International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I5P119

Volume 72 Issue 5, 185-193, May 2024

Original Article

Enhancing Cluster Node Forming Routing Protocol in Mobile Adhoc Network

S. Hemalatha[1], Shalini[2], P. Ezhilarasi[3], Thilagham K T[4]

[1]*Panimalar Engineering College, Chennai, Tamil Nadu, India.*
[2]*Department of Physics, R. M. D. Engineering College, RSM Nagar, Kavaraipettai, Thiruvallur, Tamil Nadu, India.*
[3]*Department of ECE, St. Joseph's College of Engineering, Tamilnadu, India.*
[4]*Department of Metallurgical Engineering, Government College of Engineering, Salem, Tamil Nadu, India.*

[1]*Corresponding Author : pithemalatha@gmail.com*

Received: 03 November 2023 Revised: 09 February 2024 Accepted: 11 April 2024 Published: 26 May 2024

Abstract *- Developing an Efficient power organization in wireless devices can be a challenging task, particularly in Mobile Networks. Many researchers are focusing on providing efficient power management with the support of modern algorithms and techniques. This article focuses on inventing a routing protocol with the support of clustering named Cluster Node Routing Protocol (CNRP), which executes on three stages of cluster node forming, cluster-based route prediction and packet forwarding. The proposed CNRP was implemented in the Network simulator and compared the results with existing cluster-based protocols of FLCH-AODV and SCCM-AODV with respect to the parameters of Cluster forming time, Cluster head accuracy, Connectivity analysis, Power analysis and Energy consumed. The proposed CNRP protocol performance is excellent in all the parameters computation, and the overall performance of the MANET becomes 85% to 89% even the many cluster head changes. This proposed protocol also supports Hidden and Exposed node issues and buffer overflow along with the energy optimization.*

Keywords *- MANET, Cluster node, Routing protocol, Network layer, Cluster Node Routing Protocol.*

1. Introduction

Routing the path between the sources to the destination node is an important role of the network layer in the MANET protocol stack [1]. The packet delivered in the wrong path makes the entire network collapse; also, the packet not forwarding to the next hope or floating many times by the individual nodes makes the routing protocol into to tedious task. Finally, the energy spent for the packet transmission will be wasted which affects the performance of the wireless communication. The usage of an internal battery is critical in ensuring consistent communication. When installing the MANET in an emergency situation, such as disaster management, if the battery fails, the entire communication may be lost. To extend battery life, effective power management strategies are essential. Several routing protocols have been proposed to address MANET challenges, including frequent topological changes caused by MANET characteristics, collisions caused by hidden and exposed terminal problems, and packet forwarding failures caused by internal threats or buffering capacity, all of which have an impact on MANET Quality of Service [2]. This post aimed to answer the MAENT's challenges. To handle battery power management, multiple MANET protocols [3] [4] are proposed, as well as several new types of routing protocols [4] [5]. Several research articles have recently been published to improve the performance of the AODV protocol, including AOMDV [6], SQR-AODV [7], AODV-BR [8], AODV-RD [9], AODV-BR [10], ATOMDV [11], and AMORLM [12], which assist battery life extension. MANET settings are also regarded as an important aspect in reducing battery power consumption, such as lowering MANET overhead to support better power management; many optimization strategies are based on this goal [18]. Cluster node selection with LEACH protocol improves life span with energy distribution [14], FFAOMDV incorporates a fitness function to reduce power consumption [15], and Artificial Intelligence neural network-based MANET optimizes MANET energy usage, supporting network efficiency and overall performance [16].GPS and long-range technology demonstrated long-term MANET utilization by Receiving Signal Strength Indicator-based (RSSI) from the receiver [17]. EMBOA [18] combines butterfly optimization techniques with a machine learning methodology that uses less energy to improve multipath routing. Nodes in a MANET PEO-AODV scheme [19] provided geographic position monitoring and an estimated hop count parameter to help overcome power issues. The routing protocol supports multiple power management tactics, as well as the most contemporary techniques of machine learning, artificial intelligence, and clustering, to maximize node battery power and lifetime. All these methods could not

support an efficient power-optimized routing strategy. One way to achieve energy optimization is eliminating the more number of packets forwarding by the intermediate nodes rather than using a cluster head based routing protocol for the packet route between the source to the destination node. This research article focuses on proposing a new Cluster Node forming Routing Protocol (CNRP) for optimizing the battery. The routing protocol first forms the cluster node, and the cluster node are taking responsible for the routing path decision and the packets forward to the destination. A separate cluster forwarding algorithm was established to forward the packet to the next cluster, and this research work eliminates all the internal node forwarding, which supports power optimization in MANET. This CNRP protocol indirectly supports the MANET challenges of Hidden and Exposed nodes, buffer overflow, and internal threats. The article is structured as follows: Section II summarizes the various existing routing-based power optimization methods used in MANET thus far; Section III proposes MANET's working principles; Section IV discusses the simulation setup used to implement the research work; and Section V concludes and includes feature work.

2. Research Work related to Routing protocols

This section explores further into the energy optimization routing technique, which has been a cornerstone of MANET technology since its creation. It goes into the classification parameter connected with this method, providing thorough information about its significance and ramifications in the context of MANETs. Abhilash and Shivaprakasha [1] have done a survey related to the MANET challenges with respect to the routing protocol, scheduling strategy, energy optimization, and Security factors. Finally authors explained the importance of secure routing protocol and various attacks in routing strategies in MANET. Tripathy et al. [20] authors proposed an adaptive routing protocol for Manet's communications; this protocol used the parameters and features to configure the route function dynamically. Simulation results show the best performance, but the usage of parameters like security, functional parameters, trust values, and geographical values are not easy to collect in the mobility nature of the nodes.

Arappali and Rajendran [21] authors proposed the OLSR protocol with Raspberry Pie inbuilt in the test bed; the simulation of OLSR performs better throughput, but the usage of BABEL for Vector directing is an additional task to the routing protocol. Panda & Pattanayak [22] authors enhanced the ant colony optimization algorithm (ACO) to provide a secured routing protocol in MANET to prove the QoS. An evolutionary technique-based algorithm was added to ACO. But, this work has been fundamental for the research related to ACO-based security routing. Quy et al. [23] authors made the analysis of the routing protocol for MANET-IoT with four major categories like: performance, energy, QoS and Security awareness. Finally conclude that proactive protocol work is good. This work could be the fundamental research data to the feature MANET-IoT based researchers. Maruthupandi et al [24] authors invented the DISNEY routing protocol using the SDN for MANET to provide the routing between the sources to destination nodes to overcome the congestion. The efficient route-manipulated table used for the routing support, and the simulation results perform well in all the performance factors. However, the usage of the table needs dynamic changes, which causes the routing protocol to delay on routing decision. Rajendra Prasad and Shivashankar [25] proposed the EEE Secure Routing protocol for adapting security policy in communication. The route-selected nodes have to provide the authentication and selection node energy level up to the threshold. Also, this routing protocol uses the shortest path for reliable communication route selection and the performance of the simulation was better. However, this threshold and authentication-based nodes are difficult to determine. If any condition is not met, the nodes could not be part of the communication network.

Mohammad et al. [26] anticipated the TBSMR for MANET enhancement. This routing protocol uses different factors like congestion, loss, QoS and malicious node prediction for making the route between the nodes. The simulation shows superior performance compared with other methods, but the multiple factor usage for route prediction is not possible practically when the nodes are huge. Anubhuti Roda MOHINDRA and Charu GANDHI [27] proposed the SCCM routing protocol, which has secured the transmission of packets using encryption and signature generation and decryption process. The packet is converted to an unknown packet using the ECC encryption method, which supports to provide the secure transmission of data packets between the nodes. However, the work of encryption, decryption, and ECC are overhead to the routing protocol, which makes some delay in packet computation.

Hwanseok Yang [28] author proposed a technique evaluation method of nodes using cluster and key exchange without the usage of Certificate Authority. This method assured the quality of packets as well as packet maintenance. The simulation and performance of this method are superior to other methods with respect to the parameters of PDR, delay, control packets, throughput, and path length. However, the forming of the clustering structure is not feasible in MANET. Uppalapati Srilakshmi et al. [13] authors propose that the fuzzy clustering algorithm is activated in the Cluster Heads (CHs) for trust-based protection with energy optimization. CH is engaged for the secure route selection based on the latency, node connection, and throughput, and the results are compared with the EA-DRP & EE-OHRA methods proposed methods produced energy was 0.10 m joules, latency was 0.0035 m sec, throughput was 0.70 bps, and an 83 percent detection rate. The limitation of this method is that route selection was delayed due to the cluster head forming with fuzzy logic. Routing protocols in MANET have proven successful in a

variety of applications, including routing, mobility, clustering, and hybrid techniques, as well as transmission range optimization. However, some procedures have produced dismal outcomes. Further study is required to enhance routing for power efficiency in MANETs. This paper presents a cluster-based routing protocol that aims to improve route discovery and packet forwarding to target nodes while reducing the requirement for intermediary nodes to pass packets.

3. Research Methodology

The research goal of this article is to form the cluster node that supports for MANET routing strategy to optimize the battery life of the individual nodes. The research methodology compromises the following subsection: first, forming the cluster node or Cluster head; second, the routing path selection from the sender to the receiver node; and finally, the packet forwarding.

3.1. Cluster Node or Cluster Head

In the MANET nodes cluster, node selection is based on the location of the other nodes. Nodes that are in the same region, and in the system represented in Figure 1, a single node is designated as the cluster node due to its greater energy reserves, which allow it to transfer packets across the network efficiently.

The MANET graph, denoted as MG = (M, N), is constructed as follows:

M represents the set of MANET nodes, where M = {m1, m2, ..., mm, mn}. Here, 'm' denotes the total number of nodes, ranging from 1 to n.

N represents the set of edges connecting the nodes, where N = {l1, l2, ..., lv}.

In this graph:

S represents the source node.

T represents the target node.

H represents the cluster head, which is selected based on the residual energy node, node lifetime, and connectivity with other nodes. The system model is initially established to define internal node parameters. Figure 2 illustrates the entire architecture, depicting the process of cluster formation and communication among nodes.

Overall, the MANET graph encapsulates the nodes, edges, and key components such as source, target, and cluster head, providing a visual representation of the network structure and communication flow within the MANET environment.

Several criteria influence the cluster heads chosen for each location, including battery power, mobility, link lifetime, and node mobility. The cluster node will be the one with the maximum node life length, connectivity, and battery power values, as well as the lowest node mobility and distance values.

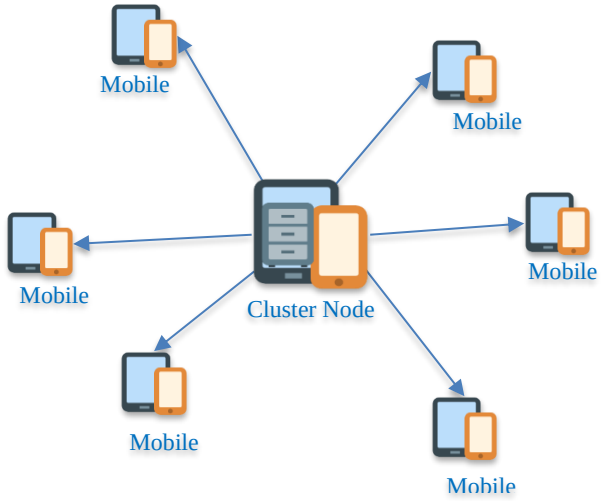


Fig. 1 Cluster node forming

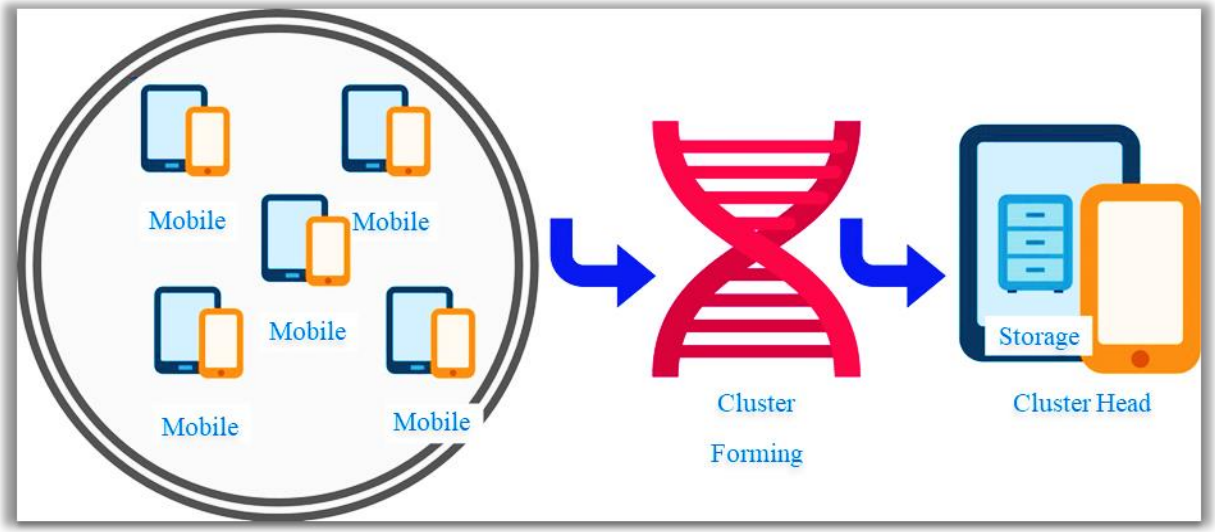


Fig. 2 Cluster node selection

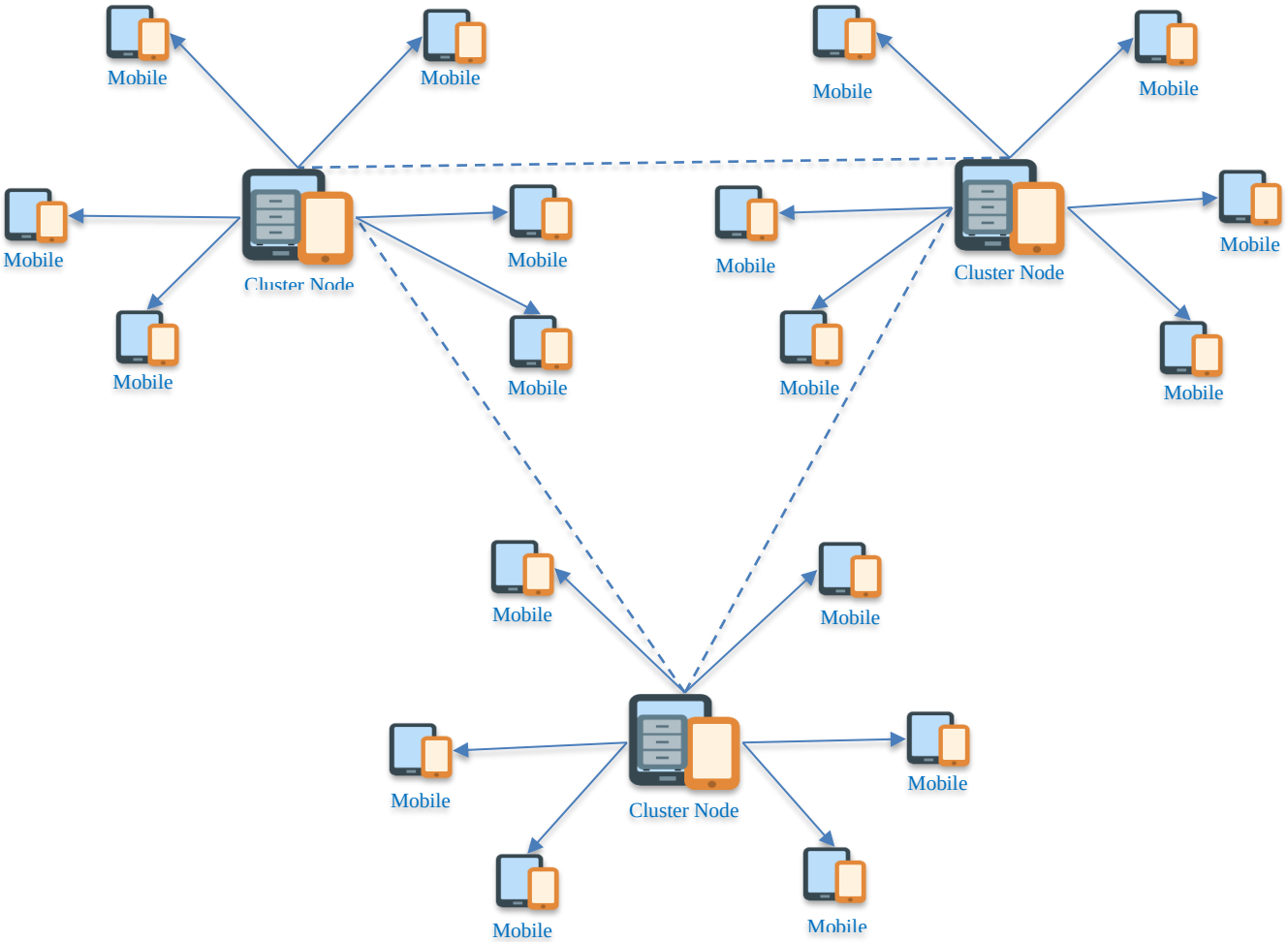


Fig. 3 Clustering groups

3.2 Cluster Node based Routing Protocol

Cluster Node-based routing protocol works as following stages depicted in Algorithm I, First the formation of the cluster Nodes in the MANET. In the second stage, the source initiates the route path to the respective cluster with the details of the destination. Next step, the Cluster Node sends the RREQ to the other clusters and makes a path. Finally, the packets are transmitted from the source to the destination by deciding the route path Cluster nodes.

Algorithm I Working of Cluster Node-based Routing Protocol

Steps for Cluster Head forming and route process

1. Begin by totaling the number of nodes in each MANET region. Define M as the set of regions within the MANET, denoted by {R1, R2, R3,..., Rn}. Each region Ri comprises N nodes, one of which is designated as the cluster head.
2. For each Region Ri, Do follow

for (i=1; i≤ n; i++)

{

//All nodes in the MANET region are evaluated on a variety of criteria, including lifetime, mobility, distance, power, and connectivity. The criteria used to designate a cluster node are:

- The cluster node must have the highest possible node longevity, connection, and battery power.
- Conversely, the cluster node should have the lowest values for node mobility and distance.
- This selection procedure guarantees that the chosen cluster node maximizes its potential for durability, connection, and power efficiency within the MANET region.

}

3. Sender Cluster node sends the REEQ to all the clusters in the MANET
4. Destination cluster node sends the RREP to the sender cluster
5. Packet Transmission from the sender to the destination node via selected cluster nodes.
6. If the cluster node residual power is less, go to step 1; otherwise process continues.

The selection of cluster heads is based on information gathered from MANET nodes, which takes into account criteria such as device mobility, lifetime, distance, power, and

connectivity. Algorithm I governs this selection process. As shown in Figure 3, the output consists of a group of nodes and the specified cluster head, which serves as the clustering head's processing output.

3.3. Route path Selection and Forwarding Packets

After selecting the cluster node amongst the MANET nodes, the transmission route path is selected. To determine the most reliable path between the source node and the destination node, the source node sends a message request to the appropriate cluster node, which then sends the route request to all other cluster nodes. In this research work, the intermediate node could not be involved in any kind of forwarding the messages, as shown in Figure 4. S node sends the request message to CN1, then CN1 forwards the RREQ to CN2, CN3, then CN3 forwards to CN4. The destination nodes are under CN4 so the CN4 sends the response via RREP to CN3, which in turn forward to the CN1. So, the final path between the S to D is CN1 →CN3→CN4→D. Once the reliable path is selected, the S nodes start sending the packet to CN1, which intern forward to the next CN to reach the destination. Other intermediate nodes could not be involved in the transmission and forwarding process. So that the power on the intermediate nodes will be optimized also there is no collision on the nodes.

4. Simulation Comparison

4.1. Parameter for Simulation

The suggested work is implemented in Network Simulator3 using a high-end system combination of an Intel core processor, 8 GB capacity of RAM, and Windows 11 operating system. Simulation Setup is used to create the simulation results. The MANET simulation was carried out on a 1000 * 1000 square meter area with a wireless physical interface and an omni antenna. Several configurations were examined, ranging from 50 to 200 nodes with a link count of 20-50. The source transmission type used was constant bit rate transmission, with each packet size set to 512 bytes and a buffer size of 40 packets.

The MAC layer employed was 802.11b, and a random simulation model was chosen. Propagation was modeled using a two-way ground approach, with nodes capable of achieving top speeds of 25 m/s and halting for 15 seconds. During simulation intervals, two packets were delivered, and the simulation time was set to 50 and 100 seconds. The initial node energy was set to 240 joules, with each node transmitting 0.9 joules and receiving 0.4 joules. Sleep power was set to 0.002 joules, with a change over duration of 0.009 seconds.

4.2. Comparative Evaluation

The proposed cluster node-based routing protocol was implemented in AODV protocol [9] and named CNRP-AODV, with the simulated values analyzed with the alive SCCM -AODV [27] FLCH-AODV [13] algorithm for predicting the comparative analysis.

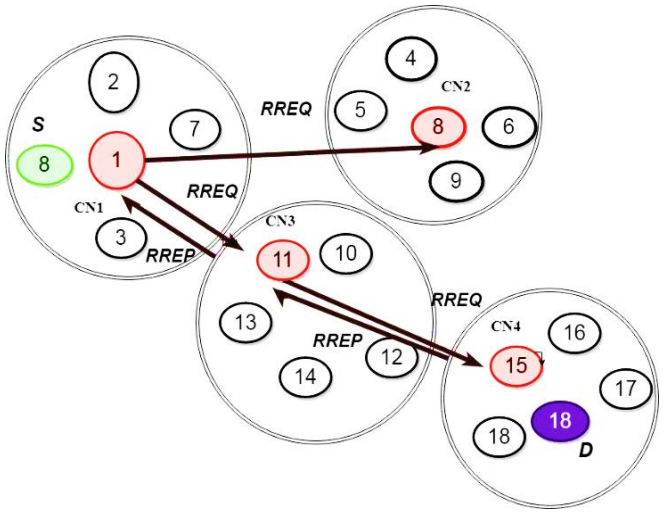


Fig. 4 Route path selection

The performance factors considered in the comparative analysis are connectivity analysis for making the route, cluster head accuracy and cluster forming time, power analysis, and energy consumed. Each performance parameter is simulated by methodically altering the total number of nodes, which might range from 50 to 200.

4.2.1. Cluster Forming Time

The working principle of the proposed Cluster Node Routing Protocol starts with finding the cluster node forming. From the simulation first comparison was made to cluster head forming time compared with the other existing cluster head-related routing protocol research Fuzzy logic cluster head AODV (FLCH-AODV)[13] and Secure Cryptography based Clustering Mechanism (SCCM- AODV) [27] with nodes count starting from 50,100,150 and 200 nodes.In all the cases, the proposed CNRP-AODV node forming times 50,60,72 and 85 ms, and FLCH-AODV cluster nodes take 80,90,95 and 98 ms and SCCM-AODV cluster forming times 82,92,97 and 100 ms, which take more time to form clusters comparing with proposed CNRP-AODV protocol as shown from the Figure 5.

Connectivity Analysis

A second connectivity comparison was made with respect to the connectivity analysis, which makes use of routing path selection between the Source nodes to the Destination node. From the simulation connectivity analysis compared with the other existing cluster head-related routing protocol research Fuzzy logic cluster head AODV (FLCH-AODV) [13] and Secure Cryptography based Clustering Mechanism (SCCM-AODV) [27] with nodes count starting from 50,100,150 and 200 nodes. In all the cases, the proposed CNRP-AODV node route connectivity times are 8, 16, 24, and 32 ms and FLCH-AODV connectivity time takes 12, 26, 40, 50 and SCCM-AODV protocol connectivity time 14, 28, 42, and 52 ms, which take more time for analysis the route paths connectivity comparing with proposed CNRP-AODV protocol as shown from the Figure 6.

Cluster Head Accuracy

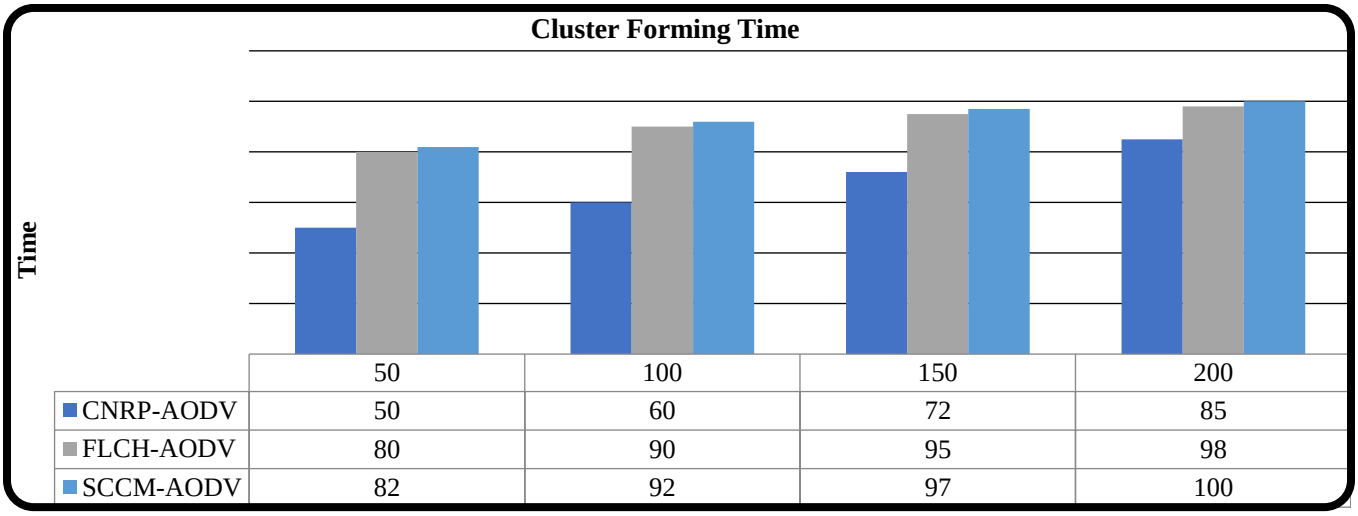
The third cluster head comparison was made with respect to the cluster head accuracy, which makes use of packet transmission on the specified routing path selection clusters in among the Sender node to the Receiver node. From the simulation Cluster head accuracy compared with the other methods of cluster head related routing protocol research Fuzzy logic cluster head AODV (FLCH-AODV) [13] and Secure Cryptography based Clustering Mechanism (SCCM-AODV) [27] with nodes count starting from 50,100,150 and 200 nodes.

All the cases the proposed CNRP-AODV node Cluster head accuracy are 90,93,97 and 103% , and FLCH-AODV accuracy of cluster head 75,80,87,90 % and SCCM-AODV protocol accuracy of cluster head 85,88,92 and 98% which provide less percent of accuracy compared with proposed CNRP-AODV protocol as shown from the Figure 7.

Power Analysis

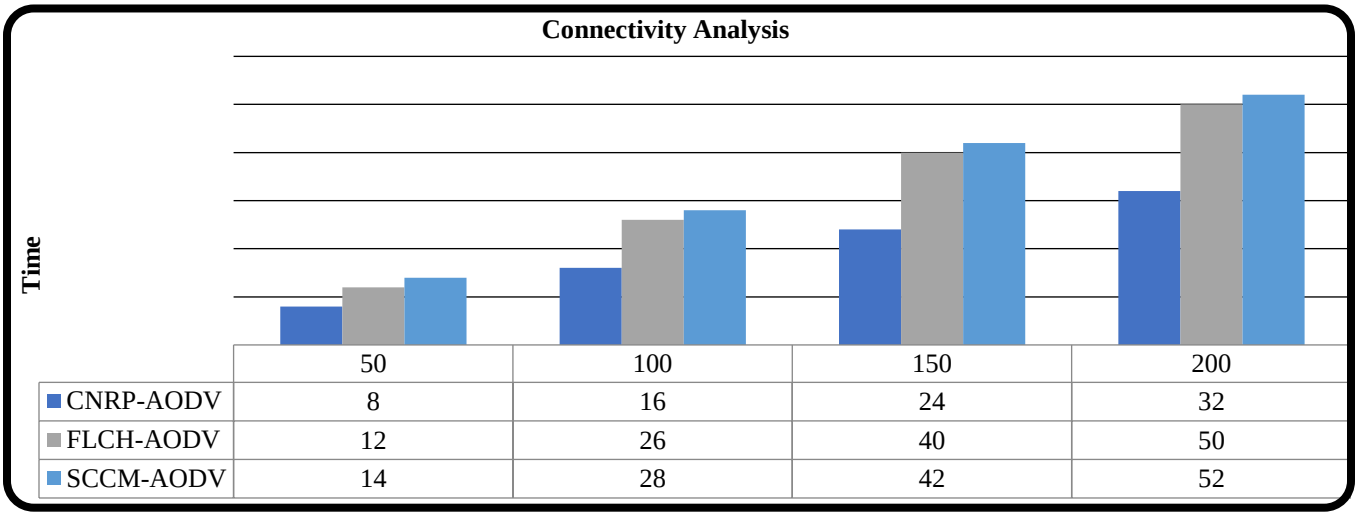
Next power comparison was made with respect to the power consumed by the cluster head to transmit the packet also the next cluster node selection based on the current cluster node power scenario. From the simulation power analysis compared with the other existing cluster head related routing protocol research Fuzzy logic cluster head AODV (FLCH-AODV) [13] and Secure Cryptography based Clustering Mechanism (SCCM- AODV) [27] with nodes count starting from 50,100,150 and 200 nodes.

All the cases the proposed CNRP-AODV node power taken 19.02,19.01,19.06,19.08 J in a constant power consuming even the nodes increased , where the FLCH-AODV power analysis 21.03,22.05,25.03,26.07J which get more power varying in ranges of cluster and SCCM-AODV protocol power analysis 21.53,22.55,25.53 and 26.57J which taken more power compared with proposed CNRP-AODV protocol as shown from the Figure 8.



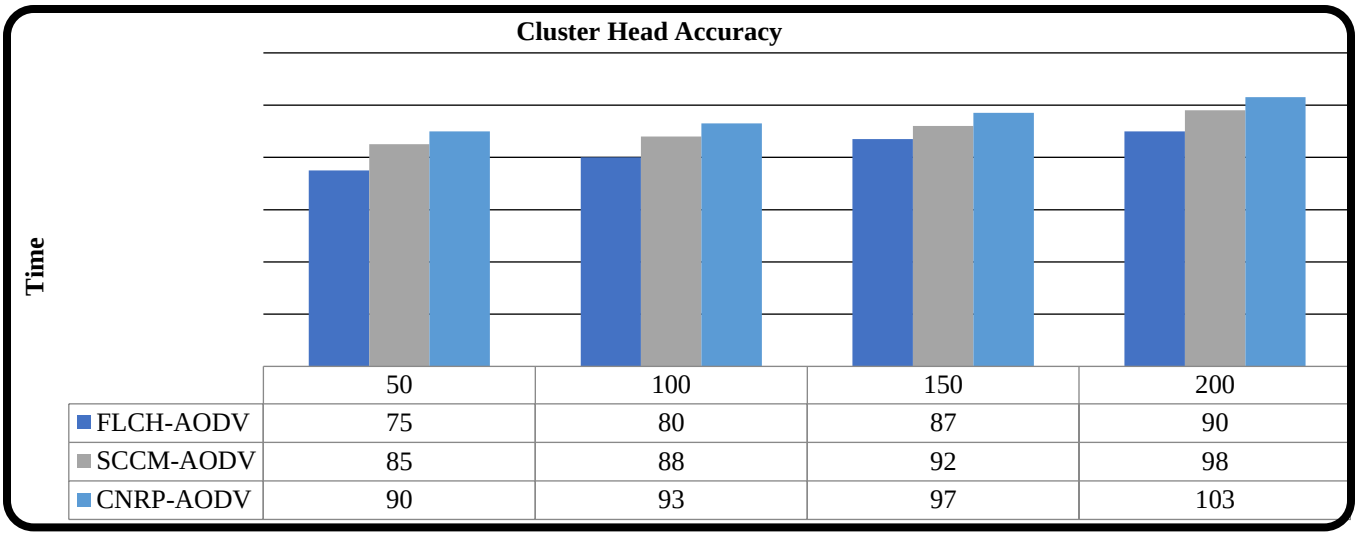
	50	100	150	200
CNRP-AODV	50	60	72	85
FLCH-AODV	80	90	95	98
SCCM-AODV	82	92	97	100

Fig. 5 Cluster Node forming time



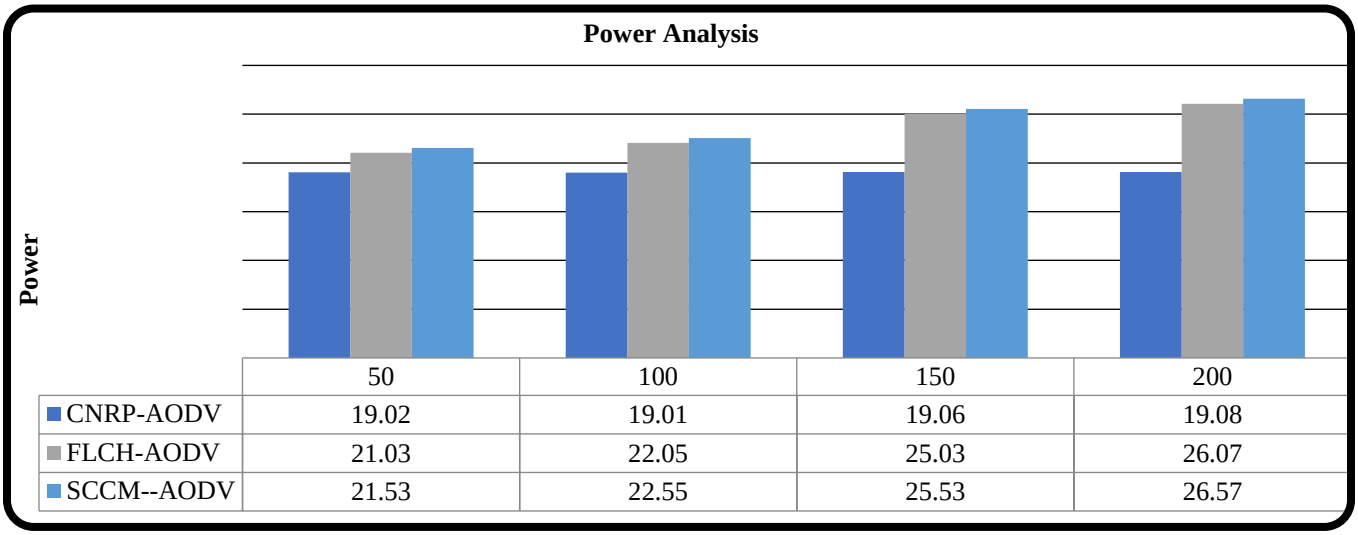
	50	100	150	200
CNRP-AODV	8	16	24	32
FLCH-AODV	12	26	40	50
SCCM-AODV	14	28	42	52

Fig. 6 Connectivity analysis



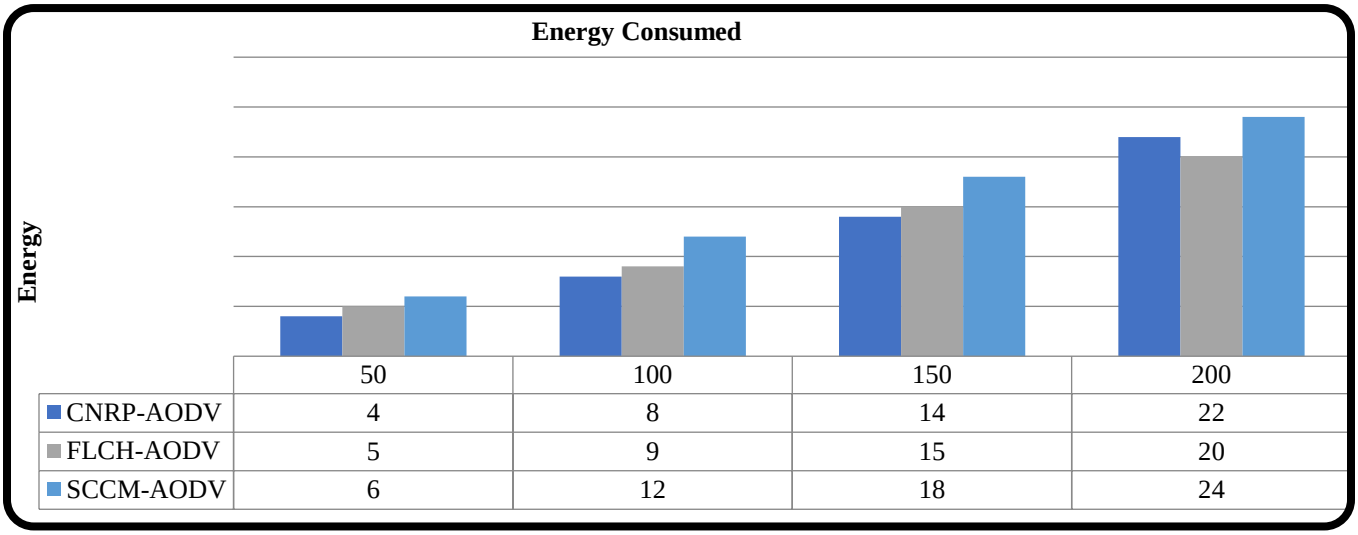
	50	100	150	200
FLCH-AODV	75	80	87	90
SCCM-AODV	85	88	92	98
CNRP-AODV	90	93	97	103

Fig. 7 Accuracy of cluster head



	50	100	150	200
CNRP-AODV	19.02	19.01	19.06	19.08
FLCH-AODV	21.03	22.05	25.03	26.07
SCCM--AODV	21.53	22.55	25.53	26.57

Fig. 8 Power analysis



	50	100	150	200
CNRP-AODV	4	8	14	22
FLCH-AODV	5	9	15	20
SCCM-AODV	6	12	18	24

Fig. 9 Energy consumed

Energy Consumed

Finally, the energy consumption comparison was made with respect to the power consumed by the cluster head to transmit the packet also the next cluster node selection based on the current cluster node power scenario. From the simulation energy compared with the other existing cluster head-related routing protocol research Fuzzy logic cluster head AODV (FLCH-AODV) [13] and Secure Cryptography based Clustering Mechanism (SCCM- AODV) [27] with nodes count starting from 50,100,150 and 200 nodes. In all the cases, the proposed CNRP-AODV node power taken 4,8,14,22 J in a constant power consuming even the nodes increased, where the FLCH-AODV power consumed 5,9,15 and 20 J which get more power varying in ranges of cluster and SCCM-AODV protocol power analysis 6,12,18,24 J which taken more energy compared with proposed CNRP-AODV protocol as shown from the Figure 9.

5. Conclusion and Future work

This article focuses the power optimization with the support of Cluster node-based routing protocol, which aids in supporting the packet transmission between the nodes. CNRP has three stages of working: cluster node selection, route path selection with cluster head, and packet transmission. The proposed CNRP was implemented in the Network simulator and compared the results with existing cluster-based protocols of FLCH-AODV and SCCM-AODV with respect to the parameters of Cluster forming time, Cluster head accuracy, Connectivity analysis, Power analysis and Energy consumed. The proposed CNRP protocol performance is excellent in all the parameters computation, and the overall performance of the MANET becomes 85% to 89% even the many cluster head changes; this proposed protocol also supports Hidden and Exposed node issues and buffer overflow along with the energy optimization.

References

[1] K.J. Abhilash, and K.S. Shivaprakasha, "Secure Routing Protocol for MANET: A Survey," *Advances in Communication, Signal Processing, VLSI, and Embedded Systems*, vol. 614, pp. 263-277, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Rajvi Trivedi, and Pimal Khanpara, "*Robust and Secure Routing Protocols for MANET-Based Internet of Things Systems—A Survey*," Emergence of Cyber Physical System and IoT in Smart Automation and Robotics, Advances in Science, Technology & Innovation. Springer, Cham, pp. 175-188, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Abdul Majid Soomro et al., "Comparative Review of Routing Protocols in MANET for Future Research in Disaster Management," *Journal of Communications*, vol. 17, no. 9, pp. 734-744, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] D. Hemanand et al., "Analysis of Power Optimization and Enhanced Routing Protocols for Wireless Sensor Networks," *Measurement: Sensors*, vol. 25, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Venkatesan Cherappa et al., "Energy-Efficient Clustering and Routing Using ASFO and a Cross-Layer-Based Expedient Routing Protocol for Wireless Sensor Networks," *Sensors*, vol. 23, no. 5, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] M.K. Marina, and S.R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," *Proceedings Ninth International Conference on Network Protocols*, Riverside, CA, USA, pp. 14-23, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[7] Shahram Jamali, Bita Safarzadeh, and Hamed Alimohammadi, "SQR-AODV: A Stable QoS-Aware Reliable on-Demand Distance Vector Routing Protocol for Mobile Ad Hoc Networks," *Scientific Research and Essays*, vol. 6, no. 14, pp. 3015-3026, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[8] S.J. Lee, and M. Gerla, "AODV-BR: Backup Routing in ad Hoc Networks," *2000 IEEE Wireless Communications and Networking Conference*, Chicago, IL, USA, vol. 3, pp. 1311-1316, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[9] Jian Liu, and Fang-min Li, "An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad Hoc Networks," *2009 Fifth International Conference on Information Assurance and Security*, Xi'an, China, vol. 1, pp. 507-510, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[10] Hui Xia et al., "Impact of Trust Model on on-Demand Multi-Path Routing in Mobile Ad Hoc Networks," *Computer Communications*, vol. 36, no. 9, pp. 1078-1093, 2013.[CrossRef] [Google Scholar] [Publisher Link]

[11] Omar Smail et al., "A Multipath Energy-Conserving Routing Protocol for Wireless Ad Hoc Networks Lifetime Improvement," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, pp. 1-12, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[12] S.M. Benakappa, and M. Kiran, "Energy Aware Stable Multipath Disjoint Routing Based on Accumulated Trust Value in MANETs," *International Journal of Computer Network and Information Security*, vol. 14, no. 4, pp. 14-26, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Uppalapati Srilakshmi et al., "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," *IEEE Access*, vol. 10, pp. 14260-14269, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] K. Rajendra et al., "Grey Wolf Optimizer and Cuckoo Search Algorithm for Electric Power System State Estimation with Load Uncertainty and False Data," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 2s, pp. 59-67, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Aqeel Taha et al., "Energy-Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," *IEEE Access*, vol. 5, pp. 10369-10381, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jayant Y. Hande, and Ritesh Sadiwala, "Optimization of Energy Consumption and Routing in MANET Using Artificial Neural Network," *Journal of Integrated Science and Technology*, vol. 12, no. 1, pp. 1-8, 2024. [Google Scholar] [Publisher Link]

[17] Guruprasath Rengarajan, Nagarajan Ramalingam, and Kannadhasan Suriyan, "Performance Enhancement of Mobile Ad Hoc Network Life Time Using Energy Efficient Techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 5, pp. 2870-2877, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] T. Saravanan, and S. Saravanakumar, "Energy Efficient Optimization Algorithms for MANET," *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*, Noida, India, pp. 572-579, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Muhannad Tahboush, Mohammad Adawy, and Osama Aloqaily, "PEO-AODV: Preserving Energy Optimization Based on Modified AODV Routing Protocol for MANET," *International Journal of Advances in Soft Computing and its Application*, vol. 15, no. 2, pp. 263-277, 2023. [Google Scholar] [Publisher Link]

[20] Bata Krishna Tripathy et al., "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1339-1370, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Nedumaran Arappali, and Ganesh Babu Rajendran, "MANET Security Routing Protocols Based on a Machine Learning Technique (Raspberry PIs)," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 6317-6331, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Niranjan Panda, and Binod Kumar Pattanayak, "ACO-Based Secure Routing Protocols in MANETs," *New Paradigm in Decision Science and Management, Proceedings of ICDSM*, pp. 195-206, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Vu Khanh Quy et al., "Routing Algorithms for MANET-IoT Networks: A Comprehensive Survey," *Wireless Personal Communications*, vol. 125, no. 4, pp. 3501-3525, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] J. Maruthupandi et al., "Route Manipulation Aware Software-Defined Networks for Effective Routing in SDN Controlled MANET by Disney Routing Protocol," *Microprocessors and Microsystems*, vol. 80, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] P. Rajendra Prasad, and Shivashankar, "Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad-Hoc Network," *Global Transitions Proceedings*, vol. 3, no. 2, pp. 412-423, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mohammad Sirajuddin et al., "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network," *Security and Communication Networks*, vol. 2021, pp. 1-9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Anubhuti Roda Mohindra, and Charu Gandhi, "A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET," *Walailak Journal of Science and Technology*, vol. 18, no. 6, pp. 1-8, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Hwanseok Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET," *Mobile Information Systems*, vol. 2020, pp. 1-17, 2020. [CrossRef] [Google Scholar] [Publisher Link]