International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A DEEP LEARNING APPROACH FOR TRUST-AWARE AND FAULT-TOLERANT SECURE ROUTING IN IOT USING MC-GRU AND GREYSTAR GOOSE OPTIMIZATION

Ramakrishna Prasad A L[1*], Dr. Shiva Murthy G[2]

[1*]Assistant Professor, VTU PG Centre, Mysuru, Karnataka, India,
[2]Associate Professor and Principal of VTU Constituent College, Chintamani, Chikkaballapur District, Karnataka, India

***Corresponding Author:** Ramakrishna Prasad A L
*(Email: ramakrishna@vtu.ac.in)

Abstract

Internet of Things (IoT) is a system of physical devices that are interconnected to collect and exchange data worldwide using the Internet. Various smart devices are embedded in IoT with software, sensors, and other technologies, like smart lights and thermostats, to complex industrial tools. However, the dynamic and massive IoT environment encounters significant challenges related to trust, reliability, and security. The existing secure routing protocols fail to effectively ensure data privacy, while maintaining energy efficiency. This paper introduces GreyStar Goose Optimization Algorithm (Grey-SGOA) for trust-aware and fault-tolerant secure routing in IoT. Here, the IoT network is simulated initially, and then, clustering is performed by K-medoids clustering algorithm. Then, the cluster head is selected using Grey-SGOA by concerning different fitness parameters and trust factors. After that, the data aggregation is performed using Multi-Context Gated Recurrent Unit (MC-GRU), and the encryption of aggregated data is executed using Fully Homomorphic Encryption (FHE). Secure routing is performed in the IoT network using Grey-SGOA. Further, the efficacy of Grey-SGOA is investigated, where the Grey-SGOA attained average residual energy, trust, delay, Packet Delivery Rate (PDR), throughput, normalized variance, and conditional privacy of 0.274 J, 81.739, 79.131 msec, 89.651%, 145.045 Kbps, 0.008, and 82.428%.

Keywords: Internet of Things, Data aggregation, Fault tolerance, Routing, Fully Homomorphic Encryption

1. Introduction

A massive network of connected devices that can interact and share data without the need of humans is termed as the IoT [7]. Over the past few years, IoT thrived as yet another worldwide innovation. The implementation of IoT in numerous schemes is expected to change the course of history in the upcoming years [9]. With the IoT, people can live in a world where the things they utilize on a daily basis can detect and collect environmental data. By collecting, analysing, and examining data generated by IoT devices, the physical environment is observed and controlled. The careful integration of the digital and physical worlds is termed as the IoT. It has intelligent objects, connectivity infrastructure, computational units, processing and sensor nodes [4]. Multiple services and applications made possible by IoT have revolutionized how it can connect with its environment [1]. The IoT is rapidly becoming crucial for many applications in communication and industrial technology. Since it is predicted that there will be 50 billion Internet-connected devices by 2020, the execution of IoT has increased exponentially [9]. The IoT generates a setting where other objects and individuals with Internet connections can access data about heterogeneous objects and their status and locations. In general, IoT devices have very limited energy sources and are typically battery-powered. Increasing the network lifetime is crucial in some situations, like when deploying IoT devices for long-term purposes, such as continuously monitoring an environment [4].

Received: August 03, 2025

In order to produce smart network schemes, the IoT has increased its global adoption. The aim is to produce a network edge that offers IoT devices with processing power and smart services [14][15]. Recently, it is extremely difficult to design secure routing in the IoT due to the continuously increasing number of unknown and known security threats [10] [11]. Routing attacks are one of the multiple security threats that present a serious issue because they directly impact the data transmission procedure, resulting in packet loss, illegal access, traffic misdirection, and service interruptions [12][13]. Routing protocols are crucial for solving the previously noted difficulties with data transfer throughout different objects [4]. Reliable communication among destination and source nodes in a network relies heavily on effective routing protocols. Routing techniques identify the ideal data routes, stability, improving efficiency, and network performance. The choice of a suitable routing protocol is based upon particular network constraints and requirements [6]. In IoT-based networks, energy-aware routing is significant, but routing protocols focus only on energy have not been very effectual in minimizing high energy usage. In networks based on the IoT, energy-aware routing protocols are essential. Consequently, the execution of a variety of routing algorithms intends to minimalize the amount of data transfer and power requirements [2]. Selecting the appropriate intermediate nodes is vital for routing decisions in IoT networks in order to assure safe and efficient data distribution [8].
Prevailing IoT routing protocol efforts frequently struggle to find a balance among security and energy efficacy. Multiple classical security measures, such malicious node identification algorithms and encryption approaches, need a lot of processing, which results in high energy consumption [7]. In addition, a number of data aggregation techniques that preserve privacy are provided to maintain users' privacy in IoT applications [20]. Recently, data aggregation has attained widespread recognition and use as a successful method to increase the nodes' lifespan and lower the transmission costs associated with the IoT [16][17]. Aggregation techniques' main intention is to minimize the total amount of data transmission before transmitting it to the base station, integrate data from several sources at specific aggregation points, and perform basic calculation at aggregation points to remove data redundancies [4]. The aim of data aggregation algorithms is to detect effectual routes for transmitting the incorporated data to base stations. According to their architecture, data aggregation algorithms can usually be categorized as either structure-based or structure-less [4]. Artificial Intelligence and machine learning serve as core pillars in the IoT ecosystem, significantly improving its ability to process data, make intelligent decisions, and realize its full potential. Huge amounts of data generated by networked devices can be assessed and interpreted by machine learning algorithms, which can then employ this information to recognize patterns, acquire valuable insight, and produce intelligent predictions. Deep learning and neural networks are two examples of artificial intelligence approaches that allow IoT schemes to learn, adapt, and make decisions in real time based upon data [18].

This paper presents Grey-SGOA for trust-aware and fault-tolerant secure routing in IoT systems. The simulation of IoT model is executed, and then, the clustering is performed using K-medoids clustering algorithm. Then, the selection of cluster head is performed by Grey-SGOA concerning various fitness parameters, such as distance among the cluster head and base station, node centrality, node degree, throughput, fault tolerance, delay, energy, and different trust factors, like indirect, historical, witness, and direct trust. After that, the data is securely aggregated using the MC-GRU, and the aggregated data is encrypted by FHE. Following this, secure routing is performed by Grey-SGOA by considering a multi-objective fitness.

The key contribution is summarized below,

- ***Designed Grey-SGOA for secure routing in IoT systems***: The trust-aware and fault-tolerant secure routing in IoT systems is performed using Grey-SGOA, where Grey-SGOA is the combination of Greylag Goose Optimization (GGO) and Star Fish optimization (SFOA).

The residual sections are organized subsequently: Section 2 discusses the existing techniques used for secure IoT routing and data aggregation, and Section 3 demonstrates the system model of the IoT network. Further, in section 4, the Grey-SGOA developed for secure routing is described. Also, the outcomes and discussions followed are portrayed in section 5, and the paper is concluded with future research directions in section 6.

2. Motivation

IoT is an advanced technology that comprises different sensing devices that are interconnected for the collection and transfer information to various sectors worldwide. Nowadays, IoT networks utilize various routing protocols that help to resolve different network-based problems, like congestion avoidance, reliability, energy conservation, and so on. Thus, data aggregation in IoT is carried out to minimize the communication cost and enhance the nodes' lifetime. Various schemes are employed for data aggregation to securely transfer the aggregated data to the base station via optimal routes. Meanwhile, these techniques failed to enhance the security of the IoT framework while maintaining the energy efficiency and high throughput. Hence, it motivates to introduce a novel optimization algorithm for secure routing in IoT frameworks.

2.1. Literature Review

Sunithanandhini, A., *et al*. [1] designed an Imperialist Competitive Algorithm with Harmony Search (ICA-HS) algorithm for multi-hop data aggregation in IoT. Harmony Search (HS) and Imperialist Competitive Algorithm (ICA) were incorporated for balancing the en
ergy consumption to minimize trust cost. This approach securely transmitted data packets in IoT framework under less end-to-end delay, but this scheme was not successful in considering the overhead issues that occurred while aggregating data packets. Ravi, G., *et al*. [2] devised a Congestion Aware-Low Energy Adaptive Clustering Hierarchy (CW-LEACH) algorithm for energy efficient data aggregation. The CW-LEACH established correlation among the energy consumption ratio and the threshold utilized by conventional Low Energy Adaptive Clustering Hierarchy (LEACH). The network lifetime was significantly increased by the model and maintained energy consumption in IoT network at an appropriate level. However, this scheme failed to perform real-time data aggregation in IoT networks. Ravi, G., *et al*. [3] established a Cluster-Based Reliable Data Aggregation (CRDA) scheme for data aggregation in IoT systems. Here, the IoT sensors were grouped by utilizing Monarch and Sine-Cosine (MSC) algorithm for ensuring effective data transmission. This model was reliable in transferring and aggregating data in IoT networks, but this scheme was not successful in utilizing cryptographic methods to increase the security of data transmitted. Mohseni, M., *et al*. [4] introduced a Cluster-based Energy-aware Data Aggregation Routing (CEDAR) protocol for data aggregation in IoT networks. Here, a Capuchin Search Algorithm (CapSA) and fuzzy logic system were integrated to design CEDAR. Moreover, the fuzzy logic-based model was employed for the organization of IoT nodes into optimal clusters. This scheme increased the network lifetime during data aggregation while minimizing the network traffic. Nevertheless, this scheme was not successful in considering temporal graphs for enhancing the efficiency in routing while transmitting data generated by sensor nodes.

Thangavelu, A. and Rajendran, P., [5] designed an Energy-Efficient Memetic Clustering Method (EEMCM) for secure IoT routing. Here, the AlexNet and Parallelized Memetic Algorithm (PMA) were integrated to increase the efficiency in anomaly detection. Moreover, the PMA was utilized for the formation of clusters and selection of optimal cluster heads. This approach was scalable and effectively minimized the energy consumption issues during secure routing in a heterogeneous IoT framework. Meanwhile, this method was not suitable for real-time scenarios, and also failed to select an optimal cluster head by utilizing hybrid algorithms. Burange, A.W., *et al*. [6] devised a Lightweight Trust-Based System for increasing the security of IoT routing. This approach effectively recognized the resource-constrained nature of IoT devices while addressing various

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

security challenges in IoT networks. This scheme recorded minimum average power consumption and effectively controlled traffic overhead during IoT routing. However, this approach failed to utilize attack detection algorithms for increasing the security of the protocol, and was also not scalable and suitable for deployment in large IoT networks. Fu, T., *et al*. [7] established an Energy-aware secure Routing scheme via Two-Way Trust evaluation (ERTWT) in IoT. In this model, the trust values were estimated to increase the network security against different attacks, and the nodes were selected dynamically considering the trustworthiness and energy availability. The ERTWT attained better data transmission rates and energy efficiency with optimal utilization of energy resources while performing secure routing in IoT. However, this scheme failed to explore its application in large-scale IoT environments and refine the trust evaluation model to improve the security in IoT networks. Hasan, A.A., *et al*. [8] introduced a trust-based route optimization framework for routing in IoT framework. This approach utilized Jeffrey's conditioning and Bayesian inference to increase the reliability of IoT networks. Also, this scheme determined the suitability for data forwarding by computing a composite trust level. This model was scalable, robust, consumed minimum energy, and reduced overhead issues while performing optimal routing in resource-constrained and dynamic IoT networks. However, this scheme failed to utilize time-sensitive trust weight adjustment mechanisms for distinguishing outdated and recent interacted histories.

2.2. Challenges

The drawbacks of previous works on secure routing are enlisted below,

- The ICA-HS model employed in [4] significantly balanced energy consumption and minimized the total trust cost during secure trust-based routing. However, this scheme failed to aggregate data in IoT networks during routing for making decisions.
- The CW-LEACH scheme utilized in [3] increased the data aggregation capacity by improving the durability of the network, but this model failed to prolong the network lifetime by optimizing the energy level drops.
- The CRDA method used in [2] effectively enhanced the network lifetime by minimizing delay that occurred during data transmission by aggregating data in an energy-efficient manner. Meanwhile, this technique was not successful in integrating other technologies to handle communication overhead issues that occurred during data aggregation.
- In [1], the CEDAR approach was utilized to reduce the overhead issues, thereby enhancing the network connectivity for data aggregation. However, this model failed to increase the security and trust during routing by utilizing hybrid optimization algorithms.
- The previous works employed for data aggregation minimized the security risks and enabled quick responses, and optimized total energy consumption to enhance the network lifetime. Meanwhile, these methods failed to attain result in minimum throughput.

3. System model of IoT framework

The system model of IoT framework with two-level gateway topology is displayed in figure 1. Here, the data collected by the IoT devices is sent to the server in a privacy-preserving way [20]. The two-level IoT topology mainly involves three types of entities, such as devices, an aggregator, and a server. Let us consider, H IoT devices are covered by each aggregator and l aggregators are covered by the servers. In IoT, the IoT devices, such as Radio-Frequency Identification (RFID) readers, a smart meter, or a sensor are used to collect data, and is allowed for pre-processing. The aggregator helps to aggregate the data collected by the IoT devices and transmits the aggregated data to the server. Moreover, the data collected by the IoT devices is stored in the server, and is retrieved by the customers, and the server is considered a powerful and trustworthy entities that helps to collect and process data.

3.1 Energy model

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The sensor nodes of the IoT system use battery power and the network lifetime is affected by the available energy of the nodes [27]. The energy model is executed in receiving, sleeping, and idle transmitting mode. Generally, a node with maximum energy is selected to identify route, whereas a minimum energy node is taken into account for data transmission. The value of energy is estimated for various time intervals, where the energy consumed is computed using the expression designated as,

$$B^k(T) = \alpha_v^k * B_v^k + \alpha_w^k * B_w^k \tag{1}$$

In the expression, B_v^k and B_w^k are the energy utilized to transmit packet and reception, the energy of k^{th} node at a time T is given by $B^k(T)$, α_w^k represents the data packets obtained by the node k^{th}, the data packets forwarded by k^{th} node is symbolized as α_v^k. The B_v^k and B_w^k are expressed by,

$$B_v^k = \alpha * O \tag{2}$$

$$B_w^k = \delta * U \tag{3}$$

where, the power required to receive and transmit data are signified as δ and U, the time taken for transmission is given by α and O. The residual energy is given as,

$$B_R = BB - B^k(T) \tag{4}$$

Here, BB is the initial energy of the sensor node and a threshold value is verified by each node's energy to measure the residual energy B_R. Moreover, the data transmission is performed using nodes with the least amount of energy.

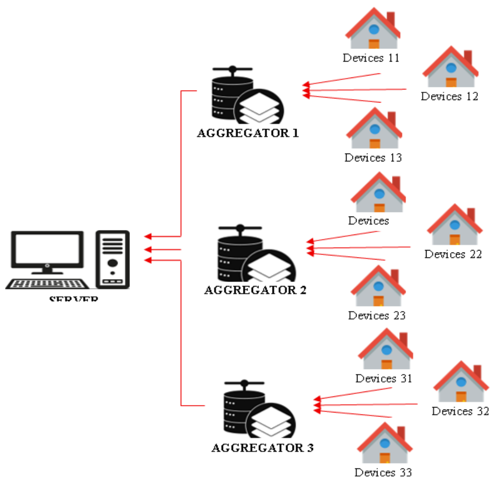


Figure 1. System model of IoT data aggregated model

3.2 Trust model

In order to enhance the performance of the IoT framework, the trust factor is used for detecting and segregating attacks. The different types oftrust, like historical trust, indirect trust, witness trust, and direct trust, are considered and they are briefly illustrated as follows,

i) Witness trust

The trust of a node on its direct neighbour or the confidence of the indirect neighbour [28] is defined as witness trust, which is formulated as,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$Trust_W = \sum_{w=1}^{h} \gamma_{wa} J_{wa} \tag{5}$$

wherein, J_{wa} indicates the weight vector of nodes w and a, the entry in option scores matrix is given by γ_{wa}, and $Trust_W$ represents witness trust.

ii) Historical trust

The trust on the physical neighbours of the node determined by contemplating the interactions over past [29] is decided by historical trust, where the historical trust is expressed as,

$$Trust_H = W_1 \times L_{wa}(g) + W_2 \times M_{wa}(g) \tag{6}$$

In the expression, W_1, and W_2 signifies weights, $Trust_H$ indicates historical trust, $M_{wa}(g)$ and $L_{wa}(g)$ are the forwarding ratio of data and control packets.

iii) Indirect trust

Indirect trust [30] defines the trustworthiness of the node based on the third-party recommendations, which the indirect trust is expressed by,

$$Trust_{ID} = \sum_{b=1}^{q} \varpi_b * Q^b_{w'a'}, \quad b = 1,2,3,...,q \tag{7}$$

Here, $Trust_{ID}$ represents indirect trust, q indicates total selected nodes, the weight is denoted by ϖ_b, and $Q^b_{w'a'}$ indicates the value of trust from node w' to node a' to node b.

iv) Direct trust

Direct trust [31] helps to assess the ability of nodes in forwarding data packets, which shows the probability of successful connection among the nodes. The direct trust is designated as,

$$Trust_D(E,F) = \frac{V_{wa}(g)}{V_{wa}(g) + K\left[\eta_{wa}(g) - V_{wa}(g)\right]} \tag{8}$$

whereas, $Trust_D$ represents direct trust, K signifies the penalty weight to misbehaving nodes, the node's evaluation duration is given by g, the total packets sent to node w' to node a' is denoted by $\eta_{wa}(g)$, and the total forwarded data packets is specified as $V_{wa}(g)$.

4. Designed GreyStar Goose Optimization Algorithm for trust-aware and fault-tolerant secure routing in Internet of Things

This paper presents Grey-SGOA for trust-aware and fault-tolerant secure routing in IoT systems. At first, the system model of IoT data aggregation model is considered, and then, clustering is performed using K-medoids clustering algorithm [21]. After that, the cluster head selection is executed using Grey-SGOA by considering different fitness parameters, like distance among the cluster head and base station, delay, fault tolerance, throughput, energy, node degree, node centrality [24], and various trust factors, like indirect, historical, witness, and direct trust. Here, the Grey-SGOA is designed by integrating SFOA [22] and GGO [23]. Later, the data is aggregated securely using the MC-GRU [25], and the data encryption is executed using FHE [26]. Following this, secure routing is performed by utilizing Grey-SGOA considering multi-objective parameters. In figure 2,

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the pictorial view of Grey-SGOA used for secure routing in data aggregated IoT system is delineated.

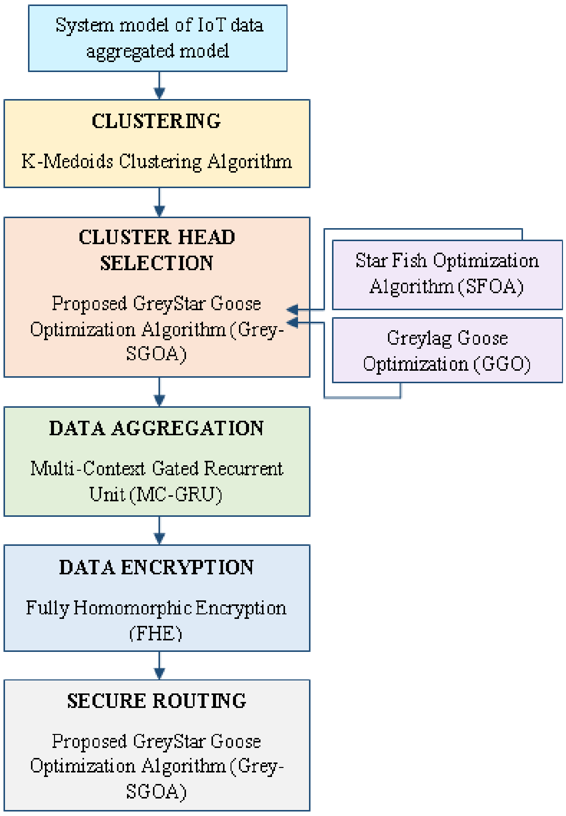


Figure 2. Workflow of Grey-SGOA for Trust-Aware and Fault-Tolerant Secure Routing in IoT

4.1. Clustering

In IoT, the cluster formation is used to increase the data transmission performance, efficiency, and longevity. During clustering, the cluster head forwards the aggregated data to the sink by reducing long-range transmissions and providing direct communication among the nodes and sink. In this research, the IoT clustering is performed using the K-medoids clustering algorithm [21]. A centre-based clustering technique, called K-medoid clustering, is used to pre-define the number of clusters to process huge data packets. The clustering is performed by initially collecting the information of remaining energy and node coordinates. Then, the group number is estimated and the residual energy as well as the central circle's midpoint are computed for optimizing the k-medoids algorithm to minimize iteration time.

In the set-up phase, the nodes in cluster head are determined and the nodes are split into appropriate groups, where the total number of groups w is expressed as,

$$w = \sqrt{\frac{X}{2}} \tag{9}$$

Here, the number of nodes is represented as X. Let us consider the central position of the nodes be ρ, which is designated as,

$$\rho = \frac{\sum_{a=1}^{X} \kappa_x}{X} \tag{10}$$

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

where, the average distance among the central position ρ, the sensor C coordinate is signified as κ_x, and all nodes is denoted as D. After that, a central circle is estimated based on the central position of nodes and the estimated distance, and the mean points are selected from the central circle randomly. Under certain cases, if two or more midpoints are near, then the initial midpoints are selected randomly by the k-medoids algorithm, and this results in a large number of iterations.

4.2. Cluster head selection using Grey-Star Goose Optimization Algorithm

After clustering using K-medoids clustering algorithm, the optimal cluster head is selected to ensure the reliability of communication and minimize intra-cluster energy consumption. The selection of cluster heads helps for improving the network lifetime and minimize the energy usage. In this research, the selection of optimal cluster head is performed using Grey-SGOA concerning trust factors as well as different fitness parameters. Here, the Grey-SGOA is designed by the combination of SFOA [22] and GGO [23]. The solution encoding performed for cluster head selection, and fitness function utilized are illustrated below.

4.2.1. Solution encoding

The total cluster heads as well as the number of nodes are taken under consideration to select optimal cluster head. The solution encoding of Grey-SGOA is portrayed in Figure 3, which represents the solutions of Grey-SGOA, and the cluster head is selected by utilizing different fitness parameters and trust factors. Here, N represents number of nodes, and the total cluster heads are given by P.

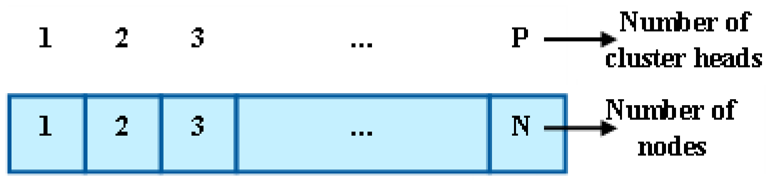


Figure 3. Solution encoding of Grey-SGOA

4.2.2. Fitness computation

The maximum fitness function determined based on various parameters is taken under consideration to select optimal cluster head. Here, the fitness parameters like distance among the cluster head and base station, throughput, fault tolerance, delay, node degree, energy, node centrality, and different trust factors, namely indirect, witness, historical, and direct trust, are considered for identifying the ideal solution, where the expression of fitness function is designated as,

$$fitness = \frac{1}{8}\left[\left(1-A_1\right)+A_2+A_3+A_4+A_5+A_6+A_7+\left(1-A_8\right)\right] \tag{11}$$

where, A_1 signifies distance among the base station and cluster head, the node degree is given by A_2, A_3 represents node centrality, the energy is symbolized as A_4, the trust factor is specified as A_5, the throughput is given by A_6, the fault tolerance is denoted by A_7, and A_8 is delay.

Distance between the base station and cluster head: In general, the energy consumed by the nodes depends on the distance between the transmitting paths [24], and an increased energy use leads to an abrupt drop in cluster head. Thus, the distance among the base station (A_1) and cluster head is computed, which is given by,

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$A_1 = \sum_{E=1}^{g} D(\zeta_F, \psi) \quad (12)$$

In the expression, the number of nodes is indicated as g, and the distance between the cluster head ζ_F and base station ψ is signified as $D(\zeta_F, \psi)$.

Node degree: The node degree (A_2) represents the total sensor nodes available in each cluster head [24], and is designated as,

$$A_2 = \sum_{E=1}^{g} \mu_E \quad (13)$$

where, μ_E is the total sensor nodes in the cluster head E.

Node centrality: The node centrality (A_3) is used to determine how far a node is from its neighbours [24], and is articulated as,

$$A_3 = \sum_{E=1}^{g} \frac{\sqrt{\frac{\sum_{F \in b}^{g} D^2(E,F)}{b(E)}}}{S} \quad (14)$$

Here, S is the network dimension, and the total neighbours of E^{th} cluster head is given by $b(E)$.

Energy: Energy (A_4) is the rest over energy in the node after processing, and is estimated by measuring the difference among the initial state and current level. The energy utilized for secure data transmission is estimated using the equation (4).

Trust: Trust (A_5) helps to assess the dependability of data transmitted to base station, which is expressed as,

$$A_5 = \frac{1}{4}\left[Trust_D + Trust_{ID} + Trust_H + Trust_W\right] \quad (15)$$

where, section 3.2 briefly demonstrates the trust parameters.

Throughput: Throughput (A_6) is the ratio of successfully transmitted data packets by the nodes over a time, and is expressed by,

$$A_6 = \frac{\chi}{\phi} \quad (16)$$

where, χ signifies number of successfully transmitted data packets, and ϕ represents time.

Fault tolerance: Fault tolerance (A_7) is the ratio of successfully recovered data packets to total attempts, and is given by,

$$A_7 = \frac{\vartheta}{\varsigma} \quad (17)$$

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

here, ς indicates total attempts, and the number of successfully recovered packets is given by ϑ.

Delay: Delay (A_8) is the time taken by data packets to reach the destination. Delay is computed by taking ratio of total nodes presented in the routing path to the total nodes during data transmission. The delay is given by,

$$A_8 = \frac{\varepsilon}{\varphi} \tag{18}$$

In the expression, the total nodes are given by φ, and ε signifies the nodes presented in the routing path.

4.2.3. Designed GreyStar Goose Optimization Algorithm for cluster head selection

The Grey-SGOA is used for the selection of optimal cluster head, where the Grey-SGOA is the combination of SFOA [22] and GGO [23]. A bio-inspired metaheuristic algorithm called SFOA is introduced based on the natural characteristics of starfish, like preying, exploration, and regeneration. The SFOA mainly performs exploitation as well as exploration phases to search for food, regeneration, and preying. In exploitation phase, the starfish follows a special movement to perform preying and regeneration behaviours. The explorative behaviour based on unidimensional and five-dimensional search patterns is carried out by the starfish in the exploration phase. In general, the SFOA converge faster to provide solutions to optimization problems with high computational efficiency. At the same time, the GGO is an optimization algorithm designed based on the dynamic and social characteristics of Greylag goose in nature. The Greylag goose generally has long-lasting and strong bonds in order to show its loyalty, and also stays vigilant when the partner is ill or injured. In GGO, the algorithmic process is carried out in exploitation as well as exploration phases, where the finest solution is obtained by altering each group size dynamically. The GGO provided good balance between the global search and local refinement. The GGO is integrated with SFOA to converge faster, escape from local optima, and avoid stagnation. The algorithmic framework of Grey-SGOA is modelled as follows.
\

i) Initialization

At first, the starfish position is created randomly among the boundaries, which is articulated as,

$$Z = \begin{bmatrix} Z_{1,1} & Z_{1,2} & \cdots & Z_{1,u} \\ Z_{2,1} & Z_{2,2} & \cdots & Z_{2,u} \\ \vdots & \vdots & \ddots & \vdots \\ Z_{p,1} & Z_{p,2} & \cdots & Z_{p,u} \end{bmatrix}_{p\times u} \tag{19}$$

In the expression, Z signifies the position of all starfishes saved in matrix form. p indicates population size, and u denotes the design variable dimension. Further, the starfish position is designated by,

$$Z_{k,l} = \lambda_l + R(\upsilon_l - \lambda_l), \quad k = 1,2,3,...,p, \quad k = 1,2,3,...,u \tag{20}$$

here, a random number set to [0,1] is denoted by R, the position of k^{th} starfish at l^{th} dimension is given by $Z_{k,l}$, the upper and lower bounds of design variables are represented as υ_l and λ_l.

ii) Fitness estimation

The equation (11) is the expression of fitness function utilized for estimating the ideal solution.

iii) Exploration phase

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Generally, the starfish utilizes its five arms to search for food sources in the nearby area by embedding eyes at the end of arms. Under certain cases, the search space is extensive, if the dimension is greater than 5, i.e. $I > 5$. In order to guide the movement of arms, basic knowledge of optimal position is required for starfish. Therefore, the updated starfish position is designated as,

$$\begin{cases} Z_{k,m}(q+1) = Z_{k,m}(q) + G_1\left[Z_{BEST,m}(q) - Z_{k,m}(q)\right]\cos\theta, & R \le 0.5 \\ Z_{k,m}(q+1) = Z_{k,m}(q) - G_1\left[Z_{BEST,m}(q) - Z_{k,m}(q)\right]\sin\theta, & R > 0.5 \end{cases} \tag{21}$$

here, $Z_{k,m}(q)$ and $Z_{k,m}(q+1)$ represents current and updated starfish position at q^{th} iteration, $R \in (0,1)$ the best starfish position is given by $Z_{BEST,m}(q)$, $G_1 = (2R-1)\pi$, $\theta = \frac{\pi}{2}.\frac{q}{q_{\max}}$ and m signifies the randomly selected dimensions.

When $R \le 0.5$, the equation (4) becomes,

$$Z_k(q+1) = Z_k(q) + G_1 Z_{BEST}(q)\cos\theta - G_1 Z_k(q)\cos\theta \tag{22}$$

$$Z_k(q+1) = Z_k(q)[1 - G_1\cos\theta] + G_1 Z_{BEST}(q)\cos\theta \tag{23}$$

The GGO [23] is integrated with SFOA [22] to converge quickly for escaping from local optima and avoid stagnation. From GGO,

$$Z_k(q+1) = Z^*(q) - Y\left|\omega.Z^*(q) - Z_k(q)\right| \tag{24}$$

Here, the optimal location of leader at q^{th} iteration is indicated as $Z^*(q)$, $Y = 2mn_1 - m$ and $\omega = 2n_2$, and the values of n_1 and n_2 are changing randomly within the range 0 to 1. Let us consider, $\omega.Z^*(q) > Z_k(q)$

$$Z_k(q+1) = Z^*(q) - Y\omega.Z^*(q) + YZ_k(q) \tag{25}$$

$$Z_k(q) = \frac{Z_k(q+1) - Z^*(q) + Y\omega.Z^*(q)}{Y} \tag{26}$$

By substituting equation (26) in equation (23),

$$Z_k(q+1) = \left(\frac{Z_k(q+1) - Z^*(q) + Y\omega.Z^*(q)}{Y}\right)[1 - G_1\cos\theta] + G_1 Z_{BEST}(q)\cos\theta \tag{27}$$

$$\frac{Z_k(q+1)[Y - 1 + G_1\cos\theta]}{Y} = \frac{\left(Y\omega.Z^*(q) - Z^*(q)\right)[1 - G_1\cos\theta] + Y.G_1 Z_{BEST}(q)\cos\theta}{Y} \tag{28}$$

Hence, the modified equation of Grey-SGOA is given by,

$$Z_k(q+1) = \frac{\left(Y\omega.Z^*(q) - Z^*(q)\right)[1 - G_1\cos\theta] + Y.G_1 Z_{BEST}(q)\cos\theta}{[Y - 1 + G_1\cos\theta]} \tag{29}$$

Furthermore, the starfish position is modified using unidimensional search patterns, if the dimension is more than 5, i.e. $I \le 5$. Hence, the starfish find the food source by using only one arm based on the information of location, where the starfish position is updated and is designated as,

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$Z_{k,m}\left(q+1\right)=\nu Z_{k,m}\left(q\right)+a_1\left[Z_{x_1,m}\left(q\right)-Z_{k,m}\left(q\right)\right]+a_2\left[Z_{x_2,m}\left(q\right)-Z_{k,m}\left(q\right)\right] \quad (30)$$

wherein, ν is the energy of the starfish, $Z_{x_1,m}\left(q\right)$ and $Z_{x_2,m}\left(q\right)$ are the dimensional positions between the starfish selected randomly, a_1 and a_2 are random numbers set to range [-1,1].

iv) Exploitation phase

The regeneration and preying behaviour of starfish is considered in exploitation. Here, the optimal location and the five distances between the other starfish are estimated initially, and then, each starfish position is randomly selected by utilizing a two-directional search strategy. Hence, the preying behaviour is given by,

$$Z_k\left(q+1\right)=Z_k\left(q\right)+R_1\tau_1+R_2\tau_2 \quad (31)$$

where, R_1 and R_2 are the distance selected randomly, the random numbers between [0,1] are given by τ_1 and τ_2. Following this, the regeneration phase is modelled by considering the last starfish in the population, and is given by,

$$Z_k\left(q+1\right)=\exp\left(-q\times F/q_{\max}\right)Z_k\left(q\right) \quad (32)$$

In the expression, $q_{\max}$ is the maximum iteration, and F represents the population size.

v) Fitness re-estimation

The fitness function given in equation (11) is used to identify ideal, and the current solution is replaced if any solution is identified to be superior to the current solution.

vi) Termination

The algorithmic procedure of Grey-SGOA is demonstrated in table 1, where the steps are repeated until getting an ideal solution.

Table 1. Pseudocode of Grey-SGOA

Pseudocode of Grey-SGOA
Input: Size of population, maximum iteration,
Output: Optimal solution
start
Set boundary, information of problem, input parameters, and so on
Compute fitness and initialize positions by utilizing equation (11) and equation (19)
while $\left(q<q_{max}\right)$ do
if $R>H_m$, where the algorithmic parameter is given as H_m
Exploration:
if $I>5$ do
Create five randomly along $m-$ dimension between l
for $l=1:5$ do
Modify position dimension by utilizing equation (29)
end for
Verify the position of boundaries
else

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Create two random numbers a_1 and a_2
Select random dimension m
Modify position $m-$ dimension by utilizing equation (30)
Verify the boundaries of starfish
End if
End for
else
Exploitation:
Find the best position and distance among the starfish
For each starfish ***do***
Determine a random number and modify the position by utilizing equation (31)
for $k = F$ do
Modify the starfish position by utilizing equation (32)
end if
Verify the boundaries of starfish
end if
Estimate the fitness of starfish
Identify global ideal solution
$q = q + 1$
end while
return
end

Therefore, the optimal cluster head is effectively selected in IoT network by Grey-SGOA, where the Grey-SGOA is designed by integrating SFOA [22] and GGO [23]. The Grey-SGOA converges faster to significantly select the honest and reliable nodes as the cluster head from all the available nodes in IoT networks to securely transmit the data packets.

4.3. Secure data aggregation

Secure data aggregation in IoT is the collection of data from multiple sensor nodes and combining them at a certain aggregation point to summarize meaningful information, conserve energy, and minimize the communication overhead. The data aggregation helps to eliminate data redundancies and minimize the total transmitted data before delivering to the sink. The aggregated data reveals sensitive information of users and devices, which also obfuscates the data to protect its privacy. In this paper, the secure data aggregation is performed using MC-GRU [25]. The MC-GRU model mainly comprises Gated Recurrent Unit (GRU) and Multiple Convolutional (MC) layers. The multiple convolutions are utilized by MC-GRU for extracting features and utilize high-level features as input to GRU network for data aggregation. The MC-GRU also comprises a batch normalization layer as well as a pooling layer. The MC layer utilizes multiple convolution kernels and a Convolutional Neural Network (CNN) with three layers to extract features from data σ_R. In MC-GRU, the pooling layer compresses the data obtained from the convolutional layer to increase the processing efficiency and accelerate the convergence of the model. Moreover, the nonlinear expression ability of MC-GRU is increased by batch normalization. After batch normalization layer, an improved GRU layer based on Long Short-Term Memory (LSTM) is utilized to learn features from time series and context in data. Furthermore, the dropout layer is used to minimize the complex coadaptive relationship among the neurons for the removal of a certain proportion of neurons. Following this, the resultant vector feature from the dropout layer is given as input to the

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

dense layer for feature fusion, and the final aggregated data is obtained from the softmax logistic egression layer. The data obtained from all nodes at the cluster head is given as input to MC-GRU and is given by σ_D, where figure 4 displays the architecture of MC-GRU.

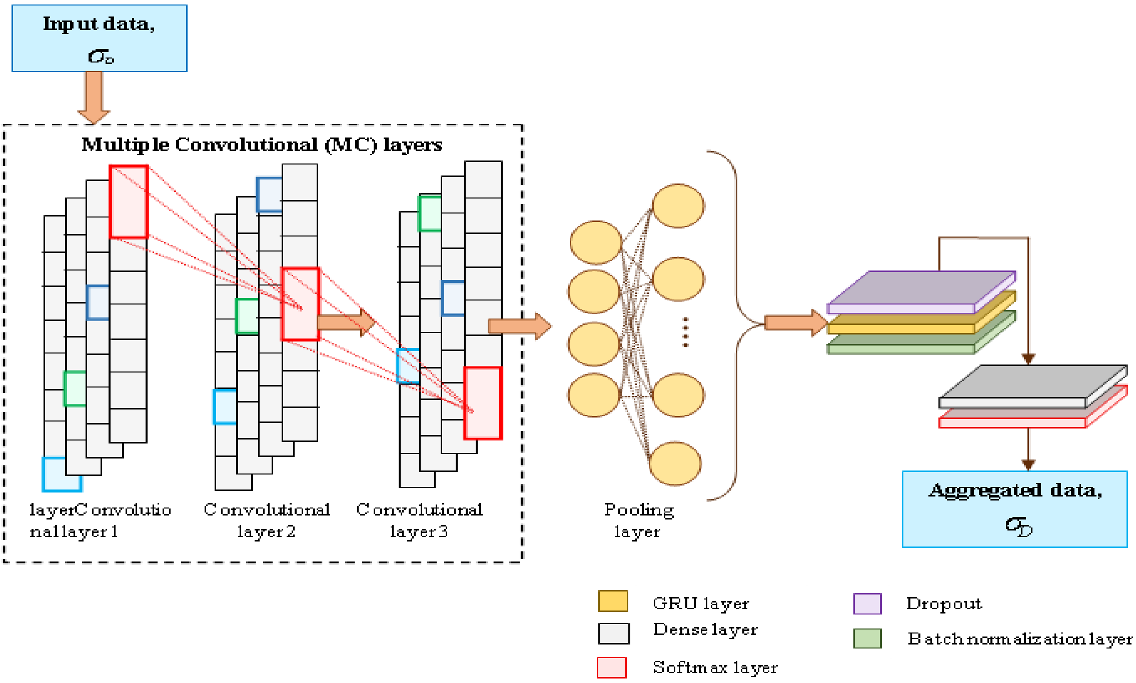


Figure 4. Architecture of MC-GRU

4.4. Data encryption

The aggregated data is encrypted before data transmission once the data is aggregated using MC-GRU. During data encryption, the data is encoded and can be accessed only by authorized parties to protect the transmitted data. The data encryption is used to minimize the total encryption operations and save processing power in nodes with limited resources. Here, the aggregated data σ_D is encrypted using FHE [26]. The FHE is a data encryption method that encrypts sensitive and personal data by managing noise automatically through bootstrapping. Generally, arithmetic operations are enabled by FHE on ciphertexts during encryption in order to preserve the privacy and confidentiality of data. The FHE process the sensitive aggregated data securely before being processed, and the encrypted data is observed clearly by the owner, if a secret key is used to decrypt the data. Thus, the resultant encrypted data obtained by FHE is expressed as,

$$\sigma_E = FHE(\sigma_D, K) \tag{33}$$

where, the encrypted data is given by σ_E, and K indicates key.

4.5. Secure routing

Secure IoT routing is the forwarding of data from source to target. Secure routing is necessary for the protection of data availability, confidentiality, and integrity due to untrusted and resource-constrained IoT environments. Here, the routing is carried out by Grey-SGOA based on various trust factors and fitness parameters. The Grey-SGOA is developed by integrating SFOA [22] and GGO [23]. Moreover, the fitness function and solution encoding are considered, and the process of routing are briefly described below,

4.5.1. Solution encoding

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 5 depicts the solution encoding of Grey-SGOA, where the secure routing in IoT framework is performed considering the index of nodes. Here, a set of nodes is represented randomly from the path using the Grey-SGOA, and the fitness function is used to identify optimal route in IoT.

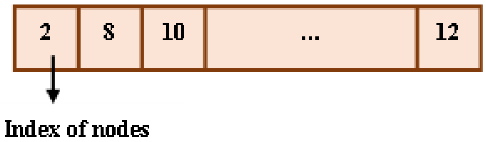


Figure 5. Solution encoding of Grey-SGOA

4.5.2. Designed GreyStar Goose Optimization Algorithm for secure routing

Secure routing is performed to select optimal route for transmitting the encrypted data in IoT networks. The secure routing is performed using Grey-SGOA, where Grey-SGOA is developed by incorporating SFOA [22] and GGO [23]. The SFOA is a designed based on the natural behaviour of starfish, and the GGO is an optimization algorithm developed concerning the natural dynamic and social behaviour of Greylag goose. The incorporation of GGO and SFOA is performed to increase the convergence to escape from local optima and avoid stagnation. The algorithmic steps followed by Grey-SGOA are briefly demonstrated in section 4.2.3. Moreover, the ideal solution is determined by the fitness function, and is given by,

$$fitness = \frac{1}{8}\left[\left(1 - A_1\right) + A_2 + A_3 + A_4 + A_5 + A_6 + A_7 + \left(1 - A_8\right)\right] \quad (34)$$

here, the distance between the nodes is given by A_1.

5. Results and discussion

The effectiveness of Grey-SGOA used for trust-aware and fault-tolerant secure routing in IoT framework is investigated based on different measures by comparing it with prevailing analogous techniques. The details of simulation environment, the outcomes obtained from the experiment, and the analysis executed are detailed as follows.

5.1. Experimental set-up

The Grey-SGOA proposed secure routing in IoT is executed in Ns2 tool with simulation.

5.2. Parameter setting

The experimental parameters of the Grey-SGOA and IoT network are summarized in table 2 and table 3.

Table 2. Experimental parameters of Grey-SGOA

Parameter	**Range**
Population size	100
Alpha	2
Random value	0-1
Beta	1
Upper bound	1
Lower bound	0
Exploration to exploitation	2-0
Iteration	100

Received: August 03, 2025

Table 3. Experimental parameters of IoT framework

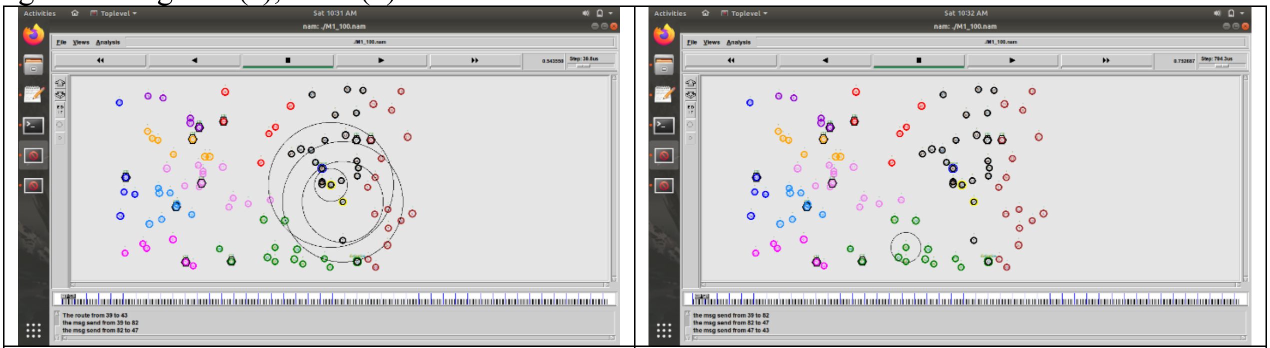
Parameter	Range
Stop time	20
Protocol	MAC protocol
Size of each packet	512 bytes
Time between packets	0.2 sec
Maximum queue length	50
Initial energy per node	10
Reception power consumption	0.1
Transmission power consumption	0.33
Power consumed during idle	0.05
Y-dimension of the simulation area	600
X-dimension of the simulation area	1501
Antenna	Omnidirectional antenna

5.3. Simulation result

This section portrays the simulation outcomes obtained by Grey-SGOA during secure routing for 100 and 150 nodes.

5.3.1 For 100 nodes

Figure 6 shows the simulation outcomes of Grey-SGOA for 100 nodes is delineated. Here, the simulation outcomes obtained by Grey-SGOA at time 39.8 milliseconds (ms) and 794.3 ms are given in Figure 6(a), and 6(b).

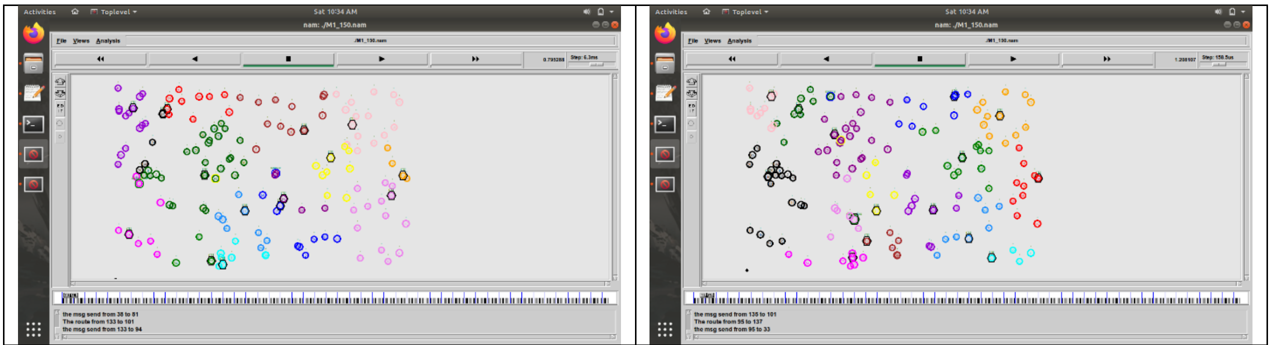


(a) **(b)**

Figure 6. Simulation outcomes of Grey-SGOA at time (a) 39.8 ms (b) 794.3 ms for 100 nodes

5.3.2 For 150 nodes

The simulation results obtained by Grey-SGOA for 150 nodes are given in figure 7, where figure 7(a), and 7(b) delineates the results obtained by Grey-SGOA at time 6.3 ms and 158.5 ms.



(a) **(b)**

Figure 7. Simulation outcomes of Grey-SGOA at time (a) 6.3 ms (b) 158.5 ms for 150 nodes

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.4. Performance indicators

The efficacy of Grey-SGOA is investigated using various measures and is demonstrated as follows,

PDR: PDR is used to estimate the ratio of total received data packets at the target to the total forwarded data packets.

Average residual energy: The average residual energy is the rest over energy of the node, which is computed by estimating the relation among the initial state and baseline. The available energy utilized to transmit data securely is estimated by utilizing the equation (4).

Trust: Trust is used to assess the dependability of data transmitted to sink, which is measured using the equation (15).

Delay: The time utilized by data packets to reach their target is termed delay, where the delay is computed by utilizing equation (18).

Throughput: Throughput is the proportion of total successfully transmitted data packets by the nodes over time, where the throughput is given in equation (16).

Normalized variance: The estimation of dispersion between the perturbed data as well as the actual data is termed normalized variance, which is designated as,

$$Normalized\ \mathrm{var}iance, x = 1 - \frac{1}{1 + y^2(\xi)} \tag{35}$$

In the expression, a random variable is given by ξ, and y represents variance.

Conditional privacy: The total protection provided by Grey-SGOA and the degree of user privacy in the IoT network is Conditional privacy is, which is given by,

$$Conditional\ privacy, z = \prod \left(c|d\right) = 2^{h(c|d)} \tag{36}$$

where, d indicates the information, and c is the describes data.

5.5. Comparative techniques

The supremacy of Grey-SGOA in secure IoT routing is validated by comparing with baseline models, like Gannet Lyrebird Optimization Algorithm+Deep Long Short-Term Memory (GLOA+DLSTM), ICA-HS [1], CW-LEACH [2], CRDA [3], and CEDAR [4].

5.6. Comparative validation

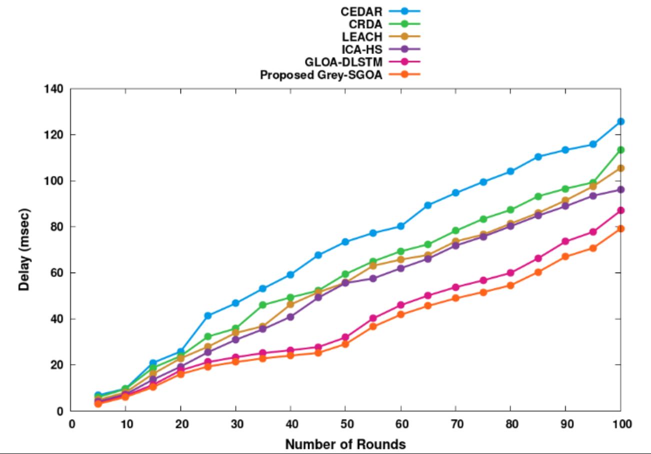
In order to investigate the efficacy of Grey-SGOA, the analysis is carried out for 100 and 150 nodes, and is demonstrated beneath,

5.6.1 For 100 nodes

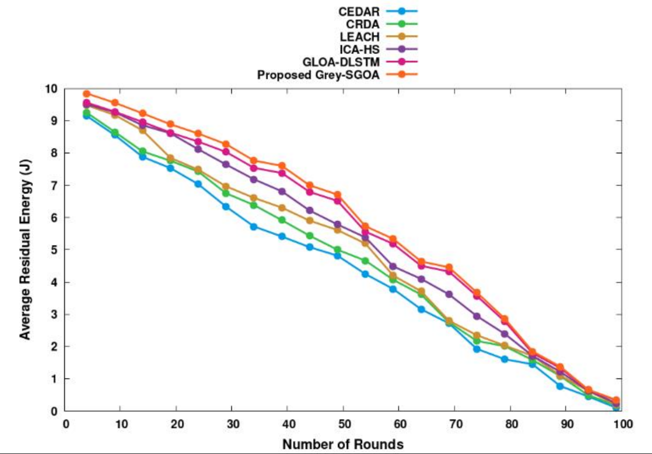
In figure 8, the evaluation of Grey-SGOA employed for secure IoT routing using different indicators for 100 nodes concerning rounds, is illustrated. Initially, the investigation of Grey-SGOA using delay is displayed in figure 8(a). The Grey-SGOA obtained a minimum delay of 80.881 msec for 100 rounds, whereas the delay observed by previous works is 75.613 msec by GLOA+DLSTM, 72.296 msec by ICA-HS, 68.481 msec by CW-LEACH, 63.137 msec by CRDA, and 59.019 msec by CEDAR. Figure 8(b) depicts the valuation of Grey-SGOA by employing average residual energy. The Grey-SGOA obtained 0.276 J of average residual energy and the existing schemes, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR measured average residual energy of 0.268 J, 0.193 J, 0.043 J, 0.042 J, and 0.029 J for 100 rounds. In figure 8(c), the evaluation of Grey-SGOA using PDR is portrayed. The results show that the Grey-SGOA recorded a PDR of 90.046% for 100 rounds, which is better than the PDR observed by other methods, such as GLOA+DLSTM at 87.424%, ICA-HS at 84.563%, CW-LEACH at 82.565%, CRDA at 80.460%, and CEDAR at 73.645%.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

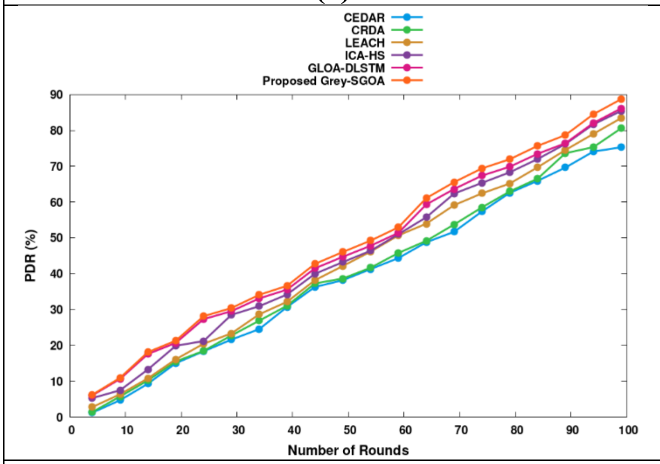
Figure 8(d) shows the analysis of Grey-SGOA utilizing throughput, where the throughput of 143.193 Kbps is yielded by Grey-SGOA for 100 rounds and the throughput observed by existing schemes, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR is 141.29 Kbps, 136.337 Kbps, 133.070 Kbps, 126.493 Kbps, and 113.753 Kbps. Figure 8(e) delineates the validation of Grey-SGOA by means of trust. The trust of 80.454 is obtained by Grey-SGOA for 100 rounds, where the trust recorded by other techniques, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR measured a lower trust value of 78.111, 76.106, 74.362, 69.844, and 65.472. Moreover, the valuation of Grey-SGOA utilizing normalized variance is given in figure 8(f). The normalized variance of 0.008 is obtained by Grey-SGOA for 100 rounds, and the normalized variance measured by previous schemes is 0.017 by GLOA+DLSTM, 0.021 by ICA-HS, 0.290 by CW-LEACH, 0.021 by CRDA, and 0.020 by CEDAR. Further, in figure 8(g), the valuation of Grey-SGOA utilizing conditional privacy is demonstrated. The Grey-SGOA attained conditional privacy of 80.881% for 100 rounds, where the conditional privacy obtained by other methods, namely GLOA+DLSTM is 78.111%, ICA-HS is 76.106%, CW-LEACH is 74.362%, CRDA is 69.844%, and CEDAR is 65.472%.



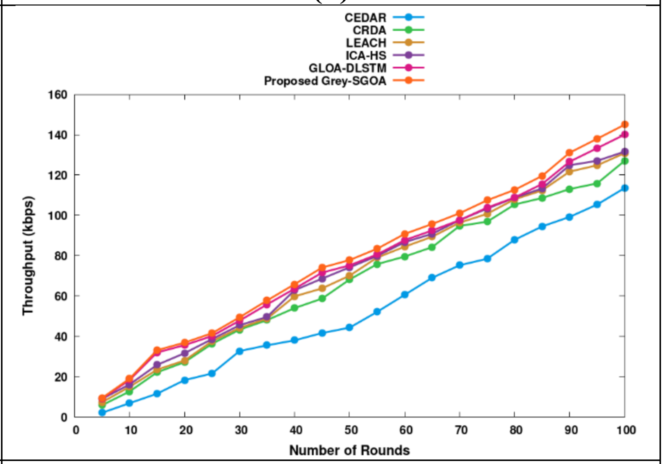
(a)



(b)



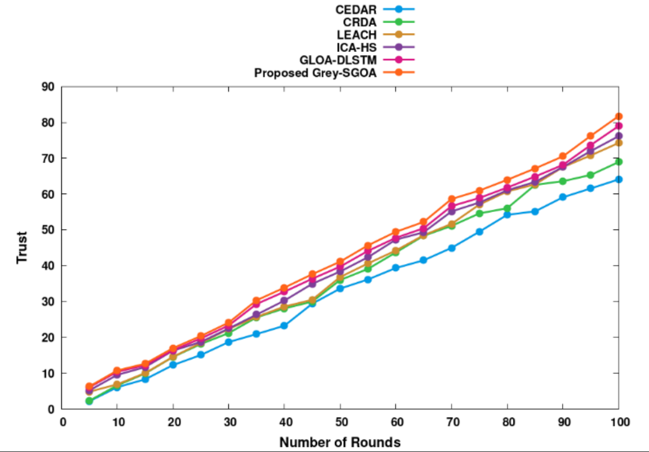
(c)



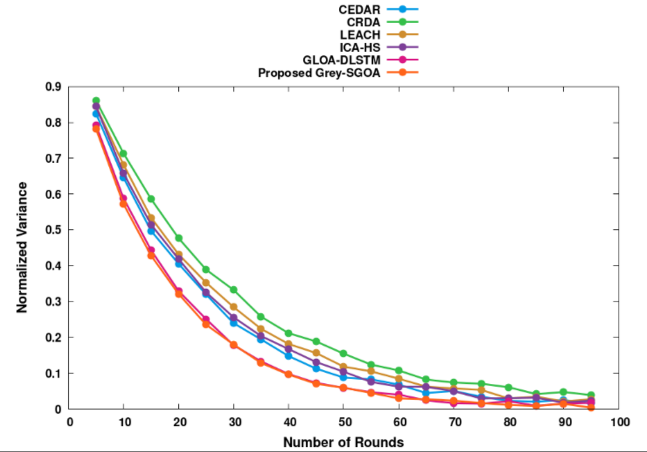
(d)

Received: August 03, 2025

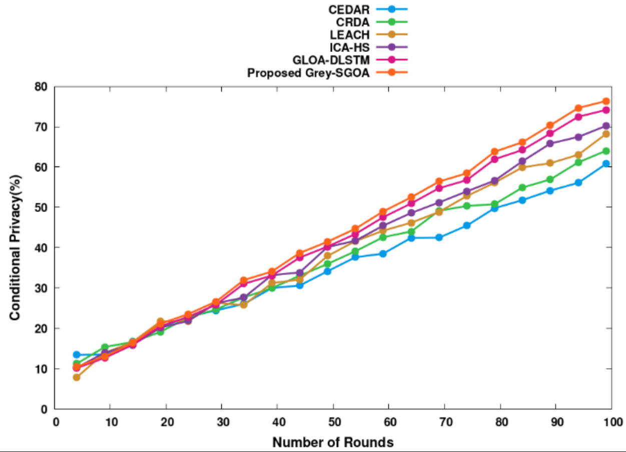
International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)



(e)



(f)



(g)

Figure 8. Investigation of Grey-SGOA (a) Delay, (b) Average residual energy, (c) PDR, (d) Throughput, (e) Trust, (f) Normalized variance, and (g) Conditional Privacy for 100 nodes

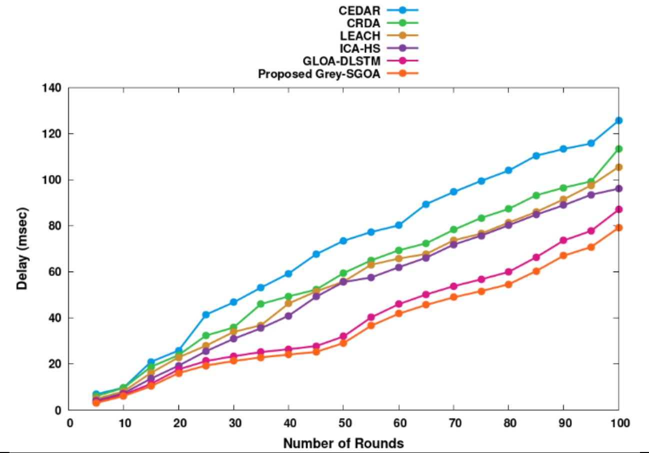
5.6.2. 150 nodes

The comparative investigation of Grey-SGOA by utilizing different metrics for 150 nodes based on the rounds is given in figure 9. The evaluation of Grey-SGOA employing delay is depicted in figure 9(a). The delay of 79.131 msec is observed by Grey-SGOA for 100 rounds, and the delay recorded by baseline schemes is 86.958 msec by GLOA+DLSTM, 96.095 msec by ICA-HS, 105.524 msec by CW-LEACH, 113.458 msec by CRDA, and 125.644 msec by CEDAR. In figure 9(b), the evaluation of Grey-SGOA utilizing average residual energy is demonstrated. The Grey-SGOA attained average residual energy of 0.274 J, where the average residual energy obtained by prevailing schemes, namely GLOA+DLSTM is 0.266 J, ICA-HS is 0.147 J, CW-LEACH is 0.091 J, CRDA is 0.031 J, and CEDAR is 0.022 J for 100 rounds. Figure 9(c) depicts the valuation of Grey-SGOA by employing PDR. The PDR of 89.651% is recorded by Grey-SGOA and the existing schemes, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR measured PDR of 87.040%, 85.630%, 83.718%, 81.140%, and 75.444% for 100 rounds.

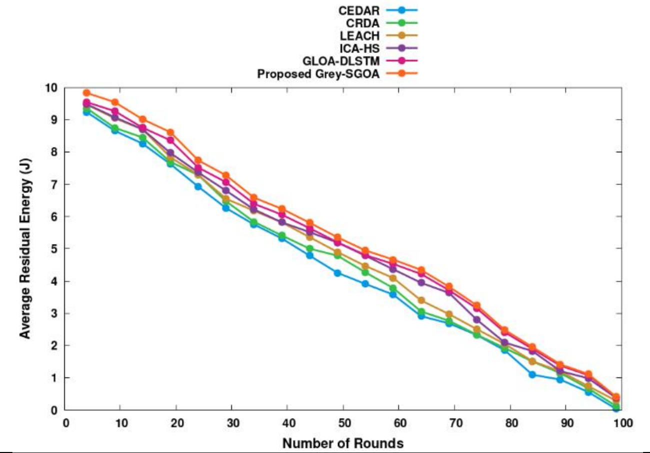
In figure 9(d), the investigation of Grey-SGOA using throughput is portrayed. The results show that the Grey-SGOA yielded throughput of 145.045 kbps for 100 rounds compared to baseline methods. Similarly, the throughput recorded by other methods, such as GLOA+DLSTM is 140.140 kbps, ICA-HS is 131.643 kbps, CW-LEACH is 130.909 kbps, CRDA is 127.132 kbps, and CEDAR is 113.608 kbps. Figure 9(e) shows the analysis of Grey-SGOA utilizing trust, where the trust of 81.739 is yielded by Grey-SGOA, and the trust observed by existing schemes, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR is lower at 78.975, 76.142, 74.247, 68.922, and 64.070

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

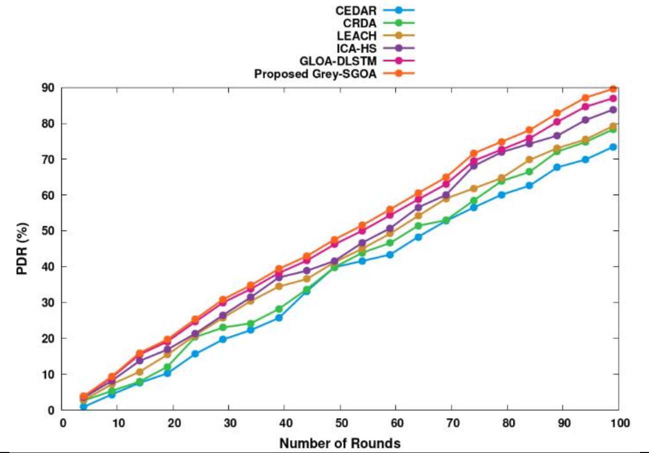
for 100 rounds. The assessment of Grey-SGOA using normalized variance is displayed in figure 9(f). For 100 rounds, the Grey-SGOA obtained normalized variance of 0.008, whereas the normalized variance observed by previous works is 0.005 by GLOA+DLSTM, 0.014 by ICA-HS, 0.020 by CW-LEACH, 0.038 by CRDA, and 0.025 by CEDAR. Additionally, figure 9(g) delineates the validation of Grey-SGOA utilizing conditional privacy. The conditional privacy of 82.428% is attained by Grey-SGOA for 100 rounds, where the conditional privacy recorded by other techniques, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR, is 76.144%, 71.979%, 68.712%, 66.856%, and 60.356%.



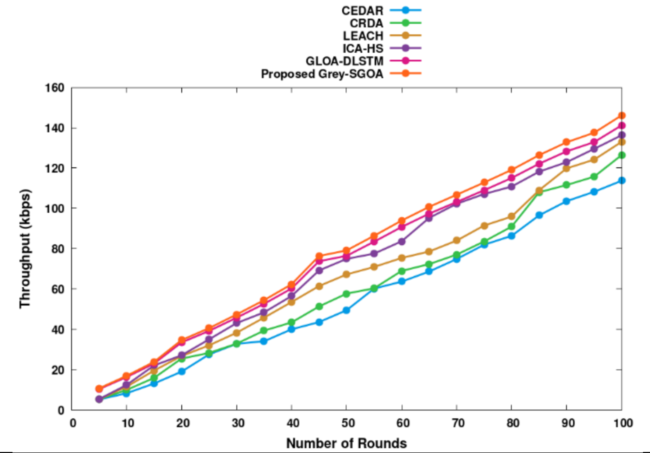
(a)



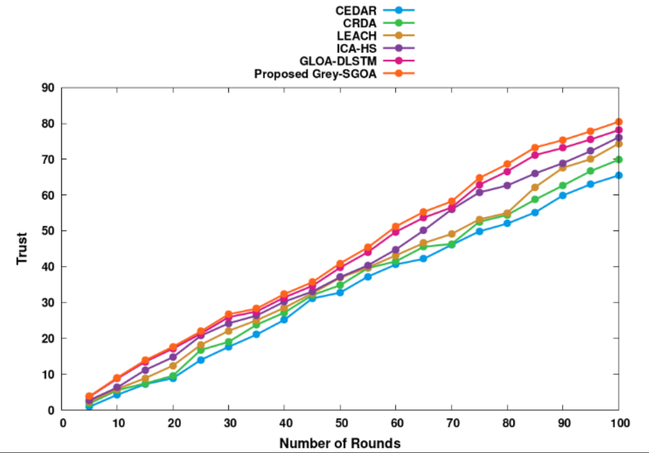
(b)



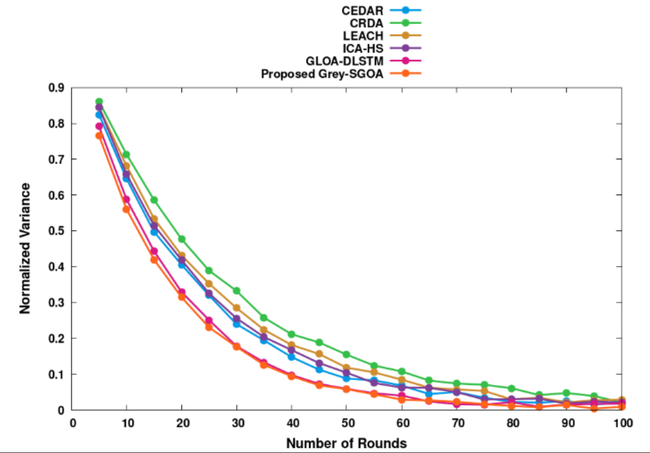
(c)



(d)

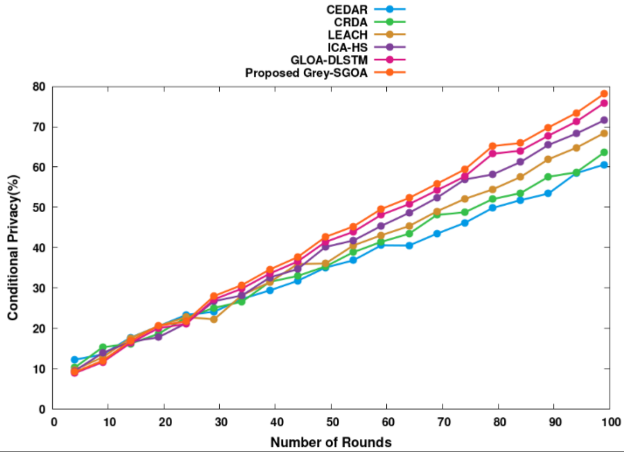


(e)



(f)

Received: August 03, 2025



(g)

Figure 9. Investigation of Grey-SGOA (a) Delay, (b) Average residual energy, (c) PDR, (d) Throughput, (e) Trust, (f) Normalized variance, and (g) Conditional Privacy for 150 nodes

5.7. Comparative discussion

The results recorded by Grey-SGOA and previous works for secure IoT routing for 100 rounds are summarized in Table 4. The results showcase that the Grey-SGOA attained PDR of 89.651%, average residual energy of 0.274 J, trust of 81.739, delay of 79.131 msec, throughput of 145.045 Kbps, conditional privacy of 82.428%, and normalized variance of 0.008. At the same time, the average residual energy obtained by other methods, namely GLOA+DLSTM is 0.266 J, ICA-HS is 0.147 J, CW-LEACH is 0.091 J, CRDA is 0.031 J, and CEDAR is 0.022 J. The delay recorded by baseline schemes is 86.958 msec by GLOA+DLSTM, 96.095 msec by ICA-HS, 105.524 msec by CW-LEACH, 113.458 msec by CRDA, and 125.644 msec by CEDAR. The existing schemes, like GLOA+DLSTM, ICA-HS, CW-LEACH, CRDA, and CEDAR, recorded trust of 78.975, 76.142, 74.247, 68.922, and 64.070. Furthermore, these techniques recorded conditional privacy of 76.144%, 71.979%, 68.712%, 66.856%, and 60.356%. Also, the normalized variance observed by previous works is 0.005 by GLOA+DLSTM, 0.014 by ICA-HS, 0.020 by CW-LEACH, 0.038 by CRDA, and 0.025 by CEDAR. The throughput recorded by other methods, such as GLOA+DLSTM is 140.140 kbps, ICA-HS is 131.643 kbps, CW-LEACH is 130.909 kbps, CRDA is 127.132 kbps, and CEDAR is 113.608 kbps. Overall, the experimental results reveal that the Grey-SGOA is more efficient in performing secure routing in IoT. The Grey-SGOA significantly increases the stability and security by favouring routes with energy-efficient and high-trust nodes. Moreover, the Grey-SGOA selects honest and reliable nodes for secure IoT routing by avoiding central failure to ensure resilient, efficient, and secure routing.

Table 4. Comparative discussion

Measures	**CEDAR**	**CRDA**	**CW-LEACH**	**ICA-HS**	**GLOA+DLSTM**	**Proposed Grey-SGOA**
For 100 nodes						
Conditional Privacy	59.019	63.137	68.481	72.296	75.613	80.881
Throughput (Kbps)	113.753	126.493	133.070	136.337	141.249	146.193
PDR (%)	73.645	80.460	82.565	84.563	87.424	90.046
Average residual	0.029	0.042	0.043	0.193	0.268	0.276

energy (J)						
Normalized variance	0.020	0.021	0.290	0.021	0.017	0.008
Delay (msec)	59.019	63.137	68.481	72.296	75.613	80.8816
Trust	65.472	69.844	74.362	76.106	78.111	80.454
For 150 nodes						
Conditional Privacy (%)	60.356	66.856	68.712	71.979	76.144	***82.428***
Throughput (Kbps)	113.608	127.132	130.909	131.643	140.140	***145.045***
PDR (%)	75.444	81.140	83.718	85.630	87.040	***89.651***
Average residual energy (J)	0.022	0.031	0.091	0.147	0.266	***0.274***
Normalized variance	0.025	0.038	0.020	0.014	0.005	***0.008***
Delay (msec)	125.644	113.458	105.524	96.095	86.958	***79.131***
Trust	64.070	68.922	74.247	76.142	78.975	***81.739***

6. Conclusion

Nowadays, secure IoT routing is crucial in IoT frameworks because of the resource-constrained and dynamically distributed nature of various IoT devices with different capabilities. In this paper, the Grey-SGOA is designed for trust-aware and fault-tolerant secure routing in IoT systems. Here, the system model of IoT network is initially, and then, the clustering is executed by K-Medoids Clustering Algorithm. Later, the optimal cluster head is selected by utilizing the Grey-SGOA based on different fitness parameters as well as trust factors. Then, the data is securely aggregated by MC-GRU, and the aggregated data is encrypted by utilizing FHE. Followed by data encryption, the secure routing in IoT is performed by Grey-SGOA based on multiple fitness parameters. In addition, the supremacy of Grey-SGOA is validated, where the Grey-SGOA yielded superior results with PDR of 89.651%, average residual energy of 0.274 J, trust of 81.739, delay of 79.131 msec, throughput of 145.045 Kbps, conditional privacy of 82.428%, and normalized variance of 0.008. Future research endeavours will focus on the integration of federated learning for making decentralized decision making, and the incorporation of blockchain is worth exploring for enhancing the trust of IoT systems.

Funding
This study received no specific financial support.

Competing interests
The authors declare that they have no competing interests.

Author contributions
Ramakrishna Prasad A L was responsible for the paper's conceptualization, methodology, software, validation, formal analysis, inquiry, resources, data curation, writing-original draft preparation, writing review and editing, and visualisation. The supervision and software administration have been done by Dr. Shiva Murthy G.

Transparency
According to the authors, the paper provides an honest, accurate, and transparent account of the investigation; it does not omit any important aspects of the study; and any planned differences have been clarified. All ethical guidelines were adhered to when authoring this study.

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

References

[1] Sunithanandhini, A., Natarajan, K. and Ramprasath, J., "Optimization of Multi Hop Data Aggregation in Medical Iot Using Trust Based Secure Routing", 2022.

[2] Ravi, G., Das, M.S. and Karmakonda, K., "Energy Efficient Data Aggregation Scheme using Improved LEACH Algorithm for IoT Networks", International Journal of Intelligent Systems and Applications in Engineering, vol.11, no.2s, pp.174-188, 2023.

[3] Ravi, G., Das, M.S. and Karmakonda, K., "Reliable cluster-based data aggregation scheme for IoT network using hybrid deep learning techniques", Measurement: Sensors, vol.27, pp.100744, 2023.

[4] Mohseni, M., Amirghafouri, F. and Pourghebleh, B., "CEDAR: A cluster-based energy-aware data aggregation routing protocol in the internet of things using capuchin search algorithm and fuzzy logic", Peer-to-Peer Networking and Applications, vol.16, no.1, pp.189-209, 2023.

[5] Thangavelu, A. and Rajendran, P., "Energy-Efficient Secure Routing for a Sustainable Heterogeneous IoT Network Management", Sustainability, vol.16, no.11, pp.4756, 2024.

[6] Burange, A.W., Deshmukh, V.M., Thakare, Y.A. and Shelke, N.A., "Safeguarding the Internet of Things: Elevating IoT routing security through trust management excellence", Computer Standards & Interfaces, vol.91, pp.103873, 2025.

[7] Fu, T., Hao, S., Chen, Q., Yan, Z., Liu, H. and Rezaeipanah, A., "An energy-aware secure routing scheme in internet of things networks via two-way trust evaluation", Pervasive and Mobile Computing, vol.105, pp.101995, 2024.

[8] Hasan, A.A., Fang, X., Latif, S. and Iqbal, A., "Context-Aware Trust Prediction for Optimal Routing in Opportunistic IoT Systems", Sensors, vol.25, no.12, pp.3672, 2025.

[9] Hussain, M.Z. and Hanapi, Z.M., "Efficient secure routing mechanisms for the low-powered IoT network: A literature review", Electronics, vol.12, no.3, pp.482, 2023.

[10] Othmen, S., Mansouri, W. and Asklany, S., "Robust and secure routing protocol based on group key management for internet of things systems", Engineering, Technology & Applied Science Research, vol.14, no.3, pp.14402-14410, 2024.

[11] Sharmin, A., Motakabber, S.M.A. and Hashim, A.H.A., "Trust-based Enhanced ACO algorithm for secure routing in IoT", Indonesian Journal of Electrical Engineering and Informatics (IJEEI), vol.12, no,2, pp.344-359, 2024.

[12] Sangeetha, K. and Arulanandam, K., "Adaptive trust-based secure routing protocol with reinforced anomaly detection for IoT networks", International Journal on Smart Sensing and Intelligent Systems, vol.18, no.1, 2025.

[13] Xiao, J., Chang, C., Ma, Y., Yang, C. and Yuan, L., "Secure multi-path routing for Internet of Things based on trust evaluation", Mathematical Biosciences and Engineering, vol.21, no.2, pp.3335-3363, 2024.

[14] Muneeswari, G., Ahilan, A., Rajeshwari, R., Kannan, K. and John Clement Singh, C., "Trust and energy-aware routing protocol for wireless sensor networks based on secure routing", International journal of electrical and computer engineering systems, vol.14, no.9, pp.1015-1022, 2023.

[15] Imam Rahmani, M.K., Mohammed, M., Irshad, R.R., Yasmin, S., Mishra, S., Asopa, P., Islam, A., Ahmad, S. and Ali, A., "Design a secure routing and monitoring framework based on hybrid optimization for IoT-based wireless sensor networks", Journal of Nanoelectronics and Optoelectronics, vol.18, no.3, pp.338-346, 2023.

[16] Pandian, I., Thirugnasambantham, S., Balasubramaniam, K. and Ravichandran, K., "Improving IoT Network Longevity with Attack Repellent Energy (SARE) Algorithm for Energy-Efficient and Secure Routing", Tehnički vjesnik, vol.32, no.3, pp.876-882, 2025.

[17] Onyema, E.M., Suguna, S.K., Sundaravadivazhagan, B., Jhaveri, R.H., Esther, U.N., Deborah, E.C. and Kumari, K.S., "A secure routing protocol for improving the energy efficiency in

wireless sensor network applications for industrial manufacturing", Next Energy, vol7, pp.100219, 2025.
[18] Wang, Y. and Yang, Y., "A novel secure and energy-efficient routing method for the agricultural internet of things using whale optimization algorithm", Journal of Cyber Security and Mobility, vol.13, no.4, pp.725-749, 2024.
[19] Naik, A.C., Awasthi, L.K., Sharma, T.P. and Verma, A., "Enhancing IoT security: A comprehensive exploration of privacy, security measures, and advanced routing solutions", Computer Networks, vol.258, pp.111045, 2025.
[20] Hu, C., Luo, J., Pu, Y., Yu, J., Zhao, R., Huang, H. and Xiang, T., "An efficient privacy-preserving data aggregation scheme for IoT", In Proceedings of Wireless Algorithms, Systems, and Applications: 13th International Conference, WASA 2018, Tianjin, China, June 20-22, 2018, Proceedings, Springer International Publishing, vol.13, pp. 164-176, 2018.
[21] Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O.I., Selvaraj, D. and Abdulsahib, G.M., "A hybrid cross-layer with harris-hawk-optimization-based efficient routing for wireless sensor networks", Symmetry, vol. 15, no. 2, pp.438,2023.
[22] Zhong, C., Li, G., Meng, Z., Li, H., Yildiz, A.R. and Mirjalili, S., "Starfish optimization algorithm (SFOA): a bio-inspired metaheuristic algorithm for global optimization compared with 100 optimizers", Neural Computing and Applications, vol. 37, no. 5, pp.3641-3683, 2025.
[23] Elkenawy, E.S.M., Alhussan, A.A., Khafaga, D.S., Tarek, Z. and Elshewey, A.M., "Greylag goose optimization and multilayer perceptron for enhancing lung cancer classification", Scientific Reports, vol. 14, no. 1, pp.23784, 2024.
[24] Adumbabu, I. and Selvakumar, K., "Energy efficient routing and dynamic cluster head selection using enhanced optimization algorithms for wireless sensor networks", Energies, vol. 15, no. 21, pp.8016, 2022.
[25] Jingjing, Z., Tongyu, Y., Jilin, Z., Guohao, Z., Xuefeng, L. and Xiang, P., "Intrusion Detection Model for Wireless Sensor Networks Based on MC-GRU", Wireless Communications and Mobile Computing, vol. 1, pp.2448010, 2022.
[26] Ebel, A., Garimella, K. and Reagen, B., "Orion: A Fully Homomorphic Encryption Framework for Deep Learning", In Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Vol.2, pp. 734-749, March 2025.
[27] Kumar, M. and Ali, J., "Taylor sailfish optimizer-based deep stacked auto encoder for blackhole attack detection in wireless sensor network", Journal of Web Engineering, vol. 21, no. 3, pp.911-940, 2022.
[28] Khalid, N.A., "Distributed trust-based routing decision making for WSN", Doctoral dissertation, Auckland University of Technology, 2019.
[29] Xia, H., Jia, Z., Li, X., Ju, L. and Sha, E.H.M., "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks, vol.11 no.7, pp.2096-2114, 2013.
[30] Ye, Z., Wen, T., Liu, Z., Song, X. and Fu, C., "An efficient dynamic trust evaluation model for wireless sensor networks", Journal of Sensors, 2017.
[31] Airehrour, D., Gutierrez, J.A. and Ray, S.K., "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things", Future Generation Computer Systems, vol.93, pp.860-876, 2019.