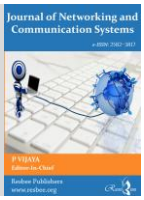
Resbee Publishers

Journal of Networking and Communication Systems

Received 17 December, Revised 18 February, Accepted 27 March



Multicast Routing in WSN using Bat Algorithm with Genetic Operators for IoT Applications

M Anandkumar
Department of Computer Science
Adigrat University, Ethiopia
anandmkumar15@gmail.com

Abstract: Wireless Sensor Networks (WSN) acts as an intermediate to link the network of Internet of Things (IoT). Trust and Energy were the two important aspects that make easy reliable communication in the network and throughout multicast routing, the Base Station (BS) connects to forward the data securely to numerous destinations. This work addresses the confronts by presenting an "energy-aware multicast routing protocol" based on optimization, Bat algorithm based on Genetic algorithm operators with the objective function modeled such as energy and trust factors of the nodes. At first, the trusts of nodes are validated to establish the routes which are selected optimally exploiting the proposed technique. The experimentation is verified by exploiting 50 and 100 nodes regarding the performance metrics.

Keywords: WSN; Iot; Base Station; Trust; Energy; Nodes

Nomenclature

Abbreviations	Descriptions
QoS	Quality of Service
IPV6	Internet Protocol Version 6
UAV	Unnamed Aerial Vehicles
CNN	Convolutional Neural Network
ADLs	Activities of Daily Living
FBCFP	Fuzzy based Cluster Formation Protocol
EE-CATS	Energy-Efficient Context-Aware Traffic Scheduling
BA	Bat algorithm
GA	Genetic algorithm

1. Introduction

In IoT, the up-and-coming applications related to federally organized WSNs, are presumptuous constantly-increasing importances for citizens working or living in extremely urbanized areas and it is believed as demanding research and industrial research areas for numerous years. The widespread construction comprises of sensors, routing nodes/ intermediate nodes and sinks in WSN-facilitated IoT appliances. Conventionally, to attain cross-regional data transmission, gathering, and several static sinks about inadequate power is organized. Therefore, the base station typically represents a performance of the system bottleneck. With no generality loss, in the worldwide WSN structural design, event-driven or data-driven sensors collect the information concerning their environs and distribute the information to their base stations; though, the data collection procedure, and transmission, mostly endures from three intolerable faults. These nodes close to a sink unavoidably require relay data, consequently, a gathering of is typically compulsory on such nodes whose energy will be worn out very quickly than other nodes.

In wireless networks, a multi-hop routing among source to base station permits development in energy consumption by minimizing the energy transmission power-constrained devices. Therefore, adapting multi-hop topologies can assist in minimizing the energy utilization of IoT devices as well in evading interference in IoT infrastructures. Actually, a large number of IoT appliances necessitate this sustain for multi-hop communiqué where mediator devices assist with one another and with end devices.

In IoT devices, intelligence can be developed during soft computing and machine learning techniques. In such cases, the sensor in IoT could employ the principles created using deep learning techniques to

https://doi.org/10.46253/jnacs.v3i2.a1

make effectual decisions to be made. In addition, device mobility is too permitted in IoT, and therefore the structure of rules for energy optimization, mobility management, and intellectual routing is the significant challenge in IoT oriented networks. In addition, an inference engine was modeled to effectual decisions making regarding enhancement in QoS in the IoT environment. Nevertheless, the data representation, collection, storage, and communication have to simultaneously assist for the effectual functioning of IoT. It could be attained using machine learning and rule-oriented techniques to make intelligent communications.

The main objectives of the paper are to model and propose an efficient method for trust and energy-aware multicast routing in WSN. Moreover, an improved edition of the renowned multicast routing method based on the BA with GA is presented. It aspires to regard as the parameters such as energy and trust that are used to devise the objective function for the developed routing model, named Hybrid Bat and Genetic algorithm.

2. Literature Review

In 2020, Ming Tao et al [1], proposed a multi-objective dual optimization concerning numerous restraints. Then, for addressing the major secure susceptibility on UAV oriented data collection, an authority substantiation technique exploiting the exact process was examined to put into effect the data collection conference to be performed with a satisfactory delay in the authentication.

In 2018, K. Thangaramya et al [2], developed a novel protocol named neuro- FBCFP that carries out learning of the network by taking into consideration 4 significant modules "current energy level, Cluster Head distance, change in the area amongst the nodes and the Cluster Head". Hence, the system was trained about CNN with fuzzy rules for weight modification. In addition, the fuzzy technique was exploited for dominant cluster configuration and to carry out cluster-based routing.

In 2017, Bilal Afzal et al [3], realized competent resource allotment to Wi-Fi-based IoT infrastructures. Initially, IoT appliances were differentiated and mapped to different biased quality classes. Subsequently, context awareness was developed along with optimization techniques that were constrained through the service quality and context priorities requirements.

In 2019, Nailah Saleh Alhassoun et al [4] developed wall-powered and battery-operated IoT devices to make sure security of inhabitants. A semantic method was used which uses the context of extracted ADLs to make optimized sensor activation. Also, a mature fall recognition system was employed that exploited the sensing devices derived from an authentic SCALE project for examining the technique.

In 2017, Manu Elappila et al [5], developed an interference and congestion aware routing model for WSN. This model was theoretical for transmitting the packets to a destiny at a similar time that was a characteristic situation in IoT. For choosing the subsequent node, the method exploits a principle with 3 factors namely "signal to interference and link noise ratio, the survivability factor the path from the subsequently hop node to the destination, and the congestion level at the subsequently hop node".

In 2016, Pan and Yang [6], developed a lightweight multicast routing approach. The proposed method comprises three stages. Initially, the primary stage chooses intermediate nodes to attain multicast destinations. Subsequently, the next stage evades loops and trims routes modeled in the primary stage. As a final point, the preceding stage ensures if the chosen multicast links can additionally be integrated. The experimentation outcomes point out that the developed model can efficiently decrease transmission links and shorten path lengths in the modeled multicast paths.

3. Adopted Protocol for Multicast Routing

In IoT, the mobile nodes are given for estimating the fit factor that is based on energy and trust. For optimum choosing of routes, they are discovered depending on the chosen secure nodes. The routes were chosen on the basis developed algorithm that is the adaptation of the genetic operators. For transmitting data, the optimal selected path was exploited which is ensued about the energy and trust update. The trust and the energy of the individual nodes are updated latterly of the individual transmission so that the secured node is chosen by exploiting the fit factor. Fig. 1 exhibits the architecture model of the proposed algorithm. The network comprises of n IoT mobile nodes which are occupied in forwarding and gathering the data to a destination.

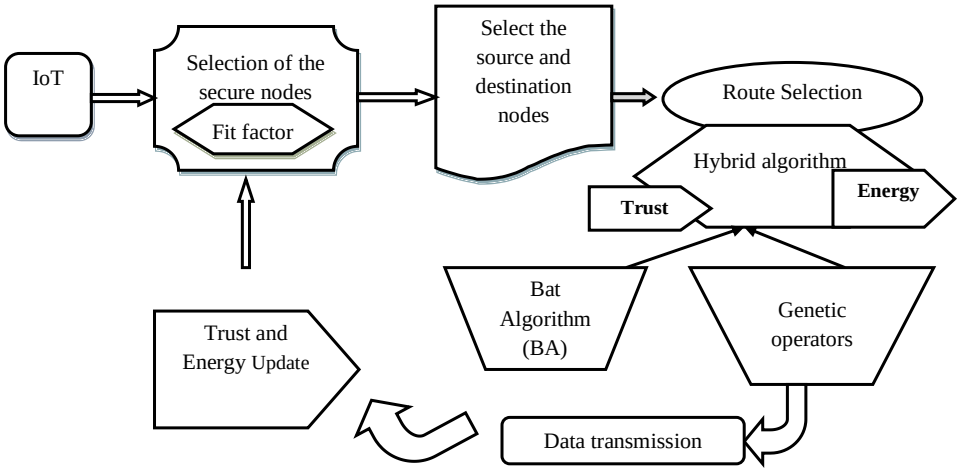


Fig. 1. *Architecture diagram for multi-cast routing exploiting proposed model*

WSN mobility technique: The mobility of the nodes [7] explains the velocity, acceleration, and position of nodes in the surroundings. The routing protocol performance is verified about the mobility model based upon the distance. Consider presume 2 nodes N_i and N_j positioned at (u_i, v_i) and (u_j, v_j) so that $\Omega^i \in (u_i, v_i)$ and $\Omega^j \in (u_j, v_j)$. N_i and N_k traverse in an exacting direction during uneven velocity by means of an angle θ_1 and θ_2. The nodes N_i and N_k travel a distance ∂_1 and ∂_2, and after moving an exacting distance, the nodes achieve a new location (u_i^{new}, v_i^{new}) and (u_j^{new}, v_j^{new}), correspondingly. Primarily, the Euclidean distance of the nodes at locations $N_i(u_i, v_i)$ and $N_j(u_j, v_j)$ is stated in eq. (1).

$$\partial_{(uv,0)} = \sqrt{|u_i - u_j|^2 + |v_i - v_j|^2} \tag{1}$$

The nodes velocity N_i and N_k is v_{N_i} and v_{N_j} creating an angle θ_1 and θ_2 to travel the distances ∂_1 and ∂_2 which is indicated as follows:

$$\partial_1 = v_{N_i} \times t \tag{2}$$

$$\partial_2 = v_{N_j} \times t \tag{3}$$

At t, the node obtains a novel location, which is stated as follows:

$$u_i^{t+1} = u_i^t + v_{N_i} \times t \times \cos\theta \tag{4}$$

$$v_i^{new} = v_i^{old} + \vartheta_{N_i} \times t \times \cos\phi \tag{5}$$

While the node $N_k(u_k, v_k)$ travels a distance ∂_2 creating an angle θ_2, N_j obtain a novel location as stated below:

$$u_j^{t+1} = u_j^t + v_{N_j} \times t \times \cos\theta \tag{6}$$

$$u_j^{t+1} = u_j^t + v_{N_j} \times t \times \cos\theta \tag{7}$$

After the nodes achieve a novel location, the distance among the nodes is calculated as eq. (8).

$$\partial_{\left(u^{t+1} v^{t+1}, t\right)} = \sqrt{\left|u_i^{t+1} - u_j^{t+1}\right|^2 + \left|v_i^{t+1} - v_j^{t+1}\right|^2} \tag{8}$$

3.1 Fit Factor Calculation

In the network, fitness is an important aspect to decide the secured nodes to develop secured communication that enhances data integrity and confidentiality. The fit factor is devised depending on the trust and energy of individual nodes in the network and the node about the maximum energy and trust is selected to be a secure node. The fitness is calculated as eq. (9).

$$Fit_{ij} = D = \frac{1}{2} \times \left[\varepsilon_i + \frac{1}{N} \times \sum_{\substack{j=1 \\ i \in j}}^{N} T_{ij} \right] \tag{9}$$

In eq. (9), T_{ij} indicates the trust factor of the j^{th} neighbor of the i^{th} node and N indicates the total number of the neighbors, ε_i indicates the energy of the i^{th} node in the IoT network. From the IoT network, the real nodes are selected based on the energy and the trust of the nodes that are subsequently subjected to the route chosen phase exploiting the developed optimization.

3.2 Trust Calculation

The energy model [9] and trust [8] of IoT nodes are calculated in eq. (10).

$$T_{ij} = T_{i,j}^{direct} + T_{i,j}^{indirect} + T_{i,j}^{recent} + T_{i,j}^{bytes} \tag{10}$$

The trust exploited to evaluating the node trust is direct trust $T_{i,j}^{direct}$, indirect trust $T_{i,j}^{indirect}$, new trust $T_{i,j}^{recent}$, and trust- based on the number of bytes transmitted $T_{i,j}^{bytes}$. Trust factors include:

Direct trust: It [8] depends upon the variation in the estimated and actual time and this calculation is based upon the witness factor that donates for the improvement of node trust. The fitness depends on i^{th} node that admits the public key and the s^{th} base station in IoT that authenticates the node interpretation of the public key. Hence, the direct trust is devised as eq. (11).

$$T_{i,j}^{direct}(t) = \frac{1}{3}\left[T_{i,j}^{direct}(t-1) - \left[\frac{T^{key} - E^{key}}{T^{key}} \right] + \omega \right] \tag{11}$$

In eq. (10), E^{key} indicate the anticipated time to receive the key, T^{key} denotes the suitable time necessary to transmit the key and ω denotes the witness factor of j^{th} destination.

Indirect trust: It [8] is important when a node obtains the public key for validation which does not embrace an observer value. Indirect trust is stated in eq. (12), N shows the total neighbor nodes in i^{th} node.

$$T_{i,j}^{indirect}(t) = \frac{1}{N}\sum_{i=1}^{N} T_{i,x}^{indirect}(x) \tag{12}$$

Recent trust: In the network, the recent trust [10] is calculated as devised in eq. (13), $\alpha = 0.3$.

$$T_{i,j}^{recent}(t) = \alpha * T_{i,j}^{direct}(t) + (1-\alpha) \times T_{i,j}^{indirect}(t) \tag{13}$$

Trust based on data bytes: The routing robustness is improved during the addition of the trust factor which is based on the data bytes that depend upon the whole count of data bytes transmitted from the source node to the total number of the data bytes and it is stated in eq. (14).

$$T_{i,j}^{\partial} = \frac{1}{2} \times \left[\frac{\partial_{i,j}^{i}}{d} + \frac{\partial_{i,j}^{j}}{d} \right] \tag{14}$$

In eq. (14), $\partial_{i,j}^{j}$ indicates the bytes achieved by the destination node and $\partial_{i,j}^{i}$ indicates the data bytes forwarded using the source node. The data packet limits are indicated as d.

3.3 Network Energy Model

In IoT, the sensors are completely battery-operated and therefore, nodes energy is the most important constraint that requires to be controlled as it is necessary to extend the life-span of the IoT network. In the node consider the energy [11] at the start of the communication is ε_0. Whilst transmitting data packets, the dissipation of energy happens as per eq. (15).

$$\varepsilon_{dis}(K_i) = \varepsilon_{elec} \times \ell_i + \varepsilon_{pa} \times \ell_i \times \left\| K_i - H_j \right\|^4 ; \text{if } \left\| K_i - H_j \right\| \geq \beta_0 \tag{15}$$

In eq. (15), $\varepsilon_{dis}(N_i)$ indicates the energy dissipation, ε_{elec} indicates the electronic energy of i^{th} node. The count of bytes transmit by i^{th} node is indicates as, ℓ_i and ε_{pa} indicates the energy of power amplifier. The dissipation of energy depends on β_0 so that the distance among the i^{th} sensor node and j^{th} head is calculated and evaluated with β_0. When the distance among nodes K_i and its equivalent H_j lies under β_0, the energy dissipation in the normal sensor node depends on eq. (15) or else, the energy dissipation of K_i is calculated depends on eq. (16).

$$\varepsilon_{dis}(K_i) = \varepsilon_{elec} \times \ell_i + \varepsilon_{fs} \times \ell_i \times \left\| K_i - H_j \right\|^2 ; \text{if } \left\| K_i - H_j \right\| < \beta_0 \tag{16}$$

$$L_{D_0} = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{pa}}} \tag{17}$$

In eq. (17), ε_{fs} denotes the energy in free space. The electrical energy is stated in eq. (18).

$$\varepsilon_{elec} = \varepsilon_{tx} + \varepsilon_{agg} \tag{18}$$

In eq. (18), ε_{agg} denotes the data aggregation energy, and ε_{tx} stands for the transmitter energy. $\|K_i - H_j\|$ symbolize the distance between the i^{th} node and j^{th} CH. The energy dissipated at j^{th} cluster head is stated in eq. (19).

$$\varepsilon_{dis}(H_j) = \varepsilon_{elec} \times \ell_i \tag{19}$$

Formerly the transmission of data and reception ends, the nodes and CHs are updated as stated below:

$$\varepsilon_{t+1}(K_i) = \varepsilon_t(K_i) - \varepsilon_{dis}(K_i) \tag{20}$$

$$\varepsilon_{t+1}(H_i) = \varepsilon_t(H_i) - \varepsilon_{dis}(H_i) \tag{21}$$

In eq. (19), (H_j) denotes the dissipated energy of CH through the transmission of data packets by the normal node.

4. Optimized Proposed Approach for Trust Energy Routing

4.1 Smart Inertia Weight

The arithmetical formulation of BA has a few resemblances to PSO [12]. Moreover, the exploitation and the exploration ability of PSO are improved by integrating inertia weight [13]. Hence, [14] have used inertia weight to the conventional Bat Algorithm. Here, an inertia weight is exploited for balancing the exploration and exploitation astutely, which is computed as follows:

$$w_{k_i} = \left(w_{end} + (w_* - w_{end}) \times \frac{(T_{max} - k)}{T_{max}} \right) \times \tau \frac{(f_{max} - f_i)}{(f_{max} - f_{min})} \times \psi \tag{22}$$

In eq. (22), w_* indicates the utmost inertia weight factor, k designates the utmost count of iterations, w_{end} point out the least inertia weight factor, f_{max} indicates the optimal fitness value, k indicates the present number of iterations, f_{min} indicates the worst fitness value, f_i indicates the fitness value of the bat, ψ and τ indicates constants. It is understandable that the developed weight comprises of 2 types. The inertia weight alters the number of iterations in the linearly minimizing part. It guarantees that the proposed method has a high inclusive penetrating ability. In addition, the other element can update the location of the bat based on the fitness value. Hence, the updated equation is defined in eq. (23), $U_i(t)$ indicates velocity, X_i indicates location.

$$U_i(t+1) = w_{k_i} * U_i(t) + (Y_i(t) - y_*) f_i \tag{23}$$

4.2 Crossover Operation

Local searching is an important segment of the conventional Bat algorithm. Nevertheless, the arbitrary walk is not adequate for multifaceted tasks. Here, the hybrid BA with the crossover functions of GA [15] to resolve this issue. The arithmetical modeling of GA is shown in eq. (24).

$$\bar{y}_{new} = w_{k_i} * p_{best} * (1 - c) + y_* * c \tag{24}$$

In eq. (24), p_{best} indicates the optimal solution of current iteration, y_* indicates the global optimal solution and c indicates constant. Fig 2 shows the flow chart of the proposed model.

4.3 Beta Distribution

In the conventional BA, the frequency is updated as per Eq. (25), β indicates the random number.

$$f_i = f_{min} + (f_{max} - f_{min})\beta \tag{25}$$

Nevertheless, the formulations do not obtain the fitness value of every bat into deliberation [16]. In the new arithmetical formulation, the frequency will be updated based on the fitness value of every bat. The beta distribution is stated in eq. (26).

$$f(y; a, b) = \frac{y^{a-1}(1-y)^{b-1}}{\int_0^1 v^{a-1}(1-v)^{b-1} du} \tag{26}$$

where $a > 0$ and $b > 0$ indicates constant.

The frequency update formulation is stated in eq.(27).

$$\begin{cases} f_i = f_{min} + (f_{max} - f_{min}) * B(a_1, b_1) \text{ if } fit(i) < avg(fit) \\ f_i = f_{min} + (f_{max} - f_{min}) * B(a_2, b_2) \text{ if } fit(i) > avg(fit) \end{cases} \quad (27)$$

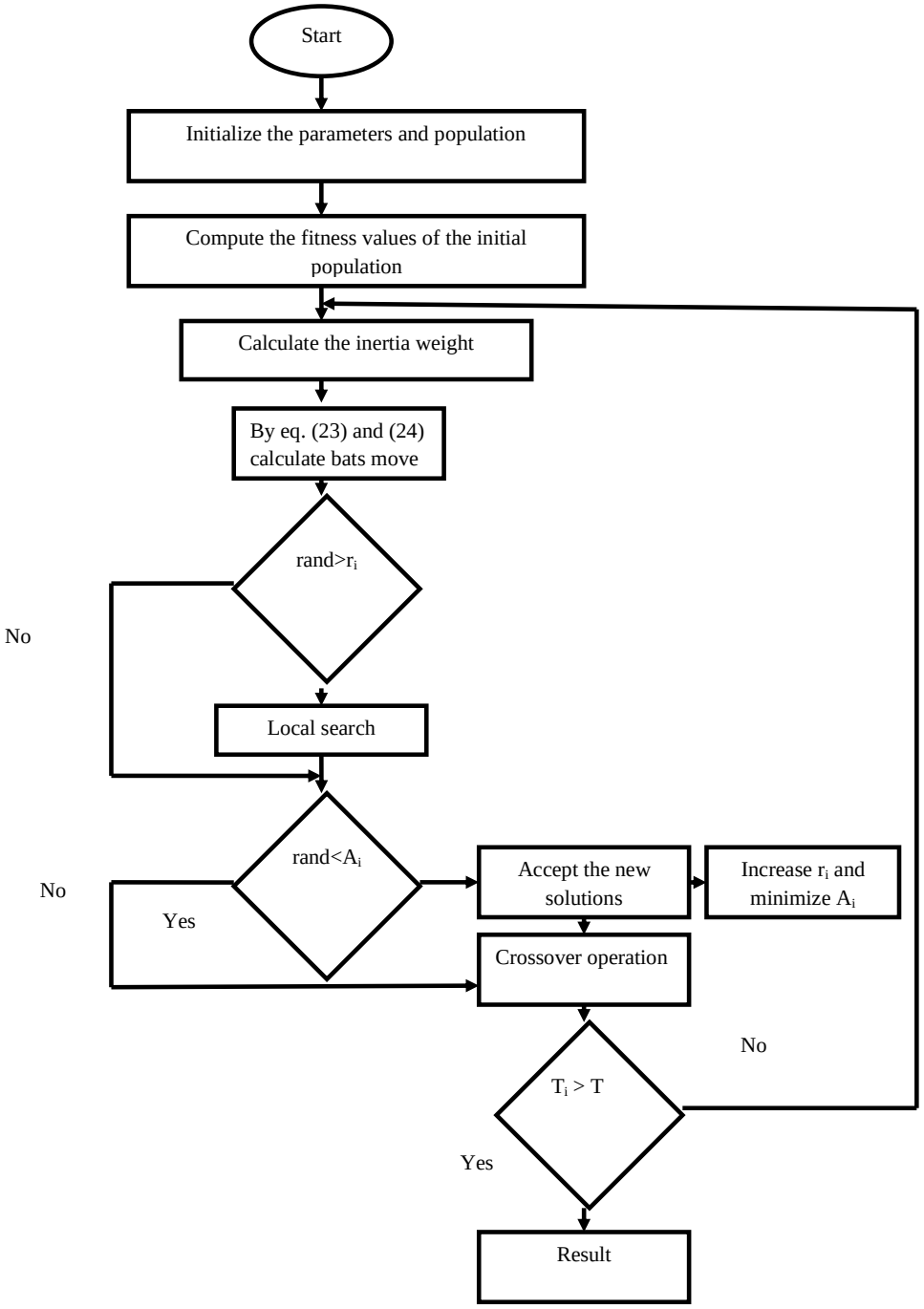


Fig. 2. *Flow chart of the proposed model*

5. Result and Discussion

5.1 Experimental Procedure

In this section, the simulation analysis of the IoTs using a developed multicast routing model was discussed. The analysis of the outcomes was extremely detailed. The experimentation has experimented in MATLAB and the experimentation was analyzed with 50 and 100 nodes to analyze the absence or presence of the two kinds of attacks.

5.2 Performance Analysis

Tables 1 and 2 summarize the analysis of 50 nodes 100 nodes based on the performance measures in the presence of attacks. In Table 1, the developed technique obtained minimal delay, maximal energy, throughput, and detection rate. The analysis is done using 100 nodes in the experimentation, the delay of the developed technique has attained minimal delay, maximal energy, throughput, and detection rate. At last, Tables 3 and 4 show the analysis in terms of attacks. The techniques are evaluated based on the performance measures and it was known that the developed technique obtained the maximal throughput, minimal delay, and maximum energy, for both nodes.

Table 1: *Analysis of adopted and existing approaches with the presence of attacks for 50 nodes*

Methods	Delay	Detection Rate	Throughput	Energy
ABC	0.4313	0.7737	0.3983	74.3481
PSO	0.4181	0.7737	0.0744	71.371
GA	0.4771	0.7737	0.3983	47.7494
CSA	0.4713	0.7737	0.0744	73.0087
WOA	0.4087	0.7737	0.0744	71.3997
Proposed	0.3739	0.7737	0.0744	77.4374

Table 2: *Analysis of adopted and existing approaches with the presence of attacks for 100 nodes*

Methods	Delay	Detection Rate	Energy	Throughput
ABC	0.3603	0.6989	76.8133	0.0663
PSO	0.3819	0.6989	76.6678	0.3983
GA	0.3336	0.6989	77.6766	0.0663
CSA	0.3638	0.6989	77.3893	0.0663
WOA	0.313	0.6989	76.0186	0.3133
Proposed	0.3123	0.7338	83.1776	0.3368

Table 3: *Analysis of adopted and existing approaches with the absence of attacks for 50 nodes*

Methods	Delay	Energy	Throughput
ABC	0.4277	44.11	0.7441
PSO	0.4977	44.4479	0.7472
GA	0.4244	42.7277	0.7422
CSA	0.4419	42.2747	0.7422
WOA	0.4422	44.9422	0.7441
Proposed	0.2491	71.0447	0.7449

Table 4: *Analysis of adopted and existing approaches with the absence of attacks for 100 nodes*

Methods	Delay	Energy	Throughput
ABC	0.303	79.533	0.9339
PSO	0.3263	79.99	0.9663
GA	0.3629	79.337	0.9723
CSA	0.335	79.927	0.9762
WOA	0.3357	90.373	0.9597
Proposed	0.1955	92.53	0.9917

6. Conclusion

In IoT applications, the energy-aware multicast routing was important that is carried out by exploiting the developed optimization, Hybrid Bat, and Genetic approach. For multicast routing, the optimal chosen of the routes was enabled exploiting the objective model based upon the energy and trust factors that select the efficient nodes to establish the routes. In the experimentation environment, the evaluation exploiting 50 and 100 nodes shows that the developed technique obtained superior performance in evaluating the conventional techniques. The evaluation with 50 nodes shown that the developed technique obtained a minimal delay, maximal energy, throughput, and detection rate. Conversely, in the non-attendance of the attacks, the developed technique obtained higher throughput. Similarly, the evaluation exploiting 100 nodes obtained superior outcomes regarding the performance measures.

References

[1] Ming Tao, Xueqiang Li, Huaqiang Yuan, Wenhong Wei,"UAV-Aided trustworthy data collection in federated-WSN-enabled IoT applications", Information Sciences, Volume 532, September 2020, Pages 155-169.

[2] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, A. Kannan," Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT",Computer Networks, Volume 15114 March 2019, Pages 211-223.

[3] Bilal Afzal, Sheeraz A. Alvi, Ghalib A. Shah, Waqar Mahmood,"Energy efficient context aware traffic scheduling for IoT applications" Ad Hoc Networks, Volume 62, July 2017, Pages 101-115.

[4] Nailah Saleh Alhassoun, Md Yusuf Sarwar Uddin, Nalini Venkatasubramanian, "Context-aware energy optimization for perpetual IoT-based safe communities, Sustainable Computing: Informatics and Systems, Volume 22, June 2019, Pages 96-106.

[5] Manu Elappila, Suchismita Chinara, Dayal Ramakrushna Parhi,"Survivable Path Routing in WSN for IoT applications", Pervasive and Mobile Computing, Volume 43, January 2018, Pages 49-63.

[6] Meng-Shiuan Pan, Shu-Wei Yang,"A lightweight and distributed geographic multicast routing protocol for IoT applications", Computer Networks, Volume 11215, Pages 95-107, January 2017.

[7] 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.

[8] Anupam Das and Mohammad Mahfuzul Islam, " SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems", IEEE Transactions on Dependable and Secure Computing, vol.9, no.2, pp.261 - 274, 2012.

[9] Rajeev Kumar and Dilip Kumar, "Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network", Wireless Networks, vol.22, no.5, pp.1461–1474, July 2016.

[10] Bo Wang, Xunxun Chen, and Weiling Chang , "A light-weight trust-based QoS routing algorithm for ad hoc networks", Pervasive and Mobile Computing, vol.13, pp.164-180, August 2014.

[11] Amol V. Dhumane and Rajesh S. Prasad, "Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT", Wireless Networks, pp.1-15, 16 August 2017.

[12] Yılmaz S, Kücüksille E U. A new modification approach on bat algorithm for solving optimization problems[J]. Applied Soft Computing, 2015, 28: 259-275.

[13] Shi Y, Eberhart R. A modified particle swarm optimizer Evolutionary Computation Proceedings, 1998. IEEE World Congress on Computational Intelligence., The 1998 IEEE International Conference on. IEEE, 1998: 69-73.

[14] Yang N C, Le M D. Multi-objective bat algorithm with time-varying inertia weights for optimal design of passive power filters set[J]. IET Generation, Transmission & Distribution, 2015, 9(7): 644-654.

[15] Holland J H. Genetic algorithms[J]. Scientific american, 1992, 267(1): 66-73.

[16] Duan L, Rayadurgam S, Heimdahl M, et al. Representation of confidence in assurance cases using the beta distribution[C]//High Assurance Systems Engineering (HASE), 2016 IEEE 17th International Symposium on. IEEE, 2016: 86-93