International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 3, May-Jun-2022, ISSN (Online): 2395-566X

Genetic Algorithm Based Routing of IOT Network

Research Scholar Shailendra Kumar Tiwari, Department Of Computer Application,
Asscoiate Prof. Dr.Ravindra Kumar Tiwari Department Of Computer Science and Engineering,
LNCT University, Bhopal, Madhya Pradesh, India

***Abstract*- Smart devices in human life brings Internet of Things in day to day uses. Routing in such network should be efficient and energy effective, as devices depends on battery. Such network are optimized by various approaches, out of different methods routing based IOT network is an effective solution. This paper has proposed a genetic algorithm that finds the path based on Biogeography genetic algorithm. Paths were filter by estimating the fitness on the basis of node spectrum utilization. Such nodes are filter by into two class real and other is malicious. Malicious nodes are identified by the Adamic Adar function. Experiment was done on different environment and results shows that proposed model has increases the work performace.**

Index Terms-IoT Network, Genetic Algorithm, Data Security, Spectrum Utilization, Trust Based Model.

I. INTRODUCTION

The Internet of Things (IoT) has in the last few years, become a topical issue in the academia and the technology industry. Although it is becoming increasingly ubiquitous, IoT supports a comprehensive representation of the physical environment and a good level of interaction with the physical world [7, 10]. Some typical areas such as logistics, intelligent transportation systems (ITS), business/process management and e-health are but a few instances of conceivable application fields where this novel paradigm is gaining attention.

The realization of IoT will greatly hinge on various criteria such as the system's architecture, networks and communications, data processing, and ubiquitous computing technologies, which support efficient, reliable, physical and cyber interconnectivity [7, 11, 12]. Again, for swift public adoption of IoT, social and technological issues emanating from the introduction of IoT will also have to be addressed. One of the fundamental driving forces of IoT is networking, which drives and facilitates the interconnection of devices [12]. Of particular importance is routing in the network; it involves how traffic routes are built, transmitted and controlled within the network so that a routed packet could travel from source to its final destination. Furthermore, with the interconnectivity among the billions of devices, the big issue is how secure is the network from various forms of attacks.

II. RELATED WORK

Hiren Kumar Deva Sarma (2016) proposed a new hierarchical based routing protocol that can be used for effectively delivering the data more reliably to the base station. The author added that both the sensor nodes and also the base station are mobile nodes as the design criteria. In this model, cluster formation is carried out that consists of the cluster head, two deputy cluster heads for each cluster head and finally the cluster nodes. Moreover, the author introduced the new concept called cluster head panel in order to minimize the energy consumption which is required for clustering and re-clustering. This panel is consisting of suitable sensor nodes that are selected from each of the clusters that are assigned as the cluster heads and also the deputy cluster head nodes respectively at a later stage. In addition, the model proposed by the author consists of four different phases namely the self-organization phase, the scheduling and Medium Access Control information computation phase, the operational phase and finally the exception handling phase. All these phases have been used for creating alternate routes for forwarding and routing with reduced delay and loss of packets.

Deyu Lin &Quan Wang (2017) proposed a new energy efficient clustering routing protocol based on game theory for effective clustering. In their model, game theory was applied in the decision making process that was used to determine the number of nodes to be allocated in each cluster.

Qinying *et al.* (2018) proposed a routing algorithm which is focusing on finding the shortest path based on grid positions for the unnamed aerial based systems. The authors were able to achieve better network performance while applying QoS parameters.

Shamim Hossain *et al.* (2019) proposed a new multimedia application based sensor network routing algorithm which focuses on reduction of delay and energy consumption. The approach used in their model is multipath routing with energy optimization. Therefore, they used intelligent techniques for planning the paths which helped to reduce the energy consumption and also to enhance QoS metrics.

Sree Rathna Lakshmi *et al.* (2017) proposed an efficient network architecture for WSN to provide QoS aware reliable routing. For this purpose, the authors considered the different issues of network design including node failures, link failures, routing overhead and finally the

QoS parameters. The authors carried out suitable experiments to prove that their model is more effective in energy optimization when the paths are selected for routing correctly.

III.PROPOSED METHODOLOGY

Proposed model Biogeography Optimization Adamic Trust IOT Routing (BOATIR) was detailed in this section of paper by explanation of various steps shown in fig. 1. Each node trust was estimate, by the behavior while transferring the packet. Packet information was stored in the centralized server that gives trust value after a fix time frame. To optimiza the network resource utilization proposed model uses biogeography optimization algorithm that generate path as per source and destination.

Trust Management

This is similar to Resource Allocation, but the denominator of the fraction is the log of the degree of the shared neighbor, rather than simply the degree [14].

$$Aa = \sum_{x \in a \cap b} \frac{1}{\log(d(x))} \text{----Eq. 1}$$

Where d(c) is the sum of the of the degrees of vertices adjacent to both a and b. d(x) is degree of x and y.

Each node in the observation matrix has a trust value. This value may increase or decrease as per the behavior of the nodes in form of transaction success. Storage tables were used to evaluates this value of work. So let successful transaction count between i, j node is represent by Ts_{ij} and total number of transaction represent by Tt_{ij} [45]. Estimation of this trust done by:

$$D_{ij} = \sum_{i,j=1}^{n} Aa_{ij} \text{----Eq. 2}$$

Above eq. gives n number of trust value for each node, but behaviors of node with node may be different. As malicious node provide good service to some node and poor service to others. This function takes all Adamic-Adar value of a node and generates a single value of the node as per different behavior operations done by node with other nodes.

Generate Path

In order to identify the network path for transfer of data between nodes this model use biogeography optimization algorithm. Biogeograpy nodes position and energy values as input. Based on current energy value of node and position selection of in between nodes were done by the centralized system.

Habitat: As per source and destination set at an instant in a network some random path s route P were generate form available set of nodes. This route need depends on distance between the next hop (node) from current/source towards destination node. So a habitat is a binary vector, where 1 means node is present in path and 0 means node is absent in path. Selection of node was depend on availability as well [15]. For a single route m number of H habitat were generate. So a population has mxP number of habitats.

$$H \leftarrow \text{Generate Habitat}(D_d, m, P)$$

Immigration & Emigration Rate: Term Emigration means chance of shifting a species from habitat one to other. Similarly Immigration means chance of accepting a new species form other habitat. So each habitat in H has its own immigration and emigration values.

$$\lambda_R = (1 - \alpha_{h_h}) \text{-------------Eq. 2}$$

$$\alpha_h = \frac{I}{m} \text{-------------Eq. 3}$$

Where I is index of habitat in H as per HIS value [16].

Habitat Suitability Index (HSI): In order to find a good route for transferring D fitness value of each route help to select a path. In this work two objectives were taken for getting optimum path first was spectrum utilization and other was energy dissipation. Eq. 5 shows estimation of energy for the path as per nodes and its distance from other.

$$F_{h,e} = \sum_{n=1}^{P'} (E_t^n + E_r^n)$$

P' is number of nodes in route P of habitat h from H. Eq. 6 shows estimation of spectrum utilization for the path as per nodes.

$$F_{h,s} = \sum_{n=1}^{P'} (S^n - D)$$

Final fitness value was estimate by summation of energy and spectrum value from eq. 5, 6.

$$F_h = \beta_1 F_{h,s} + \beta_2 F_{he}$$

Where β_1 and β_2 are constant to normalize values at same scale because energy loss value is very low as compared to spectrum utilization.

Migration Some of nodes present in path are move from one habitat to other by changing its present node status from 1 to 0 is term as migration. While for migration some other habitat should ready to accept that node by changing its presnt status 0 to1. In genetic algorithm this step is termed as crossover operation [17]. So as per immigration and emigration values of habitat migration operation perform between two habitat.

$$H(x,h) = H(y,h) \begin{cases} x \in h\, \emptyset > \lambda_h \\ y \in h\, \emptyset > \alpha_{h_h} \end{cases}$$

In above eq. ∅ is migration constant value range in 0 to 1.

Mutation For further improving the population BGO apply mutation operation on some of habitats as per HIS value. In this operation only those habitat participate which cross mutation limit contant range in 0 to 1.

$$M_h = \frac{I_h}{sum\,(h)} \text{-------------Eq. 4}$$

$$M_p = \frac{M_h}{Max\,(M_h)} \text{-------------Eq. 5}$$

Final Path After T number of iteration steps of HIS, migration and mutation habitat H fitness value HIS was estimate to get best out of H set of chromosomes (habitat). This has P number of route. Each path was estimate by energy and spectrum values.

Filter Malicious Nodes

Path generate by genetic algorithm is further scanned by the system to identify malicious node from the path. As per Adamic Adar trust value nodes having low value is consider as the malicious and other are consider as the real node. If path have malicious node then packet is not transfer on that path and it saves the spectrum and energy of the network.

IV.EXPERIMENT AND RESULTS

Experimental work was done on MATLAB platform having machine of I3 processor and 4GB RAM. For comparison existing model proposed in SACR [18] and WOATIR [19].

Results

Table 1 Spectrum utilization percentage based comparison.

Nodes	Region	Route	Sacr	Woatir	Boatir
100	100x100	3	33.27	99.8454	99.9572
100	100x100	5	39.95	99.97	99.9736
100	100x100	7	57.04	99.9	99.9181
100	100x100	10	49.95	99.818	99.8749
120	100x100	10	49.89	50.4988	99.9175
140	100x100	10	79.7848	99.796	99.91
160	100x100	10	59.8529	99.8547	99.9653
100	120x120	10	89.8519	99.843	99.9094
100	140x140	10	69.8129	89.8121	99.9314

IOT network is work in secondary channel hence its utilization is very important as waste of channel lead to increase the delay of generated information. Table 1, 2 shows spectrum utilization and Throughput of the network utilization. It was fond that Biogeography Optimization Adamic Trust IOT Routing (BOATIR) has increased the work performance in both parameters. Average spectrum utilization was improved by 6.66% as compared to WOATIR model.

Table 2 Throughput (kbps) of cognitive routing based comparison.

Nodes	Region	Route	Sacr	Woatir	Boatir
100	100x100	3	26.6152	79.9918	86.641
100	100x100	5	35.9528	95.9528	91.9842
100	100x100	7	39.9371	82.8263	82.7976
100	100x100	10	25.9734	73.98	79.895
120	100x100	10	23.9537	75.9421	77.939
140	100x100	10	51.87	69.8698	87.92
160	100x100	10	39.9202	79.9209	85.981
100	120x120	10	51.9087	57.911	79.943
100	140x140	10	47.885	67.8823	89.9414

Table 3 Transfer Time (mile.Seconds) based comparison.

Nodes	Region	Route	SACR	Woatir	Boatir
100	100x100	3	123.2917	172.0667	127.733
100	100x100	5	112.8715	112.8515	148.181
100	100x100	7	127.0107	122.7	120.616
100	100x100	10	137.7569	135.0263	87.975
120	100x100	10	142.5933	134.2446	111.743
140	100x100	10	119.1397	117.3218	98.198

160	100x100	10	130.9862	130.9762	128.267
100	120x120	10	122.1779	118.0379	113.991
100	140x140	10	99.4546	98.4546	96.9258

Table 4 Latency Time (mile. Seconds) based comparison.

Nodes	Region	Route	Sacr	Woatir	Boatir
100	100x100	3	0.5478	0.3397	0.2872
100	100x100	5	0.4284	0.2295	0.3257
100	100x100	7	0.3659	0.2189	0.2387
100	100x100	10	0.3469	0.2734	0.1258
120	100x100	10	0.3262	0.2279	0.1687
140	100x100	10	0.2675	0.1765	0.1666
160	100x100	10	0.3774	0.2224	0.2564
100	120x120	10	0.1942	0.151	0.1985
100	140x140	10	0.2405	0.1799	0.1706

Table 3, 4 shows that proposed BOATIR has reduced the time of the work as biogeography algorithm performs the crossover and mutation operation in one iteration hence more effective path is generate by the model. It was found that propose model has reduced the latency time by 3.3% as compared to SACR model and 4.01% as compared to WOATIR model.

V.CONCLUSION

The Internet of Things (IoT) integrates a large amount of everyday life devices from heterogeneous network environments, bringing a great challenge into security and reliability management. This paper has proposed a model that find path between the node without any training and reduces the network resource loess. For improving the performance of IOT network malicious nodes were detect on the basis of the adamic trust function. Use of trust function and path generation algorithm proposed model has improved the various evaluation parameter values in experiment. Results were compared with existing techniques and it was obtained that BOATIR has improved the throughput by 46.55% as compared to SACR and 8.75% as compared to WOATIR model. In future scholar can adopt some other technique of evaluating trust of nodes.

REFERENCES

1. Mohammad M Abdellatif, Jose Manuel Oliveira & Manuel Ricardo 2016, ‗The self-configuration of nodes using RSSI in a dense wireless sensor network', Telecommunication Systems, vol. 62, pp. 695–709.
2. 143. Raza, U, Alessandro Camerra, Amy L Murphy, Themis Palpanas & Gian Pietro Picco 2015, ‗Practical Data Prediction for Real-World Wireless Sensor Networks', IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 8, pp. 2231- 2244.
3. 144. Rejina Parvin, J & Vasanthanayaki, C 2015, ‗Particle swarm optimization-based Liansheng clustering by preventing residual nodes in wireless sensor networks', IEEE Sensors Journal, vol. 15, no. 8, pp. 4264-4274.
4. Hiren Kumar Deva Sarma, Rajib Mall & Avijit Kar 2016, ‗E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks', IEEE Systems Journal, vol.10, no. 2, pp. 604-616.
5. Deyu Lin & Quan Wang 2017, ‗A game theory based energy efficient clustering routing protocol for WSNs', Wireless Networks, vol. 23, no.4, pp. 1101–1111.
6. Qinying Lin, Houbing Song, XiaolinGui, Xiaoping Wang & Saiyu Su 2018, ‗A shortest path routing algorithm for unmanned aerial systems based on grid position', Journal of Network and Computer Applications, vol. 103, pp. 215-224.
7. Shamim Hossain, M, Xinghui You, Wenjing Xiao, Jiayi Luc & Enmin Song 2019, ‗QoS-Oriented Multimedia Transmission using Multipath Routing', Future Generation Computer Systems, vol. 99, pp. 226-234.
8. Sree Rathna Lakshmi, NVS, Babu, S & Bhalaji, N 2017, ‗Analysis of clustered QoS routing protocol for distributed wireless sensor network', Computers & Electrical Engineering, vol. 64, pp. 173-181.
9. W. Meng, W. Li and L. Zhu, "Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1377-1386, Nov. 2020
10. W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang and J. J. P. C. Rodrigues, "FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things," in IEEE Access, vol. 7, pp. 13476-13485, 2019.
11. X. Guo, H. Lin, Z. Li and M. Peng, "Deep-Reinforcement-Learning-Based QoS-Aware Secure Routing for SDN-IoT," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6242-6251, July 2020.
12. Y. Sun et al., "Lightweight Anonymous Geometric Routing for Internet of Things," in IEEE Access, vol. 7, pp. 29754-29762, 2019
13. K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed and N. Guizani, "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs," in IEEE Access, vol. 7, pp. 79980-79988, 2019,
14. L. Adamic, and E. Adar. Friends and neighbors on the web. Social Networks, 25(3), 2003.
15. MacArthur R., Wilson E. The Theory of Biogeography. Princeton, NJ, USA: Princeton University Press; 1967.
16. Simon D. Biogeography-based optimization. IEEE Transactions on Evolutionary Computation. 2008;12(6):702–713. doi:

10.1109/tevc.2008.919004.

17. Mohammed Alweshah. "Construction biogeography-based optimization algorithm for solving classification problems". Neural Computing and Applications, Springer volume 28 February 2018.
18. Ren Han, Yang Gao, Chunxue Wu, And Dianjie Lu. "An Effective Multi-Objective Optimization Algorithm For Spectrum Allocations In The Cognitive-Radio-Based Internet Of Things". Ieee Access March 19, 2018.