TRUST-BASED METHOD FOR MANET USING IMPROVED BACTERIA FORAGING OPTIMIZATION TECHNIQUES

Mahesh Gawali[1], Dr. Harsh Lohiya[2]

[1]Research Scholar, Department of CSE, SSSTUMS, Sehore, M.P. India.

[2]Associate Professor, Department of Computer Science & Engineering SSTUMS, Sehore M.P. India.

ABSTRACT

In the past few years, the demand on the network has increased day by day, so the need for infrastructure, security equipment and access is becoming difficult for us. Mobile ad hoc networks allow us to establish a connection between two or more nodes. In this work, we present an optimization method to improve the connection between sites and sites by using the communication from the trust to determine the optimal number of hops between nodes and to package data from source to source. The proposed algorithm IBFOA is based on finding the truth about the reliability and communication security of nodes in the network, here we show that the test type is normal in the simulation scenario. Challenge the norm and try to be more efficient than the current system.

Keywords: Bacteria foraging Optimization Algorithm, Cognitive Radio, Internet of Things, MANET, VANET.

1. INTRODUCTION

Mobile ad hoc network is used for wireless communication between all devices; it is a network of wireless sensors. In mobile ad hoc network, a collection of n nodes communicate randomly between locations and locations, where each node has its own lifetime or energy efficiency. Various routing algorithms and routing protocols are used to establish communication and send packets in an orderly manner. Routing protocols are divided into reactive routing protocols, proactive routing protocols and hybrid routing protocols [4]. Mobile ad hoc networks work with dynamic features or based on random topology features, so the power of transmitting information packets is a very important task. Here, the nodes in the cell's own organization also face the challenge or threat of a potential attack.

The attacker can be someone from inside or outside the network. The communication network for reliable communication, the cost of packet distribution between the source and destination, the end-to-end delay of the number of nodes, and the anode life or energy to improve the quality of service. Here, various technologies such as data mining technology, artificial intelligence technology, machine learning, genetic algorithms, mutual learning deep modeling and bio-inspired optimization algorithms are used to test the above services [14].
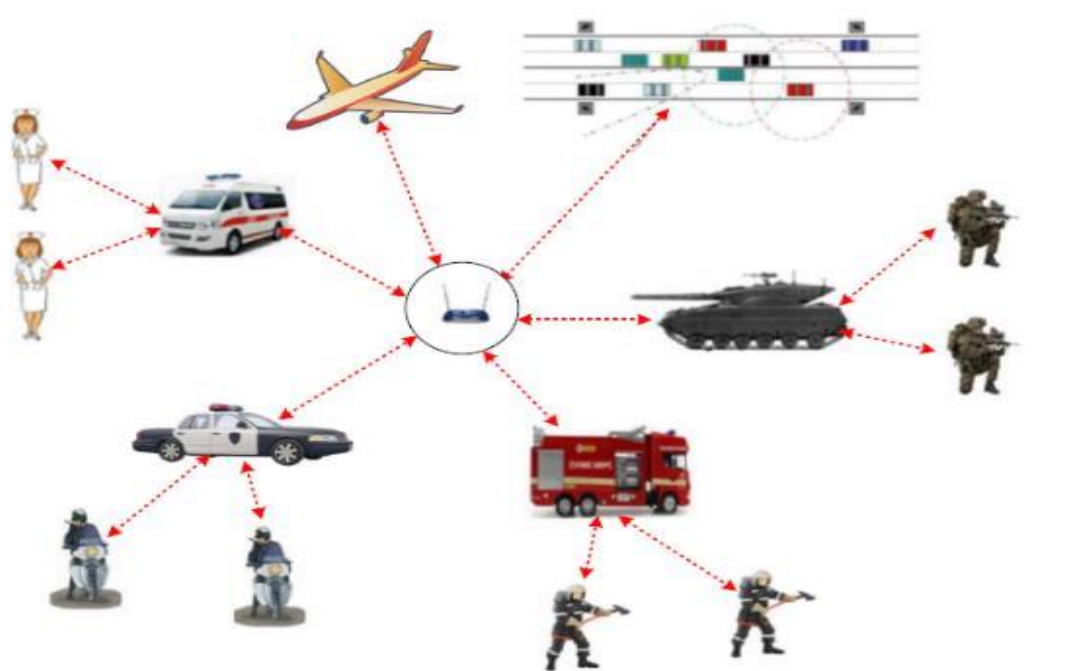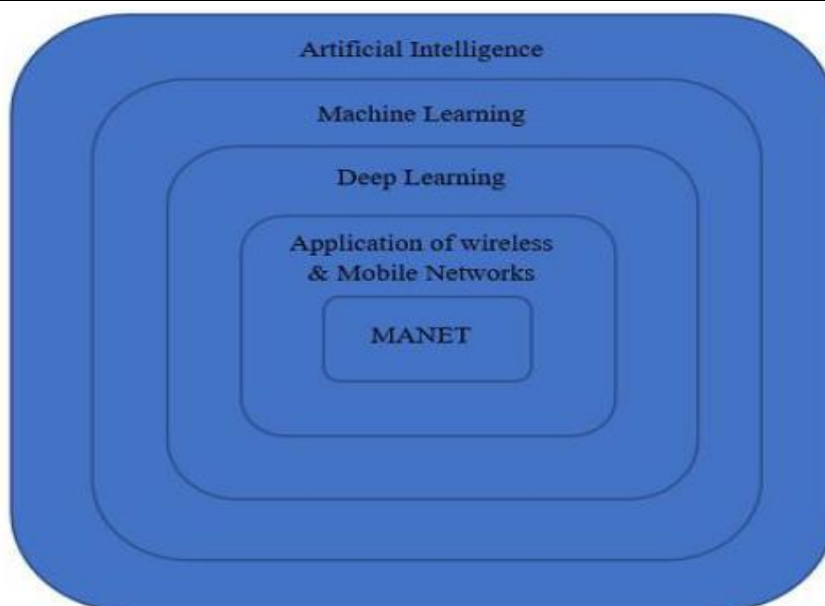

Figure 1: Mobile ad-hoc network [7].

Over the last two decades technology offer us tremendous change in every sector, artificial intelligence and optimization techniques are the most popular techniques for each sector, here we mention some bio-inspired optimization techniques for mobile ad-hoc networks and improve the performance of an existing networks. In this work, we discuss the bio-inspired optimization algorithm and improve the quality of services parameter than existing work [5].

Figure 2: The above picture represents a relationship between artificial intelligence and mobile ad- hoc network [3].

2. PROPOSED WORK

Biologically inspired techniques are used to distribute resource allocation problems and deal to the efficient quality of services in a mobile ad-hoc network. As we already discuss there are various key challenges like bandwidth utilization, reliability, scalability, and mobility.

In this section, we discuss our present work and algorithm which is based on the bio-inspired algorithm and improve obtained result value than existing work. Here our proposed work uses trust-based calculation approach for a node with proposed optimization techniques. These techniques have excellent characteristics for the proposed work and obtained solutions like scalability, and adaptability, The main aim of this proposed work is to obtain the optimal solution in a network with ensure the security of a participating node which does not affect any type of attack or any threats based of trust based routing mechanism for each node in a network.

The proposed model works on bio-inspired based technique i.e. improved bacteria for aging optimization algorithm. The proposed model has divided the works into a table which is carrying information on data retrieval and route formation of stages between the number of nodes, this model uses the ad-hoc on-demand distance vector routing protocol for transferring the packet in a network and maintaining a routing table for each node based on node trust value.
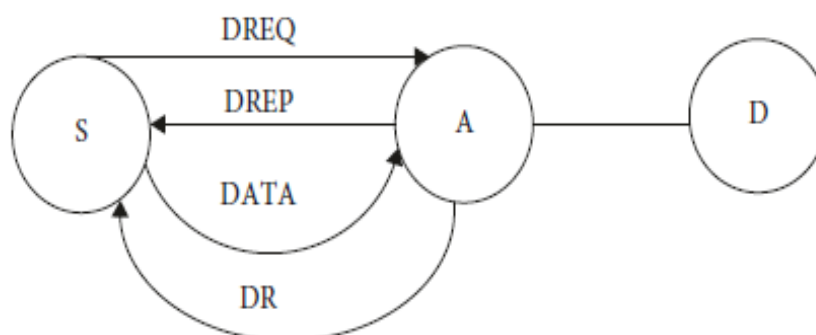
Figure 3: Data transmission using improved bacteria for aging optimization algorithm based on ad- hoc protocol.

In the above figure node S is a source node, node D is a destination node, and node A is an intermediate node between a source node and the destination node.

Here the data sending from the source node is always done only after checking the trust value of node A and sent the message data request to intermediate node A if intermediate node A is reply with a data reply message to node S after checking the congestion in a network, energy availability as required for the successful forwarding of a packet, and also check the node status which is a malicious node or not, if the node is marked with malicious node then source node discards the data sending process via an intermediate node. After receiving successful packets from the source node, node A forwards the packet to destination node D.
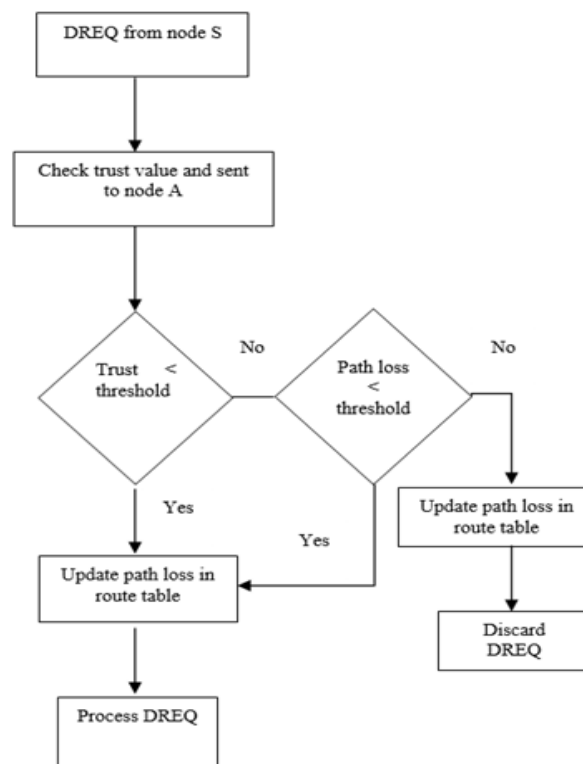
Figure 4: The above figure represents the trust-based mechanism for forwarding a packet from the source node to the destination node.

In the above figure, we represent our proposed work model which is based on the trust-based value, the node is always checking a trust value before forwarding the packets, and its compared with a threshold value, if a node value is less than the threshold value then we use respective node is a trusted node otherwise not if a node is trusted then intermediate node reply the date request otherwise the request is discarded.
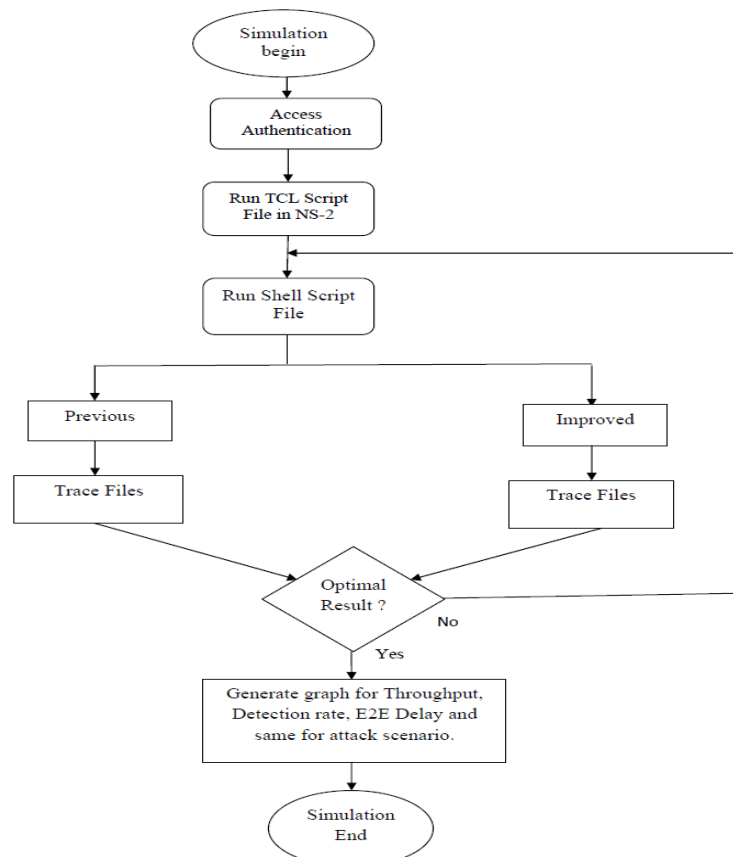

Figure 5: The above figure presents the proposed workflow graph.

There are some steps we have to follow to implement this system are following:-

Step 1- begin the process of virtualization and open the VMware machine and turn on the power of the virtual machine.

Step 2- After the successful power on for the machine log in with the id and password to enter into the machine.

Step 3- Run the tool command script file for the network simulator.

Step 4- Open the shell scripting window and run the file using the shell command.

Step 5- Apply the techniques with the network simulator s like the previous approach and proposed approach.

Step 6- Find the best route according to the applied techniques with the network simulator and find the best route or path.

Step 7- Getting the optimal routing results.

Step 8- After getting optimal results if we are not satisfied with the results then go to step 5, until we found the best results.

Step 9- Exit the experimental simulation process and end the VMware machine with a power-off signal.

3. RESULT ANALYSIS

In this section, we discuss the proposed experimental results compare with the existing techniques; also discuss the simulation experimental environment and the snapshot for the proposed and existing methods results. The proposed methods give better results than the currently existing techniques, the performance evaluation parameters are such as the delay between the packets are transmitting between a source node and destination node, throughput for a delivered number of packets, and packet delivery ratio for a packet between the source and destination, here we discuss comparative performance result summary using existing and proposed methods with tabular form and graphical representation also.
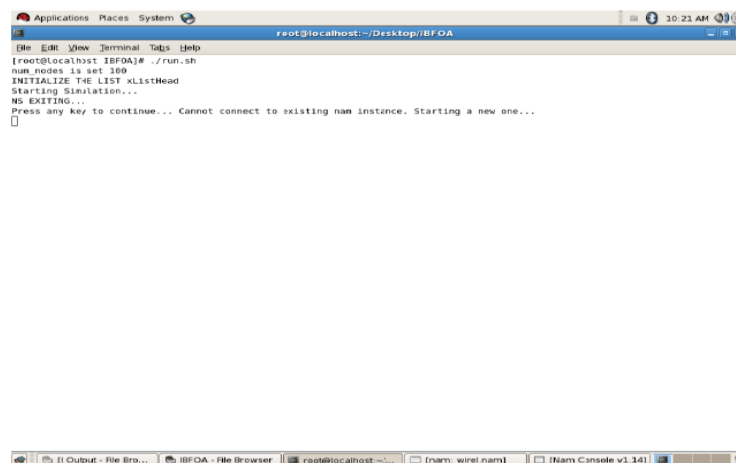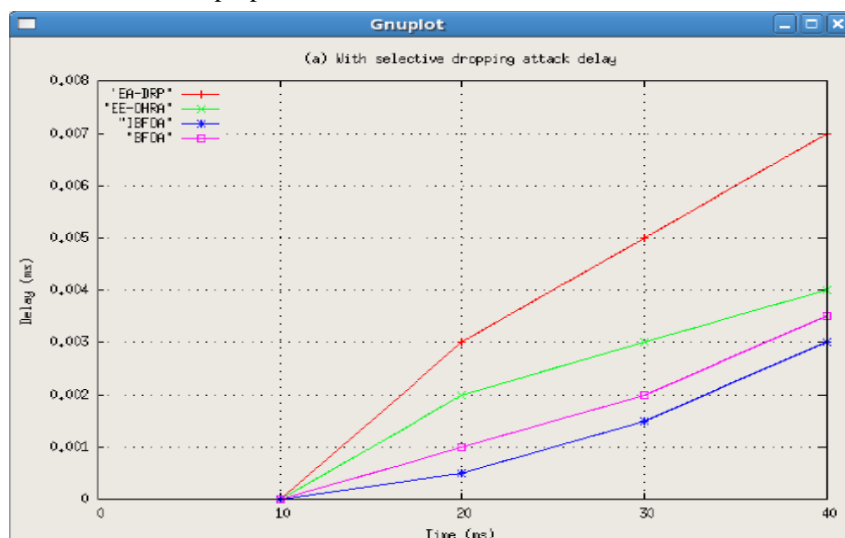

Figure 6: This window shows the running shell files output and their description used in a network simulator.
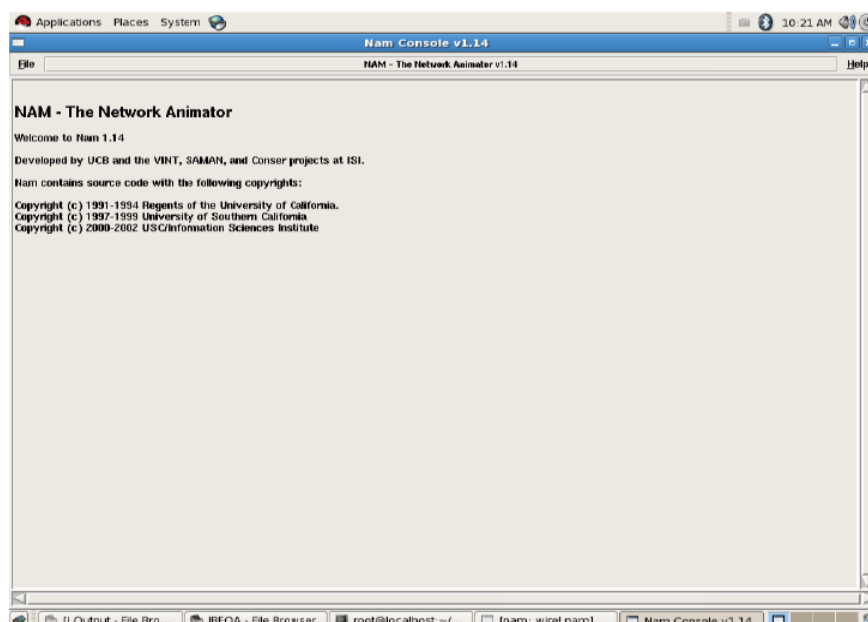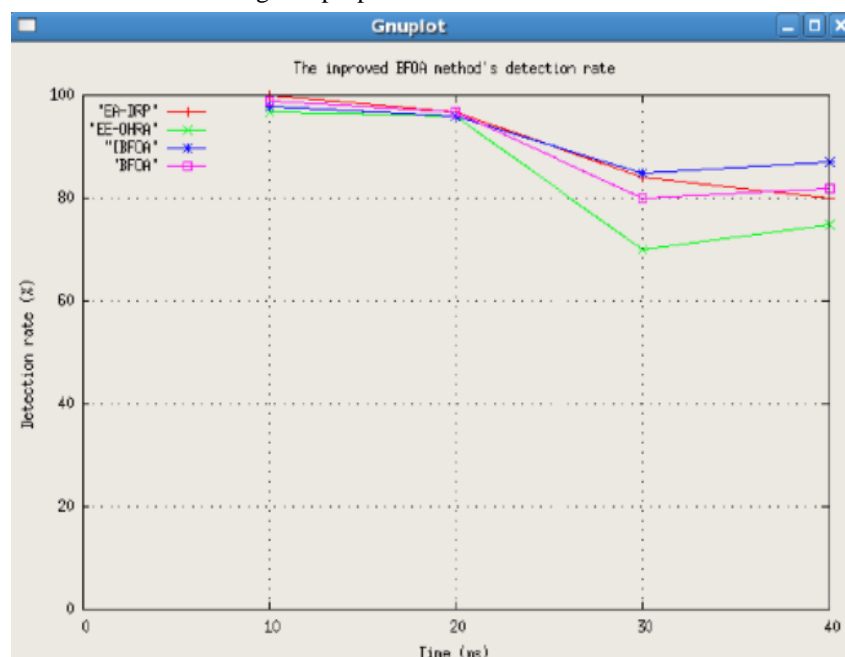

Figure 7: The above window shows the network animator files in a network simulator.
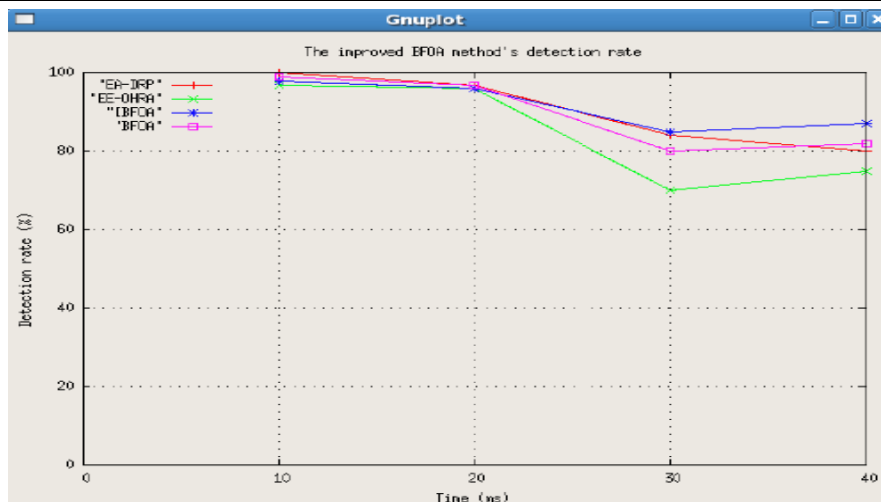
Figure 8: The above window shows the output of a performance parameter is the detection rate for the existing and proposed method in a network simulator.

Figure 9: The above window shows the output of a performance parameter a delayed with a selective dropping attack for the existing and proposed method in a network simulator.

Figure 10: The above window shows the output of a performance parameter is detection rate for the existing and proposed method in a network.

4. CONCLUSION

In this paper, our experimental result shows that better quality of services parameter value than existing work. The proposed algorithm is based on the find right node according to their trust value and makes secure communication between the nodes in a network, here in the simulation scenario we present the experimental result for the normal mode and as well as attack mode and find a better performance than the existing techniques.

5. REFERENCES

[1] Uppalapati Srilakshmi, Saleh Ahmed Alghamdi, Veera Ankalu Vuyyuru, Neenavath Veeraiah, Youseef Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks", IEEE Access, 2022, pp. 14260-14269.

[2] Uppalapati Srilakshmi, Neenavath Veeraiah, Youseef Alotaibi, Saleh Ahmed Alghamdi, Osamah Ibrahim Khalaf, Bhimineni Venkata Subbayamma, "An Improved Hybrid Secure Multipath Routing Protocol for MANET", IEEE Access, 2021, pp. 163043-163053.

[3] Raghu Ramamoorthy, Menakadevi Thangavelu, "An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks", Journal of Ambient Intelligence and Humanized Computing, 2022, pp. 1-34.

[4] Shahenda Sarhan, Shadia Sarhan, "Elephant Herding Optimization Ad Hoc On-Demand Multipath Distance Vector Routing Protocol for MANET", IEEE Access, 2021, pp. 29489-29499.

[5] K. Sakthidasan Sankaran, N. Vasudevan, K. R. Devabalaji, Thanikanti Sudhakar Babu, Hassan Haes Alhelou, T. Yuvaraj, "A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks", IEEE Access, 2021, pp. 21735-21745.

[6] Baidaa Hamza Khudayer, Mohammed Anbar, Sabri M. Hanshi,Tat-Chee Wan, "Efficient Route Discovery and Link Failure Detection Mechanisms for Source Routing Protocol in Mobile Ad-Hoc Networks", IEEE Access, 2020, pp. 24019-24033.

[7] Ahuja, Y, Rathore, D. , Mishra S K , "Efficient Routing Scheme for Vehicular Ad-hoc Network using Dedicated Short Range Communication Protocol", International Journal of Emerging Technology and Advanced Engineering, Vol-9, Issue-10, pp. 110-113.

[8] Valmik Tilwari, R. Maheswar, P. Jayarajan, T. V. P. Sundararajan, MHD Nour Hindia, Kaharudin Dimyati, Henry Ojukwu,, Iraj Sadegh Amiri, "MCLMR: A Multicriteria Based Multipath Routing in the Mobile Ad Hoc Networks", Wireless Personal Communications, 2020, pp. 1-24.

[9] Burhan Ul Islam Khan, Farhat Anwar, Rashidah Funke Olanrewaju, Bisma Rasool Pampori, Roohie Naaz Mir, "A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks", IEEE Access, 2020, pp. 124097-124109.

[10] Xiaoliang Wang, Peng Zhang, Yuyue Du, Mei Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network", IEEE Access, 2020, pp. 47675- 47694.

[11] Masood Ahmad, Abdul Hameed, Ataul Aziz Ikram, Ishtiaq Wahid, "State-of-the-Art Clustering Schemes in Mobile Ad Hoc Networks: Objectives, Challenges, and Future Directions", IEEE Access, 2019, pp. 17067-17084.

[12] Anchal Thakur, Deepak Rathore, "Analyze the Performance of Bio-Medical Image Compression Technique using Particle Swarm Optimization", International Conference on Advanced Computation and Telecommunication, 2018, IEEE, pp. 1-4.

[13] Hyun-Ho Choi, Jung-Ryun Lee, "Local Flooding-Based on-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Access, 2019, pp. 85937-85951.

[14] R Dubey, D Rathore, D Kushwaha, JP Maurya, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[15] Ibrahim Kacem, Belkacem Sait, Saad Mekhilef, Nassereddine Sabeur, "A New Routing Approach for Mobile Ad Hoc Systems Based on Fuzzy Petri Nets and Ant System", IEEE Access, 2018, pp. 65705-65720.

[16] T. Poongodi, Mohammed S. Khan, Rizwan Patan, "Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks", IEEE Access, 2019, pp. 18409-18420.

[17] Dinesh Chander, Rajneesh Kumar, "QoS Enabled Cross-Layer Multicast Routing over Mobile Ad Hoc Networks", International Conference on Smart Computing & Communication, 2018, pp. 215-227.

[18] Ishtiaq Wahid, Ataul Aziz Ikram, Masood Ahmad, Sajjad Ali, Arshad Ali, "State of the Art Routing Protocols in VANETs: A Review", Procedia Computer Science, 2018, pp. 689-694.