Power Aware MANET Routing Protocol for Efficient Packet Transmission Using T–Test and Sleep and Awake Strategy

S. Hemalatha, Harikumar Pallathadka, Rajesh P Chinchewadi

Abstract: ***The majority of the suggested routing protocols have not given any attention to energy consumption whatsoever, despite the fact that advances in battery design have not yet reached the point where a device can be able to operate for a longer amount of time. Energy-efficient routing is one of the crucial issues that must be taken into account in MANETs. Numerous scholars have offered highly effective solutions for this problem. Since all nodes in MANETs are connected to and run by low-power battery devices, energy-aware routing is without a doubt the highest design standard The lifespan of the network is eventually shortened when an intermediary node is shut down due to a power outage because it not only impacts the node's own system but also its capacity to relay packets on behalf of others. The untimely shutdown of a node damages the entire network system because packet forwarding on the route will become fully disconnected as soon as a node Electronics 2020, 9, 1129 5 of 64 fails due to a power outage. However, the preceding node continues to wastefully retransmit the same packets up to a specific threshold, wasting both its power and bandwidth in the process. The preceding node then informs the source that the path is severed as a result of this. Finally, route finding is once more carried out by the source node, which uses a lot of energy in the network. This work suggested a new routing method that uses the T-test procedure to discover the most effective path between nodes. This proposed technique recursively identifies the optimum way between nodes for communication, ensuring that each node participating in route discovery has enough energy for transmission. The T-Test procedure defines and supports the criteria for evaluating the nodes that are chosen and rejected during the route discovery process. This technique, in conjunction with T-Test, enables successful packet transmission in MANET packet flows with sleep and awake strategies. It is also developed using network simulation and compared to the present routing system, indicating that it performs better overall.***

Key words: MANET, Sleep and Awake Strategy, Routing Algorithm, T-Test,

Manuscript received on 21 November 2023 | Revised Manuscript received on 07 December 2023 | Manuscript Accepted on 15 December 2023 | Manuscript published on 30 December 2023.

******Correspondence Author(s)*

Dr. S. Hemalatha*, Professor, Department of Computer Science and Business System, Panimalar Engineering College, Chennai (Tamil Nadu), India., Post Doctorial Research Fellow, Manipur International University, Impala, Manipur, India, E-mail: pithemalatha@gmail.com, ORCID ID 0000-0002-0049-1167

Dr. Harikumar Pallathadka, PhD, DSc, Vice Chancellor and Professor, Manipur International University, Imphal, Manipur, India. E-mail: harikumar@miu.edu.in, ORCID ID 0000-0002-0705-9035

Rajesh P Chinchewadi, CTO &, Dean Innovation, Manipur International University, Imphal, Manipur, India. E-mail: Rajesh.cto@miu.edu.in, ORCID ID 0009-0001-5891-9605

I. INTRODUCTION

The Network layer in the MANET protocol is responsible for route selection and fining out the best path from the source to the destination node. For finding the route selection the MANET uses the network layer uses the route request (RREQ) [1]and route reply (RREP) messages. Route Request message contain a pair of information (Source node, Request ID). The request ID is a unique ID generated by the source node when it wants to find the destination path. When the source node initiate the route to the destination it floods the route request (RREQ) messages to the next hope node, the next hop node also floods the RREP message to its next hop until reaches to the destination node. The destination node send the acknowledgement to the source node with the route Reply message RREP in a reversal path. This Two messages support for path selection. Depending on the Protocol chosen by the network layer the path from the source to the destination is finalized. Proactive routing systems [1] are sometimes known as table-driven routing protocols. Every mobile node has its own routing database, which lists the routes to all potential destination mobile nodes. Because the topology of a mobile ad hoc network changes often, these routing tables are routinely changed. Its downside is that it struggles with large networks since storing route information to every potential node causes the routing table entries to become excessively large. Reactive routing systems are sometimes known as on-demand routing protocols. In this type of routing, the path is only discovered when it is required. To accomplish route discovery, route request packets are disseminated over the mobile network. Its two fundamental aspects are route discovery and route maintenance. A t test is used in statistics to compare the means of two groups. It is commonly used in hypothesis testing to assess whether two groups vary or whether a method or treatment has an effect on the population of interest. The null hypothesis (H0) asserts that there is no difference between these group means. The actual difference, according to the alternative theory (Ha), is not zero. A t test (also known as a pair wise comparison) should be used only when comparing the means of two groups. If you want to compare more than two groups or perform several pair wise comparisons, use an ANOVA test or a post-hoc test. The t test is a parametric difference test, which implies that its conclusions are based on the same premises as other parametric tests.

The t test assumes that your data are comparable in terms of variation within each group being compared, independent, and (nearly) consistently distributed (also known as variance homogeneity).

MANET Routing Protocol Characteristics

To avoid routing difficulties in MANET, routing protocols should have the following characteristics:

- It should be widely distributed.
- Localization is required.
- It should be adaptive to frequent changes in topology caused by node mobility.
- It must be free of impassable paths.
- The paths must shortly converge.

A.Performing a T- Test

The t test evaluates the true difference between two group means by dividing the difference in group means by the total standard errors of both groups. It can be calculated automatically or manually using statistical analysis software and a formula.T- test equation

The formula for the two-sample t test, also known as the Student's t-test, is provided in the Eq(1) below.

$t = (x1 - x2) / \sqrt{(s2(1/n1 + 1/n2))}$ Eq (1)

T represents the test statistic, x1 and x2 represent the two groups being compared, s2 represents the combined standard error of the two groups, and n1 and n2 represent the number of observations in each group. A larger t value implies a more significant difference between groups since the difference between group means is greater than the pooled standard error.

II. RELEVANT WORK

Because MANETs are dynamic, there are resources, routing, and stability difficulties, all of which are vulnerable to various attacks. The present literature study highlights the importance of energy conservation [3][19][20][8] as a critical aspect in routing algorithms for network performance and proposes an effective energy algorithm based on the shortcomings of existing energy protocols. The protocols demonstrate the significance of routing in networks and explain the various routing algorithm approaches[4] provided by MANET. Furthermore, it introduces and investigates network security issues, describes intrusion detection methods for network attacks, and proposes improving the energy technique by including a security algorithm.

The network performs badly due to the MANET architecture's fragmented and often dynamic nature. The capacity of this routing protocol to swiftly discover the best paths between sources and destinations ensures that data is transmitted reliably and within the time limit specified. The route path's establishments must adhere to the least amount of overhead. Current routing methods [6] are built for static environments and are incapable of adapting to often changing topologies, resulting in poor convergence, throughput, route loops, overhead, and congestion. This should be enhanced, thus the routing should be properly explored. Security policy methods have been developed for the many types of infrastructure networks.

It is a significant task to implement these policies in MANETs apps. To establish secure paths between source and destination, the authors used a piece of their research on secure routing algorithms [6]. Global Transitions Proceedings 3 (2022), R. Prasad and Shivashankar. The authors of paper [7] proposed a method that minimises overall energy usage while also enhancing network networking lifetime by combining compressive sensing techniques with network coding in the sensor network. By establishing the virtual coordinates, it decreases the energy required to ensure a long-lasting network. This procedure must also accommodate a changing network environment.

The research [9] evaluated the energy consumption parameters that affect network longevity. Among the energy consumption factors are the expected energy sources, the energy placement target, and the frequency and latency of data aggregation energy network concentration. A single sink location outperforms several sink sites with limiting network mobility. In [10][17][18],

Although this algorithm consumes the least amount of energy, it fails in high-speed connections because it broadcasts. Messages are constantly passing via the network, and the total overhead is significant. [11] Presented a technique for limiting the nodes' energy threshold for message forwarding. The authors [12][16] presented energy-efficient routing, which builds with multiple route paths in decreasing order, measures the energy levels of each road, introduces new paths, and extends network lifetime. When constructing the paths, the conventional DSR routing protocols [13][19] do not take energy into account. Both AODV and DSR make efficient use of resources, save energy, and allow mobile ad hoc network architectures/organizations to self-organize, self-configure, and move. Nonetheless, with limited abilities, more flexible, and Nodes in the setup should fulfil the [14] tier and routing tier for information transfer. If the node is not prepared to recognize these levels, it will be unable to join the network.

Following the distribution of inquiries over the network, each node can accept one route request from another node. These policy enforcement mechanisms are primarily meant to create safe network paths and routing; nonetheless, they fall short in defending against malicious nodes and various types of attacks. It was described in the study [15] how to build secure channels by broadcasting information hop by hop to authenticate nodes. The network's security protocol then validates end-to-end performance metrics using a symmetric key generated device. Many academics have focused on problems with secure routing paths that use the least amount of energy for transmission and have also raised security concerns about it, but they are ineffectual and struggle when dealing with various types of real-time attacks.

In MANET, there are two sorts of attacks: active and passive. Passive attacks are most common in the TCP/IP network levels and data connection layers. Such attacks have no effect on how the network runs because they ingest packet information from available network nodes. Typically, attacks send data while exchanging information. These assaults have a lower impact on the network than active attacks. These attacks produce disturbances such as information spying, packet loss, and misinformation about nodes. Eavesdropping, jamming, selfish behaviour, traffic analysis, and traffic monitoring are all examples of passive attacks.

Active attacks involve nodes purposefully changing route patterns and traffic, slowing transmission and congesting networks.

Because of this characteristic, active attacks are sometimes referred to as routing attacks. Performance is low as a result of the difficulties in identifying and mitigating these types of attacks. Worm-hole, black-hole, flooding, spoofing, and gray-hole attacks are examples of current attacks. Such protections can only be built with a thorough understanding of the dangers.

The Enhanced Energy Efficient Secure Routing (EEE-SR) protocol approach, an algorithm that identifies the lowest shortest energy path for data transmission to network nodes with secured network data communication, has been devised and applied in the proposed study attempt. This technique's greater energy efficiency boosts network throughput and network longevity. This algorithm includes energy-efficient management techniques, allowing it to make greater use of the nodes' available energy.

III. T-TEST AND SLEEP AND AWAKE STRATEGY ROUTING ALGORITHM

This article's unique routing approach follows the procedures involved in MANET routing operations, such as route request and route discovery. Finding the device's remaining power for picking the path from source to designation is one of the new aspects of the new define algorithm, and the nodes operate in two modes: sleep and awake. This will be specified by the area nodes, with one node sleeping and the others waking.

A.Sleep and Awake Node Selection

1. All the nodes send a beacon signal to other nodes to receive the current location and battery power
2. Upon receiving the beacon signal other nodes shares the current location.
3. Each and every node finds out the nodes within the transmission range based on the location
4. Form cluster nodes which are in the same region.
5. Choose the head nodes which posses the high battery power in the same region
6. Head nodes define the list of sleep nodes and awake node
7. Send information to other nodes in the region and start routing process

B.The Algorithm's Phases

1. Have the MANET's source node send a route request RREQ to every node that contains the destination node.
2. Obtain the Route Response from the Other Nodes in Order to Communicate with the Destination.
3. Determine the Remaining Power of Each Node Along its Path from the Source to the Destination.
4. Using the T-Test Procedure, Approve or Reject the Node for Route Discovery.
5. Remove Rejected Nodes and Select A New Transmission Path.
6. Finish the Transmission's Chosen Path.

C.T-Test Methodology

The number of nodes participating in the first route discovery [2]will be defined for n, and the total number of nodes in the MANET will be defined for N. The T-Test approach defines the Hypothesis. Selected nodes have more power than residual nodes. Rejected nodes identify which nodes have less remaining power.

Residual Power >=H0 is the True Hypothesis.

Residual Power: Fals Hypothesis H1

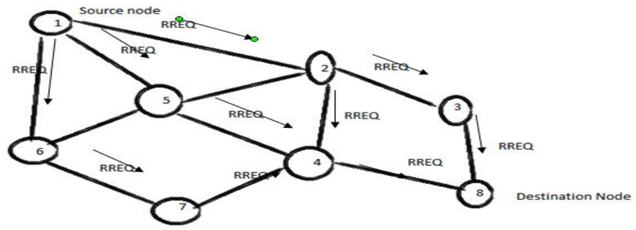


Figure 3.1: Request Route from Source to Destination Node

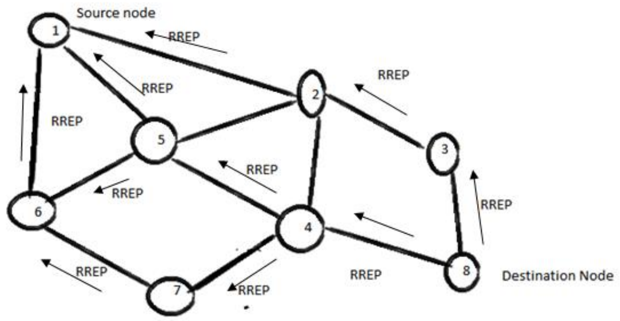


Figure 3.2: Reply Route from Destination Node to Source Node

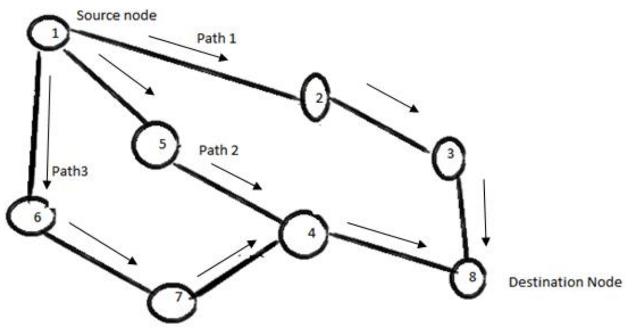


Figure 3.3: Alternative Path from Source to Destination

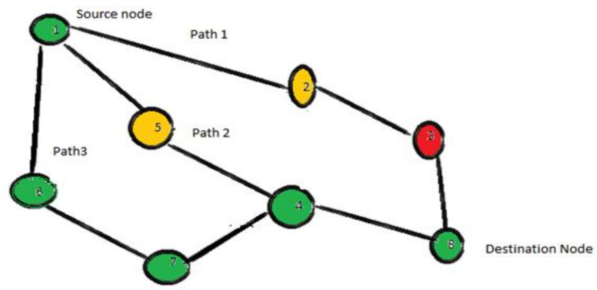


Figure 3.4: Residual Power on Two Different Paths from the Source to the Destination

The working principle of the proposed algorithm is represented in Figures 3.1 to 3.4, where a route Request is delivered from the source node to the destination node. The route reply is sent by the destination node to the source node, as shown in Figure 3.2. Figures 3.3 and 3.4 demonstrate the identification of different paths and the selection of the way that has enough energy to transport the packet, which is done by utilising the T-test process with the help of residual power availability in each node.

Retrieval Number:100.1/ijdcn.A503304011223
DOI:10.54105/ijdcn.A5033.124123
Journal Website: https://www.ijdcn.latticescipub.com

Published By:
Lattice Science Publication (LSP)

IV. SIMULATION

The suggested routing algorithm is implemented in NS-2 Simulator version 2.34. The simulation area is 500X 500 mm, and the number of nodes is 50, 100, and 150 with stop times of 5s, 15s, and 25 sec and average speeds of 10.10 m/s, 21.25 m/s, and 12.02 m/s, respectively. Table 1 shows the entire simulation setup for the MANET investigation. Table 2 displays the defined parameter value with constant bit rate traffic while estimating the Energy model for the MANET protocol performance. The Omni antenna is used to determine the routing path and packet transmission. Initially, all nodes established an ideal energy of 200 joules, and other required power is also estimated and assigned, as shown in table 2.

V. RESULT AND DISCUSSION

The suggested routing algorithm is compared [5] to the existing AODV protocol since the AODV is an on demand protocol that supports defining the optimum path between source and destination. To locate the route discovery, the source node sends the Route Request to all nodes and waits for the router response.

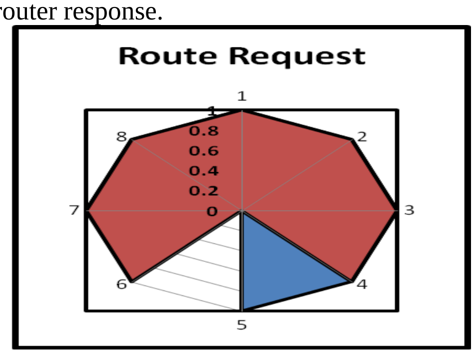
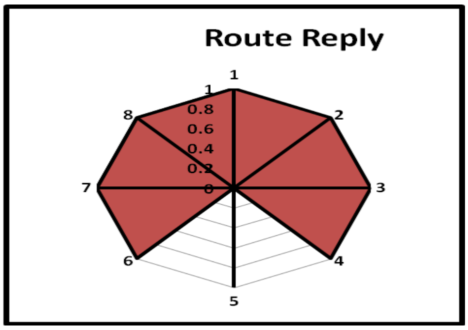


Figure 5.1: Request for Route



Route Exploration

At this step, the suggested approach is critical for selecting the most power-efficient node for packet transmission.Using the T Test Procedure, each node's residual power is evaluated, and the node path with the most energy is chosen. The comparison for taking the time to select the optimum path is made with the AODV protocol, which indicates a little delay in path selection in the PE-AODV protocol. This delay is manageable and has no effect on the MANET's performance, as demonstrated in Figure 5.2. Finally, the protocol performance parameters are summarised in Figure 5.3.

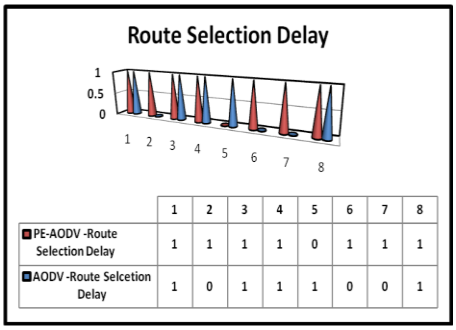


Figure 5.2: Route Selections Delay

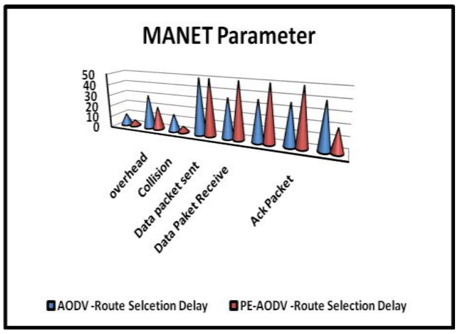


Figure 5.3: Parameter Comparisons

VI. CONCLUSION

The Routing Algorithm for Efficient Packet Transmission in MANET Using T -Test Procedure is constructed with the help of a Network Simulator, and the results were compared with the current protocol, which showed that it performed better than the other MANET protocols. The T-Test is crucial in determining the best path along the trip. This protocol could be incorporated as a feature in the Making new protocol stack for the MANET network layer route finding.

DECLARATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Gupta, A.K., Sadawarti, H. and Verma, A.K. (2011) A Review of Routing Protocols for Mobile Ad Hoc Networks. SEAS Transactions on Communications, 10, 331-340.
2. Ruta, M., Zacheo, G., Grieco, L., Noia, T., Boggia, G., Tinelli, E., Sciascio, E., et al. (2010) Semantic-Based Resource Discovery, Composition and Substitution in IEEE 802.11 Mobile Ad Hoc Networks. Wireless Networks, 16, 1223-1251. http://dx.doi.org/10.1007/s11276-009-0199-5
3. Tamilarasi, M., Chandramathi, S. and Palanivelu, T. (2001) Efficient Energy Management for Mobile Ad Hoc Networks. Ubiquitous Computing and Communication Journal, 3, 12- 19.

4. Prabha R. and Ramaraj N.: ―An improved multipath MANET routing using link estimation and swarm intelligence‖, EURASIP Journal on Wireless Communications and Networking2015:173, DOI: 10.1186/s13638015-0385-3, June 2015. https://doi.org/10.1186/s13638-015-0385-3
5. Thaseen, I. Sumaiya, and K. Santhi. "Performance analysis of FSR, LAR and ZRP routing protocols in MANET." International Journal of Computer Applications 41.4 (2012). https://doi.org/10.5120/5529-7572
6. V.K. Quy, N.T. Ban, B.D. Tho, N.D. Han, Performance analysis of MANET employing AODV, DSR, OLSR and DSDV Routing Protocols, in: Proc. Conf. on Fundamental and Applied Information Technology Research (FAIR'8), Hanoi, 2018, pp. 96–102.
7. J Xiong, J Zhao, L Xuan, Research on the Combining of Compressed Sensing and Network Coding in the Wireless Sensor Network, J. Theo. Appl. Inf. Technol. 47 (3) (2015).
8. Q.Xu S.Olariu, A. Zomaya, An Energy-Efficient Self- Organization Protocol for Wire- less Sensor Networks, in: Proc. IEEE Intelligent Sensors, Sensor Networks, and Infor- mation Processing Conf. (ISSNIP), 2014, pp. 55–60.
9. B. Krishnamachari, D. Estrin, S.B. Wicker, The Impact of Data Aggregation in Wire- less Sensor Networks, Distrib. Comput. Syst. (2013) 575–578.
10. Eduardo F. Nakamura, Heitor S. Ramos, Leandro A. Villas, Andre.de Aquino, Anto- nio. Loureiro, Reactive Role Assignment for Data Routing in Event-Based Wireless Sensor Networks, Computer Networks, 2017.
11. W. Kuo, S. Chu, Energy Efficiency Optimization for Mobile Ad Hoc Networks, IEEE Access 4 (2016) 928–940. https://doi.org/10.1109/ACCESS.2016.2633378
12. Rajendra Prasad P, Dr. Shivashankar, Energy Secured Intrusion Detection System and Analysis of Attacks for Mobile Ad-Hoc Networks, J. Commun. Eng. Tech. Pub- lish. (ETP) 15 (5) (2020) 406–414 ISSN: 1796-2021 (Online); 2374-4367 (Print), JCM, doi:10.12720/jcm.15.5.406-414. https://doi.org/10.12720/jcm.15.5.406-414
13. S Shankar, G Varaprasad, HN Suresh, Importance of on-demand modified pow- er-aware dynamic source routing protocol in mobile ad-hoc networks, Microwaves, Antennas & Propagation, IET 8 (7) (2014) 459–464. https://doi.org/10.1049/iet-map.2013.0230
14. Gang Xu, Cristian Borcea, LiviuIftode, A Policy Enforcing Mechanism for Trusted Ad Hoc Networks, IEEE Trans. Dependable Secure Comput. 8 (3) (2011) 1–15. https://doi.org/10.1109/TDSC.2010.11
15. Y.C. Hu, A. Perrig, D.B. Johnson. Ariadne, A Secure On-demand Routing Protocol for Ad Hoc Networks, in: Proceedings of International Conference on Mobile Computing and Networking, Atlanta, USA, 2012, pp. 12–23.
16. Kaur, K., & Kang, Dr. S. (2020). Routing Architectures for IoT. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 7, pp. 1089–1083). https://doi.org/10.35940/ijitee.f3431.059720
17. Kumar, N., & Singh, Dr. G. (2022). The Performance Analysis of Optimized Integrated Framework for Smart Grid. In Indian Journal of Signal Processing (Vol. 2, Issue 3, pp. 1–4 https://doi.org/10.54105/ijsp.d1010.082322
18. Vendoti, S., Muralidhar, Dr. M., & Kiranmayi, Dr. R. (2019). Performance Analysis of Hybrid Power System Along With Conventional Energy Sources for Sustainable Development in Rural Areas. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 3, pp. 5971–5977). https://doi.org/10.35940/ijrte.f2567.098319
19. Jain, N., & Kumar, R. (2022). A Review on Machine Learning & It's Algorithms. In International Journal of Soft Computing and Engineering (Vol. 12, Issue 5, pp. 1–5 https://doi.org/10.35940/ijsce.e3583.1112522
20. Sahay, R. R. (2023). Information and Security Cryptography-Encryption in Journalism. In Indian Journal of Mass Communication and Journalism (Vol. 3, Issue 1, pp. 1–16 https://doi.org/10.54105/ijmcj.a1047.093123

AUTHORS PROFILE

Dr. S. Hemalatha, has completed BE (CSE) and ME (CSE) from Arulmigu Meenakshi Amman college of engineering in the year 2000 and 2004 respectively. Completed PhD from Anna University in the year of 2016. Presently pursuing Post Doctorial Program in Manipur International University under the research area of Mobile Adhoc Security. She has more than 22 years of experience in different engineering colleges. Presently working as a professor and Head in CSBS department at Panimalar institute of technology. She has more contribution in international and national journal, books and Patents

Professor (Dr) Harikumar Pallathadka is a highly accomplished individual in Law and Management, with Post Doctoral Degrees in both fields. With over 300 published research papers in reputable journals, including SCI/Scopus, he showcases his versatility and expertise. He has also published over 300 National and International patents, with around 50 awarded. Prof. Pallathadka is also well known social activist. An experienced administrator and an authority in Constitutional Law and Machine Learning, he currently holds the position of Professor and Vice Chancellor at Manipur International University. His extensive accomplishments and dedication highlight his exceptional abilities.

Prof Rajesh Chinchewadi has completed BE (Computer Science & Engineering) from University BDT College of Engineering, Davangere, University of Mysore, Of Mysore in the year 1993. Completed EGMP (EMBA) from Indian Institute Of Management, Bangalore. He has more than 25 years of experience in different IT Technology MNCs - Hewelett Packard, Cisco, GE GXS, and Start-ups in senior management positions. Presently working as a professor and Chief Technology Officer & Dean Innovation for Manipur International University, Director, Strategy for Global Investment firm and mentor to start-ups.

Table 1: Examination Simulation Setup

Parameter Setup	Data set
Total nodes	150, 200,250,300
Name of the source node	5
Simulation time Set	**100s**
Default break time	5s ,10s, 15s, and 25 sec
speed	11.10 m/s , 11.25 m/s and 14.02 m/s
Traffic Type	CBR
Size of the Packet	512 byte

Table 2: Energy Model Parameter Specifications

Parameter	Defined
MANET Network Interface	Wireless Physical Interface
Medium Access Control type	802.11
Type of Channel	Wireless channel
Propagation method	TWO WAY GROUND
Antenna Defined	Omni Antenna
Frequency Set	280.8 mW (250 m)
Initial node Energy	240 Joule
Rest Power	1.5W
Receiving packet Power	1.0W
Transmission packet Power	1.5w
Transmission Power	1.6w
Sleep Power	0.002w
Changeover Time	0.009s