International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://theaspd.com/index.php

"Advancements In Routing And Clustering Mechanisms For Next-Generation Manets: Security, Scalability, And Smart Applications

M Lakshmi Prasanna Kumar[1], M. Sunil Kumar[2]
Research Scholar, Department of Computer Science and Engineering, School of Computing, Mohan Babu University, Tirupati, Andhra Pradesh, india, 22202r010074@mbu.asia, mlpk.cse45@gmail.com
Professor & CoE, Department of computer science and engineering, School of Computing, , Mohan Babu University , (erstwhile Sree Vidyanikethan Engineering College), Tirupathi, AP, India, sunilmalchi1@gmail.com

***Abstract*:**
MANETs which stands for Mobile Ad hoc networks, which are essentially mobile wireless ad hoc networks providing routing over Link-Layer Ad Hoc networks. All nodes within a mobile ad-hoc network are free and flexible in communicating with one another as long as they are within a physical radius of each other. There has to be the cooperation among k nodes within the mobile ad hoc network so that it functions well. However, due to the inherent characteristics of MANETs, an offending node can really disrupt the routing immediately. Indeed, clustering is very vital in effectively utilizing the routing mechanism and the network lifetime for a larger scale such as MANET. Rebellion performance of the clustering phase would diminish further, if an untrustworthy node was elected as the Cluster Leader (CL). Thus, clustering MANETs is becoming a really hard nut to crack. Some other issues that need to be addressed during the election of a Cluster Leader (CL) are Node Mobility (M), Residual Energy Level (REL), and Trust Value (TV).The scope for intelligent solutions in the fields of efficiency, convenience, and traffic safety has greatly widened with recent advancements in computer systems, smart transport systems, and communications. Despite this, MANET is still susceptible to severe security attacks that are hard to counter with current protections. As it has to take network dynamics and energy limitations into account, a MANET routing protocol is an optimisation problem. Hence, for enhancing MANET security, secure routing protocols need to be formulated. This comprehensive literature review critically examines the state of routing techniques for ad hoc networks. Routing protocols can be severely challenged by cache management, even as their role becomes more critical in enabling dynamic communication in decentralised networks. This will have a direct impact on network performance and efficiency, and ultimately network quality of service. The aims of this review are to synopsize the outcomes of previous research, determine best practice, and point out any knowledge gaps which need to be addressed in further research. This paper's findings are important because they are a complete resource on effective ways of enhancing routing and clustering and point towards interesting avenues for future research.
Keywords- *heterogeneous networks, MANETs, Clustering, Cluster leader, security and Trust*

1. INTRODUCTION:

Ad-Hoc Networks have created a prominent niche for themselves in the rapidly growing wireless communication sector due to their inherent structure and working dynamism [1-4]. In contrast to common networks, ad-hoc networks work in the absence of any fixed infrastructure or centralized control. There exist several mobile nodes that can wirelessly interconnect with each other and form a MANET. Randomly moving each node within the network over a range of time intervals can be achieved. Due to this, they are especially well-suited for a range of applications when traditional infrastructure is impractical or unavailable, such as emergency response, military deployments, remote area networking, and temporary installations like conferences or festivals. Wireless Ad Hoc Networks (WANETs) [5] and MANETs [6] are two types of wireless networks that work without any prior establishment. They are mobile, unlike standard networks, and do not need routers or access points. Routing in these networks is a cooperative process as every node is involved in the transfer of data [7-8]. Nodes in such networks are mobile and work autonomously without any human intervention. Such networks can work independently of the overall internet or connect to it due to their dynamic structure, which employs different transceivers between nodes. Due to its outstanding self-forming and self-healing capabilities, MANETs, a type of WANET, are extensively used when an immediate Local Area Network (LAN) is required [9]. When devices within a Wi-Fi network communicate directly with each other in ad hoc mode, they bypass centralised servers for printing or file sharing, establishing peer-to-peer (P2P) connections [10]. When creating an ad hoc network, wireless adapters have to work independently, and all devices need to share the same c wireless frequency channel number. This type of network is beneficial in areas where there are no routers, access points, or viable wiring alternatives. Infrastructure networks are quite distinct from ad hoc networks, which are often established using Wi-Fi routers and consist of wireless access points and controllers. Sensor networks, military communications, disaster relief, conferences, emergencies, and several short-term situations where physical infrastructure is either not available or not easy to establish have all heavily utilized MANETs over the past decade [11]. MANETs, though, have built-in threats and limitations because of their dynamic nature and absence of centralized control. Some of these include high-frequency topology changes that lead to congestion, delay, and connection loss. One of the most important parameters in determining the performance of MANETs is energy-efficient multicast [12]. Because of the limited battery capacity of the mobile node, it was expected that the above strategy will result in a higher power consumption. This can severely impact the data transmission functionality of the node and lead to other issues [13]. There are privacy and security issues because the wireless communication path is solely accessible and exploitable by MANET nodes. The open characteristic of wireless media facilitates information interchange and interoperability. Open-access media are insecure since it becomes possible for a malicious user to shut down the node's communication. Multicast is a type of data transport that takes place when there are various destinations but just one source within a network. It saves band width compared to broadcast, large information exchange, real-time media consumption, and other common data applications [14]. The significance of multicast routing as a research in networking to alleviate network overhead for military use is increasing. The main issue of multicast groups is establishing a routing path for data transmission. The protocol for multicast routing aims to minimize power usage to reduce packet transmissions [15]. The network structure is typically unstable and hard to predict because mobile nodes develop spontaneously, with an active presence and mobility from the network. The fundamental structure of MANET is illustrated in Figure 1 below.

The routing mechanism of a MANET addresses finding, establishing, and maintaining a path between two mobile nodes. Packet routing can either take one of two forms: the single-hop paradigm or multi-hop paradigm. Thus, in a single-hop paradigm, the destination is assumed to fall within the communication range of the source node, and the source can directly communicate with it. In the multi-hop case, the source node communicates its message to the destination using intermediary nodes as the destination is deployed outside the communication distance of that source node [16].

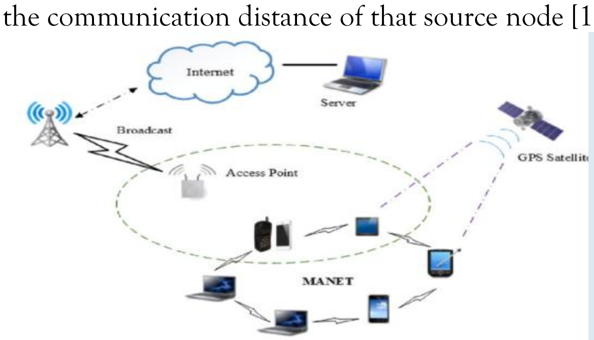

Figure 1.Basic MANET Architecture

Figure 2.Key MANET Architecture

Figure 3 MANET Characteristics

Mobile nodes usually work together to relay control or data packets from the source node toward the final destination, an easy procedure within the ad hoc framework of multiple hops. The intermediate mobile nodes that form the routes must be very helpful for route maintenance after the mobile nodes have established these routes. Therefore, it should be feasible for the routing protocols to efficiently manage routing in the MANET environment. Some challenges in route establishment from the source node to the destination node through intermediate nodes are low bandwidth, sparse coverage and connectivity (due to transmission range), high error rates, high interference, power consumption, and absence of centralized routing. Mobility, hence, changes network topology at the ever-increasing rate. Route creation between nodes through mobile intermediates would prove quite daunting. A sizable amount of work has gone into routing in MANET. Devi and colleagues [17] and Jamali and colleagues [18] Routing protocols offer a route from originator to receiver. Both the network's performance and how quickly packets are sent from source to destination are being adversely affected by different categories of network routing attacks. Kumar, Debnath, and others [19]. This type of issue can be addressed through the use of the trust route method. First, existing paths are determined by applying the route discovery method. Last, among various paths, the most reliable and best path is chosen through the use of optimisation algorithms. WSN nodes are physically spread and connected to the wireless medium, say Hu, Z. et al. [20]. The two most widespread routing methods for MANET communications are Dynamic Source Routing (DSR) [24] and AODV [10]. These protocols hinge on the extreme assumption that every node is utterly reliable and always cooperative. Though, it maximizes the risk of routing malfunction due to irresponsible nodes. To implement trust-based routing algorithms could be one probable solution [25]. The theoretical possibilities for a large variety of trust data computation open several research fronts. Thus, the authors should implement and demonstrate the proposed AODV context trust routing methods TSDR and TCOR. Ruo Jun Cai et al. [26] proposed the cutting-edge trust-based routing protocol ESCT, which simulates human cognitive mechanisms-in essence another node identifying a malicious one, would hold water only when such other node were allowed to come into the proximity of the targeted node, meaning either at the time of the source of the-data or in a transit node just entering the contact zone of the malicious node. Hence, the environment would render ESCT as useless, for example, in Vehicular Ad-Hoc Networks (VANETs), where a source is not necessarily inclined to travel to its destination. Moreover, since the protection of data transfer relies on the integrity of all nodes concerned in the network, punishing these mi-SS intermediaries involved would not be the primary focus of ESCT. This could still allow for yet another avenue of failure, particularly in cases where an evil node is awarded with malicious trust information smeared across the trusted nodes. In addition, the ESCT does not have a particular trusted route maintenance mechanism that will help to find a new path free of attackers in the event of a malicious node being encountered during transmission.

The remaining parts of the paper may be divided among further sections as follows: A literature survey analyzes thoroughly existing works in Section 2. In Section 3, the proposed routing alternatives are discussed with regards to their claimed performance. Section 4, meantime, also discusses the intended objectives of routing schemes. Finally, Section 5 gives the conclusion.

2. Related Works:

Background of the research on MANETs is explained in this section. In addition to background, nature, problems, CH selection techniques, and the implementation of the latest selection techniques, the basis of ad hoc network mobile communication is discussed. A brief description of the basic MANET routing types is discussed in Figure 4 below.

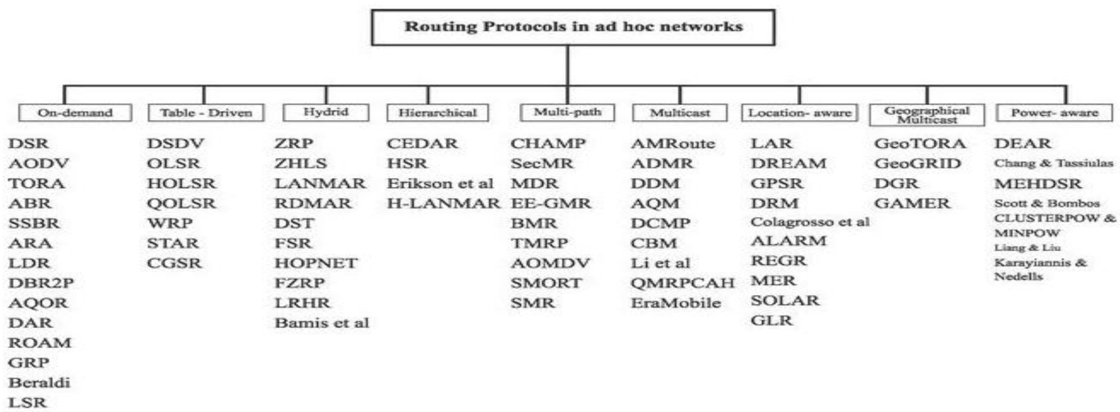

Figure 4. Basic Classification of Routing Algorithms in MANET's[48]

As per Vasseur et. al. routes metric in the context of routing protocol dimensions are qualitative metric values employed for comparing different routes under a specific routing process [27]. Therefore, when metrics are discussed related to simulation, these have generally described the intent of an algorithm; these points become very important as the locus of decision-making occurs at them. Most routing algorithms take a measure known as a hop count which refers to the number of nodes in a path. Routing metrics can typically be classified into two categories: (i) node-based routing metrics that depend on some parameters about the participating nodes, for example, energy and hop count, to select the best routes, and then (ii) link-based routing metrics which depend on all the parameters of the links to select the best routes thus: throughputs, reliability, bandwidth, etc. This study, therefore, represents a study on node-based routing metrics that consider distance for transmission, load, and energy for the purpose of enhancing efficiency in routing protocols. Energy-aware Multipath Routing Protocol (EMPR) [28]. The EMPR maximizes the resources available for the MANET by sharing information from the physical layer and MAC sub-layer to the network layer for both node energy and link bandwidth. It computes weights (w) for each node in the path and then makes the decision of which direction to go. The weight of a node consists of both energy and queue length. After that, the EMPR ranks the all existing routes according to a non-decreasing order of w and selects first N sets of the routes as primary paths to forward the network flows, while the next N sets would be treated as backup paths. The transmission of packets along multiple paths will increase the delivery percentage of packets while concurrently reducing the end-to-end delay and enhancing the throughput. As per Wenjing YANG et al, this is termed as a bandwidth-aware multipath routing protocol which regards the available bandwidth of a node to use more routes for nodes [29]. This available bandwidth of a node is determined using a BMR with a cross-layer mechanism. It could be treated as one of the statistics for discovering the routes. The available bandwidth of a node combines its local one with the local available bandwidth of the close-by nodes.BMR provides improved performance in throughput, end-to-end delay, and packet delivery ratio. Multipath Source Routing [30] was proposed by Wang I et al. using DSR and presented a multipath routing protocol delay model. They explain how load balancing can enhance the delay performance of a network. A special packet named a probing packet is periodically delivered to estimate RTT in order to follow real-time delay information on each path. Traffic distribution is the objective of this delay information. A path with greater delay will release fewer packets to ease congestion. This protocol load-balances traffic into many paths to lower the mean delay across the network. Dynamic route switching indeed caught the attention of researchers. Adaptive ad-hoc on-demand multipath distance vector [31] proposed by Ducksoo Shin et al. would be sent to solve this problem in case of a connection failure. The result is that a source node chooses a path dynamically and with respect to its latency out of many paths and evaluates how alternative paths may change from the perspectives of factors in the network. This leaves the path selection truly prioritised. Data were sent over the best primary route with its low-priority alternates. Every source node prioritises its routes in A2OMDV from highest to lowest according to the RTT value. Such management will unbundled the conflict as well as removal of the bottleneck.

Newly first introduced by Sylvie Perreau and Peter P. Pham is the Multipath Routing Protocol with Load Balance policy [32]. The primary aim of this research is to scatter traffic out over a fair use of multipaths such that they all receive an equal share of packets being congested. They develop an analytical model to account for the way on which throughput is considered on contention-based and congestion holding. Results indicated multipath routing was generally a better option when it comes to congestion and connection throughput compared to this reactive single-path based routes as it assumes the average route length to be lower than certain prescribed upper bounds determined using the analytical model.
The primary goal of the Split Multipath Routing protocol is to reduce the occurrence of route discovery processes and thus network control overheads [33]. The protocol employs a per-package allocation strategy to divide a load among multiple paths. This balancing technique based on a load is achieved by choosing cost-effective primary and alternative channels. The main path is the shortest one. The nodes of the secondary path are as disconnected as possible. This choice of path leads to a less common route discovery process for SMR, which lessens the control overhead for route failures. Alternate Path Routing [34] has the capability of load balancing and route failure protection through dispersing traffic across numerous paths. APR seems to be the best option for mobile ad hoc networks and those with limited capacity because of these advantages. APR has the ability to minimize end-to-end delay for high-traffic data streams by 20% in multi-channel cases, but the coupling issue is much more severe in single channel networks.
Minimum overhead multipath and diverse path selections Others would say AODVM-PSP in that sense incorporates the path delays in the routing decisions. The packet that the node forwards towards its destination carries information about the time the packets were transmitted. It may then be used by either destination nodes or intermediate nodes to estimate the redelayed time. To decrease congestion and transmit delay interestingly, a source node uses that time as the delay over the path explicitly defined as Pi(s,d)1/Ti(s,d), where Ti(s,d) is the transmission delay time between a source and destination nodes of the ith path. Yahya M. Tashtoush and Omar A. Darwish construct the Fibonacci Multipath Load Balancing Protocol, which uses the Fibonacci numbers to allocate packets across multiple channels via a set of mobile nodes. This distribution of packets improves the delivery ratio while reducing congestion. The FMLB protocol is assigned to the distribution of packets among the selected routes based on computations using the number of hops. Therefore, this approach finds multiple paths from the source to the destination. The length of the paths determines which paths get nominated. Those paths with minimum hops stand nominated the strongest. Fibonacci weightings are assigned to each of the paths.
The AOMDV with Load Balancing is framed by Vinod Kumar and Wahinda, which prefers a path with low hops and avoids routes with a greater number of hops for the path decision. This adaptation would work during Route Request (RREQ). RREQs get flooded to find paths, through which only those nodes are used which can construct an unimpeded way by fairly splitting the traffic. Threshold value checks on intermediate node limit usage level by queue on that node. Based on this specification, overload nodes will not accept this data packet. In other words, nodes in routes do not get overloaded with packets and, hence, do not withhold any packets. Load Balancing Hesham A. Ali et al. proposed another method of routing, Parallel Routing Protocol, intended to maximize the lifetime in MANETs by optimal load balancing. This system enables parallel transmission of data across numerous isolated channels. The protocol uses MAB for load selection and assignment. In LBPRP, the main path shall be the shortest-that is, the path with the least hops. Then, all possible rest routes remain ranked, in decreasing order, computed by value of MAB parameter with respect to travel speed, so that these rest routes are inclined to share the load as well. To distinguish between nodes' capabilities based on their remaining battery energy and the expected energy used to securely transport data packets on a given channel, Femila & Beno introduced the EPAR (Efficient Energy Aware Routing) [39] technique. Rerouting data in a highly mobile and unpredictable environment determines this. This algorithm enables the control of data transmission rates and the selection of routes with the lowest overall costs. By reducing the rate of energy consumption, the EPAR algorithm improves the performance and lifespan of the network. EPAR is a method that can reduce MANET energy usage by as much as 80%. An energy-efficient and trust-managing fuzzy EEESRP (Enhanced Energy-Efficient Secure

Routing Protocol) was presented by Malik & Rai in 2022 [40]. The suggested approach involves the distribution of keys to ensure secure data transport while using the least amount of energy possible because mobile nodes have limited energy resources. The cluster administrator creates and disperses the keys for the nodes. This model uses a node's energy value to determine how reliable it is. It is possible for every node in the network to speak to every other node. The suggested approach is tested and validated using Network Simulator-2. A protocol for centralised and on-demand clustering, the Randomised Centralised and On-Demand Clustering Protocol (RANCE)[41] was proposed by Chen et al. in 2022. It aims to extend node clustering times in mobile ad hoc networks in order to promote node collaboration while preserving energy. RANCE initially constructs a random centralised CHS mechanism, which allows any node in the local wireless network to initiate a centralised CHS mobility to maximise the selection of heads, so utilising the self-organising capabilities of the adhoc nodes. Second, by accounting for wireless network fluctuations brought on by changes in topology, obstacles, signal strength, etc., adaptive two-way heart rate packages and multi-multiple operating levels offer good cluster connection preservation. Third, to lessen the impact, RANCE uses event-based and demand-based activation instead of timed activation like LEACH-type procedures. Using the method presented by Kanagasundaram & Ayyaswamy [42], each communication node can keep an eye on the reputation factor, the suspicious factor, and the possibility of danger. The OLSR routing protocol is made more effective by adding new parameters and node energy. Security and energy efficiency were taken into account when choosing the best route (multipoint relay). In contrast to traditional energy models, this one protects and conserves energy. A new technique called Fuzzy-Enabled Particle Swarm Optimization-based Energy Efficient Algorithm (FPSOEE) for multipath routing was created to improve the quality of service in the case of a link failure. During the FPSOEE route discovery phase, the source node broadcasts the message to all adjacent nodes in order to determine the optimal path. If the route is damaged, there may be data loss and additional fees. Consequently, multipath routing—which depends on node mobility—is used by MANET. All data related to mobile nodes' energy efficiency is collected at the source node. The communication range of mobile nodes is ascertained by the source node using this information. MANET multipath routing is more efficient when an ambiguous concept is used. Zhang et al. suggested the Quantum Genetic-Based Optimised Link State Routing Protocol (QG-OLSR) [43]. The plan combined the previously suggested OLSR method for optimisation with the Q-Learning OLSR algorithm, which was implemented using MPR technology. By selecting MPR, packet data delivery rates are increased, end-to-end packet transmission latency between nodes is decreased, and network topology control energy consumption is decreased. When evaluated on ACO, smart routing enhances and saves energy. ACO lowers network latency and connection failures by confirming dispatching nodes and choosing the optimal intermediate step for intelligent routing. Using the same criterion that was used to select the coordinating nodes, the optimal dispatcher nodes are selected as the intermediate step for intelligent routing. Figure 5 illustrates the results of our systematic literature review.

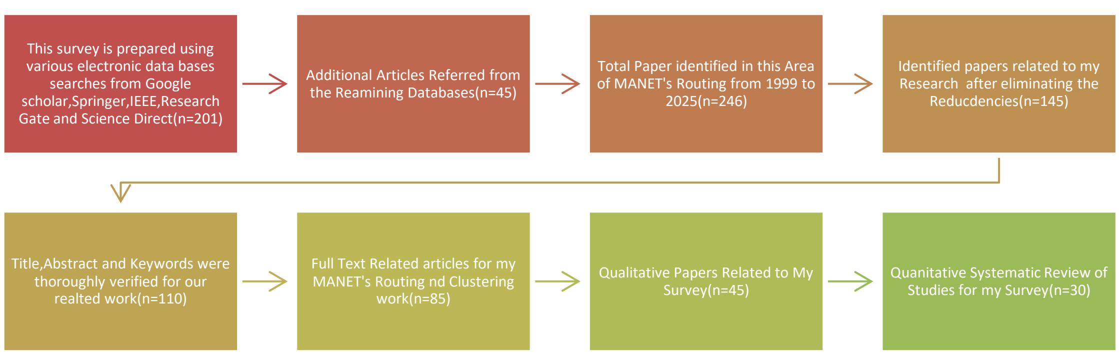

Figure 5.Systematic Literature Survey on My proposed Research

Artificial Immune System (AIS) was used by Sarkohaki et al. 2020[44] to increase the efficacy of the OLSR routing protocol. The proposed method, AIS-OLSR, integrates hop count, residual energy in intermediate nodes, and distance between nodes by combining negative selection with AIS's ClonalG algorithm. The combination of PSO and FLCR (Fuzzy Logic Controller Based Routing) was proposed by Ambika & Banga 2021 [45] for a Multiprotocol Label Switching (MPLS) based routing application on MANET. PSO optimises FLC to choose the optimal node and construct the most efficient transmission line. The proposed method is called FLCR-MPLS-MANET. Network availability, network dependability, energy efficiency, data transfer rate, and network bandwidth are used to assess this method's efficacy.

Pramila and Thebiga The Emperor Penguin Optimising (EPO) method, a revolutionary nature-inspired meta heuristics approach, was introduced in 2021[46] to solve the issue of finding a MANET routing design that satisfies QoS requirements and is energy efficient. The ideal path that meets many QoS requirements is determined by a new algorithm that was inspired by the heat output and spiral-shaped movement of Emperor penguin colonies. Although CBRP offers better performance and was created specifically for MANET use, the next section will concentrate on traditional routing methods. Using the hybrid EA for MANET, Selvakumar & Sudhakar, 2022[47] presented EECSRP (Energy Efficient Clustering with Secure Routing Protocol). The goal of the EECSRP technology is to select the best route for safe and efficient data transfer. There are two main phases to the EECSRP method. Building CHS and clusters with the appropriate mechanisms and the monarch optimisation strategy is the initial stage. In the following stage, the Grasshopper Optimisation Algorithm (GOA) is used for hill climbing in order to determine the best course in MANET. The NS2 tool will be used to evaluate the EECSRP model performance validation, and the results will be analysed from a number of angles. The experimental results demonstrate the potential performance of the EECSRP model for a range of objectives when compared to alternative approaches. The recent works in the field of quantum cryptography are compiled in table 1 below.

Table 1. Comparative Analysis of Energy-Efficient Clustering and Routing Techniques in MANET's

Author Name and Ref. No.	**Techniques Used**	**Throughput or Energy Consumption** (%)	**Major Findings**	**Limitations**
Manuel Jesús-Azabal, José García-Alonso, Jaime Galán-Jiménez	Opportunistic Mobile Ad Hoc Networks (MANETs)	Not specifically stated in the text that was extracted.	Tests conducted in the real world reveal notable variations from simulations.	It is still difficult to deploy and evaluate in practical settings.
David Samuel Bhatti, Shahzad Saleem, Azhar Imran, Hyeon Jeong Kim, Ki-Il Kim, Kyu-Chul	Simulated in NS2.30	Detection rate: 98-99%	Wormhole attacks are successfully detected and isolated by the suggested method with a high accuracy (98–99%).	The method detects and mitigates wormhole assaults after they happen, rather than preventing them in the first place.
Baidaa Hamza Khudayer, Lial Raja Alzabin, Mohammed Anbar, Ragad M Tawafak, Tat-Chee Wan, Abir AlSideiri	Evaluated based on routing overhead, scalability, and delay.	Not mentioned specifically in the abstract. Numerical results may be included in the entire document.	For greater performance, MANET routing needs to be improved; no single protocol is ideal in every situation.	High overhead and problems with scalability. route establishment-related delay. an increase in the complexity of operations.

Sudesh Kumar, Ram Shringar Raw,	Optimized Location-Aided Routing (O-LAR) protocol	lower energy consumption.	improved the effectiveness of information distribution.	When UAV swarms are extremely dynamic, performance may deteriorate. Weight function computations result in additional computational costs.
Ankita A. Mahamune, M.M. Chandane	rust-based Cooperative Routing	improved energy efficiency as a result of mitigating misbehaviour.	Enhanced effectiveness in eight important network performance measures. improved MANET routing efficiency and security.	Accurate estimations of trust metrics are essential for performance.
Ammar Kareem Obaid, Mohd Ezanee Bin Rusli	multiple academic databases	increase energy consumption	Ad-hoc networks must strike a balance between resource management, security, and caching effectiveness.	Without empirical validation, the practical application of some cache enhancements is still theoretical.
Edwin Singh C, Sharon Priya S, Muthu Kumar B	Improved Fuzzy C-Means (IFCM) Algorithm	Through the integration of trust-based routing and clustering, the OFC-TR technique successfully improves network security and lifespan.	The OFC-TR technology integrates trust-based routing with clustering to improve network security and lifespan.	The OFC-TR technique's drawbacks aren't specifically covered in the paper.
Bilal Saoud Ibraheem Shayeac	Internet of Things (IoT) for real-time data collection	5G and 6G can lower latency and increase data transfer speed.	VANETs' predictive analytics, efficiency, and traffic safety.	The majority of the conclusions are based on theoretical or simulated results; there aren't many real-world implementation studies.
Vijay U. Rathod, Shyamrao V. Gumaste	Clustering Technique	Energy Efficiency	In MANETs, the ORSMAN protocol dramatically increases the packet delivery ratio, lowers jitter and latency, and boosts throughput overall.	The ORSMAN protocol's weaknesses are not specifically covered in the paper.

Vinoth Kumar Krishnamoorthy Ivan Izonin	Energy Saving Optimization (ESO) technique	better throughput and a greater packet delivery ratio compared to traditional MANET routing technologies.	improves communication stability by offering a reliable path between gateway nodes and IoT sensors.	optimal network circumstances are assumed, which might not be the case in practical installations.

3. METRICS to be considered DURING ROUTING IN MANET'S:

The phrase "load metrics" is used to indicate a node's activity level concerning wireless media packet reception and forwarding. Processor, memory, bandwidth, energy, and load of the node are also defined. Varies load balanced ad hoc routing methods use various measures of load. They include:

(i) The total number of active routing paths supported by a node is referred to as its active path. The more active routing paths a node has, the more likely it is busier because it has to forward data packets from an upstream node to another downstream node.

(ii) The traffic volume, in terms of bytes, is the amount of traffic in the anode and its neighbours.

(iii) "Packets in interface queue" represents the number of packets buffered for the incoming and outgoing wireless interfaces.

(iv) Channel access probability is the chance of successfully accessing the wireless channel. The intensity of channel interference with neighbouring nodes is another one.

(v) Node delays are delays in packet processing, queuing, and successful transmission

(vi) Quality of service: This inherent issue with wireless transmissions is brought on by a variety of fault causes that are generated by the signals that are obtained

(vii) Self-Governing: Several independent nodes' processes are maintained without the presence of supervisory components.

(viii) Device Detection: To enable independent optimal path election, autonomous modifications are needed to locate linked and recently relocated nodes and notify them of their presence

(ix) Topology Upholding: It can be difficult to update data about the autonomous relationships between MANET nodes.

4. Objectives:

The following are the primary goals of the suggested effort, taking into account the survey mentioned above:

1. Establishing a Mechanism for Clustering Flexible and Expandable

RANCE's main goal is to create a clustering protocol which will adapt dynamically according to the changing topology of MANETs. Contrary to all those old clustering algorithms which either work with static or periodic update-based methodology, RANCE chooses cluster leaders based on a randomised centralised mechanism. This minimises the chance that at the moments of high mobility, the whole network may destabilise. In an effort to ensure that topology changes affect all routing and communication as little as possible, the protocol must also be able to dynamically form and keep clusters.

2. Improving Energy Use and Extending the Network Lifetime

Since the majority of the MANET's nodes run on batteries, energy efficiency is crucial. RANCE aims to reduce power waste, and this will be made possible by generating fewer control messages and exchanging fewer control messages during cluster creation and maintenance. Re-clustering is avoided in on-demand clustering, which further reduces battery depletion and is another energy-saving aspect of the protocol. Furthermore, cluster chiefs are chosen using a probabilistic process that prioritises nodes with higher residual energy to assume leadership positions. This balances energy consumption across the network and extends its lifespan.

3. Increase Network Stability and Decrease the Frequency of Re-Clustering

There are significant network overhead and communication interruption issues with re-clustering. Through cluster head selection that takes node degree, residual energy, and mobility patterns into account, RANCE increases network stability. In order to reduce re-clustering, this combination guarantees elected cluster heads have improved stability. Consequently, in a dynamic MANET environment, this ensures dependable communication and packet delivery rates.

4. Reduce Routing Overhead and Increase the Effectiveness of Data Transmission

The frequency of control packet exchanges for cluster or routing maintenance is another significant problem with MANETs. RANCE uses a lightweight, as-needed clustering method in an effort to reduce routing overhead. This technique will reduce the number of routing control messages by using minimal re-election protocols and stable clustering. With real-time applications like disaster response, military operations, and vehicle networks in mind, such measures will improve data transmission efficiency, lower latency, and boost overall network performance.

5. Strengthen Security Mechanisms

Recognise and counteract dangers including DoS assaults, wormholes, and black holes. Create or assess trust-based, blockchain, or cryptographic security systems.

With the use of effective routing protocols, these goals seek to overcome the core issues with MANETs and advance the creation of wireless communication networks that are more scalable, secure, and effective.

5. CONCLUSION:

This paper considers the routing of data packets as the primary challenge toward improving MANET performance, an ad hoc network that does not have any centralized management and possesses nodes moving unpredictably. Routing in place with the existing protocols is put severely under stress for this reason. There is also a working distinction of routing protocols that account for the discovery of routes and establishment into three families: The proactive approaches consist of table-driven protocols and on-demand protocols as well as hybrid approaches. In table-driven protocols, every node is to maintain a current routing table to forward the packets to any other node in the network. Such nodes are continually forced to send information so that their routing table is kept up to date. Hence overhead and scalability are the serious problems with this scenario. However, the reactive protocols do not begin their route discovery until data is to be sent. Unfortunately, it resulted in a delay time from the time the request is made for data transfer until the actual transfer can take place prior to route construction, which degrades network performance. The basic fundamental ideas and recent advances are first introduced in mobile ad hoc networks. The second part will look at the problems arising from the decentralization of mobile ad hoc networks and describe mitigation of security weaknesses in the networks. The perfected CH selection models are last but not least and consist of objectives and metrics.

REFERENCES:

1. R. Agrawal, N. Faujdar, C. A. T. Romero, O. Sharma, G. M. Abdulsahib,O. I. Khalaf, R. F. Mansoor, and O. A. Ghoneim, "Classification and comparison of ad hoc networks: A review," Egyptian Inform. J., vol. 24,no. 1, pp. 1–25, 2023.
2. T. Sharma, M. R. Kumar, S. Kaushal, D. Chaudhary, and K. Saleem, "Privacy aware post quantum secure ant colony optimization ad hoc on demand distance vector routing in intent based Internet of Vehicles for 5G smart cities," IEEE Access, vol. 11, pp. 110391–110399, 2023.
3. S. Safavat and D. B. Rawat, "On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based Internet of Vehicles for smart cities," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 8,pp. 5050–5059, Aug. 2021.
4. V. K. Quy, A. Chehri, N. M. Quy, V.-H. Nguyen, and N. T. Ban,"An efficient routing algorithm for self-organizing networks in 5Gbased intelligent transportation systems," IEEE Trans. Consum. Electron.,vol. 70, no. 1, pp. 1757–1765, Feb. 2024.
5. S. Tamizharasu and P. Kalpana, "An intelligent AODV routing with energy efficient weight based clustering algorithm (EEWCA) in wireless ad hoc network (WANET),"Wireless Netw., vol. 29, no. 6, pp. 703–2716,Aug. 2023.
6. K. Kommineni and A. Prasad, "A review on privacy and security improvement mechanisms in anets," Int. J. Intell. Syst. Appl. Eng.,vol. 12, no. 2, pp. 90–99, 2023.
7. S. Thapar and R. Shukla, "A review: Study about routing protocol of MANET," in Proc. AIP Conf., 2023, vol. 2782, no. 1.

8. M. Kaur, "Routing protocols in MANET: A review," in Proc. 2nd Int. Conf. Smart Technol. Smart Nation (SmartTechCon), Aug. 2023,pp. 1456–1461.
9. D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A review of mobile ad hoc NETwork (MANET) protocols and their applications," in Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS), May 2021,pp. 204–211.
10. N. N. Alleema and D. S. Kumar, "Volunteer nodes of ant colony optimization routing for minimizing delay in peer to peer MANETs," Peer–Peer Netw. Appl., vol. 13, pp. 590–600, Jun. 2020.
11. S. B. Kulkarni and B. N. Yuvaraju, "Node connectivity, energy and bandwidth aware clustering routing algorithm for realtime traffic multicasting in MANET," in Proceedings of the 2015 IEEE International Advance Computing Conference (IACC), pp. 760–763, IEEE, Banglore, India, June 2021.
12. P. Singh, M. Khari, and S. Vimal, "EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT," Wireless Personal Communications, vol. 126, no. 3,pp. 2149–2173, 2022.
13. U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah,and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," IEEE Access, vol. 10,pp. 14260–14269, 2022.
14. S. Pathak and S. Jain, "Comparative study of clustering algorithms for MANETs," Journal of Statistics and Management Systems, vol. 22, no. 4, pp. 653–664, 2019.
15. X. Chen, G. Sun, T. Wu, L. Liu, H. Yu, and M. Guizani,"RANCE: A randomly centralized and on-demand clustering protocol for mobile Ad Hoc networks," IEEE Internet of Internet of Things Journal, vol. 9, no. 23, pp. 23639–23658, 2022.
16. Mukta and N. Gupta, "Analytical approach towards available bandwidth estimation in wireless ad hoc networks," Wireless Networks, vol. 26, no. 4, pp. 2957–2982, 2020
17. Jamali, S.; Rezaei, L.; Gudakahriz, S.J. An Energy-Efficient Routing Protocol for MANETs: A Particle Swarm Optimization Approach. J. Appl. Res. Technol. 2013, 11, 803–812.
18. Devi, M.; Gill, N.S. Mobile ad hoc networks and routing protocols in IoT enabled. J. Eng. Appl. Sci. 2019, 14, 802–811.
19. Kumar Debnath, S.; Saha, M.; Islam, M.; Sarker, P.K.; Pramanik, I. Evaluation of Multicast and Unicast Routing Protocols Performance for Group Communication with QoS Constraints in 802.11 Mobile Ad-Hoc Networks. IJCNIS 2021, 13, 1–15.
20. Hu, Z.; Odarchenko, R.; Gnatyuk, S.; Zaliskyi, M.; Chaplits, A.; Bondar, S.; Borovik, V. Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior. IJCNIS 2021, 12, 1–13.
21. Khokhlachova, Y.; Hu, Z.; Sydorenko, V.; Opirskyy, I. Method for Optimization of Information Security Systems Behavior under Conditions of Influences. IJISA 2017, 9, 46–58.
22. Ray, S.; Mishra, K.N.; Dutta, S. Sensitive Data Identification and Security Assurance in Cloud and IoT Based Networks. IJCNIS 2022, 14, 11–27.
23. Jayalakshmi, D.S.; Hemanand, D.; Kumar, G.M.; Rani, M.M. An Efficient Route Failure Detection Mechanism with Energy Efficient Routing (EER) Protocol in MANET. IJCNIS 2021, 13, 16–28.
24. D. Johnson, Y. Hu, D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, vol. 4728, Network Working Group, Request for Comments, 2022.
25. A. Sharma, E.S. Pilli, A.P. Mazumdar, P. Gera, Towards trustworthy internet of things: a survey on trust management applications and schemes, Comput. Commun. 160 (2022) 475–493.
26. R.J. Cai, X.J. Li, P.H.J. Chong, An evolutionary self-cooperative trust scheme against routing disruptions in manets, IEEE Trans. Mobile Comput. 18 (1) (20) 42–55.
27. Vasseur J.P.,KimM., Pister K., DejeanN., and BarthelD., Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks, 2022.
28. Meng Li, Lin Zhang, Victor O., Li K., Xium Ing Shan and Yong Ren, "An Energy- Aware Multipath Routing Protocolfor Mobile Ad Hoc Networks", ACM Sigcomm, pp. 10-12, ,2025.
29. Wenjing Yang, Xinyu Yang, Guozheng Liu and Chiyong Dong, "A Bandwidth Aware Multi-path Routing Protocol in Mobile Ad Hoc Networks", Journal of Computational Information Systems, pp. 685-696, 2021.
30. Wang L., Zhang L., Shu Y., and Dong, "Multipath source routing in wireless ad hoc networks", Presented at the Canadian Conference on Electrical and Computing Engineering, Vol. 1, pp. 479-483, 2020.
31. [Ducksoo Shin, Jonghyup Lee, Jaesung Kimand Jooseok, "A2 OMDV: An Adaptive ad hoc on-demand multipath distance vector routing protocol using dynamic route switching", Journal of Engineering Science and Technology, Vol. 4, No. 2, pp. 171-183, 2019.
32. Peter Pham, Sylvie Perreau, "Increasing the network performance using multi-path routing mechanism with load balance", ELSEVIER Ad Hoc Networks, Vol. 2, pp. 433- 459, 2024.
33. Lee S.J. and GerlaM., "SMR: Split Multipath Routing with maximally Disjoint Paths in Ad Hoc Networks", Technical Report, Computer Science Department, University of California, Los Angles, 2021.
34. Pearlman M., Haas Z., Sholander P.and Tabrizi S., "On the Impact of Alternate Path Routing for Load Balancing in Mobile Ad Hoc Networks", MobiHoc"2000, August 2020.
35. Jing F., BhuvabeswarabR.,KatayamaS.,andTakahashiY.,"Amultipathon-demand routing with path selection probabilities for mobile ad hoc networks", In theProceedings of the International Conference on Wireless Communication, Networking and Mobile Computing 2021, Volume 2, pp. 1145-1148.
36. Yahya Tashtoush M. and Omar Darwish A., "A Novel Multipath Load Balancing Approach Using FibonacciSeries for Mobile Ad Hoc Networks" , InternationalJournal of Computer Theory and Engineering, Vol. 4, No. 2, April 2022.

37. Vinod Kumar R. and WahindaBanu R.S.D.,"Load-balancing Approach for AOMDV in Ad hoc Networks", IJCA Special Issue on "Mobile Ad-hoc Networks", 2020
38. Hesham Ali, Taher Hamza, and Shadia Sarhan, "Manet Load Balancing Parallel Routing Protocol" , IJCSI International Journal of Computer Science Issues, Vol. 9, No. 4, 2022.
39. Femila, L., and M. Marsaline Beno. "Optimizing transmission power and energy efficient routing protocol in MANETs." Wireless Personal Communications 106 (2019): 1041-1056.
40. Rai, Priya, et al. "Evaluation of machine learning versus empirical models for monthly reference evapotranspiration estimation in Uttar Pradesh and Uttarakhand States, India." Sustainability 14.10 (2022): 5771.
41. Chen, Xi, et al. "RANCE: A randomly centralized and on-demand clustering protocol for mobile ad hoc networks." IEEE Internet of Things Journal 9.23 (2022): 23639-23658.
42. Kanagasundaram, Hamela, and Kathirvel Ayyaswamy. "Multi Objective ALO Based Energy Efficient and Secure Routing OLSR Protocol in MANET." International Journal of Intelligent Engineering & Systems 12.1 (2021)
43. Zhang, De-gan, et al. "Novel optimized link state routing protocol based on quantum genetic strategy for mobile learning." Journal of Network and Computer Applications 122 (2021): 37-49.
44. Sarkohaki, Fatemeh, Reza Fotohi, and Vahab Ashrafian. "An efficient routing protocol in mobile ad-hoc networks by using artificial immune system." arXiv preprint arXiv:2003.00869 (2020).
45. Ambika, B. J., and M. K. Banga. "A novel energy efficient routing algorithm for MPLS-MANET using fuzzy logic controller." International Journal of Information and Computer Security 14.1 (2021): 20-39.
46. Thebiga, M., and Suji R. Pramila. "Adaptable and energy efficacious routing using modified emperor penguin colony optimization multi-faceted metaheuristics algorithm for MANETS." Wireless Personal Communications 118.2 (2021): 1245-1270.
47. Selvakumar, Muru, and B. Sudhakar. "Energy efficient clustering with secure routing protocol using hybrid evolutionary algorithms for mobile adhoc networks." Wireless Personal Communications 127.3 (2022): 1879-1897.
48. Razouqi, Q.; Boushehri, A.; Gaballa, M.; Alsaleh, L.; Abbod, M. Extended Comparison and Performance Analysis for Mobile Ad-Hoc Networks Routing Protocols Based on Different Traffic Load Patterns and Performance Metrics. Electronics **2024**, 13, 2877. https://doi.org/10.3390/electronics13142877.