Routing Algorithms: A Comprehensive Review of Classification and Security Issues in MANET

Abstract –Recent years have seen the proposal of numerous routing algorithms for potential use in a variety of application areas. In many network types, such as Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs), and other dynamic contexts, routing is a crucial difficulty. By fusing the benefits of proactive (table-driven) and reactive (on-demand) routing techniques, hybrid routing algorithms have become a notable breakthrough.

Researchers have focused on hybrid routing algorithms since traditional ones frequently fail to adjust to the changing network conditions present in MANETs. These novel methods strive to maximize speed while reducing overhead by combining the best features of proactive and reactive routing strategies. It provided a thorough analysis of these algorithms in this work, emphasizing their mechanisms, benefits, limitations, and security features. Also focused especially on the analysis of hybrid routing algorithms in a range of applications.

Keywords: Routing in MANET; Mobile Ad Hoc Networks; Wireless Sensor Networks; Hybrid Routing Algorithms; Intrusion Detection.

I. Introduction

Based on the distinct features and limitations of different network types, routing is in fact a crucial task. The decentralized, self-organizing nature of networks like Wireless Sensor Networks (WSNs)[1], Mobile Ad Hoc Networks (MANETs), and other dynamic systems frequently causes problems. Without the requirement for fixed infrastructure, mobile ad hoc networks (MANETs) are dynamic networks made up of mobile devices that can connect with one another[2].

Despite providing flexibility and quick implementation, this decentralized structure has serious problems, especially with routing. Device mobility causes frequent topological changes, making it more difficult to maintain established communication channels. Therefore, effective routing algorithms are necessary to provide dependable data transfer in these networks[3]. For less predictable routes, reactive mechanisms lower overhead by finding paths only, when necessary, while proactive techniques ensure minimal delay for routes within local or regularly accessible regions. This dual strategy enables the use of hybrid algorithms in scenarios where pure proactive or reactive algorithms often prove ineffective, such as large-scale and heterogeneous networks[4].

RoutingAlgorithms in MANET

MANETs require effective routing algorithms to create communication channels between nodes because of their multi-hop network structure, which is subject to frequent changes owing to mobility. The IETF is currently standardizing numerous alternatives that have already emerged[5]. These algorithms achieve this by regularly exchanging routing control data in response to topological changes.Mobile wireless networks without a stable infrastructure are known as ad-hoc networks. Every node function as a router and forwards traffic from other nodes; there are no fixed routers. Originally, military settings primarily employed ad hoc networks.

A MANET (Mobile Ad-hoc Network) is one type of ad-hoc network with a dynamic topology. These networks can link nodes that number anything from a few to several thousand, and they usually span a wide area. The nodes of a MANET are highly mobile, leading to constant changes in its topology and dynamic coupling in all directions. The nodes' velocity determines the rate of change. Every node in this type of network serves as a host and a router, forwarding data meant for another node. Additionally, the available transmission power is limited due to the small size of the devices[5][6].

II. Classification of Routing Algorithms

The classification of routing algorithms divides the current routing algorithms for ad hoc wireless networks into three groups based on how they update the routing information. They may be hybrid, proactive (table-driven), or reactive (on-demand)[7].

The connectionless method of forwarding packets without consideration for the desired frequency or timing of such routes is comparable to the table-driven ad hoc routing technique. Fig. 1 divides these into three categories: proactive (table-driven), reactive (source-initiated or demand-driven), and hybrid (a combination of both)[3][8].

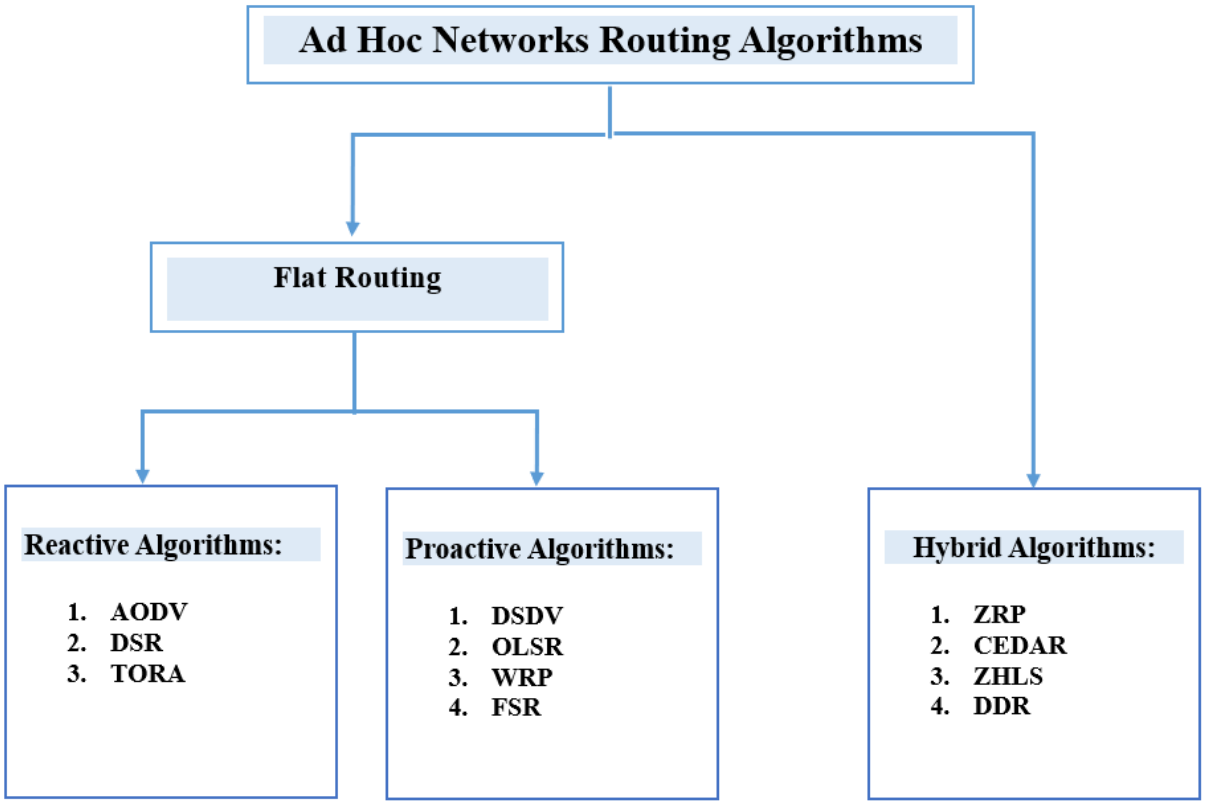

Fig. 1: Genealogy of Ad Hoc Routing algorithms[9]

Table 1. Shows the comparison of the three types of ad hoc routing techniques[10].

No.	Parameter Measure	Table-Driven (Proactive)	On- Demand (Reactive)	Hybrid
1.	Considerations for Storage	More powerful or Higher	Utilizing how several routes are required or maintained	Relevant to each zone or cluster's size
2.	Availability of Routes	Permanently accessible	calculated according to the need	Based on the destination's location
3.	Regular Route Updates	Always necessary	Not really required	utilized within all zone
4.	Further delay	Moderate	Excellent	Interzone is high while local destinations are weak.
5.	Ability to scale	100 Nodes	> 100	> 1000
6.	Coordinate Traffic	Excellent	Moderate	Weak that other two types
7.	Information Routing	Maintain in the table	Not able to store	Regarding requirements
8.	Theology of Routing	Mostly various levels	Flattered	The layered

Table 1. Provides an overall comparison of the three types of routing algorithms. In essence, the comparisons take into account the distinctive qualities of routing algorithms in networks with large traffic loads. To increase the efficiency of flat addressing, networks must reduce the amount of routing overhead. By proactively preserving intra-zone information and reactively preserving inter-zone information, the hybrid routing algorithms utilize both reactive and proactive characteristics. Using conditional updates instead of periodic ones is another method to lower routing overhead. Scalability issues will also arise with flooding-based routing protocols like DS Rand AODV in on-demand routing algorithms. Controlling route maintenance and discovery is necessary to improve scalability[10][11].

Large networks may also benefit from the performance of hybrid routing algorithms like the ZHLS. While ZRP identifies remote routes (outside the routing zone) more quickly than flooding, it proactively maintains excellent network connectivity within the routing zones. It can also use additional algorithms to perform better. Even if more recent algorithms have improved upon their predecessors, we are unable to pinpoint a single optimal approach[4].

1. Proactive Algorithms

Significantly, it regularly distributes routing tables throughout the network, maintaining up-to-date listings of destinations and associated paths. There are benefits and drawbacks specific to this category of routing methods. The ease with which nodes can obtain routing information and initiate a session is one of its primary benefits. The drawbacks include nodes storing an excessive amount of data for route maintenance and a sluggish reorganization in the event of a node link breakdown. **Table 1** presents a comparison of several current proactive routing algorithms. These come in the following varieties:

1.1. DSDV

Every node in the DSDV algorithm periodically trades its neighbor table with its neighbors. Modifications made at one network node gradually spread throughout the network. Every node keeps a table that contains the cost metric and next hope for every destination.

1.2. OLSR

Optimized link state routing reduces the overhead control packet size and quantity. Each node in this process compiles a list of its neighbors within one hop. Neighbor nodes exchange lists with each other. Every node generates its own MPR based on the received list.

1.3. WRP

Such DSDV, the WRP is a table-based algorithm that carries over the Bellman-Reactive Proactive Ford Algorithm's characteristics. Maintaining routing information about the quickest path to each destination across all nodes in the network is the primary objective. Loop-free routing techniques include wireless routing algorithms (WRP).

1.4. FSR

According to the fisheye state routing technique, a node retains path quality and accuracy for distance information about its immediate surroundings, but the amount of detail it retains diminishes as it gets farther away. By updating the network information for neighboring nodes more frequently than for distant nodes, which are outside the fisheye scope, FSR minimizes the size of the update messages.

Table 2: Proactive Routing Algorithm Comparison

No.	Criteria	DSDV	WRP	OLSR
1.	Route Updating	Periodic	Periodic	Periodic
2.	Loop Free	Yes	Yes	Yes
4.	Routing Overhead	High	High	Low
5.	Caching Overhead	Medium	High	High
6.	Throughput	Low	Low	Medium
8.	Route Tables	2	4	4

1.2. Reactive Algorithm

Instant routing creates routes when needed rather than continuously maintaining the network's most recent structure. It employs a strategy of flooding the network with control messages while finding a route. It focuses on reducing network traffic overhead and requires less routing information, but because topology changes in MANETs happen often, it generates large control packets during route discovery[12][13].

2.1. AODV

Both unicast and multicast routing are possible with AODV. AODV uses sequence numbers to ensure route freshness and prevent routing loops. AODV uses source nodes and intermediate nodes to hold the next-hop information for each data packet transmission, whereas DSR employs source routing, where a data packet contains the entire path to traverse. AODV's main benefits include self-starting, loop-free operation, and scalability to a high number of mobile nodes[14].

2.2. DSR

The two primary processes of dynamic source routing—"Route Discovery" and "Route Maintenance"—combine to enable nodes to find and maintain routes to arbitrary destinations in the ad hoc network, enabling the network to fully self-organize.

2.3. TORA

Park and Corson created the temporally-ordered routing algorithm (TORA). Based on the idea of link reversal, the Temporarily Ordered Routing method (TORA) is a distributed, highly adaptive, loop-free routing method. It defines the paths as either upstream or downstream using directed

acyclic graphs (DAG). For networks with a dense, sizable node population, this graph allows TORA to offer superior route assistance. However, TORA requires node synchronization in order to provide this capability, which restricts the algorithm's use[5]. **Table 2**Provide a comparison of some of the reactive routing algorithms currently in use.

Table 3: Reactive Routing Algorithm Comparison

No.	Criteria	AODV	DSR	TORA
1.	Route Creation	By source	By source	Locally
2.	Periodic updation	No	No	No
3.	Performance Metrics	Speed	Shortness	Speed
4.	Routing overhead	High	High	High
5.	Caching overhead	low	High	Medium
6.	Throughput	High	low	low
7.	Multipath	No	Yes	Yes
8.	Route updating	Non-periodic	Non-periodic	High routing overhead

1.3. Hybrid Algorithms

Hybrid routing combines proactive and reactive routing techniques, which is superior to using them separately. It incorporates both algorithms' benefits. For instance, by refreshing the routes of active destinations, you can enable reactive routing protocols like AODV with some proactive features. This will undoubtedly minimize overhead and delay, and the network and node performance will increase with each refresh period. Therefore, without sacrificing their own benefits, these algorithms can integrate the functionality of other protocols[15].

3.1. ZRP

Zone routing is a well-liked hybrid routing method that works best with a wide range of MANETs. Within a small area known as the routing zone, each node actively maintains routes. This algorithm uses a query-reply method to create routes. A node must first identify its neighbors in order to create distinct zones in the network. A neighbor is a node with which direct communication is possible. Intra-zone routing algorithms are based on neighbor-finding information.

3.2. CEDAR

The Core Extraction Distributed Ad hoc Routing (CEDAR) partitioning approach integrates routing and QoS support. A core node, known as the "dominator node," is a component of every partition. A set of nodes in a graph that are either present in DS or are neighbors of certain nodes present in DS is

known as the graph's dominator set (DS). The core nodes map out a path from a source to a destination using a reactive source routing method. The CEDAR process is divided into three main stages: (1) Setting up and maintaining the self-organizing routing infrastructure (core) needed to calculate routes. (2) Stable and high-bandwidth link states disperse throughout the core. (3) The core nodes execute a QoS route computing algorithm that solely utilizes locally accessible state. CEDAR accomplishes QoS routing by disseminating the bandwidth availability data of reliable links in the core sub-graph[16].

3.3. ZHLS

The hierarchical structure of ZHLS divides the network into zones that do not overlap. Geographic data determines the zone ID and unique node ID for each node. As a result, the network has a node-level and zone-level topological structure. The node-level LSP (Link State Packet) and the zone-level LSP are the two different kinds of link state updates.

3.4. DDR

In this technique, only nearby nodes exchange periodic beaconing messages, which serve to build the tree. The arrangement of these network trees resembles a forest, with the constructed gateway nodes acting as links between them. Although they are within transmission range of one another, these gateway nodes are ordinary nodes from different trees.A zone naming technique assigns a unique zone ID to each tree in the network. As a result, there are now several overlapping zones throughout the entire network.

The DDR algorithm consists of six stages: Preferred neighbor election, intra-tree clustering, inter-tree clustering, forest creation, zone naming, and zone partitioning are the first five steps. Using hybrid ad hoc routing protocols (HARP) to find routes. To find a reliable route between the source and the destination, HARP makes use of the intra-zone and inter-zone routing tables that DDR produced[17].A new class of protocols known as hybrid algorithms combines proactive and reactive algorithms. Compared to purely reactive or proactive algorithms, they may offer more scalability[18].

An arbitrary number of nodes can perform data forwarding or routing in the event that the desired path is unavailable. They typically provide hierarchical routing. Organizing the network based on network parameters is the challenge for all hybrid routing algorithms. There is a significant chance that these algorithms will be more scalable than the other two types. These algorithms aim to reduce the number of rebroadcasting nodes by establishing a zone that permits cooperation among the nodes. The best or most appropriate nodes can then carry out route discovery.

High-level topological nodes keep more routing information, which necessitates higher memory and power consumption. This is a common drawback of hybrid routing algorithms. ZRP combines the best aspects of proactive and reactive routing algorithms[19]. Table 3 presents a comparison of several current hybrid routing methods.

Table 4: Hybrid Algorithms Comparison

No.	Criteria	ZRP	ZHLS	DST	DDR
1.	Routing Structure	Flat	Hierarchical	Hierarchical	Hierarchical
2.	Multiple routes	No	Yes	Yes	Yes
3.	Beacons	Yes	No	No	Yes
4.	Route information stored in	Intra-zone & Interzone tables	Intra-zone & Interzone tables	Route tables	Intra-zone & Interzone tables
5.	Route metric	Shortest path	Shortest path	Forwarding using the tree neighbors	Stable routing
6.	Advantage	Reduced transmissions	Low control overhead	Reduced transmissions	No zone coordinator or zone map
7.	Disadvantage	Overlapping zones	Static zone map required	Root node	Neighbors may become bottlenecks

III. Security Aware Routing Algorithms

The majority of applications can use MANET, making it one of the most economically viable communication media. Apart from energy, security is another key component of MANETs; in particular, security is especially important when handling extremely sensitive data transactions[20]. Scientific research, disaster recovery, military applications, and wildlife monitoring are a few of the uses for the MANET. However, as the majority of security approaches found in the literature are computationally demanding, achieving both network security and energy efficiency at the same time is a difficult task. Applications connected to surveillance and warfare tasks need MANETs to manage a large number of sensitive transactions, so meeting their security requirements is crucial. It's intriguing to note that security is a QoS (Quality of Service) attribute, and it's true to say that

when a network's defense mechanism is weak, it allows unauthorized access, which violates the QoS restrictions. Additionally, the networks' broadcasting tendencies expose users to security risks [21][22].

The fundamental requirement for creating security-aware routing algorithms is the inherent insecurity of the physical communication link. Mobile users can benefit from the security features provided in MANETs, such as authentication, confidentiality, integrity, anonymity, and availability. Other approaches exist in the literature, and it's important to note that traditional protocols cannot handle the unique features of MANETs. Numerous research initiatives contend that there are different approaches to network security[23].

Recent years have seen the use of pricing-based techniques, trust-based security strategies, cryptographic techniques, and game-theoretic techniques to provide secure routing in MANETs. Nevertheless, the computationally demanding nature of cryptographic algorithms makes them inapplicable. Although trust-based techniques are application-specific and not dependent on MANETs, they aim to find tamper-proof hardware for each MANET node[24][25].

Due to factors such as mobile nodes, node failures, and radio channel dynamics, the links associated with a path may not always be available, thereby rendering the route invalid. There may be an additional delay in packet delivery, and there is a significant overhead in figuring out the alternate routes. Multipath routing, which provides numerous routes to a destination, successfully addresses the aforementioned issues. Therefore, given the structure and design of MANETs, it is necessary to incorporate a number of effective algorithms into the design of the multipath routing protocols[26][27].

Multipath, which transmits messages to numerous recipients from a node, is the most important function in this domain. Therefore, the research addresses multipath routing as a difficult job. More importantly, the conventional multipath algorithms failed to meet the network's needs. An intrusion detection technique rejects the intruder nodes in MANET, thereby ensuring network security. Consequently, identify and use the network's secure nodes for transmission. Lastly, the analysis shows how effective the suggested strategy is both with and without the attacks[28][29].

IV. Related Works

Many fields utilize MANET due to its rapid network building capability. Trust and cooperation between mobile nodes will make the network work. Dynamic topology and node mobility-induced

connection failures often reveal vulnerabilities, making routing challenging. Thus, MANET routing should include security measures to mitigate attacks.

J. Viji Gripsy et al.[30] Developed a secure method based on secure node discovery to prevent sequential assaults. The framework includes node authentication, secure neighbor finding and route construction, and node isolation. Findings: The packet delivery ratio and delay measure the performance of this protocol. The performance of SRD-AODV is compared with another active algorithm and AODV. Because it eliminates network attacks, has perfect routes, and prevents packet drops and connections, SRD-AODV has a PDR 4.92% higher than EDRIAODV and 12.23% higher than AODV. This is because SRD-AODV has better routes. The suggested SRD-AODV algorithm reduces E2E delay by 58.5% over AODV and 44.5% over EDRI-AODV.The hybrid cat slap single-player algorithm (C-SSA) by N. Veeraiah et al.[31]Provides safe, energy-efficient navigation in MANETs based on player trust while maintaining high performance. Fuzzy methods select initial cluster heads (CHs) based on indirect, direct, and recent trust levels. Trust levels have identified value nodes. A suggested hybrid algorithm uses CHs for multi-hop routing, selecting the best path based on latency, throughput, connectivity, and other parameters. This method should prioritize throughput over efficiency.Naji A. M. et al.[32]Outline various challenges associated with scheduling algorithms, highlighting the deficiencies that require rectification. They categorize these challenges into two distinct viewpoints: the implementation strategies of algorithms and the criteria-based metrics employed to evaluate the analysis and application of these strategies in performance assessment.

SrilakshmiUppalapati et al. [33]They developed an enhanced hybrid secure multipath routing technology specifically designed for MANETs. The suggested technique predicts cluster heads (CHs) based on the current, indirect, and direct trust levels of each network node. We use additional trust threshold-worth nodes for computation. A projected hybrid protocol utilizes the network of interconnected hops from the CHs to identify the optimal routes. The energy left in the nodes, route throughput, and path connectivity or accessibility determine the route's fitness. We select initial candidate CHs from the MANET natural environment using the Improved Fuzzy C means algorithm, giving priority to density peaks with maximum indirect, direct, and recent hope.Mallikarjuna Anantapur andVenkanagoudaC. Patil [34]Proposes a hash function with a location update approach to secure the Ad hoc on Demand Vector algorithm against selfish nodes. The Ad-hoc On-demand Distance Vector (AODV) routing mechanism transfers data packets. Thus, to prevent selfish nodes from reducing network packet loss, use a hash function with a location update technique.Saad S. Naif et al. [35]Reduce congestion in the AODV routing protocol due to connection failures and the

rebroadcasting of RREQ control packets. The MANET-related reactive protocol, Ad hoc On Demand Distance Vector Protocol, broadcasts route request packets across the network to construct a route from a source node to a target node. When a connection loss occurs, the source sends control requests (RREQ) to the network, leading to network congestion and performance degradation in this routing protocol. This study proposes a Node List (NLAODV) Node List Ad-hoc On-Demand Distance Vector routing method that uses links and path-nodes to determine if any network node is involved in route discovery for sending control packets from wireless source to wireless destination. Simulations show that the proposed NLAODV algorithm minimizes flood packets to determine the optimum network since route discovery does not require all nodes.M. Rajashanthi and K. Valarmathi[36] Propose a quality-of-service-based protected multipath routing with encryption for data transport. Additionally, the AODV-BR algorithm leverages optimal fuzzy logic for multipath routing. Grey Wolf Optimizes Adaptive Formation. Homomorphic encryption secures data key management methods to determine the optimal approach. End-to-end latency, packet distribution ratio, and other measures measure the efficiency of the strategy.H. Fatemidokht et al. [37]This research examines the use of UAVs in ad hoc mode and their collaboration with cars in VANETs to aid in routing and detecting hostile vehicles. A routing protocol named VRU is suggested to transmit packets of data between vehicles using UAVs using VRU_VU and route packets of data between UAVs using VRU. We test the VRU_VU routing components in an urban setting using the NS-2.35 simulator running on Linux Ubuntu 12.04. Additionally, we test the VRU_VU routing components in an urban setting using the NS-2.35 simulator on Linux Ubuntu 12.04. The performance research shows that the VRU protocol improves packet delivery by 16% and detection by 7% compared to other routing protocols. VRU protocol often reduces end-to-end delay by 13% and overhead by 40%.R. Nithya et al.[38]Propose a fuzzy security-aware ant colony routing optimization method for MANETs. MANET routing protocols aim to maintain a constant packet transfer ratio, minimal connection overhead, and low end-to-end latency in standard and attack scenarios. The optimized fuzzy-based ant colony optimization (ACO) algorithm for 5G makes MANET work better than AODV and other MANET routing protocols.ValantoAlappatt and Joe Prathap P M [39] Offer a trust-based, energy-efficient MANET multipath routing method. This study tests direct and indirect node and route trust and chooses the secure multipath. Trust values identify and isolate vulnerable nodes. SH2E, or secret key-centered hybrid honey encryption, protects data packets against transmission attacks. The LF-SSO algorithm must determine the optimal route from the selected multipath. Using path trust, residual node energy, and path distance to choose a route extends network lifespan. Before reaching the base station, the source node must transfer decrypted data packets to the destination node via the optimal path.Panda N. and Pattanayak B.K.[40] Brought attention to security issues.

Several techniques can solve security flaws, but evolutionary ones are the most effective. Ant colony optimization is a popular evolutionary optimization method. Our in-depth look at ant colony optimization (ACO)-based safe MANET routing algorithms could help people who study MANETs make safe routing protocols, especially when ACO is used to fix security issues.Abdali, T.A. N et al. [41]Location-aided routing (LAR) uses an enhanced traditional PSO to save energy. Simulations demonstrate that optimized particle swarm optimization (OPSO-LAR) can achieve high performance in a network setting that is comparable to the state-of-art. PSO optimizes the computation function parameter. The system also made a choice between network flooding and node coverage settings.Dsouza, Mani & D H, Manjaiah[42] Present the Energy and Congestion Aware Simple Ant Routing Algorithm (ECSARA) for data transport, which takes energy and congestion into account. The algorithm selects nodes with low congestion and high residual energy. Simulations show that the energy- and congestion-aware simple ant routing algorithm (ECSARA) boosts throughput and reduces delay in congested networks. The algorithm reduces power utilization and improves packet delivery ratios. Thus, in a denser environment, ECSARA can efficiently sustain a channel for longer and boost throughput.Veeraiah N. and Krishna.[43]Present an optimization-based complex multipath routing algorithm. The puzzle of MANET energy and security can be solved with fuzzy clustering, fuzzy Naive Bayes, and the cluster head's (CH) data collection and intrusion mitigation algorithms. The bird swarm-whale optimization algorithm (BSWOA) improves multipath routing. This routing algorithm-based method incorporates the BSA into the whale optimization algorithm (WOA), thereby enhancing multipath routing.N. A. Majedkanet al.[44]Proposed model focuses on fast crisis detection, waiting times, and regional client satisfaction. Demographics and service mechanisms make up programming algorithms. This improvement aims to investigate waiting line solutions, prevent sweeping in any outlet or accessible location, and evaluate performance.

Table 5. Summary of Related Work

Author's	Year	Scope of Work	Routing Algorithms	Advantages	Drawback
J. Viji G. et al. [30]	**2023**	Secure Route from secure node discovery, which protects from sequential attacks.	SRD-AODV	Provide security essential such as authentication, non-repudiation, secrecy, and integrity.	This strategy makes data packet routing security difficult and requires multiple solutions.

N. Veeraiah et al [31]	**2021**	Enhance fault tolerance, wireless network multipath routing is typically used instead of the original single path routing.	Genetic Algorithm with Hill climbing (GAHC).	Provide secure, energy-efficient source-to-destination routing.	Energy concerns delay will occur in cluster head selection. and needs to focus on energy issues.
SrilakshmiUppalapati et al. [33]	**2021**	Recommended to use intrusion detection, which regulates system to detect further security problems.	Cat Slap Single-Player Algorithm (C-SSA).	It ensures secure data transfer even in the presence of insecure nodes.	This strategy has to focus on energy issues.
Mallikarjuna Anantapur and Venkanagouda C. Patil [34]	**2020**	Hash function with position update secure routing algorithm for MANET.	AODV-BR, using optimal fuzzy logic, routes multipaths.	Secure routing protects data, secrecy, and non-denial of service.	This technique must address energy and delay issues.
M. Rajashanthi and K. Valarmathi[36]	**2021**	An innovative Quality of Service dependent secured multipath routing system for reliable communication of data along with encryption technique	AODV-BR protocol with Optimal Fuzzy Logic	Improve the security and speed of the ad hoc network, and UAVs identify hostile vehicles.	UAVs, despite their low costs and latency, come with various drawbacks. VANETs also need to detect malevolent vehicles.
H. Fatemidokht et al. [37]	**2022**	Developing an effective routing protocol to save time and costs is challenging due to numerous obstacles.	Artificial Intelligence Algorithms With UAV-Assisted	Maintain a high packet transmission ratio and low end-to-end latency in conventional attacks.	Energy and precise intruded node detection are priorities.
ValantoAlappatt and Joe Prathap P M [39]	**2021**	Protecting data packets (DPs) from DT assaults, the Secret key-centered Hybrid Honey Encryption (SH2E) method is used.	LF-SSO and SH2E	Provide an extremely effective secure and efficient routing.	This strategy must need to focus on energy issues.
Panda N. and Pattanayak B.K. [40]	**2020**	Addressed security issues using various algorithms, and evolutionary technique-based algorithms seem to work well.	Ant colony optimization ACO algorithm.	Focus on security issues.	This strategy needs to address energy.

Abdali, T.A. N et al. [41]	**2020**	Apply the optimized PSO (OPSO) by adopting a uniform mutation operation instead of a nonuniform one.	Energy-Aware Location-Aided Routing (EALAR)	Improve packet delivery ratio, energy use, overhead, and latency. Delays and energy use increase.	Delays and energy use increase.
Dsouza, Mani & D H, Manjaiah[42]	**2020**	Simulation findings indicate that such a modification will enhance network packet delivery and throughput.	Simple Ant Routing Algorithm (SARA) for MANET.	Enhance network throughput and packet delivery.	This strategy must address energy and security.
Veeraiah N. and Krishna [43]	**2020**	A multipath routing solution combining BSA and WOA, effectively addresses MANET's energy and security issues.	The Bird Swarm-Whale Optimization Algorithm (BSWOA).	Routes securely from source to destination.	Energy concerns will delay the cluster head selection.

Table 6. Summary of Categorization based on Security Measure in Table 5.

Measures	2020 - 2021	2021 - 2022	2022 - 2023	2023 - 2024	2024 – 2025
Secure Neighbor Discovery Nodes	----	----	----	**[30]**	----
Secure Multipath	**[35]**	**[41]**	**[31]**	----	----
Intrusion Detection	----	**[32, 36]**	----	----	----
Hash Function	**[33]**	----	----	----	----
Attack States	----	**[37]**	----	----	----
Secure Data Packets for loss	----	**[38]**	----	----	----
Secure MANET Routing	[39]	----	----	----	----

V. Discussions

This review paper presents various routing algorithms, including proactive, reactive, hybrid, and multipath-based approaches. The review includes the routing phenomena, network scenario, mobility paradigm, performance measurements, and security concerns. We assess the efficacy of different algorithms according to their scalability, dependability, and control. Reactive methodology TORA

has demonstrated considerable enhancements in scalability relative to other reactive algorithms. A proactive routing method like DSDV and OLSR employs more bandwidth but is susceptible to scalability challenges and elevated control overheads. Hybrid routing methodologies ZRP and FSR amalgamate the benefits of both proactive and reactive routing methodologies to enhance scalability, dependability, and security.

Hybrid routing methodologies exhibit reduced energy efficiency. Mobile nodes build a transient MANET network. It runs independently of infrastructure. Each network node in self-deliberate networks acts as a source or router, allowing node movement without restriction. MANET is essential for disconnected systems. To protect sensitive data, mobile ad hoc networks need strong security. Most MANET attacks are routing algorithm attacks.

Regarding the portability of many modern devices, the researchers conducted a thorough analysis to demonstrate the various routing algorithm technologies that can be used in the implementation of a network routing scheme for MANETs. The paper comprehensively examines routing algorithms, classifications, methodologies, geographical coverage, metrics, repositories, and reconfiguration strategies. This document analyzes and emphasizes the different routing methods discussed in the study.

Analyzing the frequency of the proposed methods in the routing of MANETs, one would come to the conclusion that AODV takes the lead with a mention of four, proof of its high applicability and efficiency. The other prominent methods include ACO and C-SSA, each bringing different strengths to the routing protocols.

The VRU, LAR, ECSARA, and BSWOA methods are mentioned once each; their respective benefits become apparent when applied to particular situations. Furthermore, the SRD, NL, and BR methods also come into the discussion, hence bringing out the diversity in approaches toward the challenges of MANET routing. These methods together give a glimpse of the changing landscape of routing protocols, where each focus on different aspects of improvement in security, efficiency, and network performance, as show in **Chart.1**.

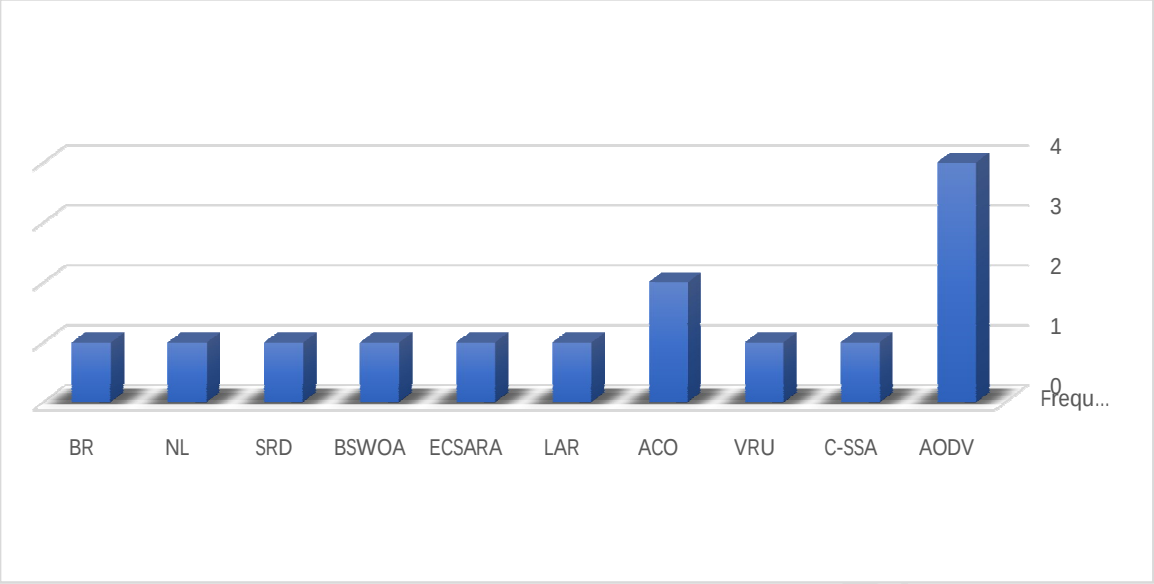

Chart1: Statistical Representation about the Proposed Method.

VI. Conclusion and Recommendations

Various MANET algorithms have been identified and discussed. Proactive, reactive, and hybrid algorithms were scanned. This evaluation addressed hierarchical, power-aware, location-aware, and other special algorithms. This evaluation addressed hierarchical, power-aware, location-aware, and other special algorithms. Developers of network simulators should incorporate the majority of these techniques from this study, allowing researchers to experiment with a select few. This will lead to the introduction of more innovative algorithms into the market. The MANET sends data to numerous nodes between the source and destination.

Security must prevent hostile nodes from accessing this data. Wireless networks employ multipath routing instead of single-path routing to improve fault tolerance. Proactive routing protocols always

have routes to all network nodes. Continuous routing becomes proactive due to its heavy routing overhead. Reactive algorithms only scan the path, when necessary, but they may generate significant traffic when networks undergo frequent changes. Hybrid or hierarchical algorithms combine the advantages of proactive and reactive algorithms, making them superior.

An algorithm is essentially a set of well-defined instructions or rules designed to solve a problem or accomplish a specific task. Think of it as a recipe: you follow step-by-step instructions to achieve a desired result, whether it's baking a cake or calculating the shortest path between two points. Algorithms are fundamental in computer science and mathematics, and they play a crucial role in various fields, including:

- **Data Processing**: Algorithms are used to process and analyze data, helping to extract meaningful information and insights.
- **Sorting and Searching**: Common algorithms in this category include Quicksort, Merge Sort, and Binary Search, which help organize data and locate specific elements efficiently.
- **Cryptography**: Algorithms are employed to secure data through encryption and decryption, ensuring privacy and integrity in communication.
- **Machine Learning**: Algorithms are at the heart of machine learning models, enabling systems to learn from data and make predictions or decisions.
- **Routing**: In networking, routing algorithms determine the best paths for data to travel across networks, optimizing performance and reliability.
- **Optimization**: Algorithms help find the best solutions to complex problems, such as minimizing costs, maximizing profits, or efficiently allocating resources.

References

[1] Y. Guo, G. Hu, and D. Shao, “Multi-Path Routing Algorithm for Wireless Sensor Network Based on Semi-Supervised Learning,” *Sensors*, vol. 22, no. 19, pp. 1–11, 2022, doi: 10.3390/s22197691.

[2] Abdul Majid, Muhammad Saim, Awad bin Naeem, Muhammad Asad Soomro, Imran Khurshid, and Muhammad Ashad Baloch, “Analysis Study of Routing Protocols in MANET for Disaster Management,” *J. Comput. Biomed. Informatics*, vol. 3, no. 02, 2022, doi: 10.56979/302/2022/51.

[3] F. Paper, A. C. Onuora, E. E. Essien, P. Ana, A. I. Federal, and E. State, “a Comprehensive Review of Routing Protocols for Mobile Ad Hoc Networks (Manets),” pp. 1–13, 2022.

[4] K. Wane, N. Chopade, and G. Rahate, “A Comprehensive Survey of Routing Techniques in MANETs,” *SSRN Electron. J.*, no. Icicnis, pp. 1–9, 2021, doi: 10.2139/ssrn.3883344.

[5] Q. V. Khanh, P. M. Chuan, V. H. Nam, D. M. Linh, N. T. Ban, and N. D. Han, “A High-Performance Routing Protocol Based on Mobile Agent for Mobile Ad Hoc Networks,” *Int. J. Interact. Mob. Technol.*, vol. 15, no. 3, pp. 30–42, 2021, doi: 10.3991/ijim.v15i03.13007.

[6] S. T. Yousif, “Simulation and Comparison of Ad Hoc Networks Routing Protocols Based on Opnet,” *Iraqi J. Inf. Commun. Technol.*, vol. 5, no. 1, pp. 42–49, 2022, doi: 10.31987/ijict.5.1.190.

[7] G. Paliwal, K. P. Sharma, D. Bhargava, and G. Paliwal, “Statistical Impact Analysis of Congestion Control Algorithm in Mobile Ad-Hoc Network Statistical Impact Analysis of Congestion Control Algorithm in Mobile Ad - Hoc Network Abstract : Kanta Prasad Sharma , PhD Deepshikha Bhargava , PhD,” no. December, 2024.

[8] J. Raja, “Comparative Evaluation of Mobile Ad Hoc Networks Routing Protocols,” no. December, 2020, doi: 10.13140/RG.2.2.29430.42561.

[9] A. A. R. Sakran, A. R. Khekan, A. F. Rashid, S. S. Ahmed, and J. A. Abbas, “Study of proactive routing protocol in wildfire detection using mobile sensor networks,” *J. Appl. Sci. Eng.*, vol. 25, no. 3, pp. 371–379, 2022, doi: 10.6180/jase.202206_25(3).0002.

[10] M. A. Mahdi, T. C. Wan, A. Mahdi, M. A. G. Hazber, and B. A. Mohammed, “A Multipath Cluster-Based Routing Protocol For Mobile Ad Hoc Networks,” *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 5, pp. 7635–7640, 2021, doi: 10.48084/etasr.4259.

[11] I. Mohamed and M. Adam, “Simulation-based Comparison between Reactive and Proactive Routing Protocols,” no. September, 2024.

[12] M. S. M. Al-dabbagh, “Exploiting Conventional MANET R outing in UAV ’ s Based Environment,” pp. 12–17, 2024.

[13] A. M. Abdelhamid and M. A. Azer, “Ad-hoc Networks Performance based on Routing Protocol Type,” *MIUCC 2022 - 2nd Int. Mobile, Intelligent, Ubiquitous Comput. Conf.*, no. June, pp. 464–467, 2022, doi: 10.1109/MIUCC55081.2022.9781747.

[14] A. M. Yassin and M. A. Azer, “Performance Comparison of AODV and DSDV in Vehicular Ad Hoc Networks,” *MIUCC 2022 - 2nd Int. Mobile, Intelligent, Ubiquitous Comput. Conf.*, no. June, pp. 402–405, 2022, doi: 10.1109/MIUCC55081.2022.9781712.

[15] T. Leenas and M. Karthik, “The Optimal Path-based AODV Routing Protocol for Mobile Ad-hoc Networks,” no. July, 2023.

[16] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, “TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network,” *Secur.*

Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/5521713.

[17] 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," *IEEE Access*, vol. 8, pp. 24019–24032, 2020, doi: 10.1109/ACCESS.2020.2970279.

[18] S. M. Alkahtani and F. Alturki, "Performance Evaluation of Different Mobile Ad-hoc Network Routing Protocols in Difficult Situations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 158–167, 2021, doi: 10.14569/IJACSA.2021.0120119.

[19] H. S. Mansour *et al.*, "Cross-Layer and Energy-Aware AODV Routing Protocol for Flying Ad-Hoc Networks," *Sustain.*, vol. 14, no. 15, pp. 1–18, 2022, doi: 10.3390/su14158980.

[20] J. J. Jayakanth, G. L. Madhumati, L. Dhanesh, P. Saranya, S. Vijayprasath, and S. Sambooranalaxmi, "International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING A Novel Approach for Intrusion Detection System Using Equalized Multi-Routing Protocol in MANET," *Orig. Res. Pap. Int. J. Intell. Syst. Appl. Eng. IJISAE*, vol. 2023, no. 6s, pp. 86–95, 2023, [Online]. Available: www.ijisae.org

[21] S. Srivastava and P. K. Singh, "A Review on Quality Assurance in MANET," no. Icacse 2021, pp. 154–158, 2022, doi: 10.5220/0010564400003161.

[22] A. H. Alsaeedi *et al.*, "Hybrid Extend Particle Swarm Optimization (EPSO) model for Enhancing the performance of MANET Routing Protocols," *J. Al-Qadisiyah Comput. Sci. Math.*, vol. 15, no. 1, pp. 1–9, 2023, doi: 10.29304/jqcm.2023.15.1.1160.

[23] F. Bensalah and N. El Kamoun, "Novel software-defined network approach of flexible network adaptive for VPN MPLS traffic engineering," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 4, pp. 280–284, 2019, doi: 10.14569/ijacsa.2019.0100433.

[24] P. V. Rao, K. S. Murthy, V. G. Krishnan, V. Divya, and K. Sathyamoorthy, "Detection of Sybil Attack in Manet Environment Using Anfis With Bloom Filter Algorithm," *Indian J. Comput. Sci. Eng.*, vol. 13, no. 1, pp. 82–92, 2022, doi: 10.21817/indjcse/2022/v13i1/221301058.

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

[26] J. A. Rathod and M. Kotari, "TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol," *Int. J. Comput. Networks Appl.*, vol. 11, no. 1, pp. 61–81, 2024, doi: 10.22247/ijcna/2024/224436.

[27] M. M. Pandith, N. K. Ramaswamy, M. Srikantaswamy, and R. K. Ramaswamy, "A

Comprehensive Review of Geographic Routing Protocols in Wireless Sensor Network," *Inf. Dyn. Appl.*, vol. 1, no. 1, pp. 14–25, 2023, doi: 10.56578/ida010103.

[28] N. Basil, S. H. Ahammad, and E. Eldesoky, "Enhancing wireless subscriber performance through AODV routing protocol in simulated mobile Ad-hoc networks," *Eng. Appl.*, vol. 2024, no. 1, pp. 16–26, 2024.

[29] S. Wang, "Multipath Routing Based on Genetic Algorithm in Wireless Sensor Networks," *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/4815711.

[30] J. V. Gripsy, A. Jayanthiladevi, N. Mahendiran, and A. S. Rini, "SRDAODV: A Hybrid Secure Routing Protocol for Mobile Ad-Hoc Networks," *Indian J. Sci. Technol.*, vol. 16, no. 32, pp. 2574–2579, 2023, doi: 10.17485/ijst/v16i32.1240.

[31] 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," *IEEE Access*, vol. 9, pp. 163043–163053, 2021, doi: 10.1109/ACCESS.2021.3133882.

[32] N. Harki, A. Ahmed, and L. Haji, "CPU Scheduling Techniques: A Review on Novel Approaches Strategy and Performance Assessment," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 1, pp. 48–55, 2020, doi: 10.38094/jastt1215.

[33] 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, no. January, pp. 14260–14269, 2022, doi: 10.1109/ACCESS.2022.3144679.

[34] M. Anantapur and V. C. Patil, "PUSR: Position Update Secure Routing protocol for MANET," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 1, pp. 93–102, 2021, doi: 10.22266/IJIES2021.0228.10.

[35] S. S. Naif, B. A. Idrees, A. J. Ibrahim, and N. A. Majedkan, "A Technique of NLAODV algorithm to get Routes of Nodes-List in Mobile Ad-hoc Network (MANET)," *Sci. J. Univ. Zakho*, vol. 10, no. 3, pp. 147–152, 2022, doi: 10.25271/sjuoz.2022.10.3.909.

[36] M. Rajashanthi and K. Valarmathi, "A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs," *Wirel. Pers. Commun.*, vol. 112, no. 1, pp. 75–90, 2020, doi: 10.1007/s11277-019-07016-3.

[37] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C. H. Hsu, "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms with UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, 2021, doi: 10.1109/TITS.2020.3041746.

[38] R. Nithya *et al.*, "An optimized fuzzy based ant colony algorithm for 5G-MANET," *Comput. Mater. Contin.*, vol. 70, no. 1, pp. 1069–1087, 2022, doi: 10.32604/cmc.2022.019221.

[39] V. Alappatt and P. M. Joe Prathap, “Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E,” *Int. J. Comput. Networks Appl.*, vol. 8, no. 4, pp. 400–411, 2021, doi: 10.22247/ijcna/2021/209706.

[40] N. Panda and B. K. Pattanayak, “ACO based Secure Routing Protocols in MANETs”.

[41] T. A. N. Abdali, R. Hassan, R. C. Muniyandi, A. H. M. Aman, Q. N. Nguyen, and A. S. Al-Khaleefa, “Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in manet,” *Inf.*, vol. 11, no. 11, pp. 1–17, 2020, doi: 10.3390/info11110529.

[42] M. B. Dsouza and D. H. Manjaiah, “Energy and Congestion Aware Simple Ant Routing Algorithm for MANET,” *Proc. 4th Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2020*, pp. 744–748, 2020, doi: 10.1109/ICECA49313.2020.9297470.

[43] N. Veeraiah and B. T. Krishna, “An approach for optimal-secure multi-path routing and intrusion detection in MANET,” *Evol. Intell.*, vol. 15, no. 2, pp. 1313–1327, 2022, doi: 10.1007/s12065-020-00388-7.

[44] N. A. Majedkan, B. A. Idrees, O. M. Ahmed, L. M. Haji, and H. I. Dino, “Queuing Theory Model of Expected Waiting Time for Fast Diagnosis nCovid-19: A Case Study,” *3rd Int. Conf. Adv. Sci. Eng. ICOASE 2020*, no. June 2021, pp. 127–132, 2020, doi: 10.1109/ICOASE51841.2020.9436601.