International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Improving Multipath Load Balancing Routing With Moth Flame Optimization Approach in Internet of Things Applications

Sukhpal Kaur, Dr. Shaveta Rani, Dr. Paramjeet Singh
Department of CSE, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, India

ABSTRACT

In the next generation technology, Internet of things, millions of smart devices will communicate with other to make more efficient and convenient human lives. As we know that we are moving to a new trend of technology which is popularly known as the Internet of Things (IoT). IoT is kind of "universal worldwide neural system" in the cloud systems which attach various belonging. The IOT is a perceptively related strategies and systems which contained of smart technologies interrelating systems and communicating with further machineries, environments, items and substructures sensor network machineries which will increase to encounter this novel challenge. As a consequence, the massive amount of statistics are being produced, deposited, and that statistics is being handled into useful movements that can "knowledge and regulate" the belongings to mark our lives much calmer and safe which help us to reduced our influence on the atmosphere. This research puts light on various issues, challenges and related works which will give ideas to various emerging researchers to give their best to the Internet of Things (IoT) environment. Also our proposed approach deals with the optimization approach using moth flame optimization to balance the load of the network and also the performance is evaluated in terms of packet loss, load balance degree and energy consumption. The energy consumption must be low for high throughput and low packet losses of the Internet of Things (IoT) network.

Keywords : Internet of Things(IoT), Wireless Sensor Network, Multipath load balancing approach, Moth Flame Optimization Algorithm

I. INTRODUCTION

Internet of Things is a network containing of multiple wireless devices also called nodes where all devices can sense, communicate and share data through private and public internet based on the protocol. Internet of Things(IoT) communications are developing key to the expanding request for broadband associations in oceans and deeps. In Internet of Things (IoT), every single systems administration capacity, for example, routing and packet forwarding, are performed. In the previous decades the world has turn into a universal town by caution IT sector. Information Technology is emerging step by step. Governments have a propensity to utilize more problematic system situations. Irrespective of the endeavors of scheme heads and IT wholesalers to secure the computing circumstances, the dangers posed to separate protection, organization security and different resources by attacks upon systems and PCs. The Internet of Things (IoT) are unquestionably a piece of this revolution [1]. The Internet of Things (IoT) is the next revolution, where the interconnection between devices creates an intelligent environment. Moreover Internet of Things (IoT) devices are connected and

communicated, IOT applications generates tremendous IoT traffic. Since transmission between devices are becomes critical due to IoT traffic. Internet of Things (IoT) is an accumulation of wireless devices or hubs that communicate by posting packets to each other or for additional device/hub, without having any outline controlling info for routing. IOT centers have boundless system and versatility to different hubs. The main key issue in IOT is secured transmission from source to destination. In this paper we are going to achieve load balancing approach to mitigate the losses of receiving packets from source to the destination and also try to achieve high packet deliveries for the less failures of node in the Internet of Things (IoT) environment.

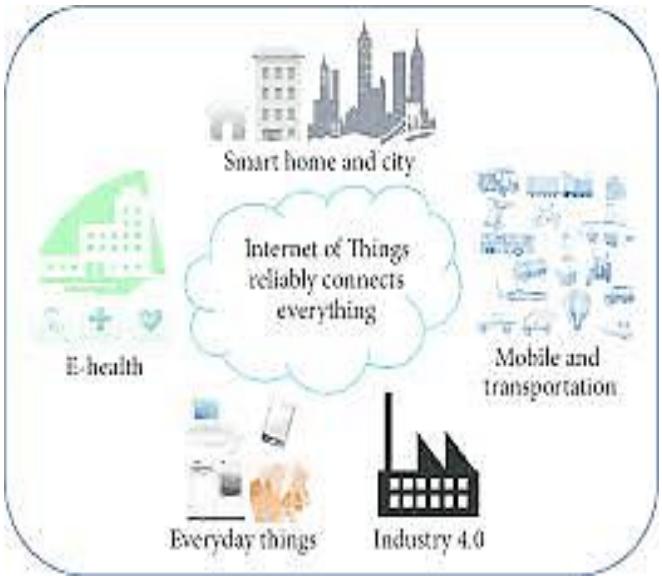

Figure 1: IOT Domains

As fig 1 shows, Internet of Things (IoT) technology are largely used in different types of areas like as military, industry, E-health, mobile and transportation, home applications and so on.

II. RELATED WORKS

Monowar H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita et al. [8] (2014) presented an approach in which information theory is used and abnormal network behaviours. Based on the mutual information between network features and the types of network intrusions, a small number of network features were closely identified with network attacks. Then a linear structure rule is derived using the selected features. The use of mutual information reduced the complexity, and the single resulting linear rule made the intrusion detection efficient in real-time environment. However, the author approach considered only discrete features.

Kalsoom Shabana, Nigar Fida, Fazlullah Khan, Syed Roohullah Jan, Mujeeb Ur Rehman [9] (2016) presented such issues to detect network anomalous. The detection rates might be increased due to quantitative features inclusion. Parameters and evolution processes are discussed in details. They have introduced issues which used evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity.

Bridges (2000) [10] implemented a method to detect both anomalies and network misuses by combing Genetic Algorithm and Fuzzy data mining technologies. In this method they have selected the most significant network features and locate the best possible parameters of the fuzzy function by using Genetic Algorithm.

Daniel-Ioan Curiac (2016) [11] proposed a methodology to detect network anomalies using Directional antennas. They provide solutions to decrease the security risks to use directional projections instead of omni-directional ones or in conjunction with them.

Gorine, habib et.al. [12] (2016) have security issues and experiments facing investigations in wireless sensor networks and measures to solve them. The transmission nature of wireless communication creates Wireless Sensor Networks disposed to numerous attacks.

Lu [13] (2010) developed a method to derive a set of classification rules by using Genetic Programming (GP) with help of past data of network. In this method using GP the practical implementation was more difficult due to the system required more data or time.

In [14] (2017) the authors presented a robust neural network detector for Distributed Denial of Service (DDoS) attacks in computers providing Internet services. A genetic algorithm was used to select a small number of efficient features from an extended set of 44 statistical features, which are estimated only from the packet headers. Most supervised neural net architectures required retraining in order to improve analysis capability due to changes in the input data, but unsupervised net offers increased level of adaptability to neural nets and were able to dynamically improve their analysis capability. Most of the network-based systems in unsupervised based IDSs used self-organizing maps (SOMs) neural nets and only a few systems used other types of unsupervised neural nets.

In [15] (2009), multiple SOMs were used for intrusion detection, where a collection of more specialized maps were used to process network traffic for each protocol separately. Each neural net was trained to recognize the normal activity of a single protocol. It mainly analyse the potential of the Kohonen self-organizing map to narrow the envelope of intrusive behaviours that could not be caught by a detection system.

Chinyang Henry Tseng et al. [16] proposed Multipath Load Balancing (MLB) Routing to substitute Zigbee AODV routing. Their proposed MLB consists of two main designs: Layer design and load balance. Layer design assigns nodes into different layers based on node distance to Internet of Things (IoT) gateway. Nodes can have multiple next-hops delivering Internet of Things (IoT) data. They have worked on connectivity ratio and load balancing proportion to evaluate the systems performance.

III. PROBLEM FORMULATION

Internet of Things (IoT) consists of spatially distributed autonomous sensor nodes to monitor surroundings at different locations. Load is one of the core issues in Internet of Things (IoT) networks because packets are having high traffic in transmission from source to destination which degrades the quality of service. It is desirable to make these nodes as cheap and reliable as possible and rely on their large numbers to obtain high quality results. As the number of packet losses increases the routing error rate increases which must be low. Consequently many protocols have been proposed in order to minimize the losses or overheads in the network. The efficiency of Internet of Things (IoT) strongly depends on the secure routing and protocol used. So this thesis will work on the balanced routing in Internet of Things (IoT) in which several simulations will be conducted to analyse the performance including the power consumption and overall network performance like packet loss, load balance degree and energy consumption.

IV. METHODOLOGY AND PROPOSED WORKS

A. Methodology Steps

The research methodology and steps which are as follows:

1. Initially we will configure the network using specifications like network length, network width, initial energy of nodes.
2. Then we will deploy the nodes in the IOT enabled network.
3. Then we will find the nodes having maximum energy than the average energy in the network.
4. Then we will implement the coverage area in which each node is having coverage nodes i.e. which node is coming in the coverage of which node and at what distance it is coming.

5. Then we will implement multipath routing and evaluate the loads in the links and perform the optimize solution for the stabilization of load.
6. Then we will evaluate the best route having fewer loads in the network..
7. Then we will compare the performance of the proposed approach with the base approach.

B. Moth Flame Optimization algorithm

It is also one of the efficient algorithm which is used to achieve optimizations and having less error rate probabilities. Moths fly in night by maintaining a fixed angle with respect to the moon, a very effective mechanism for travelling in a straight line for long distances

Step 1: Update the amount of flames

Step 2: Initialize the moths as population

Step 3: Evaluate the objective function

Step 4: For all moths

for all essential parameters

update b and t where t defines how much the next locations of the moth should be close to the flame

b=1,

t=(a-1)*rand+1,

Evaluate D=|flame(j)-moth(i)| with respect to the corresponding moth

Update the matrix M with respect to the corresponding moth

M(m(i), f(j))=D*exp(b*t)*Cos(t*2*pi)+f(j)

end

Evaluate the best possible solutions

Update flames

End

V. IMPLEMENTATION RESULTS

Fig 2 shows the network creation with the number of nodes deployed in the network. The nodes which are red in colour are the normal nodes and the nodes which are green in colour are the nodes which are having high energy than the average energy of the network. These nodes are used to start the routing from the source nodes having sufficient energies in the network to broadcast the requests in the network.

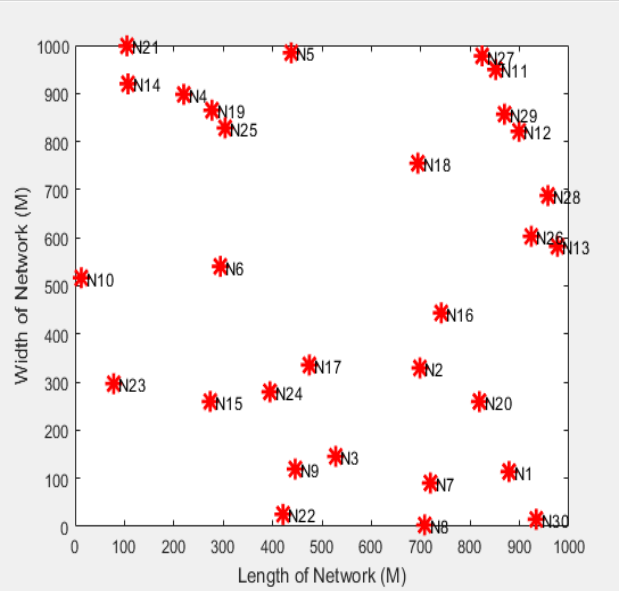

Figure 2 : Network Creation

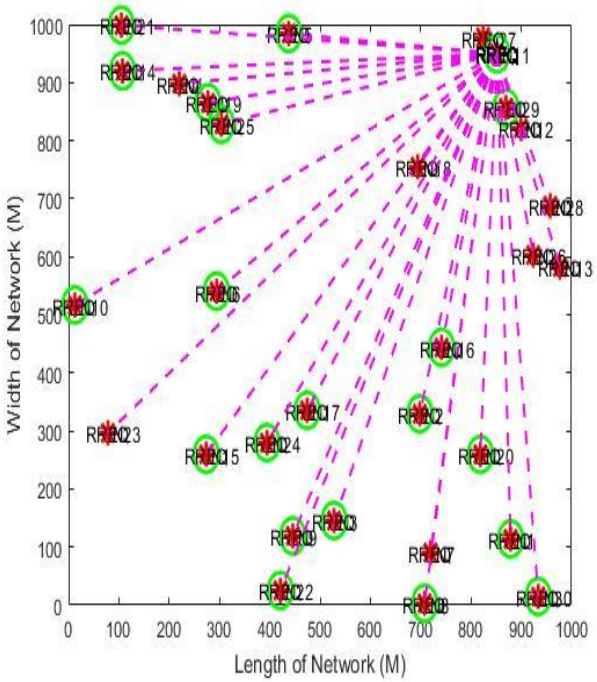

Figure 3 : Route Request

The above figure shows the route request scenario in the network to initialize the route from the source node to check the availability and acknowledgement of the nodes in the network.

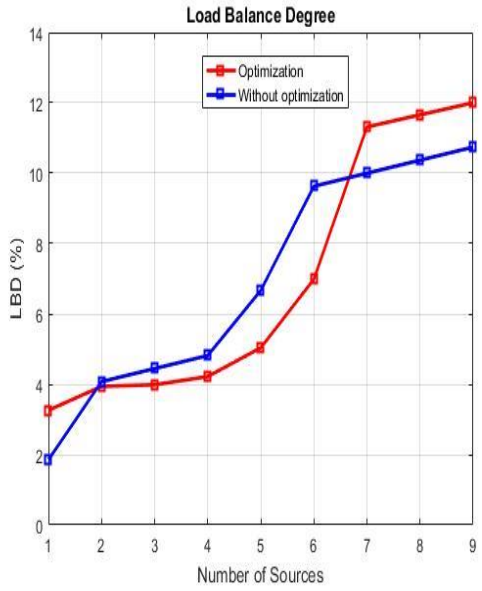

Figure 4 : Load balance degree optimization and without optimization (%)

The above figure shows the load balance degree optimization and without optimization which shows that the network is achieving approximate 11% of LBD when the optimization is not applied for the link stability and the proposed approach is able to achieve high load balance of the network which shows that our optimize approach is better.

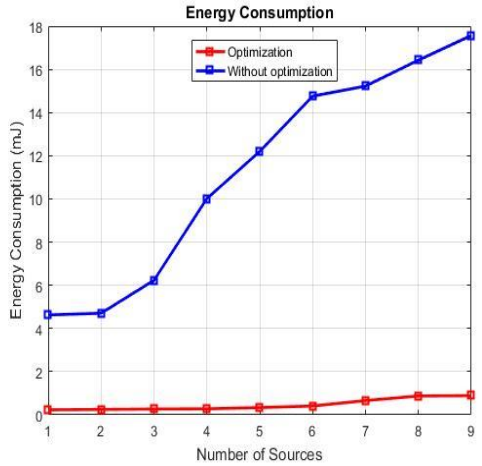

Figure 5 : Energy Consumption with optimization and without optimization

The above figure shows the overall consumption of the energy in the network which deals with the nodes energy to be consumed for the broadcasting and receiving of the requests from source to the destination. In the figure the energy consumption of the network with optimization and without optimization which shows that the proposed approach is able to achieve low energy consumption and also its able to achieve high link stability which is our desired approach

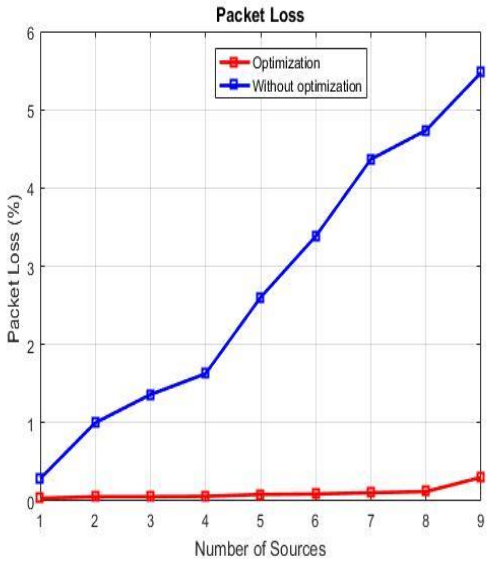

Figure 6: Packet loss (%) with optimization and without optimization

The above figure shows the packet loss percentage which shows the appropriate loss of packets which is coming good to achieve less packet loss. But it needs to be minimize more to have high packet deliveries. The above figure shows the packet loss percentage of the network with optimization and without optimization which shows that the proposed approach is able to achieve less packet loss than the approach before optimization and shows that the proposed approach is able to achieve high packet deliveries.

Table : Comparison of the proposed system with the existing system on the same type of the network.

Performance	LBD (%)	Energy consumption (mj)	Packet loss (%)
Without	11	17	5.5

Optimization			
With Optimization	12	1	0.5
Improvment	1	16	4.5
Without Optimization	9	4	3.5
With Optimization	48	2	0.05
Improvment	39	2	3.45
Without Optimization	6.5	20	6.5
With Optimization	10.5	7	2
Improvment	4	13	4.5

The above table represents the comparison of the existing and proposed system on the basis of LBD, energy consumption, Packet loss parameter. It is shown that the three parameter of the proposed system after performance it gives better result than that of the existing system on the same type of the network.

VI. CONCLUSION

In this research paper we are going to achieve load balancing approach to reduce the failure of receiving of packets from source to destination and also try to achieve high packets deliveries for the less failures of node in the Internet of Things (IoT) environment. We know that we are moving to a new trend of technology which is popularly known as the Internet of Things Internet of Things (IoT). Internet of Things (IoT) is a kind of "universal worldwide neural system" in the cloud systems which attach various belongings. The Internet of Things (IoT) is a perceptively related strategies and systems which contained of smart technologies interrelating systems and communicating with further machineries, environments, items and substructures sensor network machineries which will increase to encounter this novel challenge. So this research work deals with the efficient optimize approach to achieve less load, less packet loss and high packet deliveries with less energy consumption of the Internet of Things (IoT) network.

VII. FUTURE SCOPE

In future, this moth flame optimize technique can tested with further parameters to improve the performance of network and can be used to find better result than proposed works.

VIII. REFERENCES

[1] Akhoundi, Farhad, Mohammad Vahid Jamali, Navid Bani Hassan, Hamzeh Beyranvand, Amir Minoofar, and Jawad A. Salehi. "Cellular underwater wireless optical CDMA network: Potentials and challenges." IEEE Access 4 (2016): 4254-4268.

[2] Wahid, Abdul, and Dongkyun Kim" An energy efficient localization-free routing protocol for underwater wireless sensor networks." International journal of distributed sensor networks 8, no. 4 (2012): 307-246

[3] Climent, Salvador, Antonio Sanchez, Juan Vicente Capella, Nirvana Meratnia, and Juan Jose Serrano. "Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers." Sensors 14, no. 1 (2014): 795-833.

[4] Chen, Yuh-Shyan, and Yun-Wei Lin. "Mobicast routing protocol for IOT." IEEE Sensors journal 13, no. 2 (2013): 737-749.

[5] Kavar, Jaydip M., and K. H. Wandra. "Survey paper on Underwater Wireless Sensor Network." (2012)

[6] Raina, Ujala Zaffer, Himali Sarangal, and Neetika Soni. "A Review on Underwater Wireless Sensor Networks". Wireless Communication 8, no. 4 (2016): 119-123

[7] Cheng, En, Xizhou Lin, Shengli Chen, and Fei Yuan. "A TDOA Localization Scheme for IOT

with Use of Multi-linear Chirp Signals." Mobile Information Systems 2016 (2016)

[8] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Information metrics for low-rate DDOS attack detection: A comparative evaluation." In Contemporary Computing (IC3), 2014 Seventh International Conference on, pp. 80-84. IEEE, 2014.

[9] Shabana, Kalsoom, Nigar Fida, Fazlullah Khan, Syed Roohullah Jan, and Mujeeb Ur Rehman. "Security issues and attacks in Wireless Sensor Networks." International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 5, no. 7 (2016): pp-81.

[10] Bridges, Susan, Ray ford B. Vaughn," Intrusion Detection via Fuzzy Data Mining", In Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, Ottawa, Canada, 2000.

[11] Curiac, Daniel-Ioan."Wireless sensor network security enhancement using directional antennas: State of the art and research challenges." Sensors 16, no. 4 (2016): 488.

[12] Gorine, Habib, and M. Ramadan Elmezughi. "Security threats on wireless sensor network protocols." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10, no. 8 (2016): 1483-1486.

[13] Xiao, Yang, ed. Under-water acoustic sensor networks. Auerbach publications, 2010.

[14] Sharif-Yazd, Mohammad, Mohammad Reza Khosravi, and Mohammad Kazem Moghimi. "A Survey on Underwater Acoustic Sensor Networks: Perspectives on Protocol Design for Signaling, MAC and Routing." arXiv preprint arXiv: 1703.08353 (2017)

[15] Pompili, Dario, Tommaso Melodia, and Ian F. Akyildiz. "A CDMA based medium access control for underwater acoustic sensor networks." IEEE Transactions on Wireless Communications 8, no. 4 (2009)

[16] Tseng, Chinyang Henry. "Multipath load balancing routing for Internet of things." Journal of Sensors (2016).