instance is incorrectly classified, since it is supposed the same degree of importance for all the errors in this work, MIC adds a constant value, dependent on k. A CNN is a class of neural networks that specializes in processing data that has a grid-like topology. We assume an input $w \times g$, data size, $1 \in \mathrm{R}^{w \times g}$, represented as follows.

$$l = \left\{ b(p,q) \,|\, 1 \le p \le W, 1 \le Q \le H \right\} \tag{17}$$

when $b(p,q)$ is the data length with p, q spaces and given the $w_K \times g_K$ filters, using the filter J as the convolution, we get a feature map, Y, from the input data, l by stride T_K , and a zero padding value are used to slide the filter J over the data, l. The following is a definition of the discrete convolution.

$$(l \otimes J)_{p,q} = \sum_{u=-w_K}^{w_K} \sum_{v=-g_K}^{g_K} J_{u,v} I_{p+u,i+v} \tag{18}$$

For a given feature map, the input will be subjected to a convolution operation and an additive bias in each convolutional layer labeled with the number *l*.

$$F \in \{1,..., F(l)\}$$

So the output, $a_k^{(l)}$, of the j-th layer for the j-th feature map, is derived from the output of the previous layer, $a_k^{(l)}$, by:

$$a_k^{(l)} = \phi\left(a_k^{(l)} + \sum_{i=1}^{F^{(l-1)}} j_{j,i}^{(l)} * b_j^{(l-1)} \right) \tag{19}$$

The activation function F is the ReLU (rectified linear unit). To train our model, we used the Atadelta optimizer with the cross-entropy loss (CEL) function. When the training set is imbalanced, this feature comes in handy. Here we specify a loss function in terms of horizontal entropy as follows.

$$CEL(y, class) = -\log\left(\frac{\exp(y[class])}{\sum_{j=1}^{K} \exp(y[i])} \right) \tag{20}$$

If y is the input vector and class is the correct label, and the predicted value for labeling the sample thumbnail as i is denoted by y[j]. The cross entropy measures how far off the target distribution is from the one that was expected. Algorithm 2 explains how the optimal path finder with the CNN-BDT method operates.

Algorithm 2 Optimal path finder using CNN-BDT

Input : Number of paths, Number of route requests, threshold condition

Output : Optimal path

1. Get the population started at random
2. Estimate the initial fitness $i_I = \left\{ \left[\frac{q(a_I)}{Q+t}, \frac{q(a_I)+t}{Q+t} \right] \right\}$
3. If i=0 , j=1

4. While **Do**

5. Compute global fitness $$dacc = \frac{1}{Q_{test}} \sum_{I=1}^{Q_{test}} \frac{(corrrect)_I}{|u_I|}$$

6 Define the Shannon entropy $$G(m) = -\sum_{I=1}^{j} m(d_j) \log\, m(d_j)$$

7. If not discard **then**

8. Compute horizontal entropy loss function

$$CEL(y, class) = -\log\left(\frac{\exp(y[class])}{\sum_{j=1}^{K} \exp(y[i])}\right)$$

9. Update the tree values

10. The classes are evaluated for accuracy,

11. End

---

4. Results and Discussion

Various simulation scenarios are used to evaluate the proposed CTSR-DL. This segment provides an overview of the simulation setting before moving on to some quick comparisons. Network Simulator 3.26 (ns-3.26) is used to simulate the proposed CTSR-DL method. Supporting several kinds of network simulations, ns-3.26 is an event-based simulation tool. To begin, ns-3.26 is loaded onto an Ubuntu 14.04-based desktop. The network settings are then adjusted to match our findings. The algorithms are built in C++ and then run with Python as an auxiliary language. Through this comparison, we are able to verify CTSR-DL's efficacy. Energy usage, throughput,

delay, network lifetime, and delivery ratio are just few of the metrics used to assess the proposed CTSR-DL method. Existing routing approaches like SecDL [32], CNN [33], QoS routing [34], LEACH-CH [35], OTP [36], and Secure WSN-IoT [37] are compared to the observed results.

4.1 Simulation setup

Table 1 outlines the key simulation parameters employed in the research related to the CTSR-DL. These parameters are essential for defining the characteristics and conditions of the simulated network environment, which serves as the backdrop for evaluating the performance and behavior of the CTSR-DL approach. The simulation area is 1000×1000 m^2, representing the spatial extent of the simulated network. The network type specifies that the network operates on WiFi technology, particularly following the IEEE 802.11 standards frequently used for wireless local area networks (WiFi). The network size might vary from fifty to two hundred and fifty nodes. This range accounts for different node densities, allowing researchers to analyze network behavior under varying conditions. There's one base station (BS) within the network, serving as the central point for data aggregation and communication. Each node in the simulation starts with an initial energy level of 750 J, reflecting the available energy resources for the IoT sensor nodes. Node mobility is captured by the mobility model, described as random way, implying that nodes move unpredictably within the simulation area. The node speed is set 10m/s, representing the average node velocity. The CSI Interval is defined at 10ms, indicating how frequently the network updates information regarding the state of communication channels, critical aspect of adaptive routing. The channel bandwidth is set at 20MHz, which defines the available wireless communication bandwidth, influencing data transmission rates and capacity. Data transmission speed is set at data rate of 54 megabits per second. The size of data packets exchanged between nodes is packet size, with packets containing 1024 bits of information. The simulation duration,

simulation time 100s, establishing the observation and evaluation period for studying network behavior and performance under different settings. To assess and validate the security of both proposed and existing routing approaches, a comprehensive set of security evaluations should be conducted. This includes testing the network's resilience against various types of attacks, such as DDoS (Distributed Denial of Service), DoS(Denial of Service), Sybil, and rogue node attacks. Each of these attacks represents a different threat vector that the network may encounter.

Table 2 Simulation parameters

Parameters	Value
Simulation areas	1000×1000 m^2
Network type	WiFi
Number of node	50-250
Number of BS	1
Initial energy of nodes	750 J
Mobility model	Random way
Node speed	10 m/s
CSI interval	10 ms
Channel bandwidth	20 MHz
Data rate	54 Mbps

Packet size	1024 bits
Number of attacks	5-25
Type of attacks	DoS, DDoS, Sybil and rogue node
Simulation time	100 s

4.2 Impact of node density

Table 2 shows the results of a comparison between the proposed routing method and the current method, for a range of network densities. Comparison of energy usage between the proposed CTSR-DL routing system and other current approaches for networks with 50-250 nodes is shown in Fig. 2. When we examine the energy consumption results, it becomes evident that CTSR-DL consistently outperforms the existing methods, showcasing significant energy savings. In comparison to the Secure WSN-IoT, which serves as reference point, CTSR-DL demonstrates a remarkable enhancement in energy consumption, varying from approximately 9.2% to 16.6% as the number of nodes increases. This improvement in energy efficiency is particularly notable when compared to conventional approaches like LEACH-CH, OTP, QoS routing, and CNN. In fact, with the highest node count of 250, CTSR-DL exhibits energy savings of approximately 37.5% to 50.1% in comparison to these methods.

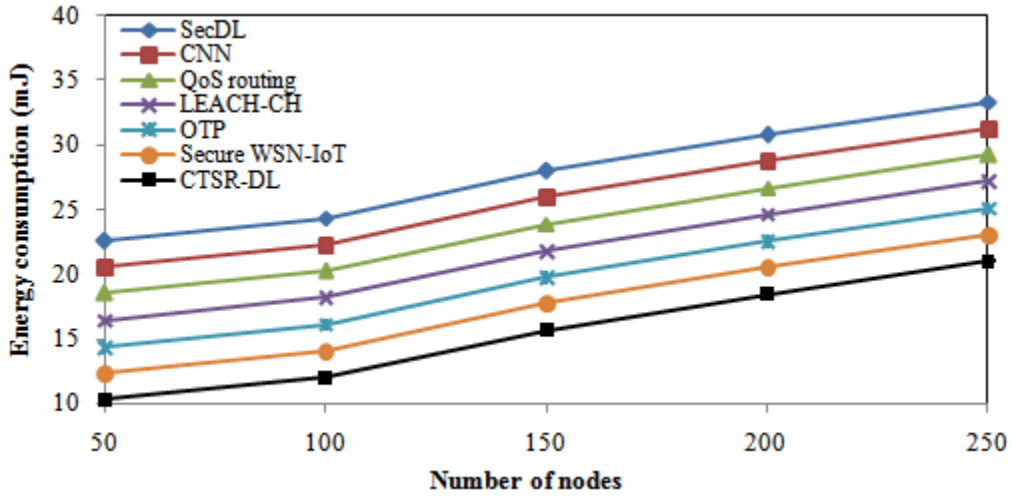

Fig. 2 Energy consumption with number of nodes

In Fig. 3, we examine the throughput comparison between the proposed CTSR-DL routing approach and several existing methods, considering different numbers of nodes within the network, ranging from 50 to 250 nodes. The results reveal several noteworthy trends. First, when we consider the performance of CTSR-DL, it consistently outperforms the existing methods across all node counts. This improvement is especially evident when compared to Secure WSN-IoT, which acts as a benchmark. The CTSR-DL approach exhibits a consistent enhancement in throughput, ranging from approximately 4.5% to 7.7%, as the no. of nodes increase. Furthermore, when we compare CTSR-DL to other existing methods like LEACH-CH, OTP, QoS routing, and CNN, the advantages of CTSR-DL become even more pronounced. With the highest node count of 250, CTSR-DL demonstrates a remarkable improvement in throughput, varying from around 9.6% to 19.8%, compared to these conventional methods. This emphasizes the potential of CTSR-DL to significantly enhance data throughput and, by extension, the overall network performance.

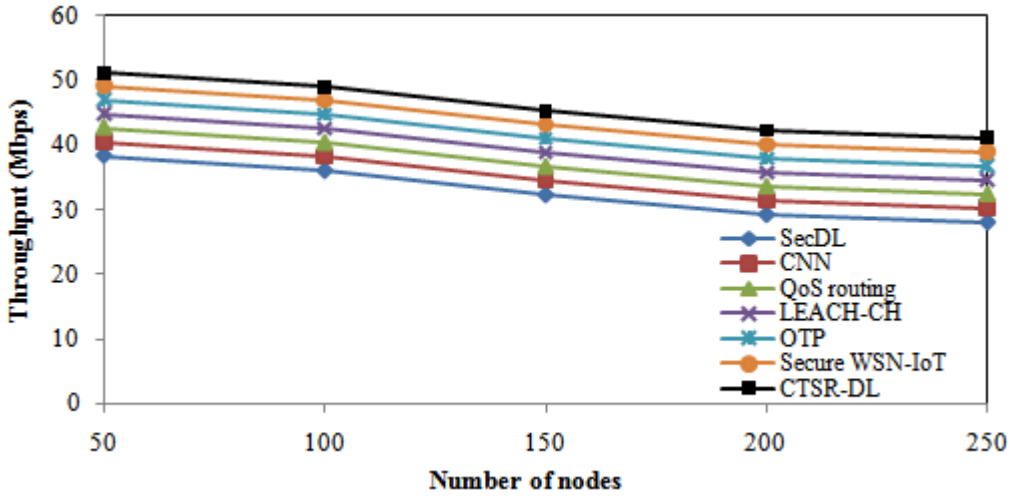

Fig. 3 Throughput with no. of nodes

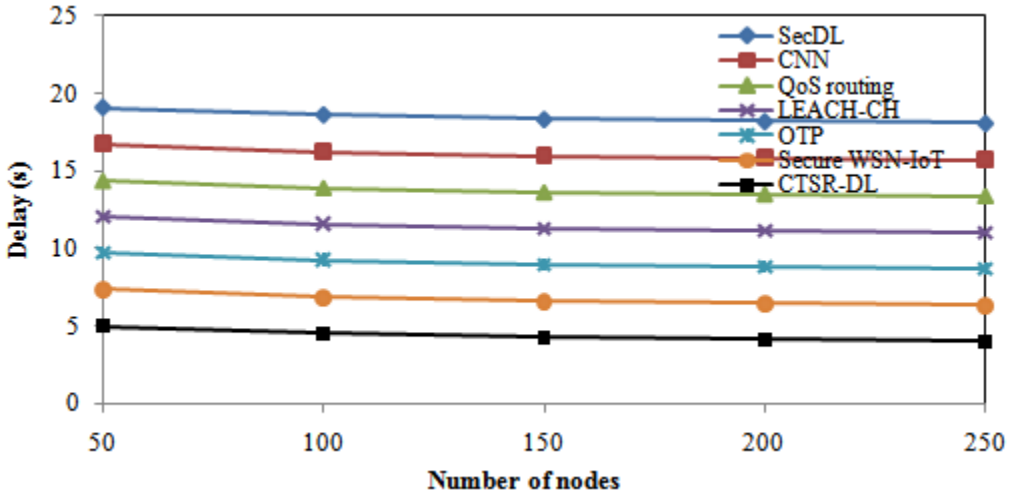

Fig. 4 Delay with no. of nodes

Table 2 Comparison of existing and proposed routing approach with impact of nodes

Routing approach	50	100	150	200	250	50	100	150	200	250	50	100	150	200	250
	Energy consumption (mJ)					Throughput (Mbps)					Delay (s)				
SecDL	22.625	24.362	28.015	30.814	33.359	38.344	36.011	32.282	29.235	28.075	19.081	18.618	18.327	18.198	18.078
CNN	20.569	22.306	25.959	28.758	31.303	40.503	38.170	34.441	31.394	30.234	16.732	16.270	15.979	15.849	15.729
QoS routing	18.513	20.250	23.903	26.702	29.247	42.662	40.329	36.600	33.553	32.393	14.384	13.921	13.630	13.500	13.380
LEACH-CH	16.457	18.194	21.847	24.646	27.191	44.821	42.488	38.759	35.712	34.552	12.035	11.572	11.281	11.152	11.032
OTP	14.401	16.138	19.791	22.590	25.135	46.980	44.647	40.918	37.871	36.711	9.686	9.223	8.932	8.803	8.683
Secure WSN-IoT	12.345	14.082	17.735	20.534	23.079	49.139	46.806	43.077	40.030	38.870	7.338	6.875	6.584	6.454	6.334

CTSR-DL	10.289	12.026	15.679	18.478	21.023	51.298	48.965	45.236	42.189	41.029	4.989	4.526	4.235	4.106	3.986

	Network lifetime (%)					Delivery ratio (%)				
SecDL	76.018	72.101	68.324	67.765	63.008	83.561	80.901	78.813	76.032	72.836
CNN	79.707	75.790	72.013	71.454	66.697	85.950	83.290	81.202	78.421	75.225
QoS routing	83.396	79.479	75.702	75.143	70.386	88.339	85.679	83.591	80.810	77.614
LEACH-CH	87.085	83.168	79.391	78.832	74.075	90.728	88.068	85.980	83.199	80.003
OTP	90.774	86.857	83.080	82.521	77.764	93.117	90.457	88.369	85.588	82.392
Secure WSN-IoT	94.463	90.546	86.769	86.210	81.453	95.506	92.846	90.758	87.977	84.781
CTSR-DL	98.152	94.235	90.458	89.899	85.142	97.895	95.235	93.147	90.366	87.170

In Fig. 4, we examine the delay comparison between the proposed CTSR-DL routing approach and various existing methods, while considering different no. of nodes in the network, ranging from 50 to 250 nodes. The CTSR-DL approach demonstrates a consistent % decrease in delay, ranging from approximately 45.8% to 51.8%, as the no. of nodes in the network increase. This signifies its capability to significantly reduce data transmission delay, even in scenarios with a substantial number of nodes, a critical factor for real-world applications. When we make a comparative analysis of CTSR-DL with other existing methods like LEACH-CH, OTP, QoS routing, and CNN, the advantages of CTSR-DL become even more pronounced. For the largest node count of 250, CTSR-DL showcases an impressive enhancement in delay, varying from around 39.5% to 47.6% when compared to these conventional methods.

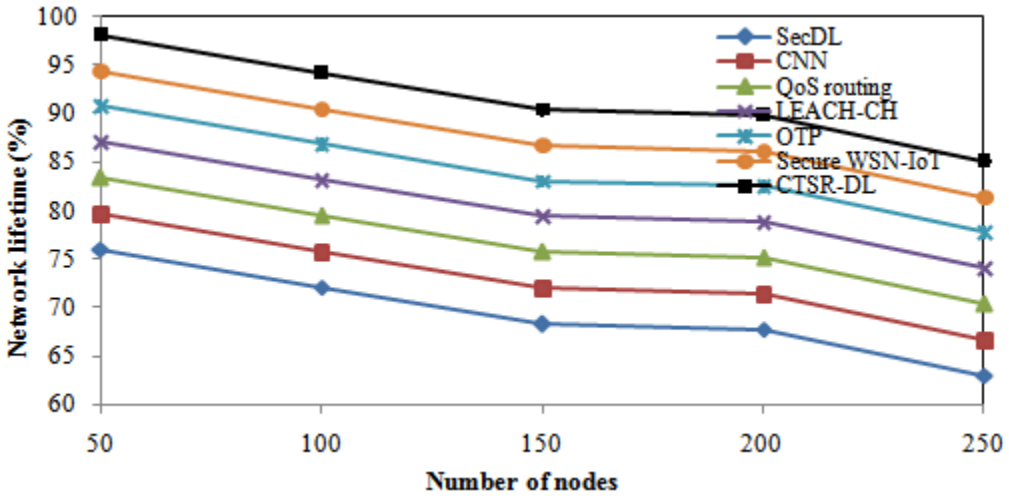

Fig. 5 Network lifetime with no. of nodes

We delve into the network lifetime comparison between the proposed and several existing methods, considering varying numbers of nodes within the network, ranging from 50 to 250 nodes in Fig. 5. Notably, the CTSR-DL approach consistently outperforms existing methods in

terms of maximizing network lifetime across all node count scenarios. This improvement is particularly significant when contrasted with Secure WSN-IoT, serving as a reference point. CTSR-DL exhibits a consistent improvement in network lifetime, ranging from approximately 3.9% to 4.6%, as the no. of nodes in the network increase. This highlights the approach's exceptional capability to expand the network operational lifespan and enhance its sustainability, even in scenarios with a substantial number of nodes, which is of paramount importance for long-term WSN-IoT deployments. Comparing CTSR-DL with other conventional methods such as LEACH-CH, OTP, QoS routing, and CNN accentuates its superior performance. At the largest node count of 250, CTSR-DL demonstrates impressive enhancement increase in network lifetime, varying from around 3.8% to 4.7% when juxtaposed with these conventional methods.

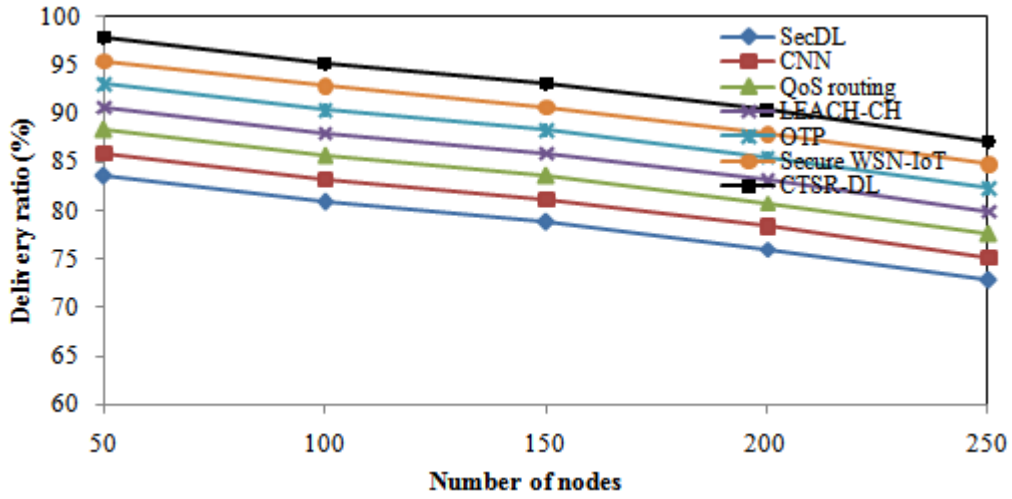

Fig. 6 Delivery ratio with no. of nodes

In Fig. 6, we analyze the delivery ratio of the proposed CTSR-DL routing approach compared to various existing methods across different network sizes, ranging from 50 to 250 nodes. It is evident that CTSR-DL consistently achieves higher delivery ratios across all node count scenarios, emphasizing its superior performance in ensuring data packet delivery within the

network. Comparing CTSR-DL with Secure WSN-IoT, serving as a reference point, showcases impressive performance improvements, with CTSR-DL exhibiting a consistent improvement in delivery ratio. The increase ranges from approximately 2.4% to 2.7% across various node count scenarios, underscoring its capability to enhance the efficiency of data packet delivery. When benchmarked against conventional methods like OTP, QoS routing, LEACH-CH, and CNN, the CTSR-DL approach consistently outperforms them in delivery ratio, highlighting its significant advantages. Even at the 250 nodes, CTSR-DL achieves remarkable improvement in delivery ratio, ranging from about 2.2% to 2.5%. This reflects the approach's effectiveness in ensuring successful data packet delivery, a critical factor for WSN-IoT applications.

4.3 Impact of attack nodes

Comparison of existing & proposed routing approach with varying number of attacks is described in Table 3. In Fig. 7, we analyze the energy consumption of the proposed CTSR-DL routing approach in comparison to various existing methods under the influence of different numbers of attacks, ranging from 5 to 25. The results highlight the significant advantages of the CTSR-DL approach when compared to the existing routing methods, especially in scenarios with varying levels of attacks. CTSR-DL consistently exhibits lower energy consumption, ensuring that sensor nodes endure less energy drain, which is crucial for prolonged network operation. Comparing CTSR-DL to Secure WSN-IoT, which serves as a reference point, we observe substantial improvements in energy conservation. CTSR-DL consistently demonstrates an enhancement in energy consumption across all attack scenarios, with the percentage-wise decrease ranging from approximately 9.1% to 9.4%. This signifies its superior ability in optimizing energy usage and extend sensor node’s lifespan even under attack conditions.

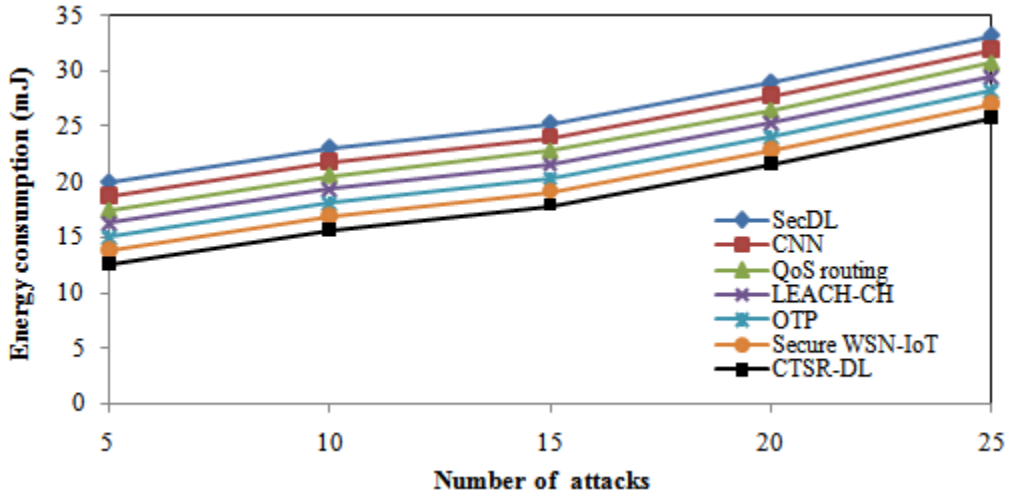

Fig. 7 Energy consumption with no. of attack nodes

We examine the throughput comparison between the proposed CTSR-DL routing approach and various existing methods in the presence of different numbers of attacks, ranging from 5 to 25 in Fig 8. The results highlight the remarkable advantages of the CTSR-DL approach when compared to existing routing methods, especially in scenarios with increasing numbers of attacks. CTSR-DL consistently exhibits higher throughput, which is essential for maintaining efficient data communication within the network, even under attack conditions. Comparing CTSR-DL to Secure WSN-IoT, acting as a reference point, reveals significant improvements in terms of throughput. CTSR-DL consistently demonstrates an improvement in throughput across all attack scenarios, with the percentage-wise increase ranging from approximately 5.8% to 6.1%. This emphasizes its superior ability to sustain data transfer rates and network performance, making it well-suited for applications where reliable data communication is vital.

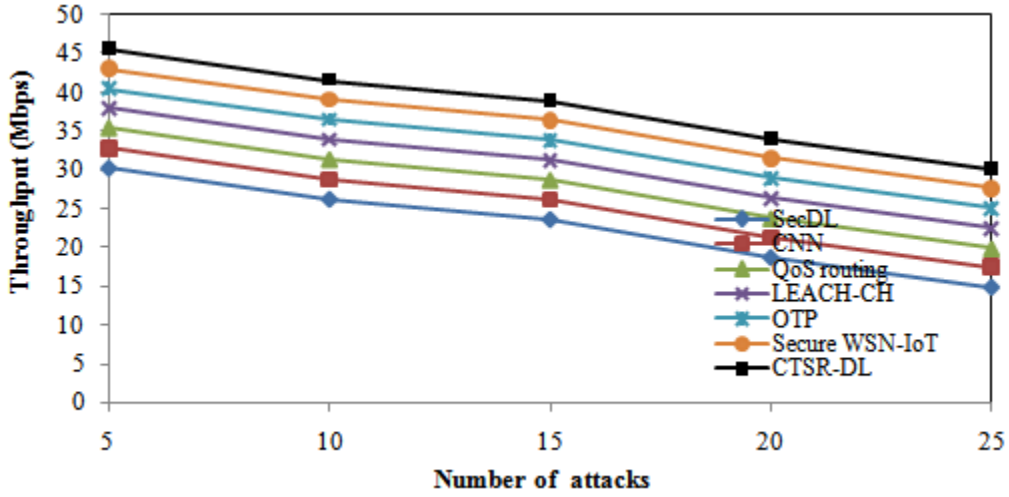

Fig. 8 Throughput with no. of attack nodes

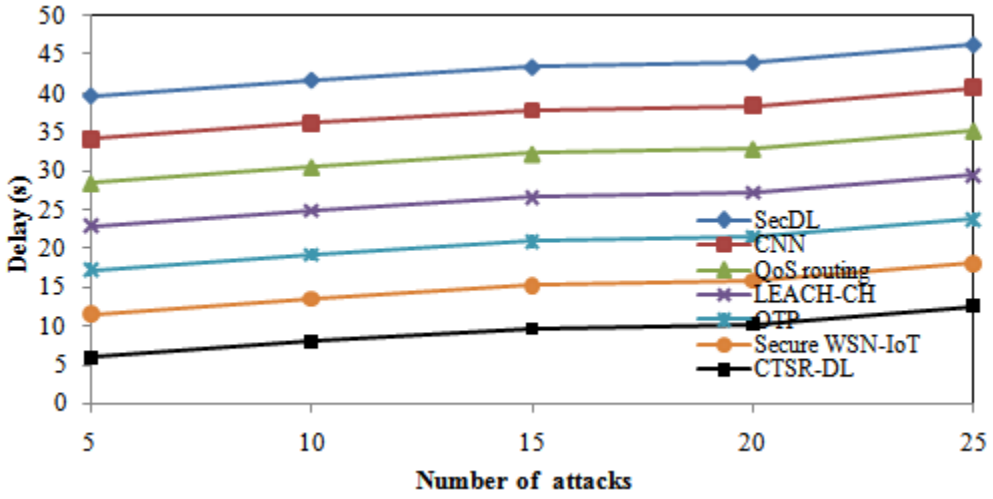

Fig. 9 Delay with no. of attack nodes

Table 3 Comparison of existing and proposed routing approach with impact of attack nodes

Routing approach	5	10	15	20	25	5	10	15	20	25	5	10	15	20	25
	Energy consumption (mJ)					Throughput (Mbps)					Delay (s)				
SecDL	19.973	23.099	25.305	28.979	33.212	30.245	26.211	23.578	18.647	14.800	39.706	41.755	43.433	44.063	46.373
CNN	18.738	21.864	24.070	27.744	31.977	32.808	28.774	26.141	21.210	17.363	34.071	36.120	37.798	38.428	40.738
QoS routing	17.503	20.629	22.835	26.509	30.742	35.371	31.337	28.704	23.773	19.926	28.436	30.485	32.163	32.793	35.103
LEACH-CH	16.268	19.394	21.600	25.274	29.507	37.934	33.900	31.267	26.336	22.489	22.801	24.850	26.528	27.158	29.468
OTP	15.033	18.159	20.365	24.039	28.272	40.497	36.463	33.830	28.899	25.052	17.166	19.215	20.893	21.523	23.833
Secure WSN-IoT	13.798	16.924	19.130	22.804	27.037	43.060	39.026	36.393	31.462	27.615	11.531	13.580	15.258	15.888	18.198

CTSR-DL	12.563	15.689	17.895	21.569	25.802	45.623	41.589	38.956	34.025	30.178	5.896	7.945	9.623	10.253	12.563

	Network lifetime (%)					Delivery ratio (%)				
SecDL	76.497	73.996	71.992	69.876	68.407	84.442	83.109	77.789	76.109	73.371
CNN	80.023	77.522	75.518	73.402	71.933	86.678	85.345	80.025	78.345	75.607
QoS routing	83.549	81.048	79.044	76.928	75.459	88.914	87.581	82.261	80.581	77.843
LEACH-CH	87.075	84.574	82.570	80.454	78.985	91.149	89.816	84.496	82.816	80.078
OTP	90.601	88.100	86.096	83.980	82.511	93.385	92.052	86.732	85.052	82.314
Secure WSN-IoT	94.127	91.626	89.622	87.506	86.037	95.620	94.287	88.967	87.287	84.549
CTSR-DL	97.653	95.152	93.148	91.032	89.563	97.856	96.523	91.203	89.523	86.785

In Fig. 9, we analyze the delay comparison between the proposed CTSR-DL routing approach and various existing methods in the presence of different numbers of attacks, ranging from 5 to 25. The results underscore the significant advantages of the CTSR-DL approach, particularly when compared to existing routing as the number of attacks increases. CTSR-DL consistently exhibits lower delays, ensuring that data traverses the network more swiftly, even under attack scenarios. CTSR-DL consistently demonstrates an enhancement in delay across all attack scenarios, with the decrease ranging from approximately 48.9% to 48.7%. This highlights its exceptional capability to minimize data transmission delays, which is important for time-sensitive & crucial for real-time applications in WSN-IoT. The decrease in delay ranges from approximately 34.5% to 34.7% across different attack scenarios.

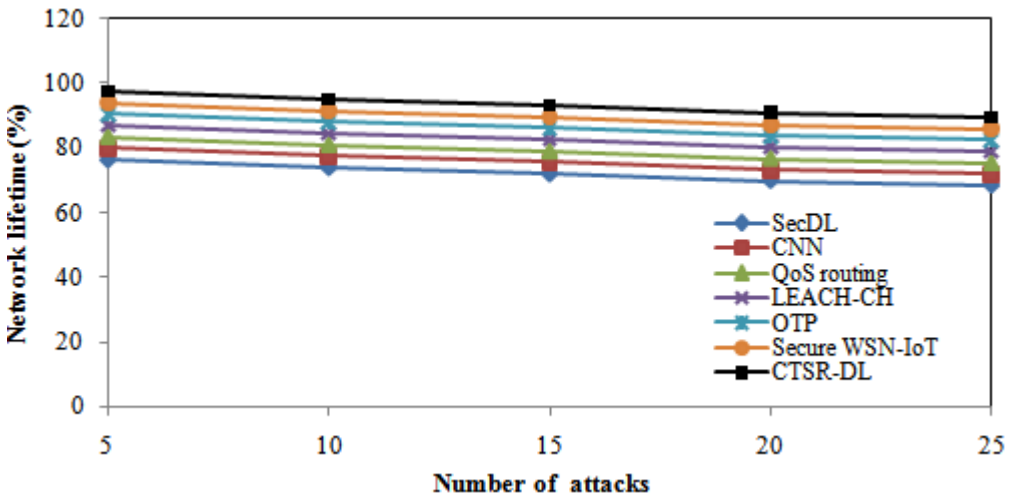

Fig. 10 Network lifetime with no. of attack nodes

In Fig. 10, we delve into the network lifetime comparison between the proposed CTSR-DL routing approach and various existing methods in the presence of different numbers of attacks, ranging from 5 to 25. The results indicate the impressive capabilities of the CTSR-DL approach

in extending the network's lifetime, particularly in the face of an increasing number of attacks. CTSR-DL consistently exhibits superior network lifetime preservation, ensuring that the network can continue functioning efficiently for an extended period even under attack scenarios. Comparing CTSR-DL to Secure WSN-IoT, a reference point, underscores its substantial enhancements in terms of increased network lifetime. CTSR-DL consistently demonstrates an enhancement in network lifetime across all attack scenarios, with the increase ranging from approximately 48.1% to 47.8%. This highlights its exceptional ability to prolong the network's functional duration, making it highly suitable for applications that demand long-lasting, resilient networks, even when subjected to attacks. When juxtaposed with conventional methods like OTP, QoS routing, LEACH-CH, CNN, and SecDL, CTSR-DL in spite of attacks, constantly outperforms them when it comes to extending the lifetime of the underlying network. The increment in network lifetime ranges from approximately 39.3% to 39.5% across different attack scenarios.

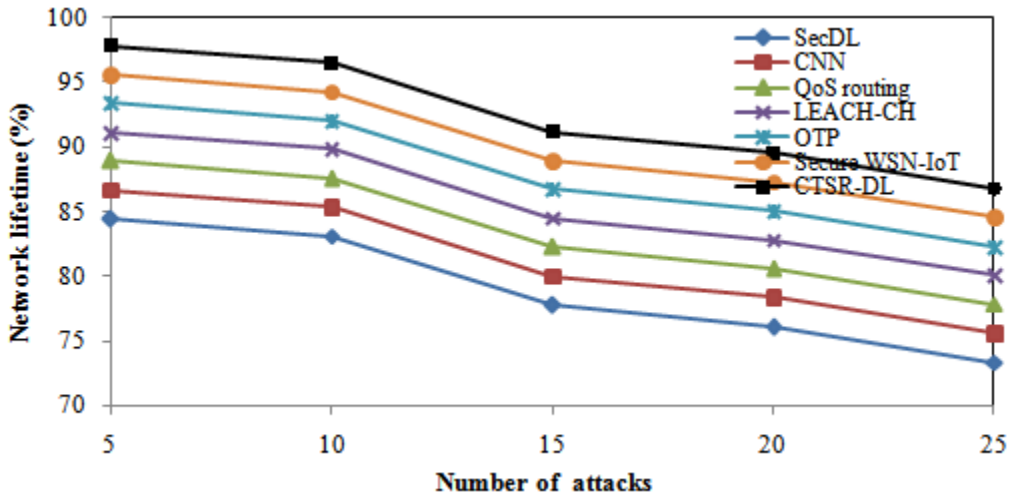

Fig. 11 Delivery ratio with no. of attack nodes

Fig. 11 illustrates the delivery ratio comparison between the proposed CTSR-DL routing approach and various existing methods when subjected to different numbers of attacks, ranging from 5 to 25. The results highlight the robust and resilient nature of the CTSR-DL approach in ensuring high delivery ratios, even in the presence of attacks. The data shows that CTSR-DL consistently outperforms other existing methods, significantly enhancing the delivery ratio under various attack scenarios. When comparing CTSR-DL to the Secure WSN-IoT approach, we observe improvement in the delivery ratio. CTSR-DL consistently exhibits a percentage-wise increase in delivery ratio across all attack scenarios, with the percentage increase ranging from approximately 46.4% to 46.3%. Additionally, when contrasted with conventional methods like OTP, QoS routing, LEACH-CH, CNN, and SecDL, CTSR-DL consistently demonstrates superior delivery ratios in the presence of attacks. The increase in the delivery ratio ranges from around 41.9% to 42.1% across different attack scenarios.

5. Conclusion

Our research introduces an approach called CTSR DL (cluster based trusted secure aware routing) for WSN IoT. We have designed an algorithm called ECGO (enhanced chaos game optimization) to efficiently manage the network load by clustering nodes. Additionally we take metrics into account, such, as node mobility received signal strength (RSS) and congestion rates to calculate trust levels. For path selection between source and destination nodes we leverage CNN BDT (convolutional neural network bagged decision tree). Through simulations we have thoroughly evaluated the performance of our proposed CTSR DL approach.The outcomes show how much better it is than the current best routing approaches. In today's world where secure and reliable data communication is crucial amidst network attacks and adversarial conditions our CTSR DL approach serves as a solution. It showcases the potential of learning techniques and

optimized routing algorithms in enhancing the performance and trustworthiness of WSNs and IoT systems. As the demand for efficient data transmission, in these domains continues to grow CTSR DL offers a solution to meet these needs effectively and reliably.

References

1. Zhang, Y., Sun, L., Song, H. and Cao, X., 2014. Ubiquitous WSN for healthcare: Recent advances and future prospects. IEEE Internet of Things Journal, 1(4), pp.311-318.
2. Alves, R.C., Gabriel, L.B., de Oliveira, B.T., Margi, C.B. and dos Santos, F.C.L., 2015. Assisting physical (hydro) therapy with wireless sensors networks. IEEE Internet of Things Journal, 2(2), pp.113-120.
3. Goratti, L., Baykas, T., Rasheed, T. and Kato, S., 2015. NACRP: A connectivity protocol for star topology wireless sensor networks. IEEE Wireless Communications Letters, 5(2), pp.120-123.
4. Shen, J., Wang, A., Wang, C., Hung, P.C. and Lai, C.F., 2017. An efficient centroid-based routing protocol for energy management in WSN-assisted IoT. Ieee Access, 5, pp.18469-18479.
5. Lenka, R.K., Rath, A.K., Tan, Z., Sharma, S., Puthal, D., Simha, N.V.R., Prasad, M., Raja, R. and Tripathi, S.S., 2018. Building scalable cyber-physical-social networking infrastructure using IoT and low power sensors. IEEE Access, 6, pp.30162-30173.
6. Gupta, V. and De, S., 2018. SBL-based adaptive sensing framework for WSN-assisted IoT applications. IEEE Internet of Things Journal, 5(6), pp.4598-4612.
7. Lin, W. and Matsumoto, T., 2018. Performance analysis of distortion-acceptable cooperative communications in wireless sensor networks for Internet of Things. IEEE Sensors Journal, 19(5), pp.1979-1989.

8. Guravaiah, K. and Velusamy, R.L., 2019. Prototype of home monitoring device using Internet of Things and river formation dynamics-based multi-hop routing protocol (RFDHM). IEEE Transactions on Consumer Electronics, 65(3), pp.329-338.
9. Suman, S., Kumar, S. and De, S., 2019. UAV-assisted RFET: A novel framework for sustainable WSN. IEEE Transactions on Green Communications and Networking, 3(4), pp.1117-1131.
10. Lenka, R.K., Rath, A.K. and Sharma, S., 2019. Building reliable routing infrastructure for green IoT network. IEEE Access, 7, pp.129892-129909.
11. Han, G., Zhou, L., Wang, H., Zhang, W. and Chan, S., 2018. A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things. Future Generation Computer Systems, 82, pp.689-697.
12. Yang, T., Xiangyang, X., Peng, L., Tonghui, L. and Leina, P., 2018. A secure routing of wireless sensor networks based on trust evaluation model. Procedia computer science, 131, pp.1156-1163.
13. Shah, S.B., Chen, Z., Yin, F., Khan, I.U. and Ahmad, N., 2018. Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks. Future Generation Computer Systems, 81, pp.372-381.
14. Gaber, T., Abdelwahab, S., Elhoseny, M. and Hassanien, A.E., 2018. Trust-based secure clustering in WSN-based intelligent transportation systems. Computer Networks, 146, pp.151-158.
15. Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K.K.R., Wazid, M. and Das, A.K., 2017. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications, 89, pp.72-85.

16. Bokefode, J.D., Bhise, A.S., Satarkar, P.A. and Modani, D.G., 2016. Developing a secure cloud storage system for storing IoT data by applying role based encryption. Procedia Computer Science, 89, pp.43-50.
17. Rouissi, N. and Gharsellaoui, H., 2017. Improved hybrid LEACH based approach for preserving secured integrity in wireless sensor networks. Procedia computer science, 112, pp.1429-1438.
18. Wang, R., Zhang, Z., Zhang, Z. and Jia, Z., 2018. ETMRM: An energy-efficient trust management and routing mechanism for SDWSNs. Computer Networks, 139, pp.119-135.
19. Sciancalepore, S., Piro, G., Vogli, E., Boggia, G., Grieco, L.A. and Cavone, G., 2016. LICITUS: A lightweight and standard compatible framework for securing layer-2 communications in the IoT. Computer Networks, 108, pp.66-77.
20. Benayache, A., Bilami, A., Barkat, S., Lorenz, P. and Taleb, H., 2019. MsM: A microservice middleware for smart WSN-based IoT application. Journal of Network and Computer Applications, 144, pp.138-154.
21. Deebak, B.D. and Al-Turjman, F., 2020. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, p.102022.
22. Ullah, A., Said, G., Sher, M. and Ning, H., 2020. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Networking and Applications, 13, pp.163-174.
23. Kim, S., Kim, C. and Jung, K., 2020. Cooperative multipath routing with path bridging in wireless sensor network toward IoTs service. Ad Hoc Networks, 106, p.102252.

24. Hameed, A.R., ul Islam, S., Raza, M. and Khattak, H.A., 2020. Towards energy and performance-aware geographic routing for IoT-enabled sensor networks. Computers & Electrical Engineering, 85, p.106643.
25. Haseeb, K., Islam, N., Saba, T., Rehman, A. and Mehmood, Z., 2020. LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustainable Cities and Society, 54, p.101995.
26. Jain, J.K., 2020. A coherent approach for dynamic cluster-based routing and coverage hole detection and recovery in bi-layered WSN-IoT. Wireless Personal Communications, 114, pp.519-543.
27. Duy Tan, N., Nguyen, D.N., Hoang, H.N. and Le, T.T.H., 2023. EEGT: Energy Efficient Grid-Based Routing Protocol in Wireless Sensor Networks for IoT Applications. Computers, 12(5), p.103.
28. Pedditi, R.B. and Debasis, K., 2023. Energy Efficient Routing Protocol for an IoT-Based WSN System to Detect Forest Fires. Applied Sciences, 13(5), p.3026.
29. Sharma, A., Babbar, H., Rani, S., Sah, D.K., Sehar, S. and Gianini, G., 2023. MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT. Energies, 16(10), p.4198.
30. Altowaijri, S.M., 2022. Efficient next-hop selection in multi-hop routing for IoT enabled wireless sensor networks. Future Internet, 14(2), p.35.
31. Srivastava, A. and Paulus, R., 2023. ELR-C: A Multi-objective Optimization for Joint Energy and Lifetime Aware Cluster Based Routing for WSN Assisted IoT. Wireless Personal Communications, pp.1-28.

32. Sujanthi, S. and Nithya Kalyani, S., 2020. SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT. Wireless Personal Communications, 114, pp.2135-2169.
33. Thangaramya, K., Kulothungan, K., Logambigai, R., Selvi, M., Ganapathy, S. and Kannan, A., 2019. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. Computer Networks, 151, pp.211-223.
34. Shah, S.B., Chen, Z., Yin, F., Khan, I.U. and Ahmad, N., 2018. Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks. Future Generation Computer Systems, 81, pp.372-381.
35. Behera, T.M., Mohapatra, S.K., Samal, U.C., Khan, M.S., Daneshmand, M. and Gandomi, A.H., 2019. Residual energy-based cluster-head selection in WSNs for IoT application. IEEE Internet of Things Journal, 6(3), pp.5132-5139.
36. Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E. and Djaba, E., 2019. Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads. IEEE Internet of Things Journal, 6(2), pp.3925-3933.
37. Jain, J.K., 2019. Secure and energy-efficient route adjustment model for internet of things. Wireless Personal Communications, 108, pp.633-657.