Research Article

Journal of Sensor Networks and Data Communications

Routing Algorithm for Efficient Packet Transmission in Manet Using T–Test Procedure

S. Hemalatha[1*], Harikumar Pallathadka[2] and Rajesh P Chin Hewadi[3]

[1]*CSBS, Panimalar Engineering College, Chennai, Tamil Nadu, India.*

[2]*Vice Chancellor and Professor, Manipur International University, Imphal, Manipur, India.*

[3]*CTO & Dean Innovation, Manipur International University, Imphal, Manipur, India.*

[*]Corresponding Author
Hemalatha S, Panimalar Engineering College , Chennai, Tamil Nadu, India.

Submitted: 2023, Aug 10; **Accepted**: 2023, Sep 11: **Published**: 2023, Sep 20

Citation: Hemalatha, S., Pallathadka, H., Hewadi, R. P. C. (2023). Routing Algorithm for Efficient Packet Transmission in Manet Using T–Test Procedure. *J Sen Net Data Comm, 3*(1), 67-75.

Abstract

One of the laborious communication tasks in a mobile ad hoc network is packet transmission. Due to the MANET node's power backup, many routing paths may experience unsuccessful packet delivery. The routing algorithm chooses the path that packets take as they travel from the source node to the destination nodes, but it makes no guarantees regarding packet delivery. In order to determine the most effective path between nodes, this paper proposed a new routing algorithm with the use of the T-test process. This suggested technique determines the best path between nodes for communication in a recursive manner, ensuring that each node participating in the route discovery has enough energy for transmission. The criteria for evaluating the nodes that are chosen and rejected throughout the route discovery process are defined and supported by the T-Test procedure. This technique, together with T-Test, supports effective packet transmission in MANET packet flow. It is also built with the help of network simulation and compared to the current routing protocol, demonstrating that it performs better overall.

Keywords: MANET, Routing Algorithm, T-Test.

1. Introduction

Because the topology of an ad hoc network is dynamic, nodes in a mobile ad hoc network (MANET) are not aware of the topology of their network and must figure it out on their own. The fundamental guidelines state that anytime a new node joins an ad hoc network, it must make an announcement of its presence and must also pay attention to comparable announcement broadcasts from existing mobile nodes.

Table-driven routing protocols are another name for proactive routing systems. Every mobile node has a separate routing database that lists the paths to every potential destination mobile node. These routing tables are updated frequently as and when the network topology changes since the mobile ad hoc network's topology is dynamic. Its weakness is that it struggles with huge networks since maintaining the route information to every potential node causes the routing table entries to grow too large.

On-demand routing protocols are another name for reactive routing systems. The path is only discovered in this sort of routing when it is necessary. Route request packets are broadcast around the mobile network to perform route discovery. Route discovery and route maintenance make up its two primary aspects.

Statistics is used to compare the means of two groups using a t test. It is widely used in hypothesis testing to determine whether two groups are different from one another or whether a procedure or treatment actually has an effect on the population of interest. The null hypothesis states that there is actually no difference between these group means (H0). According to the alternative theory (Ha), the actual difference is not zero.

Only when comparing the means of two groups may a t test be employed (a.k.a. pairwise comparison). Use an ANOVA test or a post-hoc test if you wish to compare more than two groups or do numerous pairwise comparisons. The t test is a parametric test of

difference, which means it bases its conclusions on the same premises that other parametric tests do. The t test presupposes that your data: are comparable in terms of variation within each group being compared, independent, and (almost) regularly distributed (a.k.a. homogeneity of variance)

Features of the MANET Routing Protocol

Routing protocols should have the following qualities to prevent routing issues in MANET:

- It ought to be disseminated extensively.
- Localization is necessary.
- It should be adaptable to frequent changes in topology due to the mobility of the nodes.
- It must be devoid of impassable pathways.
- The pathways must quickly merge.
- It should be mandatory for every node in the network to keep records of its reliable local topology.
- It needs to be able to deliver top-notch service.

Carrying Out a T Test

The ratio of the difference in group means over the combined standard errors of both groups is used by the t test to evaluate the genuine difference between two group means. Statistical analysis software can be used to calculate it automatically or manually using a formula.

T Test Equation

Below is a formula for the two-sample t test, often known as the Student's t-test.

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{(s^2(\frac{1}{n_1} + \frac{1}{n_2}))}}$$

In this equation, t stands for the test statistic, x1 and x2 for the two groups being compared, s2 for the combined standard error of the two groups, and n1 and n2 for the number of observations in each group. A bigger t value indicates that there is a more significant difference between the groups since the difference between group means is greater than the pooled standard error.

2. Related Work

Because MANETs are dynamic, there are issues with resources, routing, and stability, all of which are open to various attacks. The existing literature review emphasises the significance of energy conservation as a crucial factor in the routing algorithm for network performance and suggests an effective energy algorithm based on the drawbacks of existing energy protocols. The protocols illustrate the importance of routing in networks and discuss the many routing algorithm approaches that are given in MANET. Additionally, it presents and examines network security challenges, describes intrusion detection systems for network attacks, and suggests improving the energy method by incorporating a security algorithm.

Due to the MANET architecture's scattered and generally dynamic nature, the network performs poorly. This routing protocol's important characteristic is its ability to quickly identify the best paths between sources and destinations, ensuring that data is transmitted accurately and within the allotted time limit. The establishments of the route path must comply with the least amount of overhead. The current routing protocols are designed for static environments and are unable to adapt to often changing topologies, which has a negative impact on convergence, throughput, route loops, overhead, and congestion [1]. This needs to be improved, hence the routing needs to be thoroughly researched. For the different types of networks used for infrastructure, security policy methods have been created.

The implementation of these policies in the MANETs apps is a difficult problem. The authors have incorporated a piece of their research on secure routing algorithms to find secure paths between source and destination [6]. By considering compressive sensing techniques together with the network coding in the sensor network, the authors of paper have suggested an algorithm that reduces overall energy consumption while also improving the networking lifetime of the network [2]. It reduces the energy required to ensure a long-lasting network by determining the virtual coordinates. A dynamic network environment must also be supported by this process.

In paper, the authors put the self-organizing energy protocol into practise [3]. This protocol uses media access control to reduce energy consumption, with on-demand nodes identified by virtual coordination’s to determine the network's shortest path for data communication. It reduces the energy required to maintain the network lifetime by recognising the virtual coordinates. This process must also accommodate a changing network environment.

The characteristics of energy consumption that affect the network lifetime were reviewed in the paper [4]. The expected energy sources, the energy placement target, and the frequency and latency of data aggregation energy network concentration are among the energy consumption parameters. The single sink location produces better results than several sink sites with constrained network mobility.

Although this algorithm uses the least amount of energy, it fails when it comes to high-speed communications since it broadcasts [5]. Messages are constantly flowing via the network, and total overhead is considerable proposed technique that restricts the nodes' energy threshold for forwarding messages [6]. The authors presented energy-efficient routing, which constructs with many route paths in decreasing order, measures the energy levels of each road, introduces different paths, and increases network lifetime [7]. The standard DSR routing protocols do not take energy into consideration when building the pathways [8]. AODV and DSR both make effective use of resources and save energy, and enable the self-organization, self-configuration, and mobility of mobile ad hoc network architectures/organizations. Nevertheless, with con-

strained talents, more adaptable, and Nodes in the set-up should satisfy the trust tier and routing tier for transmission of information. If the node is not ready to acknowledge these tiers, then it cannot join the network.

Following the posting of queries in the network, each node can accept one route request from other nodes. These policy enforcement measures are primarily intended to create safe pathways and routing within the network; nonetheless, they fall short in protecting against malicious nodes and various sorts of assaults. In the paper, it was explained how to create secure pathways by broadcasting information hop-by-hop to authenticate nodes [9]. The security protocol used in the network then performs end-to-end performance metric validation using a symmetric key constructed device. Many researchers have concentrated on problems with secure routing paths that utilise the least amount of energy for their transmission and have also highlighted security concerns for it, but they are ineffective and struggle when dealing with different forms of attacks in real time.

The two primary types of attacks in MANET are active and passive. The TCP/IP network layers and data connection layers are where passive assaults predominate. By importing the packet information from the available network nodes, such assaults have no effect on how the network functions. Attacks typically transmit data while sharing information. Compared to active attacks, these attacks have less of an impact on the network. These attacks cause disruptions such as information snooping, packet drops, and misleading node information. Examples of passive attacks include eavesdropping, jamming, selfish conduct, traffic analysis, and traffic monitoring.

Active attacks involve nodes deliberately altering route pathways and traffic, which slows down transmission and congests networks. Due of this behaviour, active attacks are occasionally called routing attacks. Due to the difficulty in detecting and preventing these types of attacks, performance is consequently low. Examples of current assaults include worm-hole, black-hole, flooding, spoofing, and grey-hole attacks. Only with in-depth knowledge of these threats can such defences be constructed.

The Enhanced Energy Efficient Secure Routing (EEE-SR) protocol approach, an algorithm that discovers the minimal shortest energy path for data transmission to the nodes in the network with secured network data communication, has been devised and implemented in the suggested study effort. The throughput and network longevity of the network are increased by this algorithm's improved energy efficiency. This algorithm has energy-efficient management strategies built into it, allowing it to make greater use of the energy available in the nodes.

3. Routing Algorithm

The novel routing method suggested in this article follows the steps involved in MANET routing operations, such as route request and route discovery. Finding the device's remaining power for choosing the path from source to designation is one of the new features of the new define algorithm.

The Phases of the Algorithm

- Have the source node in the MANET send a route request RREQ to every node with the destination node.
- Obtain the Route Response for communication with the destination from the other nodes.
- Determine each node's remaining power along its path from the source to the destination.
- Use the T -Test Procedure to approve or disapprove the node for route discovery.
- Remove rejected nodes and choose a different transmission path.
- Complete the transmission's chosen route.

T-Test Procedure

The first route discovery participating nodes will defined for n value, and the total number of nodes in MANET is defined for N value. The Hypothesis is defined by the T-Test technique. Selected nodes are those that have more power than residual. Which nodes have less remaining power is determined by rejected nodes.

True Hypothesis: Residual Power >=H0

False Hypothesis : Residual Power< H1

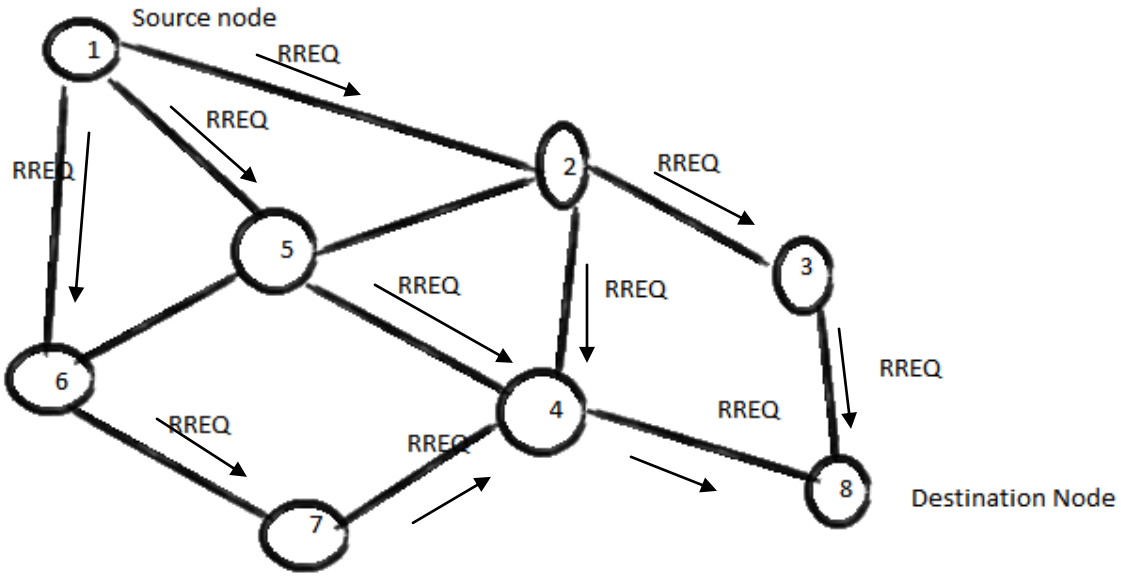

Figure 3.1: Route Request from Source Node to Destination Node

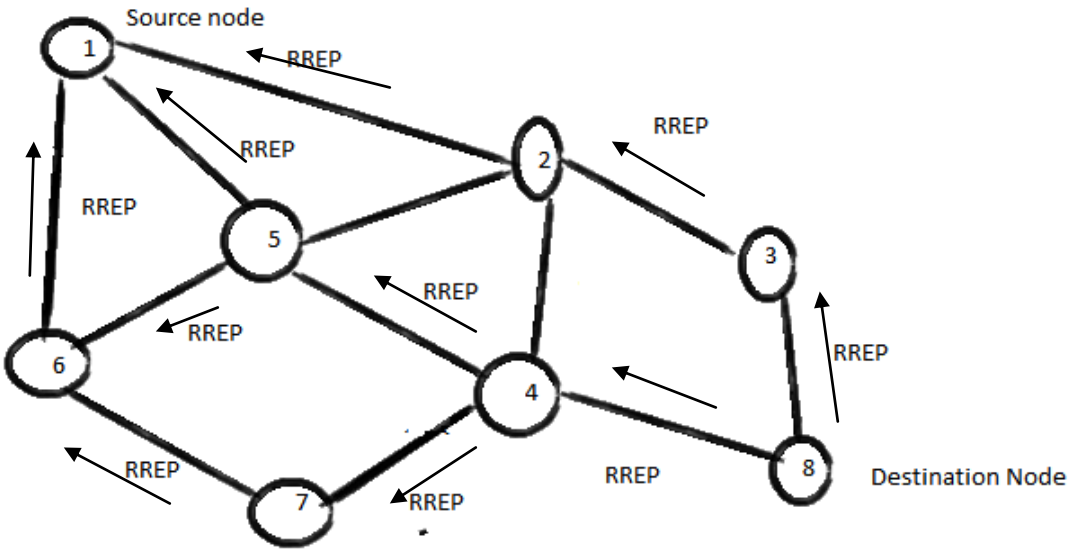

Figure 3.2: Route Reply from Destination Node to the Source Node

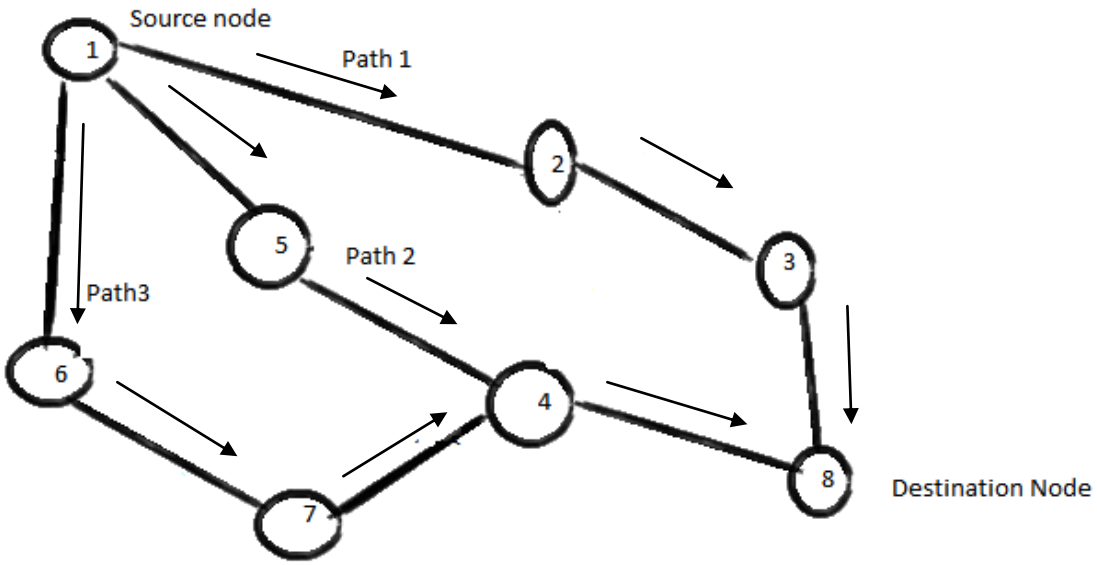

Figure 3.3: Different Path from Source Node to Destination

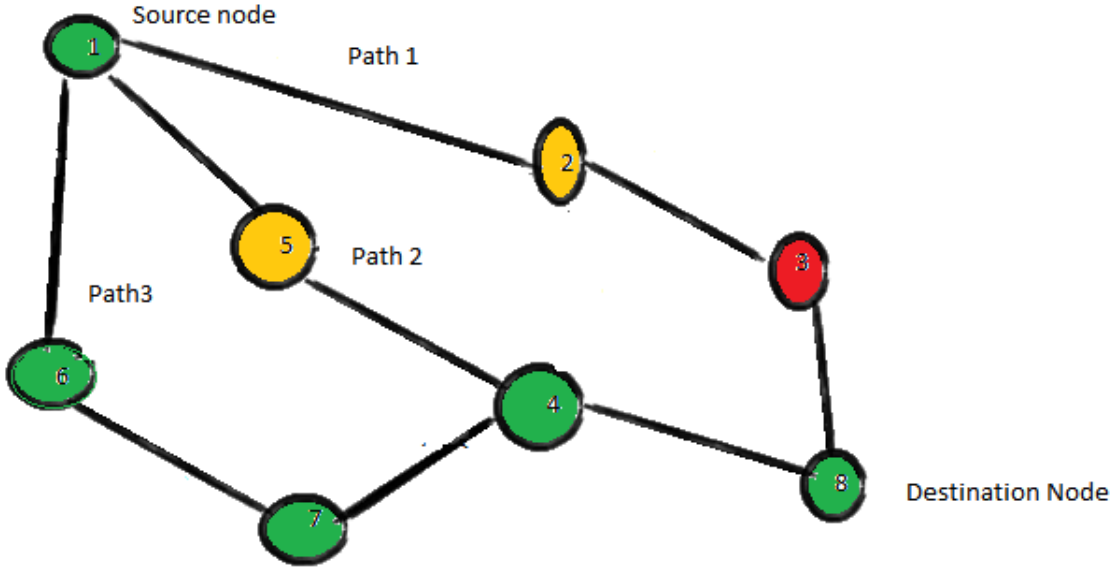

Figure 3.4: Residual Power on Two Different Path from Source Node to Destination

From the Figure 3.1 to 3.4 depicted the working principle of the proposed algorithm, route Request is sent from the source node to the destination node in the Figure 3.1. Destination node send the route reply to the source node which is shown in the Figure 3.2. From the Figure 3.3 and 3.4 shown the identification of different path and selecting the path which posses the sufficient energy for sending the packet which is done by using T-test procedure with the support of residual power availability in each node.

4. Simulation

The proposed routing algorithm is done in NS- 2 Simulator version 2.34, The area define for the simulation is 500X 500 mm and number of nodes arranges in simulation is 50, 100, 150 with the pause time of 5s , 15s, and 25 sec with the average speed of 10.10 m/s , 21.25 m/s and 12.02 m/s respectively. The detailed simulation setup for the MANET examination is given in table 1.

Parameter Used	Value set
Number of nodes	50, 100, 150
Number of source node	1
Simulation time defined	150s
Pause time set	5s , 15s, and 25 sec
Average speed	10.10 m/s , 21.25 m/s and 12.02 m/s
Traffic Type	Constant Bite Rate
Packet Size	512 bytes

Table 1: Simulation Setup for Examination

Estimating the Energy model for the MANET protocol performance the table 2 shows the defined parameter value with constant bit rate traffic. Omni antenna is selected to find out the routing path and packet transmission , all nodes defined ideal energy of 200 joules initially, and other needed power also estimated and assigned shown in the table 2.

Parameter Used	Value Set
Networking Interface for MANET	WirelessPhy
MAC type	802.11
Channel	Wireless
Propagation	TWORAY GROUND
Antenna set	Omni
Frequency	281.8 mW (250 m)
Initial Energy	200 Joule
Idle Power	1.0W
Receiving Power	1.1W
Transmission Power	1.65w
Transit Power	0.6w
Sleep Power	0.001w
Transition Time	0.005s

Table 2: Energy Model Parameter Details

5. Result

The proposed routing algorithm is compared with the Existing AODV protocol since the AODV is on demand protocol which support well for defining the best path between source to destination, for a comparison the proposed routing algorithm is named as Power Efficient AODV (PE-AODV).

For finding the route discovery , Source node send the Route Request to the all the nodes and receive the router reply. Route request and route reply is compared with Existing AODV Protocol where there is no major variation find also shown in the Figure 5.1

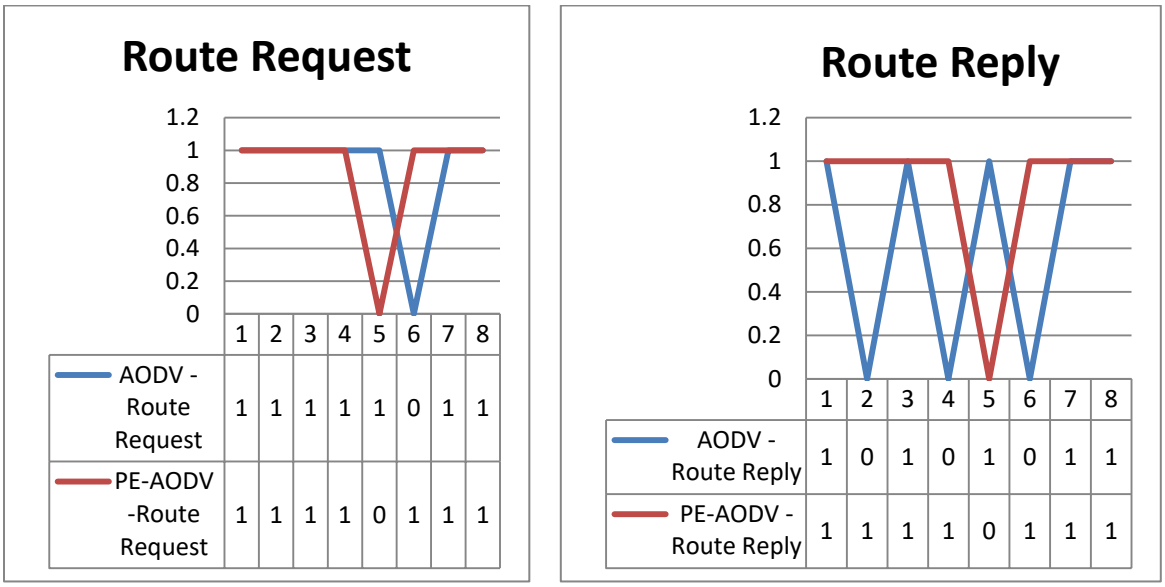

Figure 5.1: Route Request

Route Discovery

In this stage the proposed algorithm plays the vital role for selecting the power effcient node for the transmitting of packets.Each node residual power is estimated and selcte the node path which possess the sufficient energy by using the T Test Procedure . the comparison for taking the time for selcting the best path is compared with AODV protocol which shows minor delay in doing the path selction in PE-AODV protocol. This delay is managable and does not cause the any performacne of the MANET as shown in the Figure 5.2. finally the protocol perfomance parameter are compred depited in the figure 5.3.

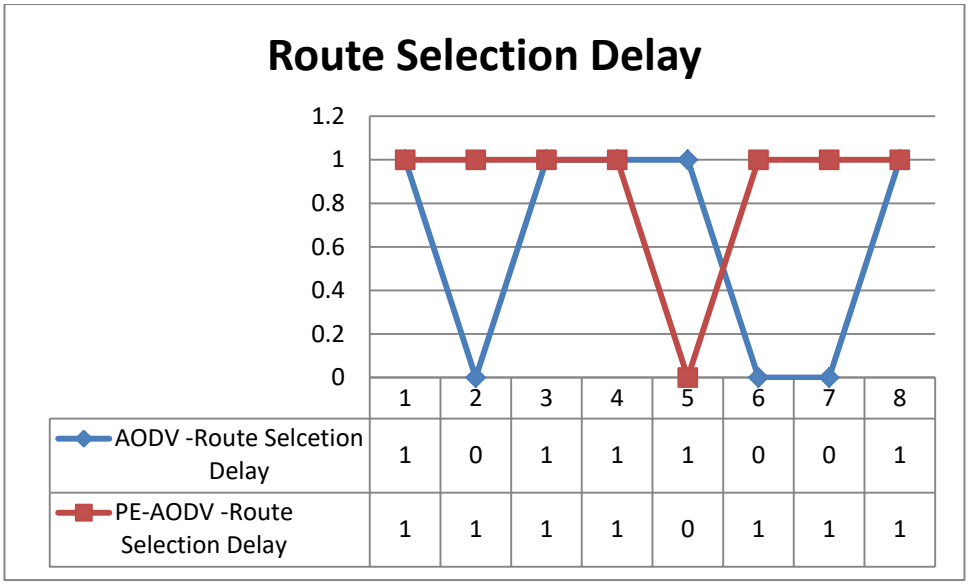

Figure 5.2: Route Selection Delay

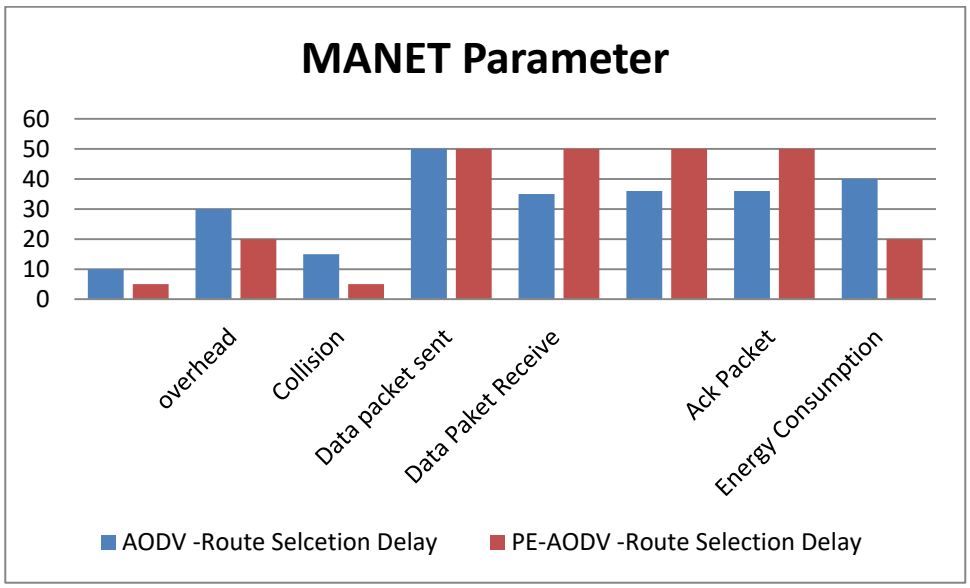

Figure 5.3: Parameter Comparison

6. Conclusion

The Routing Algorithm for Efficient packet transmission in MANET using T–Test Procedure is implemented with the support of Network simulator and the results were compared with the existing protocol as shown better comparing to the available protocols in MANET. The T-Test plays the major role in selecting the best path on the route. In feature this protocol could be included in the Making new protocol stack for the MANET network layer route discovery [10-15].

References

1. Quy, V. K., Ban, N. T., Tho, B. D., & Han, N. D. (2018). Performance Analysis of MANET Employing AODV, DSR, OLSR and DSDV Routing Protocols. In Proc. Conf. on Fundamental and Applied Information Technology Research (FAIR'8) (pp. 96-102).
2. XIONG, J., ZHAO, J., & XUAN, L. (2013). RESEARCH ON THE COMBINING OF COMPRESSED SENSING AND NETWORK CODING IN WIRELESS SENSOR NETWORK. Journal of Theoretical & Applied Information Technology, 47(3).
3. Olariu, S., Xu, Q., & Zomaya, A. Y. (2004, December). An energy-efficient self-organization protocol for wireless sensor networks. In Proceedings of the 2004 Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004. (pp. 55-60). IEEE.
4. Krishnamachari, L., Estrin, D., & Wicker, S. (2002, July). The impact of data aggregation in wireless sensor networks. In Proceedings 22nd international conference on distributed computing systems workshops (pp. 575-578). IEEE.
5. Nakamura, E. F., Ramos, H. S., Villas, L. A., de Oliveira, H. A., de Aquino, A. L., & Loureiro, A. A. (2009). A reactive role assignment for data routing in event-based wireless sensor networks. Computer Networks, 53(12), 1980-1996.
6. Kuo, W. K., & Chu, S. H. (2016). Energy efficiency optimization for mobile ad hoc networks. IEEE Access, 4, 928-940.
7. Prasad, R., & Shivashankar, D. (2020). Energy Secured Intrusion Detection System and Analysis of Attacks for Mobile Ad-Hoc Networks. J. Commun., 15(5), 406-414.
8. Shankar, S., Varaprasad, G., & Suresh, H. N. (2014). Importance of on-demand modified power aware dynamic source routing protocol in mobile ad-hoc networks. IET Microwaves, Antennas & Propagation, 8(7), 459-464.
9. Hu, Y. C., Perrig, A., & Johnson, D. B. (2002, September). Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of the 8th annual international conference on Mobile computing and networking (pp. 12-23).
10. Gupta, A. K., Sadawarti, H., & Verma, A. K. (2011). A review of routing protocols for mobile ad hoc networks. WSEAS Transactions on communications, 10(11), 331-340.
11. Ruta, M., Zacheo, G., Grieco, L. A., Di Noia, T., Boggia, G., Tinelli, E., ... & Di Sciascio, E. (2010). Semantic-based resource discovery, composition and substitution in IEEE 802.11 mobile ad hoc networks. Wireless Networks, 16, 1223-1251.
12. Tamilarasi, M., Chandramathi, S., & Palanivelu, T. G. (2001). Efficient energy management for mobile ad hoc networks. Ubiquitous Computing and Communication Journal, 3(5), 12-19.
13. Prabha, R., & Ramaraj, N. (2015). An improved multipath MANET routing using link estimation and swarm intelligence. EURASIP Journal on Wireless Communications and Networking, 2015, 1.
14. Thaseen, I. S., & Santhi, K. (2012). Performance analysis of FSR, LAR and ZRP routing protocols in MANET. International Journal of Computer Applications, 41(4).

15. Xu, G., Borcea, C., & Iftode, L. (2010). A policy enforcing mechanism for trusted ad hoc networks. IEEE Transactions on Dependable and Secure Computing, 8(3), 321-336.