International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Fuzzy C-Means Clustering Based Energy-Efficient Protected Optimal Path-Routing Protocol for MANET

V. Purushothaman[1], Jeevitha Sivasamy[2], S. Karthik[3], Abhishek Choubey[4] ,S. P. Prakash[5], T. Blesslin Sheeba[6]

Submitted: 16/07/2023 **Revised**: 08/09/2023 **Accepted**: 25/09/2023

Abstract*:* A Mobile Ad Hoc Network (MANET) protocol must be appropriately configured to maximize data flow. Use the appropriate routing protocol and the default settings for the routing protocol parameters to resolve this issue. Manet is a dynamic communication network worldwide, and Routing is the risk task for the communication network; routing optimization was the biggest problem in Manet. The existing energy-efficient algorithm has issues with increasing the maximum throughput network life, network energy consumption, minimum routing performance, less security, and minimum packet delivery ratio on Manet. The proposed Fuzzy C-Means Clustering-based Energy-Efficient Protected Optimal Path-Routing Protocol system can increase routing performance, consume less energy, and maximize network lifetime with less error rate, less time delay performances, and security using the TACIT technique has increased the Encryption and Decryption level key performances. The TACIT approach has based on advanced AES based encryption and the random key generation, HMAC algorithm using key authentication or verification for the proposed system. The system routing performance is the performance of Adov 50 nodes performance is 69%, OLSR 50 nodes performance is 72%, OLSR 50 nodes performance is 72%, BTSNADS 50 nodes performance is 82%, and DSR 50 nodes performance is 92%, and proposed 50 nodes performance is 97%. Finally, the proposed system of Fuzzy C-Means clustering-based Energy-Efficient Protected Optimal Path-Routing Protocol has good performance routing optimization.

Keywords: *TACIT ((E-TACIT), Fuzzy C-Means Clustering based Energy-Efficient (FCCEE) Protected Optimal Path-Routing Protocol, HMAC (Hash-based Message Authentication Code)*

1. Introduction

Mobile ad hoc networks are quite common in research because of their transient nature and efficiency during catastrophe management when infrastructure support is not available. Nodes may need to make several network hops in order to share data across the network since wireless network interfaces have a restricted transmission range. Each mobile node in such a network serves as a router, transmitting packets to other mobile nodes that are not in close proximity. Wired vector or link-state protocols, which were developed for wired networks, are insufficient in this aspect because they frequently not only assume fixed topologies but also have substantial overhead costs. This prompted the development of numerous routing algorithms for ad hoc networks. We discuss MANET-compatible routing protocols and their study of several performance metrics, such as throughput, control overhead, power, and packet delivery speed, delay, and throughput.

One of the varieties of data communication networks that uses wireless links to link devices for information exchange is a wireless network. The expensive process of laying cables for data communication between devices in multiple places is avoided by wireless networking technology. Wireless networks and Wi-Fi local area networks are two types of wireless networks. Wireless networks can be divided into two categories: those with infrastructure and those without. In the first, access points or routers are used to set up and manage data connections. Mobile networks are an illustration of this kind of network. Ad hoc networks are essentially the name for this last category. The stations in such a network can communicate with one another and are self-generated in the form of numerous hops without established infrastructure. Such a flexible infrastructure is beneficial in less networked areas.

The continuous and capricious changes in the network topology and geography brought about by the very unique nature of portable, specially appointed networks make

[1] *Assistant Professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, 600062, India, Email: purushothamanv@veltech.edu.in*

[2] *Assistant Professor, Department of Computer applications, B.S Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai-600 048.Tamil Nadu.Email: jeevitha@crescent.education*

[3] *Assistant Professor, Department of Biomedical Engineering, P.S.R.Engineering College, Sivakasi, Tamil Nadu 626140, India.E-mail: karthik.s1410@gmail.com*

[4] *Associate Professor, Department of Electronics and Communication Engineering, Sreenidhi Institute of Science & Technology, Hyderabad-501301, Telangana, India. Email***:** *abhishek@sreenidhi.edu.in*

[5] *Associate Professor, Department of ECE, Bannari Amman Institue of Technology, Sathyamangalam-638401*

[6] *Prfessor, Department of Electronics and Communication Engineering, R.M.K. Engineering College, Kavaraipettai, Tamil Nadu 601206, India. Email: tbs.ece@rmkec.ac.in*

steering between versatile hubs really testing and complex. The hardships and issues make directing an extremely dynamic review field inside the MANET domain, alongside the urgent job that the steering convention plays in laying out correspondence between portable nodes.

Route request packets are better confirmed utilizing a gathering mark without uncovering the characters of the node and to forestall potential execution assaults [1]. The objective of Onion directing is to prevent mediator nodes from finding the genuine objective utilizing the scrambled key and the mysterious way confirmation message. The consequences of the reenactments show that the proposed AASR technique is compelling and beats the ongoing conventions. The capacities of the AODV convention are reached out by BP-AODV utilizing fluffy designs highlights. The trial discoveries show that the BP-AODV convention is safer than the SAODV convention and can effectively forestall a dark opening assault started during the steering system by a rebel hub or maverick nodes. Discoveries demonstrate the way that BB-AOTV can successfully forestall dark opening assaults all through the sending system [2].

The topology-changing adaptive on-demand multipath distance vector (DA-AOMTV) directing convention is proposed in light of the fact that it can uphold QoS while considering fast node portability. This convention utilizes a steady course determination calculation that not just considers the assets of the hubs (leftover energy, accessible transfer speed, and line length) yet in addition the solidness likelihood of the connection between the nodes. Reproduction results demonstrate the way that the recommended approach can beat existing bleeding edge directing conventions as far as steering execution. Specifically, in both the dark opening attack and dim opening assault situations, the proposed strategy essentially outflanked different techniques concerning bundle misfortune, normal start to finish postponement, and energy productivity [4].

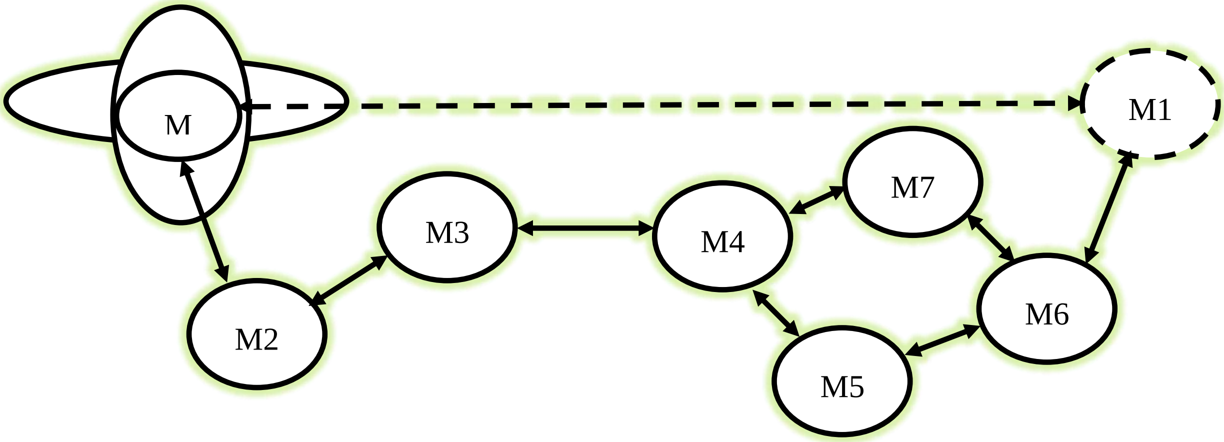

Fig.1 MANET | Mobile Adhoc Network formation

Figure.1 discuss about Based on the relative positions of other nodes, connection can alter when nodes move. To update outdated topological knowledge, a modification to the locally understood network topology must be propagated to neighboring nodes. Other network nodes must utilize this new route to send packets to M2 as M2 in the illustration switches its endpoint from M3 to M4. If M1 is inside MS3's radio range, then M3 is also within M1's radio range. Links for communication are symmetrical. Because of variations in the transmission power levels and geography, this assumption is not always true. Asymmetric network rooting is a challenging task. Asymmetric linkages can sometimes be avoided because it is challenging to return the same way. The performance issue is just one of MANET's many difficulties.

2. Related Work

Using Network Simulator 3 3, the viability of the recommended components was evaluated as far as standardized steering load, normal start to finish postponement, and parcel conveyance speed. The aftereffects of the trials show that the proposed calculation performs better compared to notable strategies like the directing convention. TSR for dynamic source, zone-and fragment based DSR, and trustworthy DSR [5]. The two most frequently involved conventions in this field, Specially Appointed On-Demand Multipath Routing with Lifetime Maximization (AOMR-LM) and AOMDV and AOMDV, are utilized to analyze the presentation. Power use, execution, bundle conveyance rate, start to finish delay, network lifetime, and execution measurements of steering above rate, node speed, parcel size, and recreation time were utilized to assess the correlation. The discoveries unequivocally show that in most network execution measurements and boundaries, the recommended FF-AOMDV beat AOMDV and AOMR-LM[6].

MANETs are self-coordinating hubs that cooperate to make a powerful organization plan and make associations in a versatile organization. Information should travel through various middle hubs in a MANET to arrive at its last objective. To keep antagonistic node from getting to this information, security should be carried out. In the writing, various ways have been proposed to get directing; these arrangements center around different security aspects. Rather than the underlying single course steering, the remote networks multipath directing is by and large utilized to support adaptation to non-critical failure [7].

In this exploration, exact shut structure conditions for the E2E lining deferral of a multicast routing tree are created utilizing reference bunch versatility models and irregular reference point portability models to contrast them and the postpone simulation results. This is one more unique commitment of the record. As far as directing time, control above and PDR, the simulation results show that the DQMR convention performs better compared to the specially appointed distance vector steering convention under multicast request [8]. In your proposition, you utilize a 3D consistent space to address the physical intra-neighbor connections of a hub and a 3D design to portray those ties in a DHT-based routing protocoln. Every hub in the proposed approach runs a disseminated calculation to create a predictable sensible ID that mirrors its spatial closeness in a three-layered consistent space. The convention likewise monitors numerous courses to an objective node utilizing a 3D construction [10]. Most of the exploration on shrewd information sharing is finished for fixed remote networking, which has drawn a great deal of interest from the multihop remote networking research local area. Entrepreneurial information sending in MANETs isn't ordinarily utilized for various reasons, one of which being the shortfall of a compelling, lightweight routing system with dependable source directing capabilities[11].

This letter offers another convention that improves automated robot network execution by utilizing Q-learning-based geographic routing (QGeo). For the remote observing and control of portable mechanical gadgets, a fast, reliable organization is required. Controlling the organization above important for course determination and fix, notwithstanding, stays a significant trouble because of the rising portability of gadgets [12]. For relapse averaging frameworks, the adequacy of ML calculations is measured in terms of root mean square error (RMSE) and mean proper error(MAE). Prescient models are utilized to pick the legitimate directing boundaries, as well as trama centers and RED boundaries, to guarantee QoS for a specific organization situation. They are accomplished up to RMSE and MAE discoveries. Standard steering convention variations are made in view of their exhibition, and the best variety that can give an observable presentation gain is found by utilizing ML calculations to conjecture QoS boundaries. Results are given to help the attestation that the nature of the assistance has altogether improved [13].

The quantity of broadcast packets rises exponentially as node density in the network rises. This may result in broadcast storms, decreased network performance, and device battery drain [14]. We keep track of the identities of participating brokers in a ledger to promote cooperation among self-interested peers. However, the integrity of that routing record cannot be explicitly guaranteed by the blockchain. Therefore, to prevent dishonest intermediaries from corrupting or interfering with the ledger listing, we have built a ledger security mechanism with bounty policies. The experimental findings demonstrate that the proposed data corridor can greatly enhance the delay and loss rate of non-cooperative MANETs' network performance [15].

MANETs have expanded quickly as a result of the inexpensiveness, adaptability, and simplicity of mobile devices. For usage as a recovery information system following a natural disaster where the communication infrastructure is no longer available or may be inaccessible, such devices can quickly establish a stable network. Routing is thought to be an extremely difficult topic in networks without centralized control since nodes can move around freely at any time [16]. By conducting thorough simulation tests against the three simulation parameters of network node count, node speed, and data packet transmission rate, the performance of the proposed system was assessed. Simulation Results Compared to other fundamental routing protocols, FT-AORP significantly increased packet delivery speed, decreased end-to-end delay, and maintained a high level of residual energy of the transmission line [17]. MANET are self-putting together, rapidly deployable, foundation free remote organizations, they are outstandingly appropriate for uses like outside exceptional occasions, correspondences in regions without radio framework, emergencies and catastrophic events, as well likewise with military activities. Because of the adaptability of its dynamic geography and designs, which are continuously changing, security might be Manet's essential shortcoming. This implies that it could be especially helpless against assaults like directing, program control, and listening in. Security issues on MANET are more terrible than the Quality of Services (QoS)[18].

MANET are a sort of systems administration that don't depend on brought together access or organization foundation. The fast and versatile systems administration style of MANET offers you different purposes specifically conditions. Open channels and rapidly changing geographies, be that as it may, may introduce security gambles. Utilizing the attributes of dynamic directing conventions, we recommended a functioning active routing authentication system (AAS) in this study [19].

A gathering of inconsistent hubs that make a powerful organization with practically no unified administration is known as a MANET. It is hard to pursue directing choices for portable interchanges since steady node development increments steering above and battery utilization. To bring down the above of steering choices and energy utilization, various examinations have been led in the MANET field. Their ideas are helpful for improving execution as far as burden adjusting, traffic the executives, and energy use [20].

A group of wireless mobile devices that capability as an impromptu networking without the guidance of any foundation or concentrated administration is known as a MANET. Since portable nodes don't have a reliable wellspring of force and their nonattendance can abbreviate the organization's usable life, energy utilization ought to be seen as one of the vital downsides of MANETs [21]. Since highlight point control messages are verifiably restricted, much effort should be placed into "tuning" them to the intricacies and potential open doors that remote settings offer. In this report, the most famous routing conventions in MANET are analyzed and differentiated [22-26].

Table.1 Comparison of different methodologies at the existing level

Author year	Learning Type	Technique used	Result achieved	Limitations
X. Wang et al.,(2020)	trust-based routing mechanisms	Fuzzy logic	Quality of service achieved 82%	Improving QoS in MANET
H. Xia, et al.,(2020)	On-Demand Multicast Routing Protocol (ODMRP)	novel trust-based routing protocol	Routing performance achieved 89%	Improved the multicast routing
M. U. Farooq et al ., (2021)	the minimum CDS (MCDS)	benchmark routing protocols	PDR performance achieved 88%	packet delivery ratio(PDR) is improved
Y. -H. Chen et al.,(2018)	Coding-Aware Multicast Protocol	random access mechanism	multicast routing performance 91%	multicast routing is improved
R. J. Cai, et al.,(2019)	Evolutionary Self-Cooperative Trust Scheme	dynamic network topology	Improved security achieved 89%	Achieved the security performance
R. Sanchez-Iborra et al.,(2014)	BATMAN Routing Protocol	OLSR routing protocol	Energy Performance archived 92%	Energy performance is archived
Shanthi, T. et al.,(2023)	multipath link routing protocol	blow fish model	Improved routing performance achieved 94%	routing performance is improved
C Senthilkumar et al.,(2022)	Multi-Agent-Based Zone Routing (MAZR) protocol	Multicasting technology	Power consumption is achieved 89%	Improved the power consumption and network life time
P.Ganeshkumar, et al., (2015)	Heavy Secured Routing Protocol	new routing protocol for WN	Throughput is performances achieved 88%	Improved the Throughput is performances
S Jaganath, et al.,(2017)	existence well-known security mechanisms	ZRP protocol And cluster based	Security performances achieved 92%	Improved the Security performances

indu bala et al. (2023)	Prevalence of internet services	DWT-incorporated LDPC STBC system	More dependable data rates	Suitable option for the deployment of 5G
Sahaya Sheela M A, Prabakaran. R (2020)	cluster-head gateway switch routing protocol	particle swarm optimization with fuzzy rules	Network lifetime improvement and increased packet delivery ratio	Suitable for Software Defined MANET

3. FCCEE (Protected Optimal Path-Routing Protocol)

The Manet is the most powerful wireless network and the fastest communication of the networks. The problem is Manet is secure communication, energy consumption, and routing optimization. The proposed system FCCEE) Protected Optimal Path-Routing Protocol system has been increased to overcome all the problems solved by encryption using the TACIT technique, and using the HMAC algorithm has been used for crucial general of next-generation of key authentication system. The following proposed architecture is figure.2.

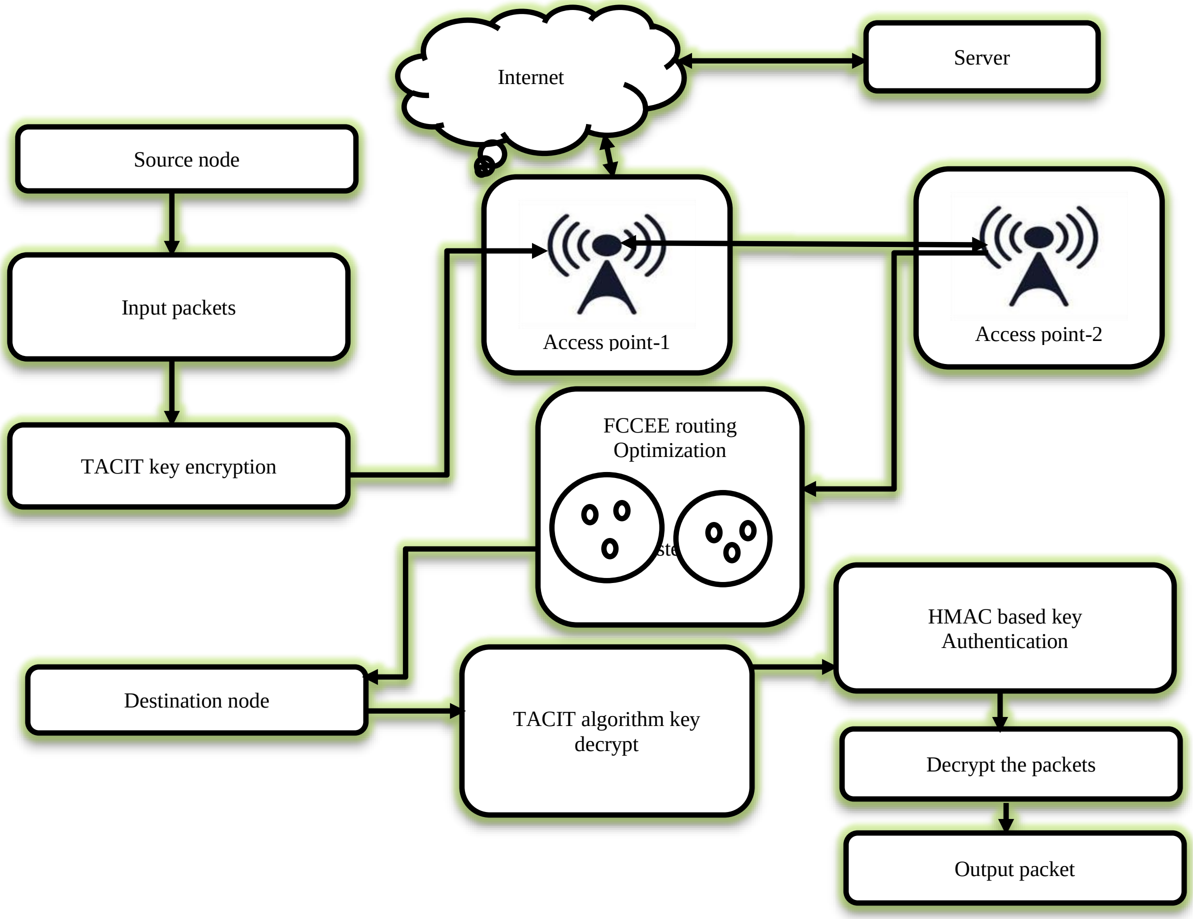

Fig..2 FCEE - Protected Optimal Path-Routing Protocol Architecture

3.1 Network node creation and cluster formation

The MANET model and network nodes are employed in accordance with the architectural model. In MANET, numerous nodes take part. Every node in a MANET must execute the necessary routing tasks and forward any traffic that other nodes will send to it. Some nodes exhibit selfish behavior among all the nodes; Because each node in the network has resource limits, such as storage and power constraints, every node in a MANET has the ability to act selfishly, that is, to solely use its limited resources for its own gain. These nodes seek to benefit from the resources that other nodes in the network make available. However, you must prevent others from using your personal resources. These nodes attempt to maximize network benefits while also attempting to safeguard their own resources. The server to support for receive or transfer the data and sharing the information's.

The Manet connects the n number nodes and access, but the communication and energy consumption problem is overcome using multiple ways; clustering the network nodes because any one node failed means a way to another node to transmit the packet data. Cluster support for grouping the nodes because grouping the nodes means easy transfer of the data or packets. The below diagram for fuzzy clustering nodes on Manets in figure.3

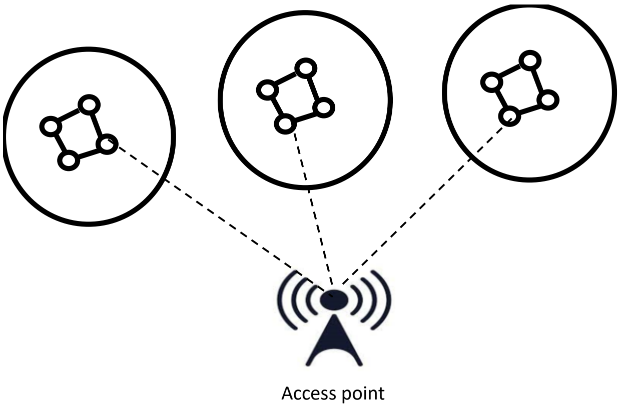

Fig..3 Fuzzy C-means Clustering node formation on Manet

The packet data is securely encrypted using the TACIT key encryption algorithm. This algorithm is based on the advanced AES concept and fully functions. After transfer to the access point, packet data is transferred to another node or access point. Then after clustering the nodes and quickly sent through packet data. The below algorithm formula for encrypting the data.

3.2 TACIT key encryption algorithm

This is sha-4 512 algorithm for 64bit range based key generate and 256 hash function has been 30 testing and 512 hash has been above 90 round testing, the follow equation generate the digital signature or random keys

$$r = \int_q^p \langle\langle g^k \rangle_p\rangle_q \tag{1}$$

$$S = \iint_q^p \langle\langle k^{-1} + Xr\rangle_q\rangle \tag{2}$$

$$g = \sum_q^p \left\langle\left\langle h^{p-1/q}\right\rangle_p\right\rangle \tag{3}$$

1<h<p-1, and 0<k<q randomly selected k, L m = 64 for any integer m, q is a prime, 2^159<q<2^260 x is a private key randomly generated, 0 < < x q; M^"+Xr is the message M

$$f(v) = \sum_q^p \langle\langle g^{u1} g^{u2}\rangle_p\rangle_q \tag{4}$$

If $v = r'$ is message verified, be noted that y, g, p, and q are transparent to both the signatory and the receiver.

Initialize:

$$A = H_0, B = H_1, C = H_2, and\ E = H_4 \tag{5}$$

$$A_{t+1} = f(T) \tag{6}$$

Perform 90 rounds; for t = 0; 90; < ++; $for\ t < 16, \dots W_t$=$W_t\ and\ for\ t > 32$

$$\sqrt{W_{t=S^1}(W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3}}$$

Final Adds round values $H_0 = H_0 + A_1 H_1 = H_1 + B_1 H_2 = H_2 + C$

$$f(H_{3)} = H_3 + D, H_4 + E \tag{7}$$

For (6) – (7) above, + denotes addition with modulation reduction

$$f(M'') = Encypt\ (\mathrm{SHA} - 4(\mathrm{M}) = \{H_0, H_1, H_2, +H_4\} \tag{8}$$

To process the round weight of the key is (Wt), the information is sectioned into 512-digit blocks. The last block is loaded up with "1" and a few "0"s and the information length to finish the 512-cycle block size. $f(M'') is\ the\ encrypted\ the\ key$ Or digest.

3.2 FCCEE routing Optimization

Fuzzy C-Means Clustering Based Energy-Efficient Protected Optimal Path-Routing Protocol has been functioning for first receiving the data of packets and transferring to the access point (AP); AP has been choosing the route of the destinations.

The number of node N, and received the packet data x, number of routing path r

$$\sum_{N+1}^{N} f(x) = f(M'') \tag{9}$$

Here $f(x)$ is received the packets and N, N+1 is number of nodes has been point out.

Then point the routing path

$$r(f(x) = -\sum_{i=0}^{n} a_i v_i - \sum_{j=0}^{m} b_i v_i - \sum_{i=0}^{n} \sum_{j=0}^{m} v h_j + f(w) \tag{10}$$

Here, $w_{i,j}$ is the weight of the data, and jth is the hidden elements.

Probability distribution path p (v)

$$P(V) = \frac{1}{Z}\sum_h e^{-E(v,h)} + f(w) + r(f)x) \qquad (11)$$

Probability distribution path P (h)

$$P(h) = \frac{1}{Z}\sum_v e^{-E(r,h)} + f(w) + r + P(V) \qquad (12)$$

$$P(h, N_1, N_2 \dots N_l) = P(r|N_1)P(N_2|N_l) \dots P(r|N_1)P(N_1|N_{l-1})P(N_{l-1}|N_1) \qquad (13)$$

$$W = cluster \sum \left[\left(P(N_1, N_2 \dots N_l)\right)\mathrm{k} + f(w)\right] + r \qquad (14)$$

Here $N_1, N_2 \dots N_l$ is the number of routing path and transfer the data to each nodes select and send to another node, each and every node has been clustering

$$r_i = path \sum W * f(x) \epsilon R \qquad (15)$$

Practically, one frequently utilizes more:

$$r_j = \sum(x_i . P(h) + W) \qquad (16)$$

The method of data, the data, has been a sequential manner for data flows and a specific window for displaying the data presented here.

$$N_j = \int [path_{\ j:m} + POS_{l:m} + W] \ + r_j \qquad (17)$$

$$N_i = \int Route_{l:m} + POS_{l:m} + \ r_i \qquad (18)$$

Here $N_i \: and \: N_j$ is specify the Routing Optimization performance for Equation (17) is routing path select and equation (18) is way the route of the node, in which route to send packet to nodes decided here. Sent the cluster no send to AP, after that node to key verification using HMAC based key

Authentication.

Algorithm: C-Means Clustering

Input: frequency rate (mfr→W), Indexing block Ib,

Output: Cluster group

Step 1: Compute the block comparison rate BQt

For each term, BQt from Ib

Compute content match case similarity measure

Mcscsm = Nc/Tn.

Nc = Number of Relative content Ti→ term Hashindex

Tn- Total Number of content terms present in the service list

End

Step 2: Calculate frequent content measure Fcm = $\int \frac{Scsm}{Numberofuser\ accessed\ service}$

For each index block content term search

Blocklist SL = Relative weightage computation.

[sscm, S, Ne] =Compute Relative bound measure (Ts).

For each related content term frequency

Step 3 **:** Compute term frequency Tf = $\frac{\sum Terms(Ts) \in O(c)}{Numberoftermsofc}$

Compute relative block term QTw = Sscm×sl

End

Step 4: Select the top Max content match case = O (Max (Sscm))

Group Max terms similar to block cluster

Return optimized block rehashing Q→t

End

Based on content match, a table with file ID, block ID, and hash ID represents various degrees of multi-hash point. The amount of block referrals to locate pertinent content has greatly increased as a result. By comparing the frequency of correlation terms at the block level, content metrics are computed for each counting period using the frequency index. The maximum match level is used to compare the relative weights of the material, and the findings are then sent back to the block for evaluation and indexing.

The key has already been encrypted, so the digest key has been decrypted. The following has used to decrypt the information.

$$r = \int_q^p \langle\langle g^k \rangle_p\rangle_q + \ f(M'') \qquad (19)$$

$$S = \iint_q^p \langle\langle k^{-1} + Xr\rangle_q\rangle + \ f(M'')) \qquad (20)$$

$$g = \sum_q^p \left\langle\left\langle h^{p-1/q}\right\rangle_p\right\rangle + \ f(M'') \qquad (21)$$

$$f(v) = \sum_q^p \langle\langle g^{u1} g^{u2}\rangle_p\rangle_q + f(M'') \qquad (22)$$

If $v = r'$ is message verified, be noted that y, g, p, and q are transparent to both the signatory and the receiver.

Initialize:

$$A = H_0, B = H_1, C = H_2, and\ E = H_4 \qquad (23)$$

$$A_{t+1} = f(T) \qquad (24)$$

Perform 90 rounds; for t = 0; 90; < ++; $for\ t < 16, \dots W_t = W_t\ and\ for\ t > 32$

$$\sqrt{W_{t=S^1}(W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3} \quad + \quad f(M'')}$$

Final adds round values $H_0 = H_0 + A_1 H_1 = H_1 + B_1 H_2 = H_2 + C$

$$f(H_{3)} = H_3 + D, H_4 + E + \quad f(M'') \qquad (25)$$

For (6) – (7) above, + denotes addition with modulation reduction

$$X = decrypt[(\mathrm{SHA} - 4(f(M'')) + f(H_{3)}] \qquad (26)$$

To process the round weight of the key is (Wt), the information is sectioned into 512-digit blocks. The last block is loaded up with "1" and a few "0"s and the information length to finish the 512-cycle block size. $X\ is\ \ the\ key\ decrpted$.

3.4 HMAC based key Authentication

A shared private key provided by HMACs is only accessible by the client and server. Each request is given a distinct hash (HMAC) by the client. In separate phases, the key and the message are both encrypted and secured. The server generates its own HMAC after receiving the request. The two HMACS are compared, and the client is regarded as valid if they are both the same.

For Bob to authenticate key authentication, must have a copy of her public-key curve point $Q_A\ Bob\ can\ verify\ Q_A$

Check that Q_A is not equal to the identity element O, and its coordinates are otherwise valid.

Check that Q_A lies on the curve.

Check that $n\ X\ Q_A = O$

Step1

[1, n-1] key is verified

Step2

e=HASH(X) where HASH is the same function used in the key generation.

Step3

Let z be the L_n leftmost bits of e.

Step4

Calculate $u_1 = zs^{-1}\ mode\ n\ and\ u_2 = mod\ n$

Step5

Calculate the curve point $(x_1, y_2) = u_1 X\ G + u_2\ X\ Q_A$

Step6

Calculate the curve point $if((x_1, y_2) = 0$

Step7

The key is valid$if\ r = x_1(mod\ n)$, invalid

That is $s^{-1}mod\ n$ only once finally data has decrypted on end of the node.

3.5 Simulation output Screenshot

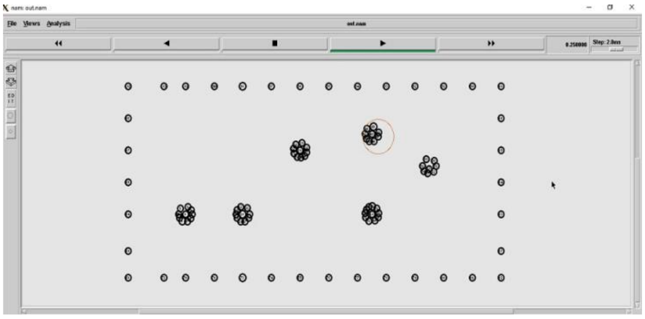

Fig..4 start the cluster formation

Figure 4 shows the network simulations using NS2 software. NS2 software is a network simulator tool. First up, create the needs of nodes; you can make 50 nodes, 100 nodes, 200 nodes, and above them.

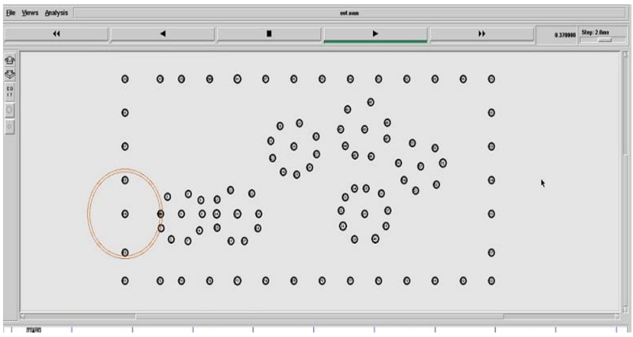

Fig..5 cluster formation starting level

Figure.5 denote the clustering formation of the nodes, cluster formation for all the nodes and clusters are grouped into 5 groups.

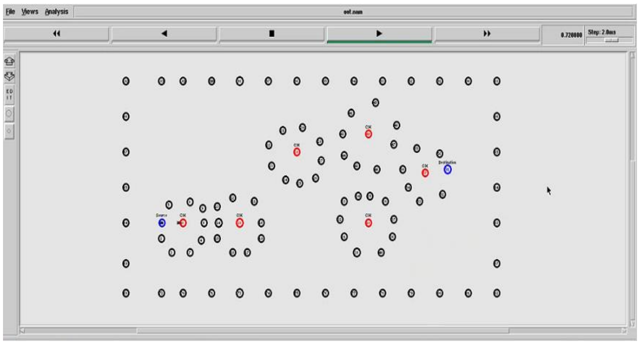

Fig..6 cluster formation ending level

Figure.6 denote the clustering formation of the nodes, cluster formation for all the nodes and clusters are grouped into 5 groups and one groups to another groups sending packet data’s.

4. **Result and Discussion**

The section discusses the result of the proposed system. The result part discusses the route optimization of the network and packet delivery ratio, throughput performance routing performance, network lifetime, energy consumption, and error rates. The existing system of with AODV, OLSR and DSR algorithms is compared to the proposed system of Fuzzy C-Means Clustering Energy-

Efficient Protected Optimal Path-Routing Protocols and secure encryption using the TACIT technique and key verification for HMAC algorithm are used here. We used 100 nodes and developed a tool using a network (NS2) simulator.

4.1 packet delivery ratio (PDR)

This section discusses the packet delivery ratio and the ratio compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given a high-performance delivery ratio. The table .1 discuss about the packet delivery ratio **(**PDR). The PDR is denote as

$$PDR = \frac{\text{Total no of packets delivered}}{\text{Total no of packets transferred}} X100 \quad (27)$$

Table.1 packet delivery ratio (PDR)

No of nodes	Method	Ratio
20	AODV	78
40	OLSR	89
60	BTSNADS	93.5
80	DSR	95.5
100	Proposed	96.5

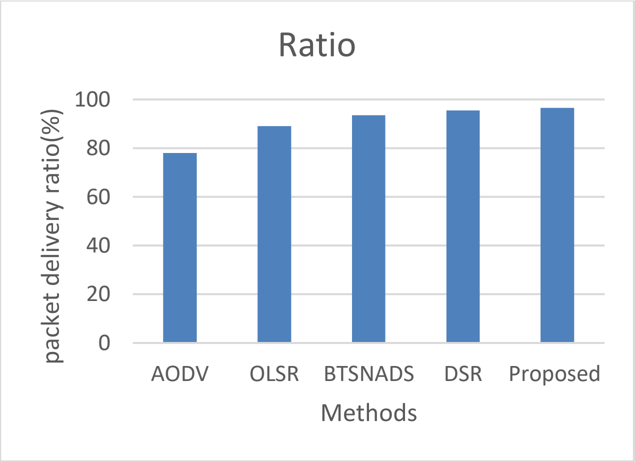

Fig.7 packet Delivery ratio

The figure.7 discuss about the packet delivery ratio are compared with existing system of AODV is 78% and OLSR is 89%, DSR is 95.5%, BTSNADS is 93.5% but proposed system of Fuzzy C-Means Clustering based Energy-Efficient (FCCEE) is 96.5 % of ratios.

4.2 Throughput performance

This section discusses the Throughput performance is compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given a Throughput performance ratio. The table .2 discuss about the packet delivery ratio. The Throughput performance is denote as

$$throughtput = \frac{file\ size}{transmission\ time(m/sec)} \quad (28)$$

Table.2 Throughput performance

Methods	file size	Transmission time(m/sec)
AODV	50	75
OLSR	150	125
BTSNADS	250	175
DSR	350	276
Proposed	500	375

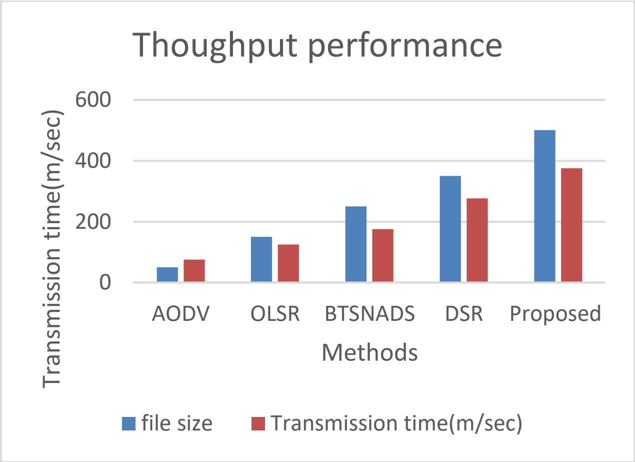

Fig..8 Throughput performance

Figure.8 discusses the Throughput performance compared with the existing system of the AODV algorithm taking 75m/sec for 50MP, the OLSR algorithm taking 125m/sec for 150MP, the BTSNADS algorithm taking 175m/sec for 250MP, and the DSR algorithm taking 276m/sec for 350 MP. And proposed algorithm took 375m/sec for 500MP.

4.3 Transmission time (ms)

This section discusses the Transmission time (bps) is compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given a Transmission time (ms) is best . The table.3 discuss about the Transmission time (bps). The Transmission time (ms) is denote as

$$\text{Packet transmission time} = \frac{\text{Packet size}}{\text{Bit rate}} \quad (29)$$

Table.3 Transmission time (ms)

methods	1 byte	10 bytes	100 bytes	1k
AODV	4.82	7.82	14.82	19.2
OLSR	4.81	7.81	13.81	18.5
BTSNADS	4.71	7.71	12.71	17.5
DSR	4.7	8.7	11.7	16
Proposed	4.66	7.76	10.76	15.5

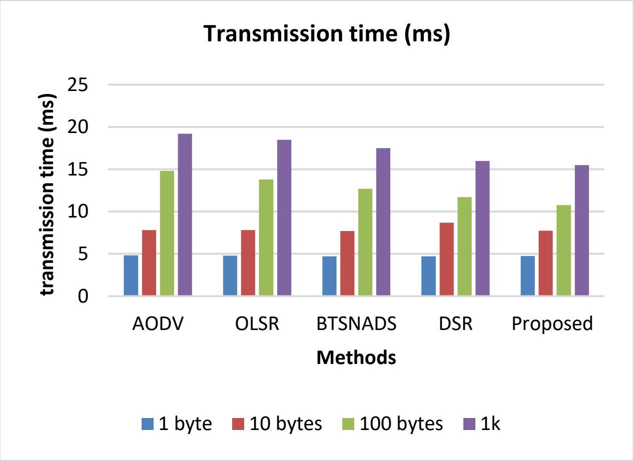

Fig. 9 Transmission time (m/sec) performance

Figure.9 discuss about the Transmission time (bps) performance of proposed system 1 byte taken time is 4.66 m/sec, 10 byte taken time is 7.76 m/sec, 100 byte taken time is 10.76 m/sec, and 1k byte taken time is 15.5 m/sec

4.4 Routing performance

This section discusses the Routing performance is compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given a Routing performance is best. The table.4 discuss about the Routing performance. Routing performance is denote as

Table.4 Routing performance 100 kbps

nodes	AODV	OLSR	BTSNADS	DSR	Proposed
10	65	70	81	91	92
20	66	71	82	92	94
30	67	72	83	93	95
40	68	74	84	94	96
50	69	72	82	92	97

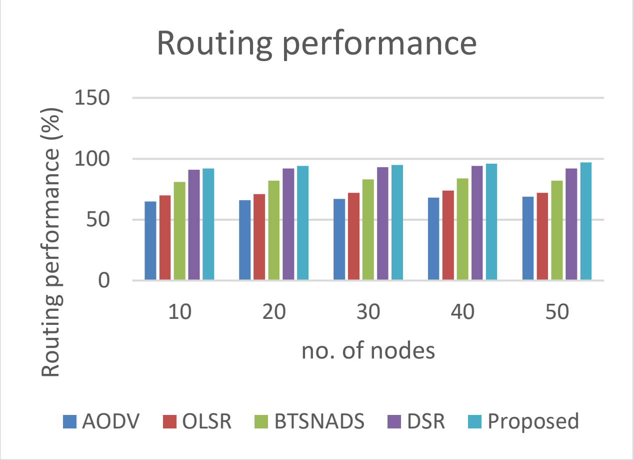

Fig..10 Routing performance

Figure.10 discuss about the routing performance, the performance of Adov 50 nodes performance is 69%, and OLSR 50 nodes performance is 72%, and OLSR 50 nodes performance is 72%,, and BTSNADS 50 nodes performance is 82%, and DSR 50 nodes performance is 92%, and proposed 50 nodes performance is 97%,

4.5 Error rate ratio

This section discusses the error rate ratio is compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given an error rate ratio is best. The table.5 discuss about the Routing performance. Error rate ratio is denote as

Table.5 Error rate performance ratio

nodes	AODV	OLSR	BTSNADS	DSR	Proposed
10	0.012	0.011	0.01	0.09	0.08
20	0.022	0.01	0.02	0.08	0.07
30	0.033	0.09	0.029	0.071	0.06
40	0.031	0.084	0.027	0.07	0.05
50	0.0334	0.072	0.036	0.06	0.03

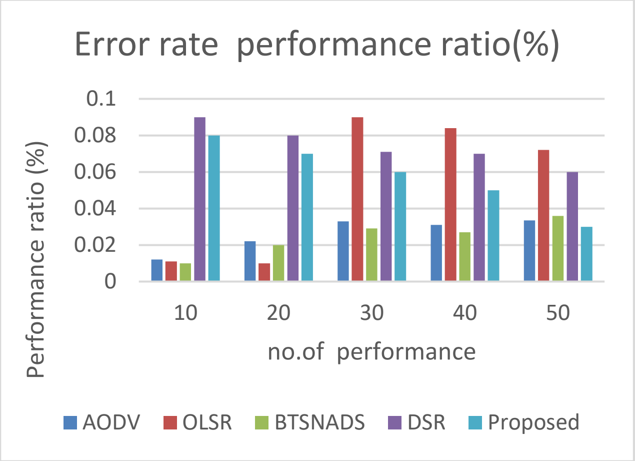

Fig.11 Error rate ratio

The following figure.11 discusses the error rate of packet transmission performances. The 50-node error rate of AODV is 0.0334%, the 50-node error rate of OLSR is 0.072%, the 50-node error rate of BTSNADS is 0.036%, and the 50-node error rate of DSR is 0.006%, and the 50-node error rate of Proposed is 0.003%.

4.6 Network Life Time

This section discusses the Network Life Time is compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given an Network Life Time is best. The table.6 discuss about the Network Life Time. Network Life Time is denote as

Network Life Time $= \mathrm{E} - (\mathrm{U} + \sigma)$

Where $U = \frac{\sum U_i}{N}$ (30)

Table.6 Network Life Time

nodes	AODV	OLSR	BTSNADS	DSR	Proposed
10	71	72	83	85	94
20	72	83	84	86	95
30	74	84	87	86	96.5
40	76	85	88	90	97
50	78	88	89	91	98.6

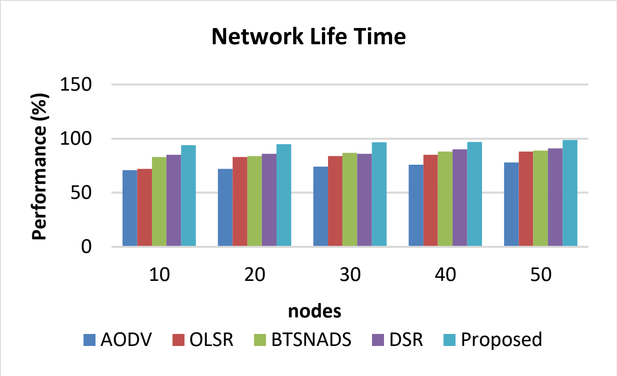

Fig.12 Network life time performance

The following is the figure.10 discuss the Network life time performance on Manet. Network life time performance for 50 nodes using the AODV algorithm is taken at 78%, The Network life time performance for 50 nodes using the OLSR algorithm is taken at 88%, and The Network life time performance for 50 nodes using the BTSNADS algorithm is taken at 89%, and The Network life time performance for 50 nodes using the DSR algorithm is taken at 91%, and The Network life time performance for 50 nodes using the proposed algorithm is taken at 98.6%.

4.7 Energy Consumption

This section discusses the Energy Consumption is compared with AODV, OLSR and DSR, BTSNADS algorithms. However, the proposed system of Fuzzy C-Means Clustering Energy-Efficient Protected Optimal Path-Routing Protocols has given an error rate ratio is best. The table.7 discuss about the Routing performance. Energy Consumption is denote as E is the total energy of each nodes U_i is the average energy used, N is overall nodes in the networks and expressed as

$$\sigma^2 = \frac{(U_i - U)^2}{N} \quad (31)$$

Table.7 Energy Consumption

nodes	AODV	OLSR	BTSNADS	DSR	Proposed
10	70	72	82	84	92
20	72	82	83	83	93
30	74	84	85	86	93.5
40	75	86	89	90	94
50	78	88	88	91	96.6

The following is the figure.13 discuss the Energy consumption on Manet. The energy consumption for 50 nodes using the AODV algorithm is taken at 78%, The energy consumption for 50 nodes using the OLSR algorithm is taken at 88%, and The energy consumption for 50 nodes using the BTSNADS algorithm is taken at 88%, and The energy consumption for 50 nodes using the DSR algorithm is taken at 91%, and The energy consumption for 50 nodes using the proposed algorithm is taken at 96.6%.

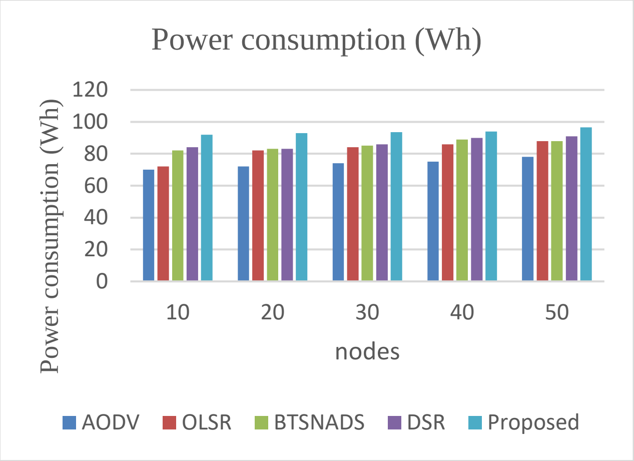

Fig.13 Power consumption

The following is the figure.13 discuss the Energy consumption on Manet. The energy consumption for 50 nodes using the AODV algorithm is taken at 78%, The energy consumption for 50 nodes using the OLSR algorithm is taken at 88%, and The energy consumption for 50 nodes using the BTSNADS algorithm is taken at 88%, and The energy consumption for 50 nodes using the DSR algorithm is taken at 91%, and The energy consumption for 50 nodes using the proposed algorithm is taken at 96.6%.

5. Conclusion

The proposed system for FCCEE Protected Optimal Path-Routing Protocol for MANET. The Manet is one mobile computing network; existing had drawbacks because of the primary significant need for secure routing performance of the Manet. The problem was identifying the routing performance, network lifetime, energy consumption error rate, etc. The problem was overcome using FCCEE Protected Optimal Path-Routing Protocol for achieved system routing performance is the performance of Adov 50 nodes performance is 69%, OLSR 50 nodes performance is 72%, OLSR 50 nodes performance is 72%, BTSNADS 50 nodes performance is 82%. DSR 50 nodes performance is 92%, and the proposed 50 nodes performance is 97% and the energy performance is 50 nodes using the BTSNADS algorithm is reserved at 88%, and The energy consumption for 50 nodes using the DSR algorithm is reserved at 91%, and The energy consumption for 50 nodes using the proposed algorithm is reserved at 96.6%.

Reference

[1] W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," in IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, Nov. 2014, doi: 10.1109/TVT.2014.2313180.

[2] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019, doi: 10.1109/ACCESS.2019.2928804.

[3] Z. Chen, W. Zhou, S. Wu and L. Cheng, "An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET," in IEEE Access, vol. 8, pp. 44760-44773, 2020, doi: 10.1109/ACCESS.2020.2978582.

[4] J. Ryu and S. Kim, "Reputation-Based Opportunistic Routing Protocol Using Q-Learning for MANET Attacked by Malicious Nodes," in IEEE Access, vol. 11, pp. 47701-47711, 2023, doi: 10.1109/ACCESS.2023.3242608.

[5] B. H. Khudayer, M. Anbar, S. M. Hanshi and T. -C. Wan, "Efficient Route Discovery and Link Failure Detection Mechanisms for Source Routing Protocol in Mobile Ad-Hoc Networks," in IEEE Access, vol. 8, pp. 24019-24032, 2020, doi: 10.1109/ACCESS.2020.2970279.

[6] A.Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," in IEEE Access, vol. 5, pp. 10369-10381, 2017, doi: 10.1109/ACCESS.2017.2707537.

[7] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf and B. V. Subbayamma, "An Improved Hybrid Secure Multipath Routing Protocol for MANET," in IEEE Access, vol. 9, pp. 163043-163053, 2021, doi: 10.1109/ACCESS.2021.3133882.

[8] T. -N. Tran, T. -V. Nguyen, K. Shim, D. B. Da Costa and B. An, "A New Deep Q-Network Design for QoS Multicast Routing in Cognitive Radio MANETs," in IEEE Access, vol. 9, pp. 152841-152856, 2021, doi: 10.1109/ACCESS.2021.3126844.

[9] S. A. Abid, M. Othman, N. Shah, M. Ali and A. R. Khan, "3D-RP: A DHT-Based Routing Protocol for MANETs," in The Computer Journal, vol. 58, no. 2, pp. 258-279, Feb. 2015, doi: 10.1093/comjnl/bxu004.

[10] Z. Wang, Y. Chen and C. Li, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks," in IEEE Transactions on Vehicular

Technology, vol. 63, no. 2, pp. 859-868, Feb. 2014, doi: 10.1109/TVT.2013.2279111.

[11] W. -S. Jung, J. Yim and Y. -B. Ko, "QGeo: Q-Learning-Based Geographic Ad Hoc Routing Protocol for Unmanned Robotic Networks," in IEEE Communications Letters, vol. 21, no. 10, pp. 2258-2261, Oct. 2017, doi: 10.1109/LCOMM.2017.2656879.

[12] Durr-e-Nayab, M. H. Zafar and A. Altalbe, "Prediction of Scenarios for Routing in MANETs Based on Expanding Ring Search and Random Early Detection Parameters Using Machine Learning Techniques," in IEEE Access, vol. 9, pp. 47033-47047, 2021, doi: 10.1109/ACCESS.2021.3067816.

[13] F. Safari, H. Kunze, J. Ernst and D. Gillis, "A Novel Cross-Layer Adaptive Fuzzy-Based Ad Hoc On-Demand Distance Vector Routing Protocol for MANETs," in IEEE Access, vol. 11, pp. 50805-50822, 2023, doi: 10.1109/ACCESS.2023.3277817.

[14] X. Ling, P. Chen, J. Wang and Z. Ding, "Data Broker: Dynamic Multi-Hop Routing Protocol in Blockchain Radio Access Network," in IEEE Communications Letters, vol. 25, no. 12, pp. 4000-4004, Dec. 2021, doi: 10.1109/LCOMM.2021.3114218.

[15] A. M. E. Ejmaa, S. Subramaniam, Z. A. Zukarnain and Z. M. Hanapi, "Neighbor-Based Dynamic Connectivity Factor Routing Protocol for Mobile Ad Hoc Network," in IEEE Access, vol. 4, pp. 8053-8064, 2016, doi: 10.1109/ACCESS.2016.2623238.

[16] D. N. M. Hoang, J. M. Rhee and S. Y. Park, "Fault-Tolerant Ad Hoc On-Demand Routing Protocol for Mobile Ad Hoc Networks," in IEEE Access, vol. 10, pp. 111337-111350, 2022, doi: 10.1109/ACCESS.2022.3216066.

[17] N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," in IEEE Access, vol. 9, pp. 120996-121005, 2021, doi: 10.1109/ACCESS.2021.3108807.

[18] J. Tu, D. Tian and Y. Wang, "An Active-Routing Authentication Scheme in MANET," in IEEE Access, vol. 9, pp. 34276-34286, 2021, doi: 10.1109/ACCESS.2021.3054891.

[19] K. Chandravanshi, G. Soni and D. K. Mishra, "Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive Multipath N-Channel Routing Approach in MANET," in IEEE Access, vol. 10, pp. 110003-110025, 2022, doi: 10.1109/ ACCESS. 2022.3213051.

[20] A.Bhardwaj and H. El-Ocla, "Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Networks," in IEEE Access, vol. 8, pp. 177534-177548, 2020, doi: 10.1109/ACCESS. 2020.3027043.

[21] T. Haque, "On the Overheads of Ad Hoc Routing Schemes," in IEEE Systems Journal, vol. 9, no. 2, pp. 605-614, June 2015, doi: 10.1109/JSYST.2013.2294881.

[22] X. Wang, P. Zhang, Y. Du and M. Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network," in IEEE Access, vol. 8, pp. 47675-47693, 2020, doi: 10.1109/ACCESS.2020.2978143.

[23] Yaseen, M., Hayder Sabah Salih, Mohammad Aljanabi, Ahmed Hussein Ali, & Saad Abas Abed. (2023). Improving Process Efficiency in Iraqi universities: a proposed management information system. Iraqi Journal For Computer Science and Mathematics, 4(1), 211–219. https://doi.org/10.52866/ijcsm.2023.01.01.0020

[24] Aljanabi, M. ., & Sahar Yousif Mohammed. (2023). Metaverse: open possibilities. Iraqi Journal For Computer Science and Mathematics, 4(3), 79–86. https://doi.org/10.52866/ijcsm.2023.02.03.007

[25] Atheel Sabih Shaker, Omar F. Youssif, Mohammad Aljanabi, ABBOOD, Z., & Mahdi S. Mahdi. (2023). SEEK Mobility Adaptive Protocol Destination Seeker Media Access Control Protocol for Mobile WSNs. Iraqi Journal For Computer Science and Mathematics, 4(1), 130–145. https://doi.org/10.52866/ijcsm.2023.01.01.0011

[26] Hayder Sabah Salih, Mohanad Ghazi, & Aljanabi, M. . (2023). Implementing an Automated Inventory Management System for Small and Medium-sized Enterprises. Iraqi Journal For Computer Science and Mathematics, 4(2), 238–244. https://doi.org/10.52866/ijcsm.2023.02.02.021

[27] H. Xia, Z. Li, Y. Zheng, A. Liu, Y. -J. Choi and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs," in IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 236-248, 1 April-June 2020, doi: 10.1109/TSUSC.2018.2817219.

[28] M. U. Farooq and M. Zeeshan, "Connected Dominating Set Enabled On-Demand Routing (CDS-OR) for Wireless Mesh Networks," in IEEE Wireless Communications Letters, vol. 10, no. 11, pp. 2393-2397, Nov. 2021, doi: 10.1109/LWC.2021.3101476.

[29] Y. -H. Chen, E. H. -K. Wu, C. -H. Lin and G. -H. Chen, "Bandwidth-Satisfied and Coding-Aware Multicast Protocol in MANETs," in IEEE Transactions on Mobile Computing, vol. 17, no. 8,

pp. 1778-1790, 1 Aug. 2018, doi: 10.1109/TMC.2017.2778262.

[30] R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," in IEEE Transactions on Mobile Computing, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019, doi: 10.1109/TMC.2018.2828814.

[31] R. Sanchez-Iborra, M. -D. Cano and J. Garcia-Haro, "Performance Evaluation of BATMAN Routing Protocol for VoIP Services: A QoE Perspective," in IEEE Transactions on Wireless Communications, vol. 13, no. 9, pp. 4947-4958, Sept. 2014, doi: 10.1109/TWC .2014.2321576.

[32] Shanthi, T. ., Sheela, M. S. ., Jayakanth, J. J. ., Karpagam, M. ., Srividhya, G. ., & Prasad, T. V. S. G," A Novel approach Secure Routing in Wireless Sensor Networks for Safe Path Establishment of Private IoT Data Transmission," International Journal of Intelligent Systems and Applications in Engineering, 2023,11(9s),., 455–460,

[33] S Manthandi Periannasamy, NC Sendhilkumar, R Arun Prasath, C Senthilkumar, S Gopalakrishnan, TT Chitra," Performance analysis of multicast routing using multi agent zone based mechanism in MANET,"2022, International Journal of Nonlinear Analysis and Applications, 13(1), 1047-1055.

[34] P.Ganeshkumar and S. Gopalakrishnan." Heavy Secured Routing Protocol: A Secured Routing Protocol for Wireless Networks,"2015, Journal of Computational and Theoretical Nanoscience,12(6), 1086-1095(10)

[35] S Gopalakrishnan, S Jaganath, P Parthasarathy, P Jesu Jairin, R Ragumadhavan," Cluster based secure performance on mobile ad-hoc network using zone routing protocol,"2017, Advances in Natural and Applied Sciences,11(9), 134-150.

[36] indu bala, K. Arora, and M. M. . Mijwil, "Novel Energy Optimized LDPC Codes for Next-Generation MIMO OFDM Systems", Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 4, pp. 1–12, Sep. 2023.

[37] Shahakar, M. ., Mahajan, S. ., & Patil, L. . (2023). Load Balancing in Distributed Cloud Computing: A Reinforcement Learning Algorithms in Heterogeneous Environment. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 65–74. https://doi.org/10.17762/ijritcc.v11i2.6130

[38] Ahmed Abdelaziz, Machine Learning Approaches for Predicting Stock Market Volatility , Machine Learning Applications Conference Proceedings, Vol 3 2023.

[39] Rajiv, A., Saxena, A.K., Singh, D., Awasthi, A., Dhabliya, D., Yadav, R.K., Gupta, A. IoT and machine learning on smart home-based data and a perspective on fog computing implementation(2023) Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries, pp. 336-349.