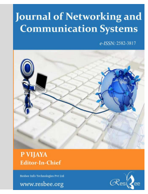
Vol.3 No.1 Jan 2020

Journal of Networking and Communication Systems

Received 12 October, Revised 29 November, Accepted 15 January



Multipath Transmission in IoT using Hybrid Salp Swarm-Differential Evolution Algorithm

Amol V. Dhumane
NBN Sinhgad School of Engineering,
Pune, Maharashtra, India
amolvdhumane@gmail.com

Rajesh S. Prasad
NBN Sinhgad School of Engineering,
Pune, Maharashtra, India

Abstract: The improvements in technology in the field of communication did Wireless Sensor Network (WSN) on the basis of the IoT desirable and appropriate to several regions. It is encompassed that IoT nodes perform on restricted battery provisions. Therefore, a maximum-routing protocol performance is necessary for routing in such networks to surmount the energy constraint issues. For multipath data transmission, an energy-efficient routing algorithm named Hybrid Salp Swarm and Simulated Algorithm (Hybrid SS and SA) is adopted in this work. The adopted approach enhanced the routing procedure in a dual-phase procedure. Initially, the cluster heads are chosen by exploiting the Salp Swarm Algorithm. Subsequently, multiple paths are produced from the sender to the receiver by exploiting DE. Here, inter and intra-cluster distance, energy, delay and lifetime is considered as the objective function. In the fitness model, an optimal path for the transmission is presented. Finally, the investigational outcomes exhibit that the performance of the proposed model shows maximum performance with respect to the alive nodes and energy in contrast with the conventional approaches.

Keywords: IoT; Cluster Head; Energy; Delay; Distance; Fitness Model

Nomenclature

Abbreviations	Descriptions
IoT	Internet of Things
SDN	Software-Defined Network
TPR	True Positive Rate
ABC	Artificial Bee Colony
CC	Computational Cost
GWO	Grey Wolf Optimization
EDT	Early Data Transmission
SD-IoT	Software-Defined IoT
CU	Cloud Users
CHS	Cluster Head Selection
CO	Communication Overhead
ES	Early Sleeping
SNs	Sensor Nodes
HNS-CODML	HNS Cost Optimized Deep Machine Learning
RCSMMA	Random Coefficient Selection and Mean Modification Approach
BS	Base Station
ML	Machine Learning
HNS	Hashed Needham Schroeder
PKG	Public Key Generation
ORSIN	One-Request Scheme for Software-Defined IoT Networks
CH	Cluster Head
PF	Pareto front
ACO	Ant Colony Optimization
LLT	Link Lifetime
GSA	Gravitational Search Algorithm

https://doi.org/10.46253/jnacs.v3i1.a3

1. Introduction

Since the IoT is primary to understanding urban sensing, it must be stretchy adequate to maintain numerous requirements technology and suitable infrastructure management [3]. SDN is a rising prototype that assures to lithely control network resources and to maintain an enormous number of data deliveries by meeting the exact requirements of end-to-end [5]. For flow-based routing, SDN permits for rapid and lithe configuration; it allows the network components rescheduling, and it is chiefly helpful for acclimatizing networks to ever-altering traffic volumes with dissimilar demands. As a result, the incorporation of SDN methods and IoT is magnetizing growing concentration from both the industrial and the academic communities; for smart urban sensing, an SD-IoT network is exploited [3].

The model of IoT constructs many absurd developments. In IoT, trillions of electronic units are associated with the internet and these electronic units are given with sensors that control many features of human life. However, this incorporation begins novel apprehensions for security, privacy, at both social levels and system between objects and humans. The IoT comprises three elements, such as computer systems, communication networks, and things, [5]. Researchers were earlier functioning on novel approaches and effectual methods on how to enhance introduced WSNs into the IoT circumstances. In a WSN based IoT, the objects, like SNs, turn out to be smarter as they can converse expediently with each other and human beings. This reality has paved the method for introducing factories, smart buildings, and generally, smart cities [8]. However, because of the fast improvements in communication and information applications, how to deal with the privacy and security apprehensions is a huge compact in such environments [11]. The IoT aids new business methods by means of secure remote access to associated applications and other devices.

ML-based model [1] was developed to scrutinize inward communication and was established to be dependable. In an IoT environment, communication was calculated on the basis of frequent trust features. At first, a general trust computational representation with a feature extraction technique suitable in IoT was developed [17]. Subsequent to this extraction procedure, a method to label data on the basis of their trustworthiness was evaluated. In accordance with the unsupervised learning models, trustworthy interactions were calculated [18]. The trust prediction model calculated learnt optimal parameters and trust boundaries to obtain last trust value exploiting a renowned SVM technique. The method was competent in precision and TPR. In spite of precision being attained, the CC, and overhead acquired in trust-worthiness recognition, was found to be superior.

The main contribution of this work is to propose the hybrid algorithm for the multi-path data transmission in IoT. Here, the proposed approach has two main stages, such as Multipath data transmission and CHS. The Salp Swarm algorithm is exploited to enhance the node's lifetime with an important number of network energy and alive nodes. Subsequently, by the hybridization of the SS and DE algorithm, the multipath data transmission is done. Finally, the main aim is to consider the evaluation of the fitness function of the adopted model.

2. Literature Review

In 2019, Jafar A. Alzubi et al [1], proposed the HNS-CODML algorithm in order to secure Industrial IoT data transmissions through a cloud environment. Moreover, the requirement of offering Industrial IoT security by exploiting the ML approach was indicated. Initially, the HNS PKG method calculates a flag and the public key value, subsequently exploiting public key, the execution time was enhanced as merely authenticated CU were permitted. Hence, exploiting two passes, the cost function was calculated. At the initial pass, the cost function was calculated whilst in the second pass, the complete cost function was attained, consequently minimizing the CO, and CC creation the whole procedure much convenient to control and monitor.

In 2019, Debasish Ghose et al [2], presented two models, such as EDT and ES and, to additional decrease latency and energy utilization in WuR-enabled WSNs/IoT. In order to address bit-by-bit, the ES model was utilized to examine and decodes, permitting those non-destined devices to go to sleep at a previous phase. For data reception, the EDT model allows a source to destination diminutive IoT data together with WuC packets with the intention that the chief radio does not must be in complete operation.

In 2019, Nasir N. Hurrah et al [3], focused on the preservation of confidentiality and privacy of data in an insecure environment of multimedia exchange among two IoT hops. With the intention of preventing an adversary and guarantee data confidentiality, a robust multi-level security method on the basis of the chaotic theory and information hiding was proposed. Even though, a few conventional block-based robust data hiding models on the basis of the transform domain present better outcomes; nevertheless the incompetent block and coefficient modification/selection outcomes in deprived performance to a variety of usually happen cyber-attacks. The developed model was on the basis of the RCSMMA.

In 2019, Arezou Ostad-Sharif et al [4], presented a safe and inconsequential authentication and key agreement protocol for IoT based WSNs which was free from the security concerns of preceding protocols. By exploiting the renowned and extensively-accepted automated corroboration of applications tool and Internet Security Protocols, formal security confirmation of the developed protocol was developed.

In 2019, Rihab Boussada et al [5], developed a new privacy-preserving IoT-based e-health solution. This solution assures contextual and content privacy requirements. Moreover, it was on the basis of an exact communication situation and a new identity-based encryption method, with regard to the inadequate resource nature of smart-things. To confirm the proposed method, a wide security study was presented. Additionally, a performance analysis efficiency of the proposed method was shown.

In 2019, Xiaowei Chen et al [6], addressed the issue in the transmission of the data among different service mechanisms in the IoT data transmission, there was an enormous transmission delay procedure that will affect the complete system performance. Hence, concerning the minimization of delay in transmission as the optimization objective, and iDiSC was suggested. In the edge-cloud-hybrid system, a novel heuristic model for IoT-data-intensive service component deployment was presented. Additionally, the iDiSC model was presented, and subsequently, the model was optimized to choose the optimal deployment circumstances with the least definite latency.

In 2019, Yuichi Inagaki et al [7], developed an IoT device control system that minimizes the number of broadcast data exploited as input for real-time prediction whilst preserving the prediction precision. The most important objective of this work was that the developed model maintains data transmission from the mobile IoT devices on the basis of the significance of data extraction from the ML method exploited to the prediction. For extraction, the selection of feature was extensively exploited the significance of data from the ML model. Additionally, in distributed learning, feature selection approaches were exploited to decrease communication overhead.

In 2018, Chao Song et al [8], examined the redundant requests that happened by the asynchronous M2P data transmissions in the SD-IoT network. The association among the sensing events and the uploading gateways was modeled by exploiting their spatial locations and the distribution of mobile SNs.

3. Network Model

In WSN, the sensors are collected into clusters in that a node is chosen as CH because of the energy constraint issue. In WSN based IoT, every SN, indicated as IoT nodes gather the information and route them to the BS by means of its equivalent CH. As it takes substantial energy to transfer the data, the IoT node which has the least amount of distance evaluated with the other nodes in that meticulous cluster is selected as the CH. Let us assume a simulation area A with dimension $Y \times Z$, whereas WSN comprises of a BS and a number of IoT nodes N dispersed as clusters with CH. Every IoT node $n_j, 1 < j < N$ is positioned at (y_j, z_j), whilst the position of BS is indicated (Y^{BS}, Z^{BS}). Fig. 1 shows the system model for the WSN based IoT. Here, the node n_j in each cluster transfers the data to its CH as $n_{cl}, 1 \le cl \le CH$. For the CH node CH, CH^u indicates a set of IoT nodes with $u - CH$ as the number of normal nodes.

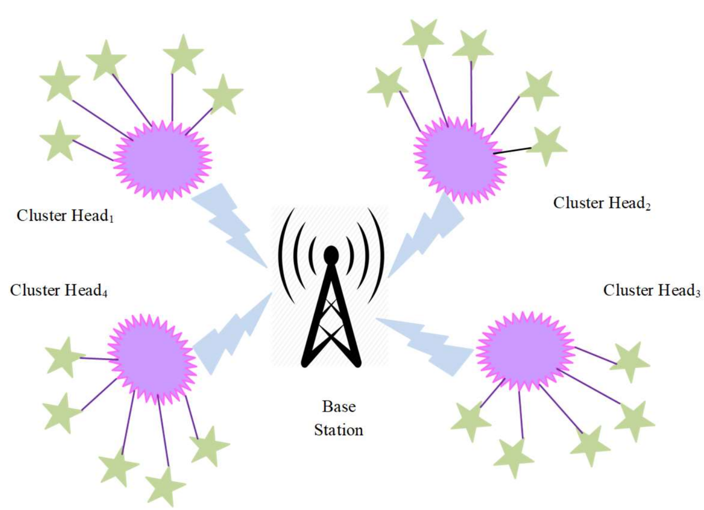


Fig. 1. *Network model of WSN based IoT*

3.1. Energy Model

In power amplifier and radio electronics, the debauched energy is calculated using the energy at the transmitter. Eq. (1) indicates the energy dissipation in j^{th} node [9]. E_0 indicates the initial energy of a node, during the transmission it cannot be re-energized. Here, the energy loss is represented as free space energy loss and multipath fading model.

$$E_{dis}^{j} = \begin{cases} E_{ee} * P_s + E_{fs} * P_s * \left\| n_j - n_{cl} \right\|^4; \text{if} \left\| n_j - n_{cl} \right\| \geq p_0 \\ E_{ee} * P_s + E_{fs} * P_s * \left\| n_j - n_{cl} \right\|^4; \text{if} \left\| n_j - n_{cl} \right\| < p_0 \end{cases} \tag{1}$$

$$p_0 = \sqrt{\frac{E_l}{E_{fs}}} \tag{2}$$

In eq. (1), P_s indicates the packet size; E_{fs} and E_l indicates the energy loss given by multipath fading and free space model; $\left\| n_j - n_{cl} \right\|$ indicates the distance among a normal node and a cluster node. E_{ee} indicates the electronic energy stated in eq. (3).

$$E_{ee} = E_t + E_d \tag{3}$$

In eq. (3), E_d and E_t indicates the data aggregation and transmitter the energy, correspondingly.

On one occasion the CH receives the packet, it transfers the packet to the BS, to update the energy measure. During the transmission, the energy dissipated in the cluster node is stated in eq. (4).

$$E_{dis}(n_{cl}) = E_{ee} * P_s \tag{4}$$

For each transmission or reception of P_s bytes of data, the energy measured is updated. The energy update while the normal node receives a data packet $E_{g+1}(n_j)$ and which in the cluster node $E_{g+1}(n_{cl})$ is stated in eq. (5).

$$E_{g+1}(n_j) = E_g(n_j) - E_{dis}(n_j) \tag{5}$$

$$E_{g+1}(n_{cl}) = E_g(n_{cl}) - E_{dis}(n_{cl}) \tag{6}$$

In the node, the energy minimizes promote as the transmission carries on and turns out to be a dead node.

3.2. Mobility Model

In [10], the mobility model indicates the movement of the IoT nodes in the network based on the position, acceleration, and velocity. In the network, this approach, in order, decides the performance of the method for data transmission. Consider n_1 and n_2 be two IoT nodes located at (y_1, z_1) and (y_2, z_2), correspondingly. At a time $t = 1$, both the nodes move to a novel position (y'_1, z'_1) and (y'_2, z'_2), such that the movement of the nodes is in a particular region. At each time immediately, the nodes will be positioned to a new position on the basis of their distance measures DM_1 and DM_2. The Euclidean distance among the IoT nodes and it is stated in eq. (7).

$$DM(0) = \sqrt{|y_1 - y_2|^2 + |z_1 - z_2|^2} \tag{7}$$

In eq. (7), $DM(0)$ indicates the distance measured at $t = 0$ among the nodes. While the nodes are implicit to be moving in directions δ_{n1} and δ_{n2}, the velocities in the nodes are indicated as ω_{n1} and ω_{n2}, and the distance measure for the two nodes are stated in eq. (8) and (9).

$$DM_{n1} = \omega_{n1} \times 1 \tag{8}$$

$$DM_{n2} = \omega_{n2} \times 1 \tag{9}$$

In eq. (8), 1 represents the time instant, ω_{n1} represents the velocity of node one and ω_{n2} represents the velocity of node two.

Therefore, the location (y'_1, z'_1) of the IoT node n_1 irregular to the new positions can be attained at a distance DM_{n1} is stated in eq. (10) and (11).

$$y'_1 = y_1 + \omega_{n1} \times 1 \times \cos(\delta_{n1}) \tag{10}$$

$$z'_1 = z_1 + \omega_{n1} \times t \times \cos(\delta_{n1}) \tag{11}$$

Likewise, the location (y'_2, z'_2) of n_2 at DM_{n2} is indicated in eq. (12) and (13).

$$y'_2 = y_2 + \omega_{n2} \times t \times \cos(\delta_{n2}) \tag{12}$$

$$z'_2 = z_2 + \omega_{n2} \times t \times \cos(\delta_{n2}) \tag{13}$$

Hence, the distance among the IoT nodes at any time t in the new positions can be calculated as eq. (14).

$$D(t)=\sqrt{\left|y_1'-y_2'\right|^2+\left|z_1'-z_2'\right|^2} \tag{14}$$

In eq. (14), (y_1',z_1') and (y_2',z_2') indicates the new locations obtained by the nodes n_1 and n_2, correspondingly.

4. Adopted Methodology

For multipath routing, the proposed method in WSN is explained and it is demonstrated in Fig. 2. It is an optimization-based routing which comprises of two most important stages: Multipath data transmission and CHS. The configuration of CH is on the basis of the [11], whereas the collection of heads based upon multiple objectives, namely distance, energy, delay, and LLT. The major contribution of the proposed model is multipath data transmission by exploiting the HSS-DE method which integrates SS and DE. The fitness models selected for this optimization method are energy, distance, intra-cluster delay, inter-cluster delay, and LLT that are chosen such that the energy, and the network lifetime, is high.

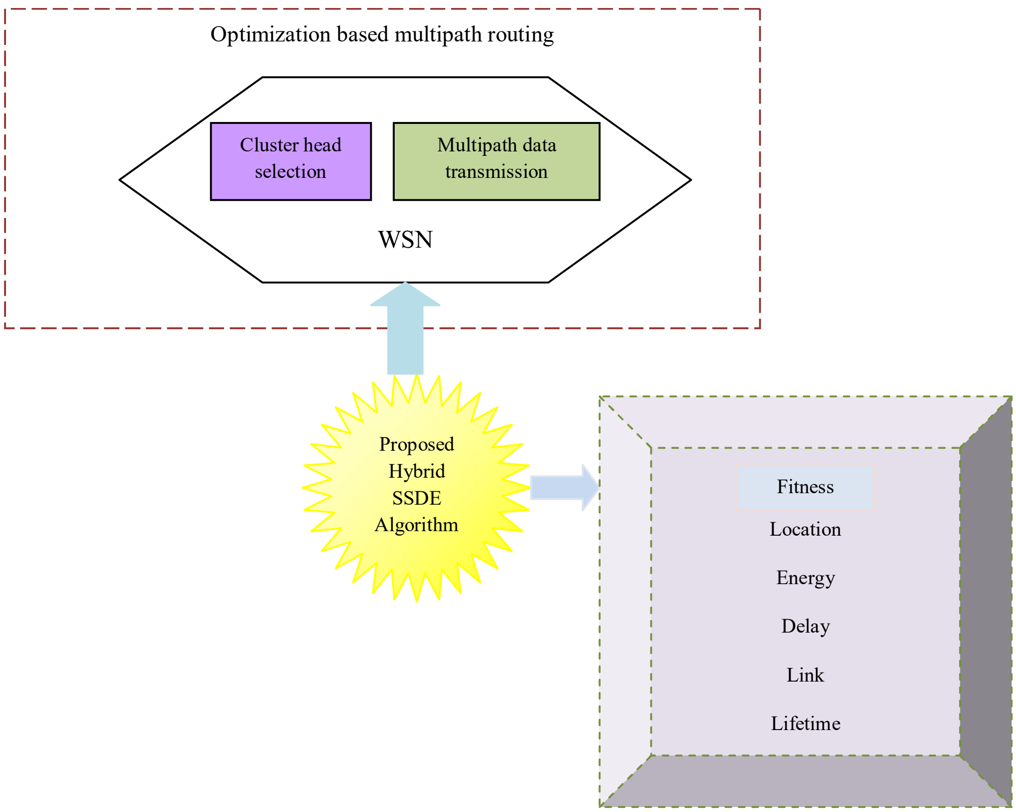


Fig. 2. *Schematic illustration of the adopted hybrid SS-DE algorithm*

In WSN based IoT, the CHS is necessary to present an effectual data transmission without packet loss. The communication can be done possible whilst the N number of devices indicated here as nodes, are collected into clusters in a wireless environment. For each cluster, it needs to discover CH, that directly engrosses in the transmission. As a result, it is essential to discover the CHs which have the necessary energy to transmit the data to the BS. In stage I, this is performed on the basis of the Salp Swarm and DE approach. This approach can choose the CHs from a collection of nodes by exploiting DE. The multiple objectives considered in the fitness model consecutively choose the CH consequently that the least obligation of a node to form a CH is obtained. Hence, the algorithm forms the CH with enhanced convergence.

4.1. Fitness Model

The basic issue which drives the optimization method is the fitness model. This objective model is consists of various parameters in order to select the CH to present an effectual transmission. In this approach the fitness metrics represent are node's position, delay energy, and LLT. For a transmission without packet drops, or other comparable effects, the position or the distance of the CH node from the BS is to be less. Therefore, in a cluster, the nodes which are in nearness to the BS are frequently chosen as CHs. Correspondingly, the LLT and energy have to be maximal for the nodes to take steps as CHs. Superior node energy, greater will be the LLT. In the fitness evaluation, the subsequent element is the delay which needs to be less. For the transmission, this refers that the CH select is suitable regarding the energy, distance, delay, and LLT. The fitness model of the proposed optimization algorithm is stated as eq. (15).

$$F_f^i = \gamma_1 * \left(1 - F_{f(lc)}^i\right) + \gamma_2 * \left(1 - F_{f(ef)}^i\right) + \gamma_3 * \left(1 - F_{f(dl)}^i\right) + \gamma_4 * \left(1 - F_{f(LLT)}^i\right) \tag{15}$$

In eq. (15), $F_{f(ef)}^i$ denotes the energy function, $F_{f(lc)}^i$ denotes the position, $F_{f(dl)}^i$ denotes the delay and $F_{f(LLT)}^i$ denotes link lifetime, which is stated in [11]. The CH encompassing least distance, superior energy and LLT with minimized delay are said to be the optimum CH which can get element in the communication [12].

4.2. Conventional Salp Swarm Algorithm

Generally, the Salp Swarm algorithm [13] starts by a population that is produced arbitrarily Y, with size N and dimension d. Subsequently, this population is partitioned into a follower group and a leader group. The leader's location y^1 indicates the solution of the stated issue, and this solution is updated in accordance with [13]:

$$y_i^l = \begin{cases} y_i^b + p_1\left(\left(u_i - l_i\right) \times p_2 + l_i\right) & p_3 \le 0 \\ y_i^b - p_1\left(\left(u_i - l_i\right) \times p_2 + l_i\right) & p_3 > 0 \end{cases} \tag{16}$$

In eq. (16), y_i^b and y_i^l indicates the optimal solution and the leader's location in the i^{th} dimension, correspondingly [13]. u_i and l_i indicate the upper and lower bound of the i dimension, correspondingly. p_2 and p_3 represents a uniform arbitrary set fits into the interval [0, 1] to protect the search domain. The parameter p_1 is used to preserve the balance among feature exploitation and exploration is calculated as [13]:

$$p_1 = 2e^{-\left(\frac{4t}{t_{max}}\right)^2} \tag{17}$$

In eq. (17), t states the current iteration and t_{max} indicates the utmost number of iterations correspondingly. Subsequent to updating the location of the leader, the locations of the followers y^j, $j = 2, ..., N$ are updated by exploiting the eq. (18).

$$y_i^j = \frac{1}{2}\left(y_i^j + y_i^{j-1}\right) \tag{18}$$

4.3. Conventional Differential Evolution (DE)

Generally, DE [14] initiates by initializing the arbitrary population Y, with d dimensions and solution N. By exploiting three operations named mutation, crossover, and selection, the population Y is updated.

Mutation Operation: The mutant vector is modeled by integrating the difference among two solutions with one more third solution subsequent to multiplying the difference using an amplification factor (δ); this approach is named DE/rand/1 and it is stated in eq. (19).

$$U_j^t = Y_{c_1}^t + \delta \times \left(y_{c_2}^t - y_{c_3}^t\right) \tag{19}$$

In eq. (18), c_1, c_2, and c_3 indicates mutual arbitrary limited integers chosen from $[1, N]$, and t indicates the number of the generation.

Crossover Operation: Here, an offspring solution X_j represents produced from two solutions Y_j and U_j, important to enhanced population diversity. Generally, two crossover approaches can be exploited such as the exponential and the binomial and the exponential. The creation of offspring solutions based upon the crossover probability $C_P \in$ [0, 1] in the binomial crossover.

$$X_{ji}^{t} = \begin{cases} U_{ji}^{t} & \text{if} \lambda \le C_P | i == i_r, i_r \in [1,2,....,d] \\ Y_{ji}^{t} & O.W \end{cases} \tag{20}$$

In eq. (20) $\lambda \in 2$ [0, 1] and i_r indicate an arbitrary number and an arbitrarily chosen dimension index. The exponential crossover approach possesses two parameters p and P (fits into $[1, d]$) which are chosen arbitrarily, whereas p indicates the index of the first location in target X_j from that and swap of elements with V_j begins. P indicates the total number of elements V_j given to X_j; this operation is stated in eq. (21).

$$X_{ji}^{t} = \begin{cases} U_{ji}^{t} & \text{for} i == < p >_d, ..., < p + P - 1 >_d \\ Y_{ji}^{t} & O.W \ \forall_i \in [1, d] \end{cases} \tag{21}$$

In eq. (21), $< p >_d$ indicates the modulo model with a modulus of d and p.

Selection Operation: Here, the offspring (X) survives whilst its fitness model is superior to that of its parents; this operation is stated in eq. (22).

$$Y_j^{t+1} = \begin{cases} X_j^t & \text{if} (X_j^t) \le f(Y_j^t) \\ Y_j^t & O.W \end{cases} \tag{22}$$

In eq. (22), $f(Y)$ indicates the objective function value of Y.

4.4. Adopted Hybrid SS-DE Technique

Fig. 3 demonstrates the flow chart of the proposed model, which is the amalgamation among the SS and DE algorithm. Generally, the proposed model, named Hybrid SS and DE, begins from the known issue as input and subsequently carries out the major steps for a particular number of iterations t_{max}.

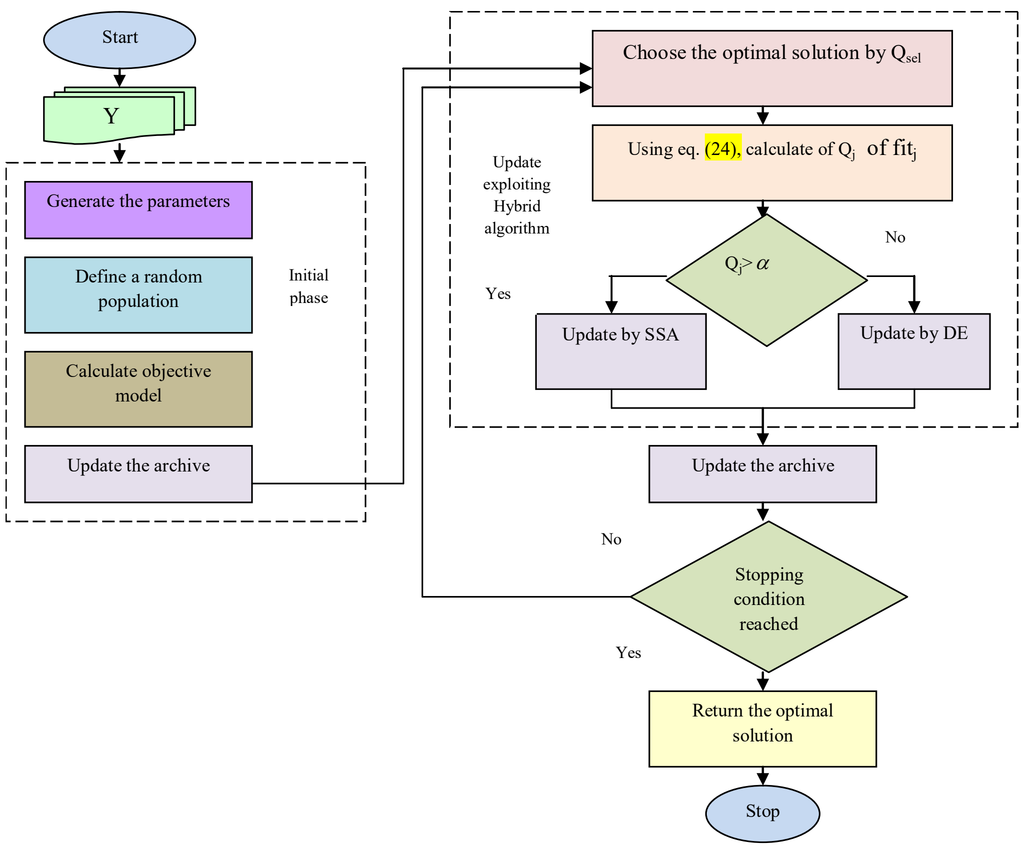


Fig. 3. *Flow chart of the proposed Hybrid SS-DE algorithm*

In the proposed technique, the DE is exploited to enhance the feature exploitation capability of the SSA as DE is exploited as a local search approach. The subsequent step is to update the archive which comprises the nondominated solutions. The proposed method verifies if the stopping criterion is convened. The proposed algorithm, three major phases will be done on every salps location: initialization, updating the salp location exploiting the proposed technique, and updating the archive to decide the estimate to the PF.

Here, an arbitrary population Y (with dimension d and size N) which indicates the solutions of the stated issue is produced. The input to this approach is N, d, l, and u, that indicate the population size, the dimension of the stated issue, the upper bound and the lower bound, correspondingly. Subsequently, the population is produced by exploiting the eq. (22).

$$Y = rn(N,d) \times (u - l) + l \tag{23}$$

In eq. (23), $rn(.,.)$ indicates a model that creates an arbitrary number from the uniform distribution. Every solution's objective model is subsequently calculated, in that it is stated as $F_i = [f_1, f_2]^T$ and should assure $-8 \le S \le 8$, whereas f_1 and f_2 is stated as objective models, correspondingly. Subsequently, the nondominated solutions are decided and the archive is updated.

In this work, the DE is used to enhance the feature exploitation capability of the SSA in attaining the best solution. The leader chosen method is applied to choose the optimal solution from the archive A_r which controls the nondominated solutions. The leader chosen method chooses a single nondominated solution from the minimum crowded segment as the optimal solution (y_b) [15]. The roulette-wheel method is used to select y_b by exploiting the following probability (Q_{sel}):

$$Q_{sel} = PA \times N_{seg_j} \tag{24}$$

In eq. (24), N_{seg_j} and $PA > 1$ indicates the number of Pareto optimal solutions of the i^{th} segment and a constant, correspondingly.

Subsequent to choosing the optimal solution, the subsequent step is to calculate the probability ($Prob$) which is exploited to update the solutions by either DD or SSA. For each solution, this $Prob$ is computed regarding the first objective model's value.

$$Q_j = \frac{f_1}{\sum_{j=1}^{N} f_1} \tag{25}$$

Subsequently, the present solution y_j is updated by exploiting the conventional DE or SSA on the basis of the value of Q_j and y_b. For instance, if the value of $Q_j > \alpha$ (whereas $\alpha \in [0, 1]$; in reality, the mainly appropriate value of was established to be 0.65), after that the operator of the SSA is exploited to update y_j; else, the operators of the DE are exploited to update y_j. Hence, in the scenario that Q_j is fewer than the threshold, these ways in which the present solution y_j has a possibility to be involved to a stagnation point, and consequently, the operators of DE work over this propensity. Generally, the objective of eq. (25) is to give an appropriate scheme for switching among SSA and DE rather than exploiting an arbitrary approach, in that a small Q_j indicates that the present solution requires to be enhanced by exploiting the DE operators. Additionally, the first fitness model can be returned by another model before by constraints to select the model in eq. (25).

Subsequent to the DE operators are used to enhance the feature exploitation capability of the SSA; A_r is updated by deciding the non-dominated solutions and addition them to A_r. Hence, selecting the optimal non-dominated solutions to improve convergence to the PF is significant. This procedure resembles the schemes which employ Pareto supremacy to discover non-dominated solutions and subsequently employ density estimation information to sustain population diversity [16].

The procedure of updating the archive begins by the addition of the novel population to A_r, subsequent to that the dominated and non-dominated solutions are decided. Subsequently, every solution is evaluated over all the non-dominated solutions in A_r by exploiting Pareto supremacy. If any solution dominates a solution in A_r, subsequently the two should be exchanged. Additionally, if a solution controls a set of solutions in A_r, after that this set should be separated from A_r, and the solution is further to A_r. Furthermore, if any solution in A_r (as a minimum 1) controls the present solution, after that it should be mistreated. Nevertheless, few particular scenarios subsist whereas the solution controls other solution(s) in A_r, and A_r turns out to be complete. Two approaches can be exploited to solve this circumstance: a) eliminate a solution in A_r arbitrarily after that swap it with the solution which is nondominated or b) remove one of the solutions which are nondominated and related in A_r, whereas the non-dominated solution which encompass the greatest possibility of being removed from A_r is a solution in a well-populated area. During the iterations, this approach improves the elements distribution of A_r.

To decide those solutions, the method calculates the number of neighboring solutions with a particular distance, whereas the distance is calculated by exploiting the eq. (26).

$$D = \frac{\max(f_j) - \min(f_j)}{|A_r|}, \quad i = 1,2 , \tag{26}$$

In eq. (26), $|A_r|$ indicates the archive size. The optimal scenario is while A_r contain one solution in every section. Subsequent to deciding the rank of every element of A_r in accordance with the number of neighbouring solutions, the chosen of one of them is done exploiting a roulette wheel. The solution which possesses the highest rank number is established, and that solution possesses the maximum probability of being deleted from A_r. The solutions of the population Y are updated on the basis of the updated A_r by selecting the optimal N solutions from it. These solutions are chosen from the primary front; if this does not produce adequate solutions, subsequently the residual solutions are chosen from the second front.

5. Results and Discussions

5.1. Experimental Setup

In this section, the simulation outcomes of the proposed technique for multi-path data transmission in IoT were presented. For the comparison analysis, the simulation was performed in five rounds, such as 100, 200, 300, and 400 and 500. Here, the proposed technique was evaluated with four traditional techniques such as ABC, ACO, GWO, and GSA. Moreover, the performance is analyzed with respect to the network energy and alive nodes, which was explained as follows.

5.2. Performance Analysis

Fig. 4 exhibits the performance analysis of the proposed technique with conventional techniques regarding the number of alive nodes. Here, the performance of the proposed method is 15% better than the ABC, 12% better than the ACO, 15% better than the GWO and 7% better than the GSA algorithm for round 500.

Fig. 5 shows the performance analysis of the proposed technique with conventional techniques regarding network energy. Here, the performance of the proposed method is 25% better than the ABC, 11% better than the ACO, 36% better than the GWO and 6% better than the GSA algorithm for round 100.

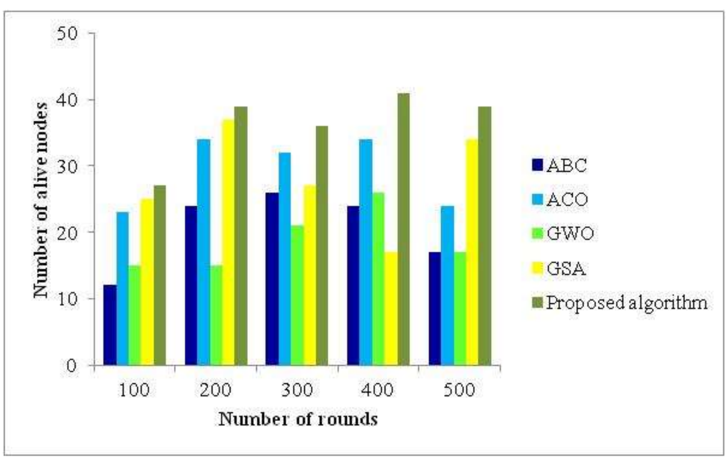


Fig. 4. *Performance analysis of the proposed technique concerning the number of alive nodes*

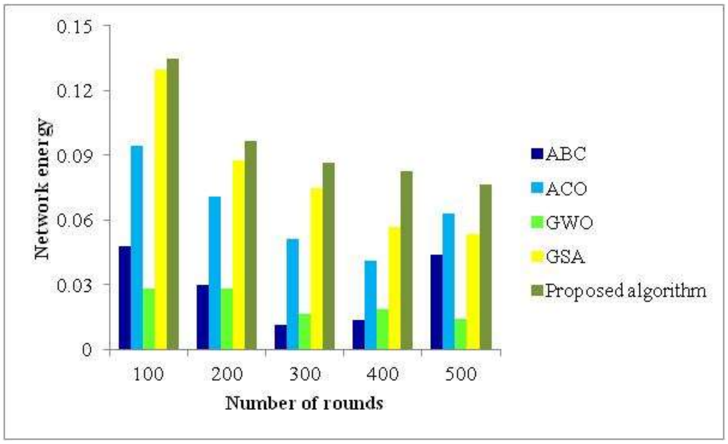


Fig. 5. *Performance analysis of the proposed technique concerning network energy*

6. Conclusion

In this paper, the hybrid SS-DE algorithm with an enhanced lifetime was proposed for multipath transmission in IoT. This proposed method was performed in two phases. At the initial phase, CHS was done based on the SS algorithm. In the subsequent stage, the multipath transmission was performed by using the DE method. The fitness model of the proposed method contemplates the metrics, like distance, energy, inter and intra-cluster delay and LLT to choose the optimal solution. Hence, the proposed approach discovers the routes with maximum energy, least distance minimized delay and an enhanced lifetime as the optimum paths for the multipath transmission. In data transmission, to calculate the performance level of the proposed technique the performance of the proposed method was evaluated with three conventional models concerning maximum energy and the number of alive nodes.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Jafar A. Alzubi, Ramachandran Manikandan, Omar A. Alzubi, Issa Qiqieh, Ashish Khanna, "Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud", Measurement, Volume 150, January 2020.
[2] Debasish Ghose, Anders Frøytlog, Frank Y. Li, "Enabling early sleeping and early data transmission in wake-up radio-enabled IoT networks", Computer Networks, Volume 153, 22 April 2019, Pages 132-144.
[3] Nasir N. Hurrah, Shabir A. Parah, Javaid A. Sheikh, Fadi Al-Turjman, Khan Muhammad, "Secure data transmission framework for confidentiality in IoTs", Ad Hoc Networks, Volume 95, December 2019.
[4] Arezou Ostad-Sharif, Hamed Arshad, Morteza Nikooghadam, Dariush Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme", Future Generation Computer Systems, Volume 100, November 2019, Pages 882-892.
[5] Rihab Boussada, Balkis Hamdane, Mohamed Elhoucine Elhdhili, Leila Azouz Saidane, "Privacy-preserving aware data transmission for IoT-based e-health", Computer Networks, Volume 162, 24 October 2019.
[6] X. Chen et al., "iDiSC: A New Approach to IoT-Data-Intensive Service Components Deployment in Edge-Cloud-Hybrid System," IEEE Access, vol. 7, pp. 59172-59184, 2019.
[7] Y. Inagaki, R. Shinkuma, T. Sato and E. Oki, "Prioritization of Mobile IoT Data Transmission Based on Data Importance Extracted From Machine Learning Model," IEEE Access, vol. 7, pp. 93611-93620, 2019.
[8] C. Song, Y. Qi and M. Liu, "One-Request Scheme for M2P Data Transmissions in Software-Defined IoT Networks," IEEE Access, vol. 6, pp. 13090-13100, 2018.
[9] Rajeev Kumar and Dilip Kumar, "Multi-objective fractional artificial bee colony algorithm to energyaware routing protocol in wireless sensor network," Wireless Networks, vol. 22, no. 5, pp. 1461–1474, July, 2016.
[10] Ajay Kumar Yadav and Sachin Tripathi, "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 897-909, July, 2017.
[11] Amol V. Dhumane, Rajesh S. Prasad, "Multi-objective fractional gravitational search algorithm for energy efficient Routing in IoT," Wireless network, pp. 1-15, August, 2017.

[12] Amol V. Dhumane and Rajesh S. Prasad, "Fractional Gravitational Grey Wolf Optimization to Multi-Path Data Transmission in IoT", Wireless Personal Communications, September 2018, Volume 102, Issue 1, pp 411–436.
[13] S. Mirjalili, A.H. Gandomi, S.Z. Mirjalili, S. Saremi, H. Faris, S.M. Mirjalili, Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems, Adv. Eng. Softw. 114 (2017) 163–191.
[14] R. Storn, K. Price, Differential Evolution: A Simple and Efficient Heuristic for global Optimization over Continuous Spaces, J. Glob. Optim. 11 (1997) 341-359.
[15] S. Mirjalili, S. Saremi, S.M. Mirjalili, L.S. Coelho, Multi-objective grey wolf optimizer: A novel algorithm for multi-criterion optimization, Expert Syst. Appl. 47 (2015)106119.
[16] K. Deb, S. Agrawal, A. Pratap, T. Meyarivan, A Fast Elitist Non-Dominated Sorting Genetic Algorithm for Multi-Objective Optimization: NSGA-II, in: Int. Conf. Parallel Probl. Solving from Nat., 2000: pp. 849-858.
[17] Christin D, Reinhardt A, Mogre PS, Steinmetz R., "Wireless sensor networks and the internet of things: selected challenges," in Proceedings of the 8th GI/ITG KuVS Fachgesprach Drahtlose Sensornetze, pp. 31-33, August, 2009.
[18] Alessandro Di Stefano, Aurelio La Corte, Marco Leotta, Pietro Lio, Marialisa Scata, "It measures like me: An IoTs algorithm in WSNs based on heuristics behavior and clustering methods," Ad Hoc Networks, Vol. 11, no. 8, pp. 2637–2647, November, 2013.