International Journal of Business Data Communications and Networking
Volume 17 • Issue 2

Adaptive-Sunflower-Based Grey Wolf Algorithm for Multipath Routing in IoT Networks

Reena P. Pingale, Sinhgad College of Science, India*
Shinde S. N., CMCS College, India

ABSTRACT

This paper devises a routing method for providing multipath routing in an IoT network. Here the fractional artificial bee colony(FABC) algorithm is devised for initiating the clustering process. Moreover, the multipath routing is performed by the newly devised optimization technique, namely adaptive-sunflower-based grey wolf (adaptive-SFG) optimization technique, which is designed by incorporating adaptive idea in sunflower-based grey wolf technique. In addition, the fitness function is newly devised by considering certain factors that involve context awareness, link lifetime energy, trust, and delay. For the computation of the trust, additional trust factors like direct trust, indirect trust, recent trust, and forwarding rate factor are considered. Thus, the proposed adaptive-SFG algorithm selects the multipath for routing based on the fitness function. Finally, route maintenance is performed to ensure routing without link breakage. The proposed adaptive-SFG outperformed other methods with high energy of0.185J minimal delay of 0.765 sec maximum throughput of 47.690% and maximum network lifetime of 98.7%.

KEYWORDS

Clustering, Internet of Things, Multipath Routing, Route Maintenance, Trust

1. INTRODUCTION

The advancement in the internet has progressed quickly in ancient times, devising several applications, including transport, entertainment, industry, and education. In these years, several services, devices, and protocols are designed wherein the internet grew exponentially. The upcoming worldwide network is IoT, in which a huge number of things are part of the internet that can devise novel opportunities. The things like identification of radio frequencies, sensor nodes, and wireless gadgets interact with each other and with the classical network to offer futuristic applications and create various solutions for addressing the research communities (Kharrufa, et.al., 2019). IoT overlaid path for devices with less power to befall component of the network and donate to compilation and data swap to meet the deployed models' needs. The exploitation of these models transfigured information exchange and tasks in different domains, including monitoring health and the environment. Thus, energy-aware routing is most important for IoT applications (Safara, et.al., 2020). The energy consumption is more significant for the IoT applications because 50% of energy consumption is by heating effect; 80% is from houses. Hence, energy efficiency is considered an important aspect in IoT applications (Metallidou, et al., 2020). Besides, the security plays an important role in the IoT applications. Hence, for secure data-sharing, a suitable authentication mechanism is necessary (Saxena, et al., 2021). The

DOI: 10.4018/IJBDCN.286699 *Corresponding Author

majority of IoT applications focused on scrutinizing discrete events which produce a huge amount of data. Sensors help to provide a secure connection between the devices for the data transmission (Bhushan, et al., 2021). The huge IoT applications utilized wireless networks for data transformation and communication, which confront security related issues (Souri & Norouzi, 2019). Besides, with the help of a unique identifier, the data can be accessed without human intervention (Sethi, et al., 2020), but privacy issues exist (Saxena, et al., 2021).

For IoT networks, the minimization of power usage and less delay is imperative to facilitate efficient transmissions. The small world's features represent that the count of hops is minimized by adding shortcuts in the network. The features of the world, the less-power devices can exchange data by minimal hops to save energy and simultaneously can minimize the overall delay. Hence, it is important to devise IoT routing methods controlling the small world features (Jiang, et.al., 2019). Multipath routing is more effective than presently utilized routing methods. It can minimize congestion by deviating traffic on unexploited networks, improving network utilization, and balancing loads (Iyer, et.al., 2002). The multipath routing protocols aimed to send data using different paths and provide communication that provides load balancing and reliability for minimal energy consumption (Dhumane & Prasad, 2018). For routing, the congested links resulted in reduced performance and high variance. The routing with different paths can provide stable and smoother data (Bertsekas & Gallager, 1992). The techniques based on multipath routing splitted traffic between provided paths and examined in flow control. The choice of routing poses several impacts on the resultant's efficiency. Even though several flow-control techniques are used for routing, but its performance is altered with different path sets (Banner & Orda, 2007).

The routing method is splitted into two parts, namely braided and disjoints multipath routing. In disjoint multipath routing (Yadav, 2016), there is no connection between subsequent routes, whereas other multipath routing poses no disjoint paths. The multiple disjoint paths are categorized into two kinds, named node-disjoint multipath that failed to share nodes amongst paths, and the other is link-disjoint multipath which shares nodes (Kumar & Kumar, 2016). In (Liu, et.al., 2012), a technique is devised to address optimization issues using a secret-sharing-based multipath routing method. The method is implemented to offer security in-network and lifetime when fed to energy-related issues. However, the method failed to solve delay and packet loss, which can degrade routing performance. In (Teo, et.al., 2008), a method is devised for analyzing the path quality for load balancing using impacts of wireless interferences, which may hinder offering communication. Moreover, Interference-Minimized Multipath Routing (I2MR) protocol is devised for discovering zone-disjoint paths to perform load balancing that needs reduced localization support for maximizing throughput. In (Rahat, et.al., 2016), a multi-objective-based evolutionary technique is devised for determining different routes that estimate balance among a lifetime of network and strength. In this method, the issue is that evaluation is done using linear models for the battery.

The research aims to perform multipath data transmission using a newly devised optimization algorithm, namely Adaptive SFG. Initially, the IoT nodes are simulated, and the selection of cluster head and multipath routing is performed. Here, clustering is performed using the FGSA algorithm. The obtained clusters are employed to transmit data using different paths, which is achieved by the proposed Adaptive SFG and is devised by combining adaptive concepts with the SFG algorithm. The routes are produced to transmit data from source to base station considering certain factors that involve context awareness, link lifetime, Energy, Trust, and Delay in the fitness function. The routes generated using the proposed Adaptive SFG for multipath data transmission are effective regarding energy, trust, and link lifetime. Finally, route maintenance is done to ensure routing without link breakage.

The key contribution of the paper is:

- **Proposed Adaptive SFG for multipath routing:** Devise novel routing strategy, namely Adaptive SFG, by incorporating adaptive idea in SFG for performing multipath data transmission in IoT network.

- **Fitness function to select the best path:** The fitness function offers energy-effective routes for multipath data transmission using certain objectives that include Context awareness, link lifetime, Energy, Trust, and Delay.

2. MOTIVATIONS

The majority of protocols failed to employ node status or intermediate nodes like congestion or an estimated lifetime in the node. Moreover, the network must have adequate energy for handling the transmission of data and routing information from source to target node. However, the selection criterion to enhance link lifetime and QoS attributes in multipath is complex. Thus, the issue mentioned above and conventional methods' challenges are considered motivations for devising novel multipath techniques.

2.1. Literature Survey

The eight classical multipath routing techniques are devised with their benefits and issues. Chen, et.al., 2016 devised Multipath Planning for Single-Source-based transmissions routing (MPSS) method that formed enviable multiple route paths using B-spline trajectories with inter-path distance and the sink node. The method utilized hop distance to minimize cumulative error to assure QoS needs. In addition, Multipath Planning with Multi-Source (MPMS) was adapted to satisfy QoS requirements by offering high energy savings. However, less network time was spotted that may degrade the performance of the network. Jabbar, et.al., 2018 devised hybrid multipath energy with QoS-aware optimized link-state routing protocol (MEQSA-OLSRv2) to form multipath routing in the network. This method utilized the rank of the node using different rank metrics. Here, different parameters are accumulated based on QoS and energy to minimize the complexity of different constrained nodes. The method adapted a multipoint relay (MPR) set to select the energy. Al-Turjman, 2017 devised an agile data delivery model and used applications for smart cities, in which the multimedia data was transmitted. Here, an optimized routing technique was devised for operating resources using dynamic topologies. The technique specified paths in which a data packet determined optimal resource usage by fulfilling the QoS constraints. However, the method failed to address the issues of huge-scale routing. Dhumane & Prasad, 2019 designed a multiobjective fractional gravitational search algorithm for determining the optimum cluster head. The Fractional Gravitational Search Algorithm (FGSA) was devised to determine the optimal cluster head node. Here, the cluster head was selected in FGSA, computed by fitness that considered different parameters, like link lifetime, distance, energy, and delay. The method extended nodes lifetime with the huge number of alive nodes and high network energy. However, the method required a long transmission range. Deebak & Al-Turjman, 2020 devised a two-fish (TF) symmetric key approach to find antagonists in the global sensor network. The method is devised using the Authentication and Encryption Model (ATE). Here, the sensor guard nodes are chosen with Eligibility Weight Function (EWF) using a complicated symmetric key method. Moreover, the secure hybrid routing protocol is chosen for inheriting the features of Ad hoc On-Demand Multipath Distance Vector (AOMDV) and Multipath Optimized Link State Routing (OLSR). However, the method failed to include IoT-based WSNs for authentication. Jaiswal & Anand, 2019 devised an effective routing protocol that enhanced network performance and improved service quality. Here, an energy-effective routing method was devised for IoT, which chooses the optimal transmission path. The method employed three factors for choosing the optimum path, which includes traffic intensity and reliability. The method poses improved scalability as compared to other protocols. However, the method did not include a cluster-based routing protocol for optimizing parameters of QoS. Kim, et.al., 2020 devised a routing method for facilitating cooperation amongst the paths considering a bright node. The nodes monitor the transmission of a packet on paths, which helps recover the issues involving delay and transmission failure. The multipath resists the cooperation through inter path communication considering bridge node. Hence, the method attained reliability at WSN, considering

lesser paths. The method attained less delay packet delivery and was more reliable. Dhumane & Prasad, 2018 devised an effective routing method, namely Fractional Gravitational Grey Wolf Optimization (FGGWO), to transmit data from different paths. The method established multiple paths considering the clustering method. The method enhanced the routing process using two steps. The first step was to choose the cluster heads using the Fractional Gravitational Search Algorithm (FGSA). The next step was multipath generation using the proposed FGGWO, which combines FGSA and Grey Wolf Optimizer. The method utilized an objective function that considers certain factors that involve intra-cluster distance, energy, link-lifetime, inter-cluster distance, and delay to offer optimal paths for transmission. (Anand, et al., 2021) devised IoT-based secure and energy-efficient scheme using the blockchain and Improved leach algorithm. The energy consumption improved Low-energy adaptive clustering hierarchy (LEACH) algorithm is used for efficient data transmission. They achieved better throughput, but they failed to analyze the energy consumption by considering the sensor nodes. (Bhushan and Sahoo, 2019) developed an acknowledgment-based routing protocol with rechargeable sensors. In this, energy-efficient secured ring routing (E2SR2) protocol is used to load balancing based routing with an improved network's improved lifetime. They achieved enhanced performance in identifying the misbehavior of the routing but failed to prevent all the attacks. (Rajesh, et al., 2020) developed fuzzy genetic-based dynamic spectrum allocation (FGDSA). The FGDSA is devised to use the channel without any interference. They achieved average utilization of the channel. The drawback of the system is that it evaluates only the optimization rules. (Bhushan & Sahoo, 2020) developed an Intelligent and secure fuzzy clustering algorithm using the balanced load subcluster formation. In this, fuzzy-based clustering is developed, and efficient routing with a better lifetime of the network is obtained, but the priority transmission is not applicable. (Somauroo & Bassoo, 2020) developed chain-based protocol for cluster head (CH) selection. Power Efficient Gathering in Sensor Information Systems (PEGASIS) is used for the CH selection using the rotation policy. They achieved energy-efficient routing. The clustering is not efficient.

2.2. Challenges

The issues confronted by conventional multipath routing techniques are devised below:

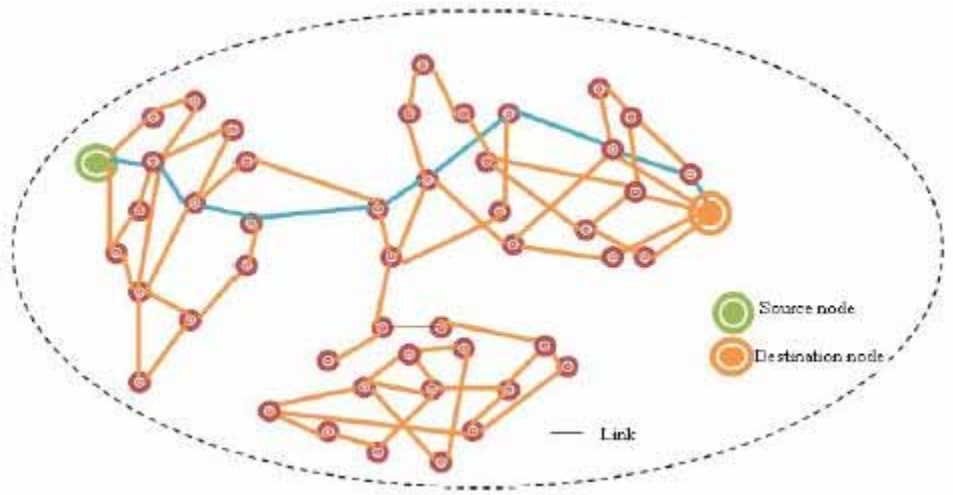
- The industries and organizations continuously offer security to IoT sensor networks. These aspects are responsible for avoiding data catastrophe on IoT users. However, the catastrophe condition is susceptible to complicated communication networks, leading to multifaceted communication (Deebak & Al-Turjman, 2020).
- The development of an effective and resourceful communication protocol for IoT may produce several issues that involve limited resources and the unreliability of low-power wireless links (Jaiswal & Anand, 2019).
- Several routing techniques are devised for IoT, which is capable of attaining reliability on IoT applications. However, these methods pose energy constraints and may degrade the performance of IoT's services (Kim, et.al., 2020).
- In (Dhumane & Prasad, 2018), FGGWO is devised for multipath data transmission in IoT networks. Here, the method carries out a clustering process with FGSA. However, the determination of cluster heads from clusters in the unbalanced platform is a major issue. Moreover, the need for energy and bandwidth raise for multipath data transmission.
- Many routing techniques are devised for facilitating multipath routing in the IoT network. However, the network configuration for performing IoTs services may not offer adequate resources for devising multipath. Subsequently, these constraints may cause degradation in performance.

3. SYSTEM MODEL OF IOT NETWORK

This section portrays the system model of an IoT that acquires the standard behavior of IoT devices and services to establish effective communication amongst the devices. IoT comprises different objects that include smart devices associated with each other to exchange the acquired data in the network. The smart devices in IoT are resource-constrained, which holds communication and processing abilities to exchange data. In the IoT, the IoT nodes are connected to the network with a gateway node to establish effective data transmission on the nodes. Hence, data transmission is an effective part of the network that inspires an effective trust-based routing in an IoT network.

Assume an IoT model comprises A IoT nodes in which each IoT node k holds a set of data points ∂_f. Here each IoT nodes endeavor to find efficient paths for initiating multipath routing. Moreover, each IoT node is used for evaluating energy, trust, and link lifetime. Figure 1 depicts the model of IoT, in which nodes are interlinked with each other to establish communication amongst nodes.

Figure 1. Model of IoT



3.1. Energy Model in IoT

The energy model (Chen, et.al., 2015) in IoT is illustrated considering data transmission from different nodes. The IoT holds several distributed sensors that operate with batteries so that the increasing count of rounds may drain energy, thereby affecting network lifetime. Consider starting nodes energy be given by ε_0 which specifies that batteries are non-rechargeable. When the transmitter receives data, little energy is lost and depends on communication distance. The network transmission is done with protocol and energy dissipation considering occurrence of radio electronics and power amplifier accessible in transmitter. Hence, it is noted that lots of energy is dissipated while transmitting data considering distance and node's nature. When normal sensor node sends g bits of data packet then the energy model for the IoT network is given as,

$$\varepsilon_d(g) = \varepsilon_c(g) + \varepsilon_b(g,a) \tag{1}$$

where, $\varepsilon_d(g)$ indicates transmitted energy, ε_b signifies consumed energy whenever node transmits 1-bit data, ε_c symbolizes consumed energy when the node receives and sends 1-bit data, a signifies communication distance, and g represents data bits.

$$\varepsilon_d(g) = \begin{cases} g \times \varepsilon_c + g \times \varepsilon_h \times a^2; \; if \;\; a \le a_0 \\ g \times \varepsilon_c + g \times \varepsilon_k \times a^4; \; if \;\; a > a_0 \end{cases} \tag{2}$$

where, ε_c signifies the consumed energy whenever node transmits 1-bit data in free space model, ε_h symbolizes the consumed energy whenever node transmits 1-bit data in multipath fading model.

$$a_0 = \sqrt{\frac{\varepsilon_h}{\varepsilon_c}} \tag{3}$$

In the multipath fading model, the receiver receives the signal from various paths. Thus, phase distortion and symbol interference occur, while in free space, a straight path is maintained, and the loss and energy consumption is reduced. When the radius of the transmission network less or equal to a_0 then all the nodes in the network satisfy the free space communication, and hence the energy consumption is reduced, and efficient transmission is achieved.

The energy utilized by sensor nodes to receive g bits of data is expressed as,

$$\varepsilon_e(g) = g \times \varepsilon_c \tag{4}$$

where, $\varepsilon_e(g)$ signifies received energy.

$$E = \varepsilon_d + \varepsilon_e \tag{5}$$

3.2. Link Lifetime Model

LLT (Balachandra, et.al., 2014) represents the lifetime of network links that link two sensor nodes until the data packet exists in the IoT network. However, the breakage of network links may lead to routing failure that may arise in the IoT network. For reducing the link failure effect, the routing protocol evaluates the lifespan of network link. The lifespan of the network link is evaluated using certain factors that involve certain factors like the direction of mobility, nodes coordination, and mobility of nodes. Assume D_1 and D_2 represent two mobile nodes positioned at E_{D1}, F_{D1} and E_{D2}, F_{D2} for which the LLT is evaluated as

$$LLT = \frac{-\left(mn + pq\right) + \sqrt{\left(m^2 + q^2\right)l^2 - \left(mq - pn\right)^2}}{\left(m^2 + q^2\right)} \tag{6}$$

such that, $m = C_{D1}\cos\theta_{D1} - C_{D2}\cos\theta_{D2}$,

$n = E_{D1} - E_{D2}$,

$$p = C_{D1}\sin\theta_{D1} - C_{D2}\sin\theta_{D2} \tag{7}$$

$q = F_{D1} - F_{D2}$

where, l represent transmission range, C_{D1} signifies mobility speed of sensor node D_1, C_{D2} symbolizes mobility speed of sensor node D_2, E_{D2}, F_{D2} represents coordinate of node D_2, E_{D1}, F_{D1} signifies coordinate of node D_1, θ_{D1} signifies the direction of motion of node D_1, and θ_{D2} represents the direction of motion in node D_2.

3.3. Trust Model

The trust model offers privacy in the proposed model to establish trust-based data transmission. The trust factor of all IoT nodes is evaluated to compute a group of trusted nodes. Hence, the trust is adapted to discover trusted nodes and is expressed based on four factors, namely direct trust, recent trust, indirect trust, and forwarding rate factors, and is formulated as,

$$T = \frac{1}{4}\sum_{k=1}^{A} DT + IT + RT + FRF \tag{7}$$

where, DT signifies direct trust, IT symbolizes indirect trust, RT represent recent trust, and FRF symbolizes forwarding rate factor.

3.3.1. Direct Trust

The direct trust (Chen, et.al., 2015) is also named local trust based on approval existing in node interactions. The direct trust between a node b on path s is devised using consistency factor, sending rate factor, and packet loss rate factor. When the node b feels satisfied with the path s then, the satisfaction degree becomes high that renders a local trust. The direct trust is devised based on consistency factor, sending rate factor, and the packet loss rate factor between the node and path, which is represented as,

$$T^{s}_{r,t}(u) = (1-\eta) * B_{r,t}(u) * G_{r,t}(u) * H_{r,t}(u) + \eta * T^{s}_{r,t}(u-1) \tag{8}$$

where, $B_{r,t}(u)$ symbolize sending rate factor, $G_{r,t}(u)$ signifies consistency factor, $H_{r,t}(u)$ represent packet loss rate factor, and η indicate constant-coefficient ranging between 0 to 1. The value $T^{s}_{r,t}(u)$ varies from 0 to 1. Thus, $T^{s}_{r,t}(u) = 0$ represent that node is abnormal and untrusted to initiate communication, whereas if $T^{s}_{r,t}(u) = 1$ then, the node is normal and is trusted to initiate communication. The evaluating node r observes sending capacity of the path t. If the number tends to less than the lower limit threshold I_j, then the node is known as selfish node; else, if the count is more than the

upper limit threshold, then the node has performed an attack. The formula of sending rate factor is formulated as,

$$B_{r,t}(u) = \begin{cases} \dfrac{J_{r,t}(u) - I_j}{\exp_{r,t}(u) - I_j}; B_{r,t}(u) \le \exp_{r,t}(u) \\ \dfrac{I_\ell - J_{r,t}(u)}{I_\ell - \exp_{r,t}(u)}; B_{r,t}(u) > \exp_{r,t}(u) \end{cases} \tag{9}$$

where, $J_{r,t}(u)$ represent quantity sending of the period u, $\exp_{r,t}(u)$ represent expected quantity sending of the period u, $I_j = 300$, $I_\ell = 700$, and $\exp_{r,t}(u) = 500$. The evaluating node r monitors the path t, and the node r compares data accumulation by itself with data collection by the path t. If the difference between data is in range, then evaluating node r has a consistent opinion about the path t. The consistency factor is represented as,

$$G_{r,t}(u) = \frac{K_{r,t}(u)}{K_{r,t}(u) + K'_{r,t}(u)} \tag{10}$$

where, $K_{r,t}(u)$ indicate the count of nodes with the similar packet and evaluated node, and $K'_{r,t}(u)$ signifies the count of the inconsistent packet. The energy of nodes is lesser in IoT due to battery constraints in IoT nodes. Some nodes cannot communicate with BS and need other nodes as a relay node to transmit data to BS using a multihop topology. The packet drop probability contains packet transmission that causes information loss. The packet loss rate factor is formulated as,

$$H_{r,t}(u) = \frac{L(u)}{M(u)} \tag{11}$$

where, $L(u)$ symbolize quantity of all transmitted packets, and $M(u)$ represent the quantity of received packet.

3.3.2. Indirect Trust

$$T^I_{r,t}(u) = fun(T^s_{r,t}(u), T^s_{o,t}(u)) \tag{12}$$

where, $T^s_{r,t}(u)$ symbolize direct trust value of r^{th} node in t^{th} path, $T^s_{o,t}(u)$ signifies direct trust value of o^{th} node in t^{th} path, $fun(.)$ is discovered considering network needs and is expressed as,

$$fun(.) = \rho * T^s_{r,t}(u) + \gamma * T^s_{o,t}(u) \tag{13}$$

where, ρ and γ is determined based on the network.

3.3.3. Recent Trust

The recent trust (Das & Islam, 2011) is utilized to describe recent trust model behaviors. It is weighted of indirect and direct trust. Here, the direct trust is provided with more weight as evaluating agent carries out more communication with the target agent that is valuator and terms to be more confident about its own experience than taking suggestions from others. Assume $RT_n^t(p,q)$ indicate recent trust that agent p poses on agent q and is formulated as,

$$RT_u(r,t) = \beta \times T_u^s(r,t) + (1-\beta) \times T_u^I(r,t) \tag{14}$$

Where, β signifies direct trust weight and is computed as,

$$\beta = \frac{P^i(r,t)}{P^i(r,t) + Q^i(r,t)} \tag{15}$$

Where, $P^i(r,t)$ signifies count of interactions that node r conducted with path t and $Q^i(r,t)$ symbolize the mean number of interactions with other agents

3.3.4. Forwarding Rate Factor

The nodes in IoT pose a lesser amount of energy which is relayed by sensing and transmitting data. Hence, the forwarding rate factor (Zhu, 2018) is formulated as,

$$N_{\upsilon,\kappa}(\hbar) = \frac{\beta_{\upsilon,\kappa}(\hbar)}{\mu_{\upsilon,\kappa}(\hbar)} \tag{16}$$

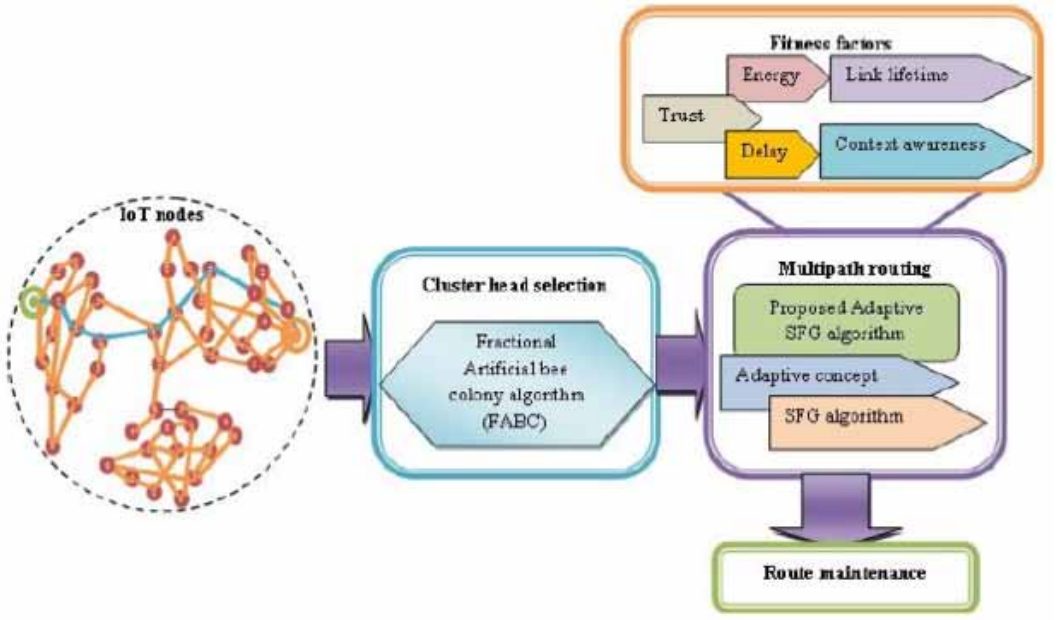
where, $\beta_{\upsilon,\kappa}(\hbar)$ signifies count of feedback packets, $\mu_{\upsilon,\kappa}(\hbar)$ symbolizes count of packets to forward.

4. PROPOSED ADAPTIVE-SFG FOR MULTIPATH ROUTING

Nowadays, the multipath routing method is spotted as an effective method to improve the Quality of Service (QoS) in IoT networks. Several techniques are carried out for multipath routing, but the impacts of inter-path interference and forming low-interference paths are expensive. Even though the energy based problems are considered for designing the protocol, the properties of the wireless link and their impacts on performance are ignored. The goal is to devise a routing protocol using the Adaptive SFG algorithm to improve the network's lifetime. Initially, IoT is simulated, and there exist two major steps that involve selecting optimal cluster head and multipath routing. The FABC (Kumar & Kumar, 2016) algorithm is utilized to select cluster heads. The routing protocol is devised based on the Adaptive SFG algorithm. Moreover, the Adaptive SFG algorithm selects multipath for routing using multiple objectives that include multiple factors, such as Context awareness, link lifetime, Energy, Trust, and Delay. For the computation of the trust, various trust factors like direct trust, recent trust, indirect trust, and forwarding rate factor are considered. The multipath routing occurs in the IoT network through routing wherein the optimal path is selected using the Adaptive-SFG. The proposed Adaptive-SFG is the combination of adaptive ideas with SFG, wherein the SFG combines SFO (Gomes, et.al., 2019) and GWO (Gao & Zhao, 2019). Hence, the proposed Adaptive-

SFG is responsible for the selection of optimal routes. Finally, route maintenance is done to facilitate routing without link breakage. Figure 2 represents the architecture of the multipath routing model with the proposed Adaptive-SFG.

Figure 2. Schematic view of proposed Adaptive-SFG algorithm for multipath routing



4.1. Selection of Efficient Cluster Heads Using FABC Algorithm

The selection of cluster head is essential in IoT as it assists in sending data between IoT nodes. The selection of cluster heads is essential for transmitting data between the nodes to establish communication. The cluster head is chosen optimally using energy and location. The cluster head is chosen optimally in the IoT network amongst nodes to evaluate each node's energy utilization. Here, the cluster head is selected using the FABC algorithm. The FABC (Kumar & Kumar, 2016) algorithm is employed for initiating cluster head to transfer the collected data to the target node. The FABC is designed by incorporating FC in the ABC algorithm. FC (Pires, et.al., 2010) is termed an expansion of classical mathematics and is adapted for optimal computing solutions from prior iterations and evaluated to update solutions from the current iteration. Meanwhile, ABC (Karaboga, et.al., 2012) is an evolutionary technique devised by the motivation of intelligent foraging behavior. Thus, the incorporation of FC and ABC is done to enhance solution search space. Thus, the FABC assists in solving exploration and exploitation issues and provides improved usage of global information. The algorithmic steps of the FABC algorithm for cluster head selection are illustrated below:

Step 1: Initialization

Consider X_R be a food source initialized randomly, and the food source size is assumed as $X_R \times g$. The values of the integer are filled in the matrices in a random manner ranging between 1

to p. Here, IoT nodes are deployed in the network, and energy is initialized to all nodes. The information of the location with each node is known to sink node for performing routing.

Step 2: Employed bee

In FABC, the sources of food are encoded, and each attribute of the food source is represented as the sensor node index, and the length of the food source is assumed to be the count of cluster head in IoT. The food source for the first half of the colony is updated with the bee phase, and the production of the new bee phase is done using ABC (Karaboga, et.al., 2012) using the equation is given as,

$$X_{u,v}^{s+1} = X_{u,v}^{s} + Z_{u,v}\left(X_{u,v}^{s} - X_{l}, v\right) \tag{17}$$

where, $X_{u,v}^{s}$ indicates u^{th} food source of v^{th} value in s^{th} iteration, $Z_{u,v}$ indicates random value in [-1,1], $u \in \{1,2,\ldots,g\}$ and l symbolize index of neighbour such that $l \in \{1,2,\ldots,X_{R}\}$.

After rearranging original food source to improve solution derivative order, the obtained equation is represented as,

$$X_{u,v}^{s+1} - X_{u,v}^{s} = Z_{u,v}\left(X_{u,v}^{s} - X_{l}, v\right) \tag{18}$$

Here, $X_{u,v}^{s+!}$ signifies discrete version of derivative with order $\alpha_{X} = 1$ is represented as,

$$D^{\alpha_{Q}}\left[X_{u,v}^{s+1}\right] = Z_{u,v}\left(X_{u,v}^{s} - X_{l}, v\right) \tag{19}$$

The order of food source is modeled in a real number if the FC (Pires, et.al., 2010) perception is adapted, which results in the smooth variation and long memory effects. Thus, the equation mentioned above is obtained by assuming two terms of differential derivatives and is formulated as,

$$X_{u,v}^{s+1} - \alpha_{X} X_{u,v}^{s} - \frac{1}{2}\alpha_{X} X_{u,v}^{s-1} = Z_{u,v}\left(X_{u,v}^{s} - X_{l}, v\right) \tag{20}$$

$$X_{u,v}^{s+1} = \alpha_{X} X_{u,v}^{s} + \frac{1}{2}\alpha_{X} X_{u,v}^{s-1} + Z_{u,v}\left(X_{u,v}^{s} - X_{l}, v\right) \tag{21}$$

$$X_{u,v}^{s+1} = \left| \alpha_{X} X_{u,v}^{s} + \frac{1}{2}\alpha_{X} X_{u,v}^{s-1} + Z_{u,v}\left(X_{u,v}^{s} - X_{l}, v\right) \right| \tag{22}$$

After generating food sources, the optimization models bound constraints for capturing the solution's value in specific integer intervals.

Step 3: Determination of fitness function

The obtained food source is analyzed with fitness. If the fitness of the updated food source $X_{u,v}^{s+1}$ is less than the old food source $X_{u,v}^{s}$ then, the solution is updated with the old best solution $Q_{u,v}^{s}$, or otherwise, the solution is based on the new food source $X_{u,v}^{s+1}$.

Step 4: Onlooker bee

The food sources of the second half of the population are updated with onlooker bee wherein the food source is chosen as,

$$y_u = \omega_1 \times \frac{fit_u}{Max_{u=1}^{X_R} fit_u} + \omega_2 \tag{23}$$

where, ω_1 and ω_2 indicate constant and fit_u represent the fitness employed for choosing the best path. The chosen food source is replaced with a new solution $X_{u,v}^{s+1}$. The bee searches for the new food source if the fitness of $X_{u,v}^{s+1} < X_{u,v}^{s}$, otherwise, remains same.

The fitness of the FABC algorithm is formed considering three attributes, distance, delay, and energy. When selecting a path, the distance should be less, the energy of nodes present in the path should be elevated, and the delay must be low. Thus, the design issues are employed for path selection. Thus, the goal is to reduce the objective function, which is represented as,

$$fit_u = \eta_1 h_u^{loc} + \eta_2 h_u^{energy} + \eta_3 h_u^{delay} \tag{24}$$

where, η_1, η_2 and η_3 represent weighted constants, and h_u^{loc} indicates the distance of cluster member to CH. Similarly, h_u^{energy} indicates the energy of the nodes present in a path and h_u^{delay} is the delay incurred in the transmission.

Step 5: Scout bee

These phases are implemented if no sources of food are altered for past Z cycles. Here, the chosen source of food is discarded and updated with the randomly produced new food source.

Step 6: Termination

The steps mentioned above are repeatedly executed till s reaches the utmost cycles $Z_{\max}$. The best food source is solution output. After choosing the optimum cluster head, the communication between CH and IoT nodes is performed for exchanging information.

4.2. Proposed Adaptive-SFG-based multipath routing

Once the optimum cluster head is selected, the next process is the transmission of multipath data. Generally, the breakdown of the main path is essential in IoT because of dynamic network topologies. The factors such as energy deficit, breakage of links, and trust may lead to route failure, affecting

the system performance. In these cases, the rerouting is complex as time consumption is more and the energy is wasted. Thus, the optimal or subsequent paths, if offered, can simplify the process of routing. Thus, multipath data transmission is adapted for undergoing transmission using multiple paths from source to target node. In IoT, the transmission is performed using cluster heads of each cluster which are chosen using FABC. Here, the motive is to perform multipath transmission using optimal paths considering the proposed Adaptive-SFG. Moreover, the fitness is newly devised by combining different objectives like energy, link lifetime, delay, trust, and context awareness, offering optimal paths for transmission using improved link lifetime, trust, and energy. Furthermore, the fitness function, solution encoding, and algorithm of Adaptive SFG are portrayed.

4.2.1. Solution Encoding

The representation of the solution is obtained using the proposed Adaptive SFG. Here, the solution is optimal paths wherein each path comprises cluster heads selected for transmitting the data. The proposed Adaptive SFG algorithm utilizes fitness function, which is newly devised based for determining optimal path. Here, the paths comprise CH that can offer effectual routing in the network by minimizing the loss of information throughout transmission. Let the total number of paths existing between the source node S_1 and target node S_4 be represented O. Then, the proposed Adaptive SFG algorithm with a newly devised fitness function assists in selecting the optimal paths that comprise cluster heads for transmission. Let x represent the optimal path used for data transmission considering the proposed Adaptive SFG algorithm and is represented in figure 3. Thus, the dimension of the solution vector is $\left[1 \times x\right]$.

Figure 3. Solution encoding of proposed Adaptive SFG algorithm for choosing optimal paths

4.2.2. Fitness Function

The fitness is evaluated to discover the best solution using a set of solutions with parameters. The fitness of the proposed Adaptive SFG algorithm is devised with five factors, namely, link lifetime, energy, delay, trust, and context awareness. Here, the fitness is adapted as a maximization function. The fitness of the proposed Adaptive SFG algorithm is given by,

$$Fitness = \sum_{r=1}^{\kappa} (LL_{r,t} + E_{r,t} + T_{r,t} + (1 - U_{r,t}) + R_{r,t}) \tag{25}$$

where, $LL_{r,t}$ *specifies the link lifetime of* r^{th} *node in* t^{th} *path,* x *represents the number of paths in the solution vector,* $E_{r,t}$ *is the residual energy,* $T_{r,t}$ *indicates the trust value, and* $R_{r,t}$ *denote the context-awareness. The trust value* $T_{r,t}$ *is the combination of direct and indirect trust values. Here, link*

lifetime, energy, and trust are already described in section 3. The remaining delay and context awareness parameter is described below.

4.2.3. Delay

The delay is evaluated considering the count of nodes that exist in the path and is expressed as $U_{r,t}$.

4.2.4. Context Awareness

The context-aware model (Musolesi & Mascolo, 2008) is known as a system that uses contextual information and repeatedly performs configuration to offer each user's context service. The context-awareness is expressed as,

$$R_{r,t} = function\left(\lambda_{energy}^{\vartheta}, \omega_{consumption}, \alpha_{res-energy}, \beta_{pending-task}, \tau\right) \tag{26}$$

where, $fun\left(.\right)$ symbolize naïve Bayes input function, $\lambda_{energy}^{\vartheta}$ signifies the rate of nodes energy consumption at the time ϑ, $\omega_{consumption}$ refers to the instantaneous value of consumption, $\alpha_{res-energy}$ denote lifetime of residual energy, $\beta_{pending-task}$ signifies queue of pending task data. The rate of nodes energy consumption (Chen, et.al., 2012) is the value of residual energy in a battery and is expressed as,

$$\lambda_{energy}^{\vartheta} = \frac{E_{\vartheta+1} - E_{\vartheta}}{1}(J \,/\, \min) \tag{27}$$

where, E_{ϑ} represent the value of residual energy in the battery of node. The instantaneous value of consumption (Chen, et.al., 2012) is produced by accumulating an instant energy consumption rate at a specific time instant and is expressed as $\omega_{consumption}$. The lifetime of residual energy (Chen, et.al., 2012) is a residual energy value of a battery in the node, which is expressed as,

$$\alpha_{res-energy} = \frac{\frac{E_{\vartheta+1}}{\omega_{cons}^{\vartheta+1}} - \frac{E_{\vartheta}}{\omega_{cons}^{\vartheta}}}{\frac{E_s}{\omega_{cons}^{\vartheta}}} \tag{28}$$

where, E_{ϑ} refers residual energy, and $\omega_{cons}^{\vartheta}$ symbolize instantaneous energy consumption. The queue of pending task (Chen, et.al., 2012) data is generated by residual queue data of node and is expressed as $\beta_{pending-task}$. The length of the queue is evaluated based on a concrete IoT environment with fixed-length data.

4.2.5. Proposed Adaptive-SFG Algorithm

The multipath routing is performed by employing the proposed Adaptive-SFG, which combines the Adaptive concept in SFG. The proposed Adaptive-SFG poses both SFG and adaptive concept benefits, which offer improved performance for initiating multipath routing. The SFG is an algorithm obtained by incorporating the benefits of the SFO and GWO algorithm, and further, the adaptive

concept is combined to perform better. SFO (Gomes, et.al., 2019) algorithm is simple to adapt and can solve constrained issues with optimization techniques. The SFO is adapted as an effective method in optimization, whereas GWO (Gao & Zhao, 2019) aims to speed the convergence rate with a single value of the parameter. Here, the self-adaptive concept is incorporated to provide various benefits as it can switch amongst different operators to maintain efficiency and robustness. This method is easier and is capable to effectively handle numerous local optima, significant nonlinearity, ruggedness, and interdependence. Moreover, it opens a way for enhancing the efficiency and robustness of optimization algorithm. The method assists in handling optimization issues with different constraints without any additional parameters. The self-adaptive method is a method in which the selection of learning strategy and control parameters are not specified before, and parameter settings are self-adapted using the learning experience. Thus, the incorporation of adaptive concepts in the SFG algorithm improves the overall performance, and the steps of the proposed Adaptive-SFG are given as:

Step 1. Initialization

The foremost step is an initialization, in which the population of grey wolves and the other parameters, such as iteration counter, o are initialized. The total grey wolf population is formulated as,

$$Y = \{Y_1, Y_2, \ldots, Y_\eta, \ldots, Y_\rho\} \tag{29}$$

where, η represent total grey wolf population, Y_ρ symbolize ρ^{th} grey wolf.

Step 2. Computation of fitness function

The fitness is obtained by fitness generated in equation (25) under section 4.2.

Step 3. Discovering update equation

To improve search space, the proposed algorithm uses the update rule of GWO. As per GWO (Gao & Zhao, 2019), the update position adapted in the algorithm is expressed as,

$$\vec{Y}(w+1) = \frac{\vec{Y}_1 + \vec{Y}_2 + \vec{Y}_3}{3} \tag{30}$$

where, $\vec{Y}_1 + \vec{Y}_2 + \vec{Y}_3$ represent position vector of grey wolves.

In SFG, the update is made by adding $\vec{Y}_4$ to $\vec{Y}_1 + \vec{Y}_2 + \vec{Y}_3$ Thus, new update equation is expressed as,

$$\vec{Y}(w+1) = \frac{\vec{Y}_1 + \vec{Y}_2 + \vec{Y}_3 + \vec{Y}_4}{4} \tag{31}$$

where, $\vec{Y}_1 + \vec{Y}_2 + \vec{Y}_3$ represent the position vector of grey wolves and $\vec{Y}_4$ is devised using update equation of SFO (Gomes, et.al., 2019). The update position of grey wolves using the SFO algorithm is expressed as,

$$\vec{Y}_4 = \vec{Y}_\psi + y_\psi \times z_\psi \tag{32}$$

$$y_\psi = \upsilon \times P_\psi(|| Y_\psi + Y_{\psi-1} ||) \times || Y_\psi + Y_{\psi-1} || \tag{33}$$

where, $P(.)$ represent the probability of pollination constant and υ is constant.

$$z_\psi = \frac{Y^* - Y_\psi}{|| Y^* - Y_\psi ||} \tag{34}$$

Each position vector of grey wolves can be expressed as,

$$\vec{Y}_1 = \vec{Y}_\alpha - V_1(\vec{W}_\alpha) \tag{35}$$

$$\vec{Y}_2 = \vec{Y}_\beta - V_2(\vec{W}_\beta) \tag{36}$$

$$\vec{Y}_3 = \vec{Y}_\gamma - V_3(\vec{W}_\gamma) \tag{37}$$

Where, $\vec{Y}_\alpha$ is first best search agent, $\vec{Y}_\beta$ represent second-best search agent and $\vec{Y}_\gamma$ represent third best search agent. Y_ψ Indicate search agent offered by SFO. In addition, V is a coefficient vector which is expressed as,

$$V = 2\vec{x}.\vec{r}_1 - x \tag{38}$$

where x is a random number that linearly decreases from 2 to 0 after certain iterations. The random number x changes the V, which changes the omega wolves to run away or approach towards the dominat wolf like beta, delta and the alpha. Moreover, if $\left|V\right| > 1$, the omega wolf runs away from the dominant wolf, if $\left|V\right| < 1$, the omega wolf approach towards the dominant wolfs.

During update, the self adaptive constants alter control parameters without interaction of user. As per equation (38), the update is carried out with SFG algorithm by making constants self adaptive. To incorporate adaptive concept x is made self-adaptive. For the self-adaptive concept, the coefficient vector from equation (38) is considered, which is used to adjust the settings of the control parameters. Here, the $\vec{x}$ has components linearly decreasing from 2 to 0 and is made self-adaptive, which is expressed as,

$$x = x_v e^{-o/T} \tag{39}$$

Table 1. Pseudo-code of proposed Adaptive SFG

Adaptive SFG algorithm
Input: Population Y
Output: Optimal Solution Y^*
Begin
Initialize the population
while($w < w_{\max}$)
for each solution
Evaluate fitness with equation (25)
Update position with equation (31)
Re-compute the fitness using equation (25)
Select solution providing maximum fitness value Y^*
End for
$w = w + 1$
Return Y^*
Stop

Where, x_v signifies maximal value, o symbolizes current iteration, and T shows admissible maximal iteration. Here, the self adaptiveness is achieved in every iterations by evaluating the x, which in turn varies the coefficient vector V. Thus, the position of the omega wolf varies and hence, the position of other wolves also varies, which in turn enhances the convergence rate.

Step 4: Finding fitness of solutions: After updating the positions of the grey wolf, the fitness of the updated solutions is evaluated. The fitness function is devised using the fitness derived in equation (25), which must be the maximal selecting optimal solution. Here, the optimal solution is nothing but optimal paths which can be used to transmit data packets to target nodes.

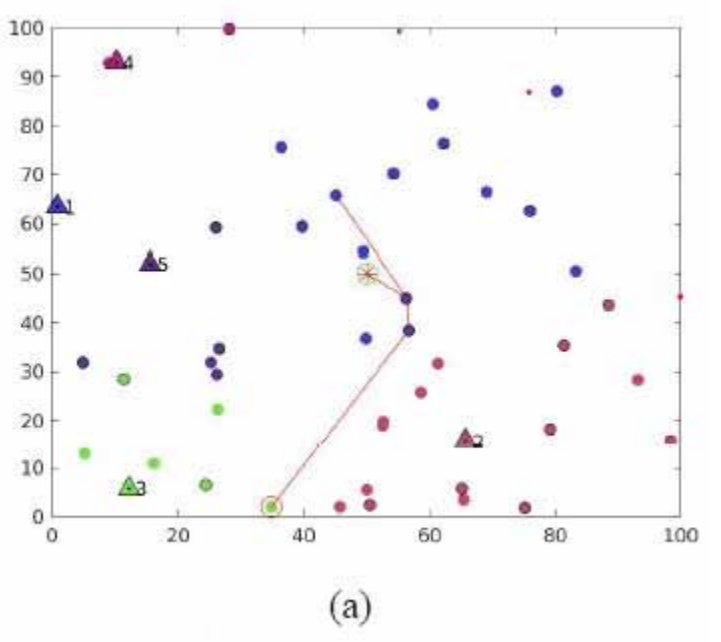
Step 5: Termination: The termination is done using the stopping criterion, which is checked to mark the end of the optimization process. The optimum solutions are obtained in a repeated manner till maximal iterations are attained.

Table 1 describes the pseudo-code of the proposed Adaptive SFG.

4.3. Route Maintenance

In the route maintenance process, the link lifetime is continuously monitored. Here, if the source node acquires reliable routes to the target node, it can send data packets. While receiving data, the node checks if the link is reliable using the link lifetime parameter. Here, the cluster head sends the data packet to the next hop, which transfers the ACK message in return. After receiving the ACK message,

Figure 4. Simulation results of proposed Adaptive SFG with 50 nodes



it finds link reliability between the cluster head using the link lifetime parameter. After receiving the ACK message from the source node, it removes the corresponding route from the routing cache. Here, the link lifetime is compared with the threshold, in which if the link lifetime is less than the threshold, then rerouting will be done. Furthermore, it examines if there are other routes to the destination in the routing cache. If feasible routes are found, it chooses the best route to transmit packets else; the source node will commence new route discovery.

5. RESULTS AND DISCUSSION

This section elaborates the effectiveness of the proposed technique with classical techniques by simulating IoT networks with 50 and 100 nodes. The analysis is performed by altering the count of rounds.

5.1 Experimental Setup

The implementation of the proposed technique is carried out in MATLAB with 50 and 100 nodes. The proposed technique is implemented on a PC with Windows 10 OS, 2GB RAM, and an Intel i3 core processor.

5.1.1. Simulation Results

Figure 4 portrays the simulation results of the proposed Adaptive SFG with 50 nodes. Here, the triangle node depicts the cluster heads employed for routing. The source nodes are indicated in double round shape, which transmits data packets to destination nodes, indicated by small circles. The green, red and blue circles represent the normal nodes. The data transmission is done by selecting a specific path wherein the path is represented in a red line. The optimal path using the proposed Adaptive SFG algorithm is chosen to establish transmission of data between source and destination nodes. Thus, secure transmission is attained in the IoT network.

5.2 Performance measures

The metrics adapted to analyze techniques involves delay, energy, and throughput.

5.2.1. Throughput

The throughput indicates total data rates sent over the network at a particular time.

$$Throughput = \frac{Number\ of\ packets\ received}{Time} \tag{40}$$

5.2.2. Delay

The delay defines the total time utilized to transmit data irrespective of the attacker. The formula of delay is modeled as,

$$Delay = \frac{N_b}{R} \tag{41}$$

where, N_b indicate the number of bits and R represent the rate of transmission.

5.2.3. Energy

The energy of the node is elaborated in section 3.1.

5.2.4. Network Lifetime

The lifetime of a network is a period wherein a node can communicate with other nodes present in the network.

5.3. Comparative Methods

The methods adopted for analysis involve: Particle Multi-Swarm Optimization (PMSO) (Hasan & Al-Turjman, 2017), MPSS (Chen, et.al., 2016), MOFGSA (Dhumane & Prasad, 2019), SFG, and proposed Adaptive SFG algorithm.

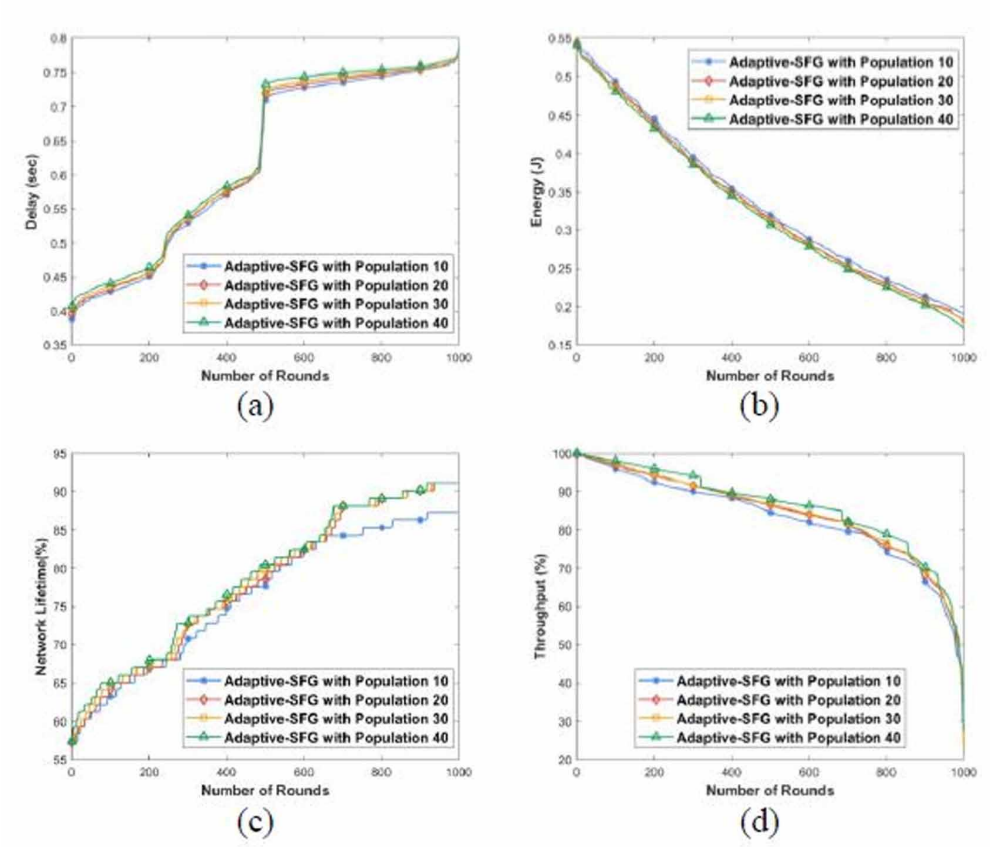
5.4. Performance Analysis

The performance evaluation is done using the proposed Adaptive SFG considering delay, energy, throughput, and network lifetime parameters. The analysis is performed by altering the count of rounds from 1 to 1000. In addition, the population size of the proposed Adaptive SFG is altered to prove the efficiency of the proposed technique. In addition, the analysis is performed with 50 and 100 nodes.

5.4.1. Analysis Based on 50 Nodes

Figure 5) illustrates the analysis of the proposed Adaptive SFG with 50 nodes by varying the population size from 10 to 40. The analysis of the proposed Adaptive SFG based on delay is portrayed in figure 5a). For 1000 rounds, the delay values computed by proposed Adaptive SFG with population size =10, population size =20, population size =30, and population size =40 are 0.775sec, 0.779sec, 0.780sec, and 0.786sec. The analysis of the proposed Adaptive SFG based on energy parameters is illustrated in figure 5b). For 1000 rounds, the energy values computed by proposed Adaptive SFG with population size =10, population size =20, population size =30, and population size =40 are 0.190J, 0.180J, 0.177J, and 0.171J. The analysis of the proposed Adaptive SFG using network lifetime is portrayed in figure 5c). For 1000 rounds, the network lifetime values computed by proposed Adaptive

Figure 5. Analysis of proposed Adaptive SFG with 50 nodes considering a) Delay, b) Energy, c) Network lifetime, d) Throughput



SFG with population size =10, population size =20, population size =30, and population size =40 are 87.308%, 91.154%, 91.154%, and 91.154% respectively. The analysis of the proposed Adaptive SFG using throughput is portrayed in figure 5 d). For 1000 rounds, the throughput values evaluated by proposed Adaptive SFG with population size =10, population size =20, population size =30, and population size =40 are 22.865%, 22.936%, 23.086%, and 27.407%.

5.4.2. Analysis Based on 100 Nodes

Figure 6) portrays an analysis of the proposed Adaptive SFG with 100 nodes by varying the population size from 10 to 40. The analysis of the proposed Adaptive SFG based on delay is portrayed in figure 6a). For 1000rounds, the values of delay computed by proposed Adaptive SFG with population size =10, population size =20, population size =30, population size =40 are 0.777sec, 0.778sec, 0.779sec, and 0.779sec. The analysis of the proposed Adaptive SFG using energy is portrayed in figure 6b). For 1000 rounds, the energy values computed by proposed Adaptive SFG with population size =10, population size =20, population size =30, population size =40 are 0.150J, 0.128J, 0.127J, and 0.119J. The analysis of the proposed Adaptive SFG using network lifetime is portrayed in figure 6c). For 1000 rounds, the network lifetime values computed by proposed Adaptive SFG with population size =10, population size =20, population size =30, population size =40 are 80.231%, 81.769%, 81.769%, and 84.846%, respectively. The analysis of the proposed Adaptive SFG using throughput is portrayed in figure 6d). For 1000 rounds, the throughput evaluated by proposed Adaptive SFG with population size =10, population size =20, population size =30, population size =40 are 20.128%, 23.238%, 25.356%, and 25.872%, respectively.

5.5. Comparative Analysis

The proposed Adaptive SFG technique with conventional methods in terms of delay, energy, throughput, and network lifetime parameters is evaluated. The analysis is carried out by varying the number of rounds using 50 and 100 nodes, respectively.

5.5.1. Analysis Based on 50 Nodes

Figure 7) illustrates the analysis of methods with 50 nodes by varying the number of rounds from 0 to 1000. The analysis of methods based on delay is illustrated in figure 7a). For 1000 rounds, the delay values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 0.789sec, 0.785sec, 0.786sec, 0.785sec, and 0.778sec, respectively. The analysis of methods using energy is portrayed in figure 7 b). For 1000 rounds, the energy values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 0.099J, 0.095J, 0.106J, 0.203J, and 0.218J, respectively. The analysis of methods using network lifetime is portrayed in figure 7 c). For 1000 rounds, the network lifetime values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 92.308%, 90.385%, 94.231%, 96.154%, and 97.000%, respectively. The analysis of methods using throughput is portrayed in figure 7 d). For 1000 rounds, the throughput

Figure 6. Performance analysis of proposed Adaptive SFG using 100 nodes considering a) Delay b) Energy c) Network lifetime d) Throughput

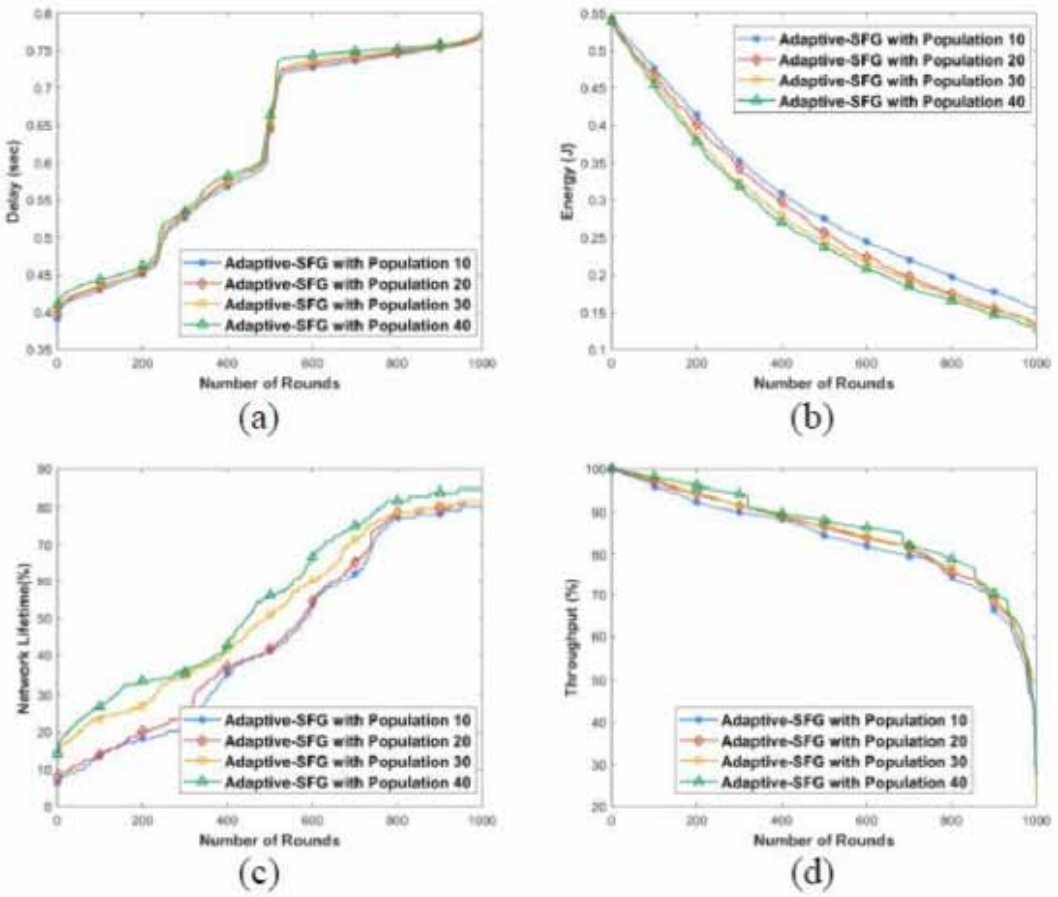
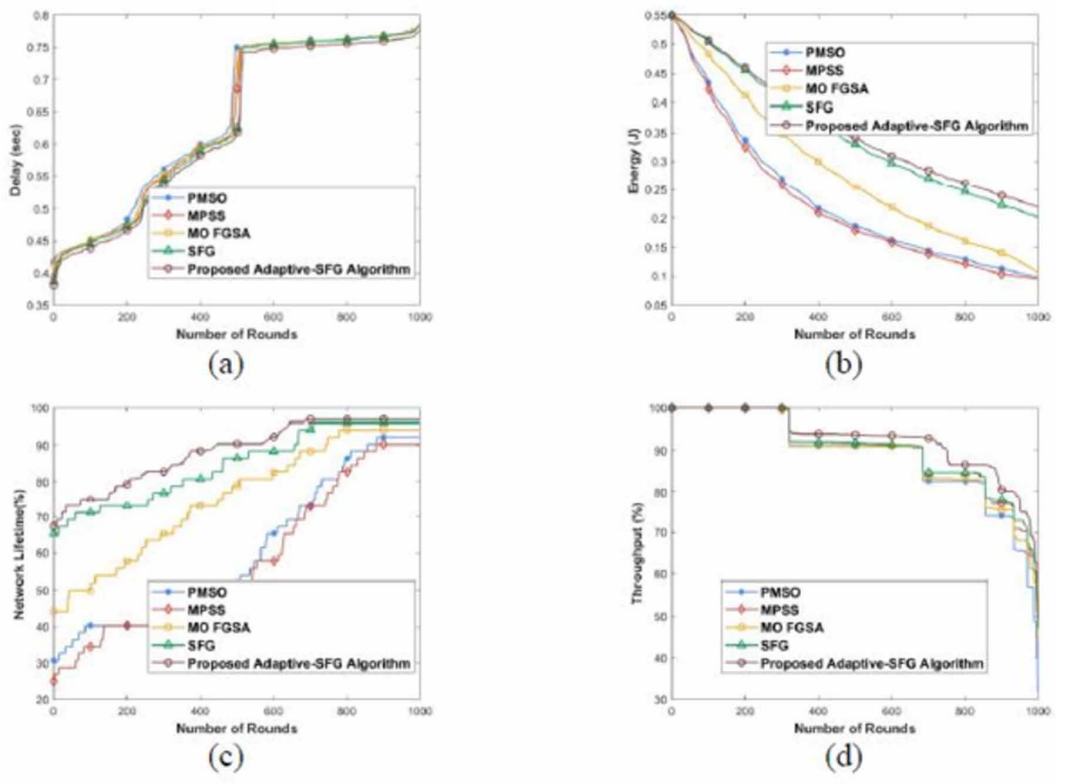


Figure 7. Comparative analysis using 50 nodes considering a) Delay, b) Energy, c) Network lifetime, d) Throughput



values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 31.818%, 47.368%, 44.186%, 47.368%, and 49.368%, respectively.

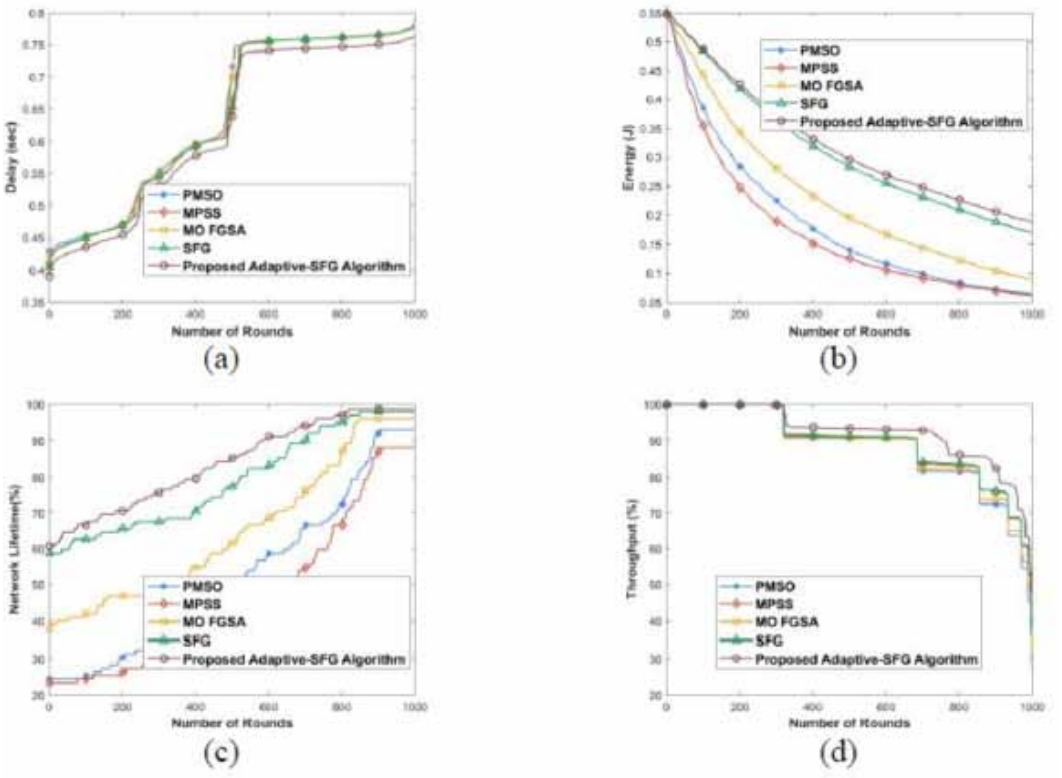
5.5.2. Analysis Based on 100 Nodes

Figure 8) illustrates the analysis of methods with 100 nodes by varying the number of rounds from 0 to 1000. The analysis of methods based on delay is portrayed in figure 8 a). For 1000 rounds, the delay values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 0.792sec, 0.780sec, 0.788sec, 0.779sec, and 0.765sec, respectively. The analysis of methods based on energy is portrayed in figure 8 b). For 1000 rounds, the energy values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 0.0643J, 0.0615J, 0.0892J, 0.1697J, and 0.1854J, respectively. The analysis of methods based on network lifetime is portrayed in figure 8 c). For 1000 rounds, the network lifetime values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 93.137%, 88.235%, 96.078%, 98.039%, and 98.700%, respectively. The analysis of methods based on throughput is portrayed in figure 8 d). For 1000 rounds, the throughput values computed by PMSO, MPSS, MOFGSA, SFG, and proposed Adaptive SFG algorithm are 27.402%, 37.190%, 30.890%, 37.931%, and 47.690%, respectively.

5.6. Comparative Discussion

Table 2 portrays an analysis of techniques using delay, energy, network lifetime, and throughput parameters using 50 and 100 nodes. For 50 nodes, the best performance is showed by the proposed Adaptive SFG with a minimal delay of 0.778sec, whereas the delay of existing PMSO, MPSS, MOFGSA, and SFG are 0.789sec, 0.785sec, 0.786sec, and 0.785sec, respectively. The maximal

Figure 8. Analysis using 100 nodes considering a) Delay, b) Energy, c) Network lifetime, d) Throughput



performance is shown by the proposed Adaptive SFG with maximal energy of 0.218J, whereas the existing PMSO, MPSS, MOFGSA, and SFG is 0.099J, 0.095J, 0.106J, and 0.203J, respectively. The proposed Adaptive SFG gains the optimal performance with a maximal network lifetime of 97%. In contrast, the network lifetime of existing PMSO, MPSS, MOFGSA, and SFG is 92.308%, 90.385%, 94.231%, and 96.154, respectively. The optimal performance is gained by the proposed Adaptive SFG with maximal throughput of 49.368%, whereas the network lifetime of existing PMSO, MPSS, MOFGSA, and SFG is 31.818%, 47.368%, 44.186%, and 49.368, respectively. In 100 nodes, the best performance is showed by the proposed Adaptive SFG with a minimal delay of 0.765sec, whereas the delay of existing PMSO, MPSS, MOFGSA, and SFG are 0.792sec, 0.780sec, 0.788sec, and 0.779sec, respectively. The maximal performance is shown by the proposed Adaptive SFG with maximal energy of 0.1854J, whereas the existing PMSO, MPSS, MOFGSA and SFG is 0.0643J 0.0615J, 0.0892J, and 0.1697J, respectively. Proposed Adaptive SFG gains the optimal performance with a maximal network lifetime of 98.700%, whereas the network lifetime of existing PMSO, MPSS, MOFGSA, and SFG is 93.137%, 88.235%, 96.078%, 98.039%, respectively. The optimal performance is gained by the proposed Adaptive SFG with maximal throughput of 37.931, whereas the energy of existing PMSO, MPSS, MOFGSA, and SFG is 27.402%, 37.190%, 30.890%, 37.931%, respectively.

Table 2. Comparative Analysis

Nodes	Metrics	PMSO	MPSS	MOFGSA	SFG	Proposed Adaptive SFG
Using 50 nodes	**Delay (sec)**	0.789	0.785	0.786	0.785	**0.778**
	Energy (J)	0.099	0.095	0.106	0.203	**0.218**
	Network lifetime(%)	92.308	90.385	94.231	96.154	**97.000**
	Throughput (%)	31.818	47.368	44.186	47.368	**49.368**
Using 100 nodes	**Delay (sec)**	0.792	0.780	0.788	0.779	**0.765**
	Energy (J)	0.064	0.061	0.089	0.169	**0.185**
	Network lifetime(%)	93.137	88.235	96.078	98.039	**98.700**
	Throughput (%)	27.402	37.190	30.890	37.931	**47.690**

6. MANAGERIAL APPLICATIONS

The proposed Adaptive SFG applies to many managerial related applications, which are detailed below:

Monitoring and Control: With the help of IoT, home automation is enabled, and it can be controlled anywhere and at any time using the smartphone.
Health Management: The patient's health record maintained in the cloud helps to access anywhere, and hence the monitoring is continued, and hence better diagnosis is possible.
Information sharing: By using the trust factors, the information shared will be authenticated and energy-efficient with less delay.

Besides, it is widely used in traffic management, environmental monitoring, business analyst, etc.

7. CONCLUSION

This paper devises a technique, namely Adaptive SFG, with an improved link lifetime for attaining multipath transmission in IoT networks. Here, the IoT nodes are simulated, and there exist two major steps, such as selection of CH and routing with multiple paths. The first step is selecting a cluster head, which is performed using FABC that involves fractional calculus in the ABC algorithm. Then, the multipath transmission is done by adapting the proposed Adaptive SFG, which combines the Adaptive concept in SFO. In addition, fitness is devised with several factors that include Context awareness, link lifetime, Energy, Trust, and Delay. For the computation of the trust, the trust factors are considered that include direct trust, recent trust, indirect trust, and forwarding rate factor to choose the best solution. Hence, the proposed Adaptive SFG is utilized to discover the route that poses high energy of 0.185J, minimal delay of 0.765sec, maximum throughput of 47.690%, and maximum network lifetime of 98.7% as the best paths for performing the multipath transmission. Finally, route maintenance is done to ensure routing without link breakage. In the future, the hybridization of advanced optimization techniques will be considered for multipath routing to enhance optimal routing.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

Funding Statement

No funding was received for this work.

Process Dates:

Received: May 21, 2021, Revision: June 16, 2021, Accepted: July 23, 2021

Corresponding Author:

Correspondence should be addressed to Reena P. Pingale, pingalereenap@gmail.com

REFERENCES

Al-Turjman, F. (2017). Energy-aware data delivery framework for safety-oriented mobile IoT. *IEEE Sensors Journal*, *18*(1), 470–478.

Anand, S. J., Priyadarsini, K., Selvi, G. A., Poornima, D., & Vedanarayanan, V. (2021). Iot-Based Secure And Energy Efficient Scheme For Precision Agriculture Using Blockchain And Improved Leach Algorithm. *Turkish Journal of Computer and Mathematics Education*, *12*(10).

Balachandra, M., Prema, K. V., & Makkithaya, K. (2014). Multiconstrained and multipath QoS aware routing protocol for MANETs. *Wireless Networks*, *20*(8), 2395–2408.

Banner, R., & Orda, A. (2007). Multipath routing algorithms for congestion minimization. *IEEE/ACM Transactions on Networking*, *15*(2), 413–424.

Bertsekas, D., & Gallager, R. (1992). *Data Networks*. Prentice-Hall.

Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2021). Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wireless Networks*, 27.

Bhushan, B., & Sahoo, G. (2019). E2SR2: An acknowledgement-based mobile sink routing protocol with rechargeable sensors for wireless sensor networks. *Wireless Networks*, *25*, 2697–2721.

Bhushan, B., & Sahoo, G. (2020). ISFC-BLS (Intelligent and Secured Fuzzy Clustering Algorithm Using Balanced Load Sub-Cluster Formation) in WSN Environment. *Wireless Personal Communications*, *111*, 1667–1694.

Chen, M., Wang, J., Lin, K., Wu, D., Wan, J., Peng, L., & Youn, C. H. (2016). M-plan: Multipath planning based transmissions for IoT multimedia sensing. *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 339-344.

Chen, Z., He, M., Liang, W., & Chen, K. (2015). Trust-aware and low energy consumption security topology protocol of wireless sensor network. *Journal of Sensors*.

Chen, Z., Wang, H., Liu, Y., Bu, F., & Wei, Z. (2012). A context-aware routing protocol on internet of things based on sea computing model. *Journal of Computers*, *7*(1), 96–105.

Das, A., & Islam, M. M. (2011). SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, *9*(2), 261–274.

Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. *Ad Hoc Networks*, *97*, 102022.

Dhumane, A. V., & Prasad, R. S. (2018). Fractional gravitational grey wolf optimization to multipath data transmission in IoT. *Wireless Personal Communications*, *102*(1), 411–436.

Dhumane, A. V., & Prasad, R. S. (2019). Multiobjective fractional gravitational search algorithm for energy efficient routing in IoT. *Wireless Networks*, *25*(1), 399–413.

Gao, Z. M., & Zhao, J. (2019). An improved grey wolf optimization algorithm with variable weights. *Computational Intelligence and Neuroscience*.

Gomes, G. F., da Cunha, S. S., & Ancelotti, A. C. (2019). A sunflower optimization (SFO) algorithm applied to damage identification on laminated composite plates. *Engineering with Computers*, *35*(2), 619–626.

Hasan, M. Z., & Al-Turjman, F. (2017). Optimizing Multipath Routing With Guaranteed Fault Tolerance in Internet of Things. *IEEE Sensors Journal*, *17*(19), 6463–6473.

Iyer, S., Bhattacharyya, S., Taft, N., McKeoen, N., & Diot, C. (2002). *A measurement based study of load balancing in an IP backbone.* Sprint ATL,Tech. Rep. TR02-ATL-051027.

Jabbar, W. A., Saad, W. K., & Ismail, M. (2018). MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 76546–76572.

Jaiswal, K., & Anand, V. (2019). EOMR: An energy-efficient optimal multipath routing protocol to improve QoS in wireless sensor network for IoT applications. *Wireless Personal Communications*, 1–23.

Jiang, Y., Ge, X., Zhong, Y., Mao, G., & Li, Y. (2019). A new small-world IoT routing mechanism based on Cayley graphs. *IEEE Internet of Things Journal*, *6*(6), 10384–10395.

Karaboga, D., Okdem, S., & Ozturk, C. (2012). Cluster based wireless sensor network routing using artificial bee colony algorithm. *Wireless Networks*, *18*, 847–860.

Kharrufa, H., Al-Kashoash, H. A., & Kemp, A. H. (2019). RPL-based routing protocols in IoT applications: A Review. *IEEE Sensors Journal*, *19*(15), 5952–5967.

Kim, S., Kim, C., & Jung, K. (2020). Cooperative Multipath Routing with Path Bridging in Wireless Sensor Network toward IoTs Service. *Ad Hoc Networks*, 102252.

Kumar, R., & Kumar, D. (2016). Multiobjective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network. *Wireless Networks*, *22*(5), 1461–1474.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58.

Liu, A., Zheng, Z., Zhang, C., Chen, Z., & Shen, X. (2012). Secure and energy-efficient disjoint multipath routing for WSNs. *IEEE Transactions on Vehicular Technology*, *61*(7), 3255–3265.

Metallidou, C. K., Psannis, K. E., & Egyptiadou, E. A. (2020). Energy Efficiency in Smart Buildings: IoT Approaches. *IEEE Access : Practical Innovations, Open Solutions*.

Musolesi, M., & Mascolo, C. (2008). Car: Context-aware adaptive routing for delay-tolerant mobile networks. *IEEE Transactions on Mobile Computing*, *8*(2), 246–260.

Pires, E. J. S., Machado, J. A. T., Oliveira, P. B. M., Cunha, J. B., & Mendes, L. (2010). Particle swarm optimization with fractional-order velocity. *Nonlinear Dynamics*, *61*, 295–301.

Rahat, A. A. M., Everson, R. M., & Fieldsend, J. E. (2016). Evolutionary multipath routing for network lifetime and robustness in wireless sensor networks. *Ad Hoc Networks*, *52*(1), 130–145.

Rajesh, G., Raajini, X. M., Sagayam, K. M., Bhushan, B., & Köse, U. (2020). Fuzzy genetic based dynamic spectrum allocation approach for cognitive radio sensor networks. *Turkish Journal of Electrical Engineering and Computer Sciences*, *28*, 2416–2432.

Safara, F., Souri, A., Baker, T., Al Ridhawi, I., & Aloqaily, M. (2020). PriNergy: A priority-based energy-efficient routing method for IoT systems. *The Journal of Supercomputing*, 1–18.

Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, *181*(5).

Sethi, R., Bhushan, B., Sharma, N., Kumar, R., & Kaushik, I. (2020). Applicability of Industrial IoT in Diversified Sectors: Evolution, Applications and Challenges. *Multimedia Technologies in the Internet of Things Environment*, 45-67.

Somauroo, A., & Bassoo, V. (2020). *Energy-efficient genetic algorithm variants of PEGASIS for 3D Wireless Sensor Networks*. Applied Computing and Informatics.

Souri, A., & Norouzi, M. (2019). A state-of-the-art survey on formal verifcation of the internet of things applications. *J Serv Sci Res*, *11*(1), 47–67.

Teo, J.-Y., Ha, Y., & Tham, C.-K. (2008). Interference-minimized multipath routing with congestion control in wireless sensor network for high-rate streaming. *IEEE Transactions on Mobile Computing*, *7*(9), 1124–1137.

Yadav, P. (2016). Case retrieval algorithm using similarity measure and adaptive fractional brain storm optimization for health informaticians. *Arabian Journal for Science and Engineering*, *41*(3), 829–840.

Zhu, J. (2018). Wireless sensor network technology based on security trust evaluation model. *International Journal of Online and Biomedical Engineering*, *14*(4), 211–226.

Reena P. Pingale is currently working at the Sinhgad College of Science.

S. N. Shinde is currently working at the CMCS College.