



REVIEW

Machine Learning-Based Routing Protocol in Flying *Ad Hoc* Networks: A Review

Priyanka¹, Manjit Kaur¹, Deepak Prashar¹, Leo Mrsic² and Arfat Ahmad Khan^{3,*}

¹Department of Computer Science and Engineering (CSE), Lovely Professional University, Phagwara, 144411, India

²Department for Program Engineering, Algebra University, Gradiscanska 24, Zagreb, 10000, Croatia

³Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, 40002, Thailand

*Corresponding Author: Arfat Ahmad Khan. Email: arfatkhan@kku.ac.th

Received: 26 September 2024; Accepted: 08 January 2025; Published: 17 February 2025

ABSTRACT: “Flying *Ad Hoc* Networks (FANETs)”, which use “Unmanned Aerial Vehicles (UAVs)”, are developing as a critical mechanism for numerous applications, such as military operations and civilian services. The dynamic nature of FANETs, with high mobility, quick node migration, and frequent topology changes, presents substantial hurdles for routing protocol development. Over the preceding few years, researchers have found that machine learning gives productive solutions in routing while preserving the nature of FANET, which is topology change and high mobility. This paper reviews current research on routing protocols and Machine Learning (ML) approaches applied to FANETs, emphasizing developments between 2021 and 2023. The research uses the PRISMA approach to sift through the literature, filtering results from the SCOPUS database to find 82 relevant publications. The research study uses machine learning-based routing algorithms to beat the issues of high mobility, dynamic topologies, and intermittent connection in FANETs. When compared with conventional routing, it gives an energy-efficient and fast decision-making solution in a real-time environment, with greater fault tolerance capabilities. These protocols aim to increase routing efficiency, flexibility, and network stability using ML’s predictive and adaptive capabilities. This comprehensive review seeks to integrate existing information, offer novel integration approaches, and recommend future research topics for improving routing efficiency and flexibility in FANETs. Moreover, the study highlights emerging trends in ML integration, discusses challenges faced during the review, and discusses overcoming these hurdles in future research.

KEYWORDS: FANET; protocol; machine learning

1 Introduction

Flying *Ad Hoc* Networks (FANET) is a new wireless *ad hoc* network using Unmanned Aerial Vehicle (UAV) nodes. UAVs are essential for surveillance and reconnaissance, wireless communication, geographical mapping, agricultural study, and smart transportation systems. FANET comes from Vehicular *Ad hoc* Network (VANET) and Mobile *Ad hoc* Network (MANET). So, it extends many features from this network. Features such as moving node, limited energy, and topology but with their uniqueness such as: High mobility of nodes, Dynamic topology, Sparse network, Three-Dimensional deployment, Small size with limited energy, Integration with ground station/satellite, Maintain low latency, Line-of-sight communication, Multi-hop communication, Rapid development, High bandwidth.

For comparison, integrating FANETs with VANET to improve transportation efficiency has become an interesting subject of research. VANET nodes are widely dispersed, causing frequent connection issues. “Unmanned aerial vehicles” may act as relay nodes to restore vehicle-UAV communication after separation. Intelligent transportation systems need “Cognitive Radio (CR)” [1]. The researcher is endeavoring to



integrate Machine Learning (ML) techniques into the FANET network to facilitate efficient routing, which is necessitated by its frequent topology changes, energy constraints, and high mobility.

ML has the capacity for real-time decision and data-driven optimization, that enables energy-efficient and delay-tolerant routing protocol with predictive maintenance of energy and mobility of nodes, with robust communication strategies during unforeseen conditions like node failure. For energy optimization, ML-based nodes use sleep-awake methodology, which means if nodes are not participating in any tasks inside FANET, they go to sleep to reduce energy consumption. Also, it works not only for routing but with using ML techniques, various other tasks can be performed such as security of network/nodes, energy management, network reliability, and better self-decision. ML-based routing protocols enhance routing decisions using data-driven methods. ML-based protocols use predictive modeling, context-aware modifications, and optimization to adapt to FANETS' dynamic conditions. Historical and real-time data anticipate node behaviors, optimize network resources, and identify abnormalities. This creates durable and efficient routing strategies. FANETS' continuously changing and complicated environments need adaptability for dependable communication.

Over the last decade, UAVs have been deployed in many applications and services. Drone or UAV connections can carry out intricate operations and create FANETs. It is a tiny portion of VANET and MANET [2]. These systems share characteristics such as portable devices, wireless communication channels, distributed control, and the ability to transmit data across several intermediate nodes [3]. Nevertheless, a FANET has distinctive characteristics like rapid node migration, frequent topology changes, and a sparse network. Fig. 1 depicts a FANET. This network has many uses in both military and civilian domains. Military uses include protecting the public, intelligence gathering, tracking targets independently, border checks, estimating wind conditions, ensuring internal security, fighting fires, traffic monitoring, remote sensing, and communication networks [4]. Moreover, drones possess several business uses in civilian domains, including but not limited to film production, agricultural surveillance, online delivery, transportation, and monitoring of architecture and infrastructure [5].

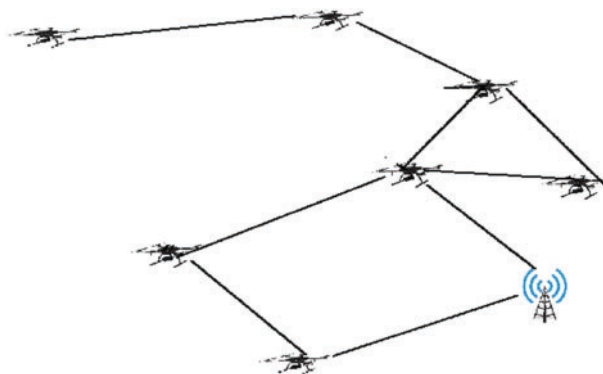


Figure 1: Flying *ad hoc* network

Developing a robust routing protocol is a critical research undertaking in FANETs because of their unique characteristics, such as a highly dynamic topology, rapid node movement, and frequent disconnection. The routing method typically involves addressing the question “How do unmanned aerial vehicles (UAVs) transfer information packets from the point of origin to the destination?”

Without a direct connection between the point of destination and the source of information, the data packets may be transmitted through intermediate nodes, functioning as routers, to reach the intended

destination [6]. The routing route, as defined, is a sequence of hops, which are intermediary nodes that transmit data packets [7]. A routing protocol is tasked with establishing a path from source to destination. In addition, protocols must effectively handle connection failures by identifying suitable alternate routes. FANETs have several issues that might impact the routing process. Routing protocols are required to address the problems associated with sporadic connections, frequent changes in network structure, network fragmentation, and relocation of nodes [8,9]. It also needs to consider energy usage, processing capability, and latency. These protocols must be scalable, self-healing, and free-looping. Communication quality is affected by the three-dimensional environment in which unmanned aerial vehicles operate [10]. Designing routing protocols in FANETs is a significant problem. Recent efforts by several scholars have focused on enhancing the efficiency of the FANET routing technology. Despite several efforts in this domain, designing a system of routing that ensures effective interaction in these networks remains a highly challenging task [11].

Machine learning can solve numerous problems, including FANET routing. ML can be divided into three categories: “Unsupervised Learning (UL)” “Supervised Learning (SL)”, and “Reinforcement Learning (RL)”. SL trains the model to detect correlations between labeled training data to reliably anticipate the problem’s solution using unlabeled data [12]. Train a model utilizing starting data to reliably predict future data labels. UL seeks data sample patterns. Although the approach necessitates an unprocessed dataset, reinforcement learning” can acquire knowledge about the environment without data samples. “Reinforcement Learning” shares similarities with human learning, even though it does not use extensive datasets and the trainee agent lacks awareness of data labels. Without a dataset, RL learns by interactions in its surroundings. This prevents supervised and unsupervised learning from finding FANET routing solutions [13]. Neither supervised nor unsupervised learning methods can learn from failed connections or routes without a dataset. Due to its capacity to handle dynamic and real-time environments, reinforcement learning is ideal for FANET. RL can learn about FANETs and node communication links. FANET routing modeling is difficult. Since no dataset exists for model training, supervised and unsupervised learning algorithms must be developed to imitate this process. The model is trained using this dataset. Reinforcement learning is the sole ML technique capable of acquiring routing knowledge without a dataset. Trial and error is used in reinforcement training to find a network route model.

This approach has the potential to streamline both supervised and unsupervised to replicate and effectively address this issue in FANETs.

UAVs can be autonomously controlled by an integrated controller or remotely controlled by a ground station operator. It also propagates well in networks. Fig. 2a,b shows that UAV networks may be single or multi-UAV. Large UAVs directly connected to a ground control center and/or satellite network are called single-UAV networks. This network is often utilized for specific activities. For communication with the ground control station, UAVs must have complex hardware technologies. The procedure would cease if the UAV fails [14].

A multi-UAV network is a collection of interlinked UAVs positioned on the top of sensors, a base station, and an orbital satellite. In terms of redundancy, dependability, finishing of the assigned task, and durability the performance of a multi-UAV network surpasses that of a single-UAV system. This implies that in case, one of the UAVs fails, the other UAVs can sustain operations [15]. Furthermore, UAVs in multi-UAV systems can be implemented in several topologies, depending upon the specific needs.

The addition of more UAVs to the infrastructure allows for the expansion and adjustment of a multi-UAV platform’s connectivity [16]. Several UAVs work together in this FANET-style network using an inter-UAV radio communication interface [17]. Conversely, creating a reliable communication architecture for multi-UAV systems is a challenging task.

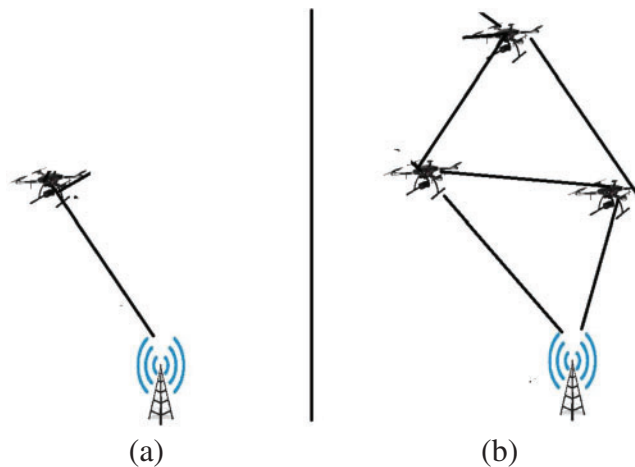


Figure 2: (a) Single-unmanned aerial vehicles network; (b) multi-unmanned aerial vehicles network

Multiple reviews of FANET routing methods are given in references. [Table 1](#) summarizes these assessments' primary strengths and weaknesses. This study addresses FANETS-specific topology-based routing protocols that have not been previously studied. This article addresses the latest routing protocol core properties, limitations, routing algorithms, and application situations. To attain the desired goals, an effort was made to include extensively analyzed and intellectually stimulating solutions of FANET routing approaches. This was done to provide interested researchers with accurate and tangible deductions. The highlights of this research are outlined as follows:

- i. A comprehensive examination of the current optimal routing methods in FANETs based on topography. This research reviews and compares topology-aware routing methods designed specifically for FANETs, in contrast to prior research which focuses on classical routing techniques.
- ii. Segmentation of topology-based protocols for routing for FANETs according to the fundamental routing operations. Considerable analysis and documentation have been conducted on a comprehensive set of 22 topology-based protocols for routing, encompassing both existing and emerging ones.
- iii. The quantitative evaluation of topology-based protocols for routing is conducted by considering their fundamental characteristics, routing mechanism, limitations, mobility models, tools for modeling, operational aspects, and applications. The current study does not compare and analyze data using all these factors. This comparison can help engineers and researchers choose the best topology-based routing protocol.
- iv. The present active research effort in the field of FANETs informs the identification of the primary research challenges and considerations in developing a topology-based routing system.

The dynamic and unpredictable nature of the FANET environment is a significant obstacle to the deployment of machine learning-based routing strategies. FANETs provide a unique difficulty due to aerial nodes' quick movement and mobility. The network topology changes often, making it challenging to develop and sustain stable and efficient routing systems. ML algorithms need to continuously adapt to changes and learn from massive amounts of temporal data while implementing routing decisions. Algorithm stability and scalability under various operating conditions, low-latency decision-making, fluctuating connection quality, and intermittent connections make the problem harder.

Table 1: A summary of recent works reviewing routing protocols in FANETs

S. No.	Reference/ Publication year	Analysis and comparison of routing protocols	System of classification of mobility models	Routing challenges	Communication links of FANET	Routing protocols	Comparison analysis of mobility models	Open issues
1	[11]	X	X	X	✓	✓	X	✓
2	[13]	✓	X	X	✓	✓	X	✓
3	[18]	✓	X	X	X	✓	X	✓
4	[19]	✓	X	X	✓	✓	X	✓
5	[20]	✓	X	X	✓	✓	X	✓
6	[21]	X	X	✓	✓	✓	X	✓
7	[22]	X	X	X	✓	✓	X	✓
8	[23]	✓	X	✓	X	✓	X	✓
9	Present work	✓	✓	✓	✓	✓	✓	✓

This review paper aims to conduct a methodical examination and consolidate current research on machine investigation of learning-based algorithms for routing in flying *ad hoc* systems. The concentration is on exploring the way machine learning can effectively address the distinctive difficulties encountered in a dynamic and highly mobile environment. This paper presents an exhaustive survey of various ML-based techniques applied to routing in FANETs, emphasizing how effective they have been in terms of routing efficiency, adaptability, and scalability.

Machine learning is becoming one of the excellent tools for the FANET network, due to its intelligent decision which enhances performance, reliability, and efficiency. FANET which is highly dynamic, with energy constraints needs ML-based solutions in route optimization, energy management, network stability, collision avoidance, security enhancement, scalability, and environment awareness. For route optimization, reinforcement learning is used which predicts the node effectively as per prior knowledge gained. For energy management, energy-efficient machine learning-based algorithms are used, which allow nodes to sleep, while no task is there to perform. For collision avoidance and network stability, clustering-based routing algorithms are implemented, which reduce network overhead also. To enhance security, various machine learning techniques are used, especially supervised learning.

The major contributions made are in identifying strengths and limitations in various ML-based approaches, proposing new integration techniques, and suggesting future research directions to overcome gaps existing in them. The review shall therefore consolidate available knowledge and make a critical contribution to the advancement of robust and intelligent routing methods for FANETs. This study aims to fill these gaps through the following contributions: Scalable Framework, Transparent Decision Processes, Dynamic Adaptability, Energy Efficiency and Optimized Decision-Making.

This paper gives an extensive study of the literature, having a specific analysis of Routing protocol and machine learning: Exploring the recent research trends. The study offers a thorough examination of the existing literature and presents a methodology that utilizes rigorous research techniques such as Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) to investigate and evaluate FANET. The material also includes the findings and analysis high derived from the investigations.

2 Research Methodology

The current work is aimed at making an extensive literature review for the research articles published within 2021–2023, which means the review is marked for previous 3 years research articles on Routing protocol and machine learning. The methodological flow is being presented in the form of the PRISMA model which shows the screening process for the entire literature analysis/systematic review. The initial phase of the systematic review is the planning phase which includes making questions for the requirement of the

review and also presenting a defined search strategy so that the defined database can be surfed. Based on the search strategy, the literature search was conducted for 3 years for the SCOPUS database for defined keywords as 'Routing protocol and machine learning'. Based on the search strategy and following all exclusion and inclusion criteria the final data is retrieved. The next and last phase of the process is the analysis phase based on clustering the literature is analyzed and grouped into some common categories.

2.1 Planning Stages

ML-based routing protocols in FANETs use advanced algorithms to overcome the obstacles given by aerial networks' dynamic and frequently changing nature. FANETs, which are differentiated by high mobility, variable link quality, and intermittent connection, need complex routing algorithms that can adapt to frequent topology changes and unexpected situations. ML gives smart solutions that can be easily adapted in case of changing topology, mobility, and link quality. RL is recently popular in FANET, learns quickly, and generates optimal paths in a real-time environment, creating routing mechanisms. Growing techniques like unsupervised learning, supervised learning, deep neural networks, and hybrid ML can work well in reducing delay, increasing packet delivery, and energy management. But routing protocol and machine learning are still an unsolved domain that needs huge exploration to understand the applicability and solutions provided. The current is aimed at providing the subject or topic overview with the help of proper citations of recent publications and good priority journals. Literature analysis gives insight into how ML can recreate the future of FANETs from a single UAV to a large-scale, dynamic network.

The work explores the applicability of Routing protocol and machine learning and shows the growing technical advancement in the field with some bibliometric trends for the domain. The presented work can certainly mark a positive presence to better understand the current, and past and make valid predictions for future timelines based on analyzed records for the literature. The presented literature analysis marks the resolutions for the research questions provided below:

- i. What is the year-wise trend for publication for Routing protocol and machine learning?
- ii. What is the country-wise trend of publication for Routing protocol and machine learning?
- iii. What are the various techniques used for machine learning?
- iv. Which feature extraction technique best fits the process to present an efficient framework for machine learning?

The current research has used key terms such as Routing protocol and machine learning for exploring recent research trends and has counted 3 years timeline. The literature search is conducted for the SCOPUS database and keyword matching is considered for title match reason is the keywords Routing protocol and machine learning are frequent and popular terms and have shown huge retrieved results.

2.2 Review Stages

The current stage is to mark the inclusion and exclusion criteria for the literature search, the defined criteria are better shown as under:

- i. Search is made for the year 2021–2023 for the SCOPUS database,
- ii. Excluding the document other than the article,
- iii. Excluding the research papers whose publication stage is not final,
- iv. Excluding the paper which is in other than English language.
- v. Excluding the research papers which are not open access nature.

In the final stage, the remaining list of research articles was accessed and explored thoroughly to present a literature analysis for the fulfillment of the defined research questions. The figure below shows the PRISMA model for the literature search and screening.

Fig. 3 presents a systematic procedure for choosing publications to include in a final assessment, using particular criteria for retrieval with PRISMA. The PRISMA framework can be used to systematically identify, document, and analyze information from journals, whether the focus is on specific types of journals (e.g., open access, high-impact, or discipline-specific) or the articles published in them. PRISMA makes the selection process transparent and reproducible, which is essential for identifying journals relevant to a research question or systematic review. The initial phase entails conducting a search using certain keywords relevant to both Routing protocol and machine learning in the abstracts of articles that appeared in the SCOPUS repository between the years 2021 and 2023. The initial search produces a total of 474 results. This leads to an initial set of records. The starting filtering process eliminates non-article documents, resulting in a reduction of the collection by 459 records, leaving a total of 15 articles. Literature records only 166 articles written in English are selected and only 1 article is excluded. The subsequent stage focuses exclusively on papers that have reached the final publishing stage, further reducing the pool by 6 records. As a result, papers that are not accessible for free access are eliminated, resulting in the removal of an extra 84 files. All inclusion and exclusion are defined in Table 2. After going through the procedure, a final list of 82 papers is generated which is also available as supplementary materials. These papers match all the criteria and are being selected for the final evaluation.

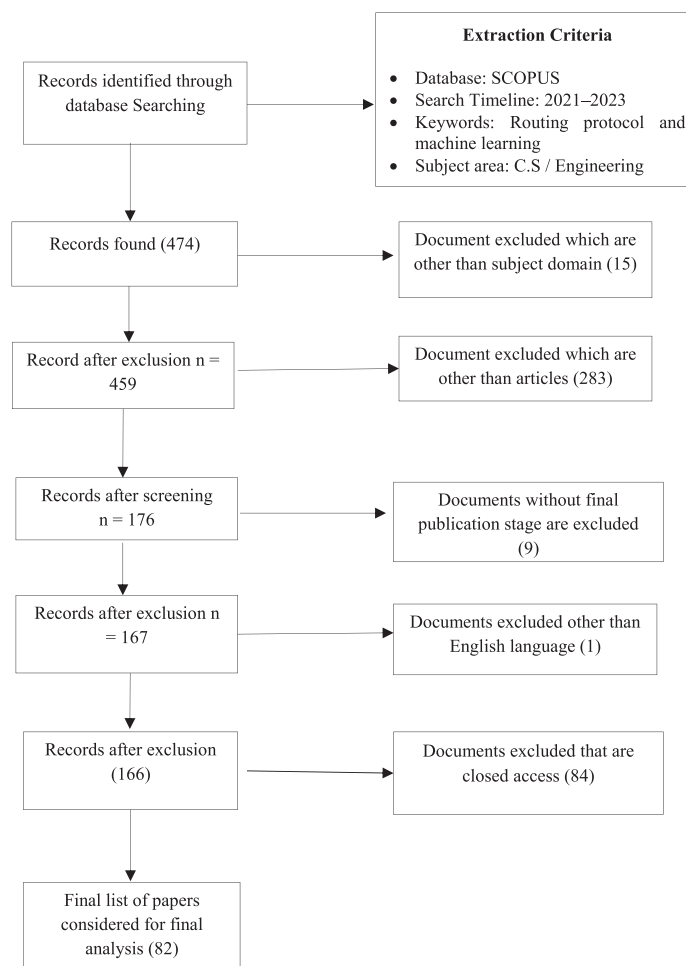


Figure 3: PRISMA model for the literature analysis

Table 2: Criteria for inclusion and exclusion

Criteria	
Inclusion	<ol style="list-style-type: none"> 1. Publication must be written in English. 2. The papers' publication years range from 2001 to 2023. 3. Keywords must be present in the abstract of the paper.
Exclusion	<ol style="list-style-type: none"> 1. Articles not explicitly focusing on standard FANET routing or FANET routing based. 2. Closed-access articles are excluded. 3. Pending final publication is rejected.

3 Literature Analysis

As per the facts analyzed in the demonstrated literature, various key points and dimensions have been seen in Routing protocol and machine learning. The dataset used, key techniques for feature extraction/selection, techniques used for preprocessing, featured techniques for optimization and recognition, also the literature have marked the channel towards the key consideration of techniques such as Deep learning and Machine learning. Based on the above shown variables or factors the retrieved literature is analyzed. The literature gathered from the defined themes is analyzed and assessed to provide a comprehensive analysis and a relevant recommendation for future study on the Impact of Routing protocol and machine learning. The determinants of Routing protocol in this study are perceived to be the quality of services and convenience of use. These predictors have been supported and examined by several literature studies, which are assessed below through thematic analysis and evaluation. The literature is also well explored based on some bibliometric data in a pie-chart format and textual as well. Documents searched for the subject base, year-wise research publication, country country-wise publication trends for subject-oriented research.

Fig. 4 presented is a Pie Chart titled "Documents searched by Subject Area", showcasing the distribution of document searches across various academic disciplines. The chart is laid out with the subject areas and the percentage of documents searched. The pie chart depicts the pattern of data distribution across different academic fields. The highest frequency is observed in Computer Science with a value of 39%. Engineering follows with a frequency close to 28%. Materials Science and Mathematics have significant frequencies, recorded at 9% and 7%, respectively. Physics and Astronomy show a value of 4%, while Biochemistry and Chemistry are both at around 3%. Disciplines such as Genetics and Chemical Engineering exhibit minimal frequencies close to 2%. Other fields, including Social Sciences, Business, Management, Energy, Decision Intelligence, Earth Sciences, Environmental Science, Health Care, Medicine, Neuroscience, and Nursing, all have negligible frequencies, generally around 1 or less.

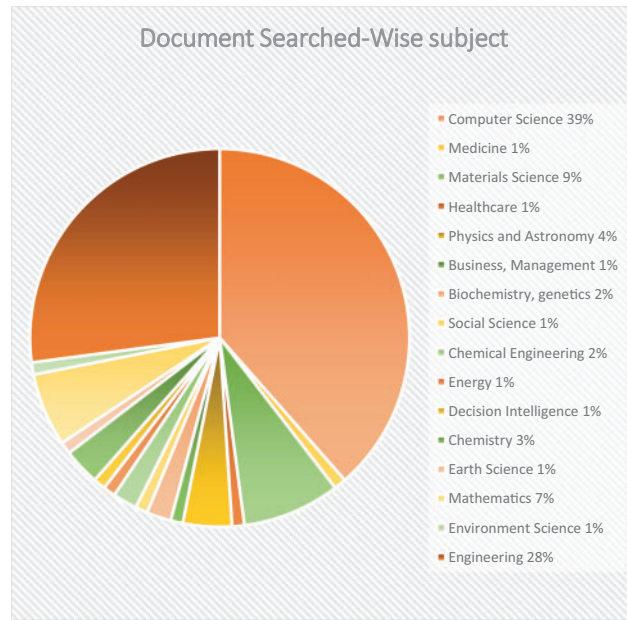


Figure 4: Subject-based research paper retrieved

Fig. 5 demonstrates the “Documents Searched by Country” shows the number of documents searched across various countries. In the pie chart, there are approximately 20 countries are considered. The United Kingdom stands out with the highest value at approximately 39% followed by Saudi Arabia, which holds a value of 11%. Malaysia is next with a value close to 8, while the United States registers around 6. Canada and Spain each display values between 4 and 5. The remaining countries including Iraq, Brazil, Ethiopia, Kuwait, United Arab Emirates, Colombia, France, Italy, Jordan, Nigeria, Poland, Romania, Sri Lanka, and Tunisia are all situated between 1 and 3 on the scale. Overall, the pie chart demonstrates a steep decline in values after the United Kingdom, with Saudi Arabia significantly lower, and a more gradual decrease among the other listed nations.

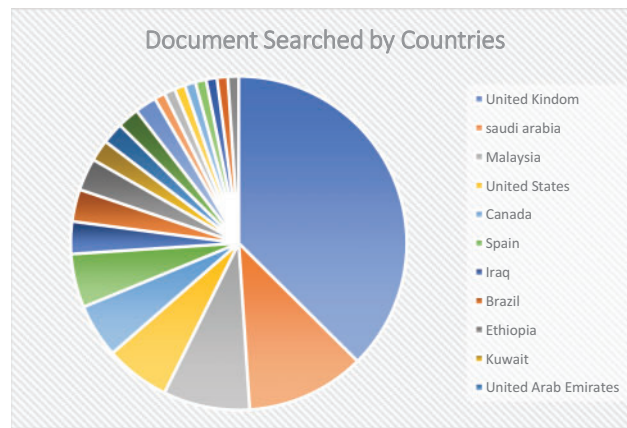


Figure 5: Country-based research paper retrieved

Fig. 6 asserted the year-wise publication trends from 2021 to 2024. It shows the number of publications for each year, with 2023 having the highest number of publications, which comes out to be 38%. The year 2022 follows with around 32% of publications, while 2021 shows a lower count, nearly 23%. The year 2024 has the fewest publications, with less value & percentage recorded so far. This trend indicates a significant peak in publications in 2023, followed by a decline in subsequent years.

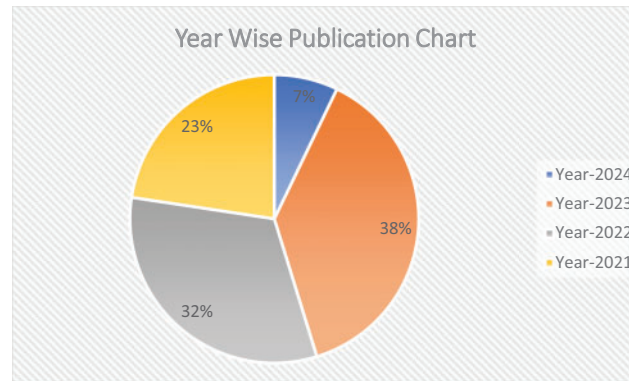


Figure 6: Year-wise research paper retrieved

3.1 Literature Depiction ML Techniques for Routing Protocols and Machine Learning

The literature review covers a wide spectrum of works aiming at many facets of routing protocols and machine learning applied using different ML techniques and approaches shown in Table 3. Reference [24] employs a Machine Learning-based Multi-Class Classifier to handle multiple classification tasks. Reference [25] uses Density-Based Spatial Clustering of Applications with Noise (DBSCAN) for clustering data based on density for a secure network by detecting malicious neighbors. Reference [26] applies a Smart Contract Incentive Algorithm, integrating ML into smart contract mechanisms. Reference [27] enhances the Extreme Learning Machine (IELM) to improve learning efficiency. Reference [28] combines K-means Clustering with hybrid optimized ML approaches for better data segmentation. Reference [29] uses Support Vector Machine (SVM) for mischievous nodes and reference [30] utilizes the Ant Colony Algorithm. Reference [31] introduces Incremental Machine Learning Approaches with concept-drift detection mechanisms like Adaptive Windowing (ADWIN), Drift Detection Methods (DDM), and Early Drift Detection Method (EDDM). Reference [32] focuses on Deep Learning, particularly Deep Neural Networks (DNNs) for complex pattern recognition. Reference [33] utilizes Neural Networks for various ML tasks. Reference [34] applies Decision Trees to find a trusting node and discard the doubtful node from the network. Reference [35] uses OS-ELM (Online Sequential Extreme Learning Machine) in conjunction with Q-Network (QN) and Deep Q-Network (DQN) for reinforcement learning [36] to explore general Machine Learning Algorithms for various applications. Reference [37] employs Deep Learning Models including the YOLO Image Classifier (YOLOv3) for object detection. Reference [38] integrates Deep Learning and Machine Learning techniques for enhanced model performance. Reference [39] applies Machine Learning Algorithms within Digital Twin Networks (DTNs) for simulated environments. Reference [40] develops ML-AODV, a hybrid approach combining ML with the AODV routing protocol. Reference [41] implements K-means Data Clustering for organizing data into meaningful groups. Reference [42] explores various Learning-Based Approaches for different ML problems. Reference [43] applies CatBoost (GBDT) for gradient boosting tasks. Reference [44]

employs multiple techniques, including K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision Trees (DT), Linear Discriminant Analysis (LDA), Naive Bayes (NB), and Convolutional Neural Network (CNN), for diverse machine-learning tasks. Reference [45] focuses on IPv6-based RPL (Routing Protocol for low-power and Lossy Networks) for low-power network environments. Reference [46] introduces e-RLRP (Enhanced Routing Protocol based on Reinforcement Learning), reference [47] combines DTN (Delay-Tolerant Networking) with Greedy Perimeter Stateless Routing (GPSR). Reference [48] uses Reinforcement Learning for adaptive learning. Reference [49] utilizes LSTM (Long Short-Term Memory) networks for reducing time and sequence data.

Reference [50] proposes Group'n Route (GnR) for group-based routing strategies and reference [51] combines Supervised and Semi-Supervised Deep Learning methods for enhanced learning. Reference [52] develops a Self-Organizing Network (SON) for dynamic network management. Reference [53] integrates support Vector Machine with Harris Hawks Optimization (SVM-HHO) for improved classification performance. Reference [54] focuses on RPL integrated with WOABC (Whale Optimization Algorithm-Based Clustering) and reference [55] explores a Machine Learning (ML) Mechanism for general optimization. Reference [56] uses Restricted Boltzmann Machine (RBM) and LSTM for advanced learning and prediction tasks.

Reference [57] utilizes both the K-means Algorithm and K-medoids Algorithm for clustering and partitioning data. Reference [58] applies Reinforcement Learning (RL) and Q-learning algorithms to optimize decision-making processes. Reference [59] focuses on K-means Clustering for data segmentation. Reference [60] uses the Random Forest Classifier for robust classification tasks. Reference [61] implements Reinforcement Learning (RL) for adaptive learning and decision-making. Reference [62] proposes the Improved Efficient Shuffle Bidirectional COOT Channel Attention Network for advanced neural network tasks.

Reference [63] explores variations of RPL, including its integration with DODAG (Destination Oriented Directed Acyclic Graph), and reference [64] explores General Machine Learning Algorithms for various applications. Reference [65] employs SVM, KNN, and Logistic Regression (LR) for classification and regression tasks. Reference [66] uses Q-learning combined with Fuzzy Logic for adaptive learning and decision-making. Reference [67] explore OS-ELM and Penicillium Reproduction Algorithm (PRA) for dynamic learning tasks. Reference [68] applies the K-means Clustering Algorithm for data clustering and reference [69] explores WiCHORD+ enhanced protocol in the non-wired network. Reference [70] focuses on reinforcement learning to learn optimal policies. Reference [71] uses Incremental Online Learning Algorithms like Adaptive Random Forest (ARF) and KNN for evolving learning tasks. Reference [72] employs Collaborative Learning techniques for shared learning across multiple models. Reference [73] applies Forest Boost Regression (FR) and Artificial Neural Networks (ANNs) for regression and prediction tasks. Reference [74] uses various Machine Learning Models for general ML tasks. Reference [75] applies Bayes Category Algorithm and other Machine Learning Algorithms for classification. Reference [76] focuses on Extreme Learning Machine (ELM) for fast learning and prediction. Reference [77] uses a combination of SVM, Random Forest (RF), ANN, and Fuzzy Logic for comprehensive classification and regression. Reference [78] applies SVM, Ensemble Models, Gaussian Process Regression, and Adaptive Neuro-Fuzzy Inference System (ANFIS) for various ML tasks. Reference [79] focuses on Logistic Regression for binary classification tasks. Reference [80] uses Federated Learning and Byzantine-Robust Federated Learning for decentralized learning environments. Reference [81] explores Deep Learning-based Autoencoder, Deep Neural Network, and Machine Learning-based RF Fingerprinting for advanced learning and security applications.

Reference [82] examines RPL, emphasizing its role in energy-efficient networking, and reference [83] proposes a Lightweight Trust-Based System leveraging ML for secure communications. Reference [84] explores IPv6 with Neighbor Discovery Protocol (NDP), and reference [85] utilizes Neural Networks for modeling complex data relationships. Reference [86] uses Regression Models and execute with Root Mean Square Error and Mean Absolute Error, and reference [87] develops a Network Intrusion Detection System (NIDS) for security applications. Reference [88] develops the Trust-Based Multipath Routing Protocol (TBSMR), and reference [89] evaluates Epidemic, Prophet, and Privacy-Preserving History-Based routing in the opportunistic networks (PPHB++) routing protocols. Reference [90] uses Deep Reinforcement Learning (DRL) for advanced learning strategies.

Reference [91] proposes the ML-based Intelligent Routing Algorithm (ML-RA), and reference [92] explores Clustering and Multi-hop Routing, combining these approaches for efficient communication. Reference [93] explores Extreme Learning Machine (ELM), Weighted Extreme Learning Machine (WELM), and Improved Weighted Extreme Learning Machine (IWELM) for enhanced learning models. Reference [94] utilizes Long Short-Term Memory (LSTM) networks for analyzing sequential data.

Reference [95] applies Q-learning for reinforcement learning tasks and reference [96] explores Elite Opposition-centered Mine Blast Algorithm for cluster head selection. Reference [97] focuses on Extreme Learning Machines for efficient classification. Reference [98] integrates a Random Forest Model with a Reinforcement Learning Module for improved decision-making. Reference [99] also uses Extreme Learning Machines for various learning applications. Reference [100] focuses on Reinforcement Learning (Q-learning) for adaptive learning scenarios. Reference [101] works on unsupervised learning algorithms, so that clusters do not overlap. Reference [102] also investigates RPL, reinforcing its application in low-power networks, and reference [103] employs the Light Gradient Boosting Machine for efficient gradient boosting.

Table 3: The Literature depiction of ML techniques for routing protocols and machine learning

Serial no.	Number	ML techniques
1	[24]	Machine learning-based multi-class classifier for various types of attack classification
2	[25]	DBSCAN for clustering data based on density
3	[26]	Smart contract incentive algorithm to increase bandwidth, so that more packet transfer
4	[27]	Improved Extreme Learning Machine (IELM) to improve learning efficiency
5	[28]	K-means clustering, hybrid optimized machine learning approaches for clustering of nodes to avoid malicious nodes
6	[29]	Support Vector Machine (SVM) to find the mischievous node
7	[31]	Concept-drift detection mechanisms using incremental machine learning techniques (ADWIN, DDM, EDDM) for complex pattern recognition
8	[32]	Deep learning, specifically a Deep Neural Network (DNN) model for complex pattern recognition
9	[33]	Neural network for implementing ML-related task
10	[34]	Decision Tree finding trusting node and discarding the doubtful node from the network.
11	[35]	OS-ELM (Online Sequential Extreme Learning Machine) with Q-Network (QN), and Deep Q-Network (DQN) to explore general Machine Learning Algorithms for various applications
12	[36]	Machine Learning Algorithm combines linear regression and K-mean clustering to find malicious nodes.
13	[37]	Deep Learning Models, YOLO Image Classifier (YOLOv3) for the object detection
14	[38]	Deep Learning, Machine Learning to enhance the performance of the model
15	[39]	Machine-learning algorithms are applied through Digital Twin Networks (DTNs) in a simulated environment
16	[40]	ML-AODV, a combination of machine learning techniques in AODV protocol
17	[41]	K-means Data Clustering for better decisions on the quality of water
18	[42]	Learning-based Approaches based on machine learning approach
19	[43]	CatBoost (GBDT) technique for decision on routing

(Continued)

Table 3 (continued)

Serial no.	Number	ML techniques
20	[44]	KNN, SVM, DT, LDA, NB, CNN
21	[46]	Reinforcement Learning (RL)
22	[49]	LSTM (Long Short-Term Memory) to reduce the time and sequence data
23	[51]	Hybrid Deep Learning (supervised and semi-supervised) for traffic analysis of network
24	[52]	Self-organizing Network (SON) for dynamic network management
25	[53]	Support Vector Machine with Harris Hawks Optimization (SVM-HHO) to locate the Distributed Denial-of-Service (DDoS) attack
26	[55]	Machine Learning (ML) based attack detection and isolation process
27	[56]	Restricted Boltzmann Machine (RBM) and Long Short-Term Memory (LSTM) for prediction tasks
28	[57]	K-means Algorithm and K-medoids Algorithm
29	[58]	Reinforcement Learning and Q-Learning Algorithm for optimizing decision-making
30	[59]	K-means Clustering for data segmentation
31	[60]	Random Forest Classifier for robust classification task
32	[61]	Reinforcement Learning (RL) for adaptive learning and decision-making
33	[62]	(IEsBCCA-Net) for advanced neural network tasks
34	[64]	General machine learning algorithm
35	[65]	SVM, KNN, and LR for classification
36	[66]	Q-Learning, Fuzzy Logic for adaptive learning and decision-making
37	[67]	(OS-ELM) and Penicillium Reproduction Algorithm (PRA)
38	[68]	K-means clustering algorithm
39	[70]	Reinforcement learning for learning optimal policies
40	[71]	Incremental online learning algorithms Adaptive Random Forest (ARF) and KNN for evolving learning tasks
41	[72]	Collaborative Learning for shared learning across multiple models
42	[73]	Forest Boost Regression (FR) and Artificial Neural Networks (ANNs) for regression and prediction task
43	[74]	Machine learning models for general ML tasks
44	[75]	Bayes Category Algorithm and Machine Learning Algorithms for classification
45	[76]	Extreme Learning Machine (ELM) for fast learning and prediction
46	[77]	SVM, RF, ANN, and Fuzzy Logic for comprehensive classification and regression
47	[78]	Support Vector Machine (SVM), Ensemble Models, Gaussian Process Regression, and ANFIS to implement various ML tasks
48	[79]	Logistic Regression for binary classification tasks
49	[80]	Federated Learning and Byzantine-Robust Federated Learning for Decentralized Learning Environments
50	[81]	Deep Learning-based Autoencoder, Deep Neural Network, Machine Learning-based RF Fingerprinting for advanced learning and security applications.
51	[83]	Lightweight Trust-Based System for security
52	[85]	Neural Network for modeling complex data relationship
53	[86]	Regression models, performance evaluation using Root of the Mean of the Square of Errors (RMSE) and Mean Absolute Error (MAE)
54	[87]	Network Intrusion Detection System (NIDS) for security application
55	[90]	Deep Reinforcement Learning (DRL) for advanced learning strategies
56	[93]	Extreme Learning Machine (ELM), Weighted Extreme Learning Machine (WELM), and Improved Weighted Extreme Learning Machine (IWELM) for enhanced learning model
57	[94]	Long-Short-Term-Memory (LSTM) for analyzing sequential data
58	[95]	Q-Learning for various RL-based tasks
59	[96]	Elite Opposition-centered Mine Blast Algorithm for cluster head selection
60	[97]	Extreme Learning Machines (ELM) for efficient classification
61	[98]	Random Forest Model, Reinforcement Learning Module for better decision-making
62	[99]	Extreme Learning Machines (ELM) for robust learning tasks
63	[100]	Reinforcement Learning (Q-learning) for adaptive learning scenarios
64	[101]	Unsupervised Learning Algorithm for non-overlapping clusters

(Continued)

Table 3 (continued)

Serial no.	Number	ML techniques
65	[103]	Light Gradient Boosting Machine
66	[104]	Ant Colony Optimization for Traveling Salesman Problem

3.2 Literature Depiction Datasets for Routing Protocols and Machine Learning

The review of the literature covers a wide spectrum of works aiming at many facets of routing protocols and machine learning applied using different datasets and approaches, as shown in Table 4. Reference [24] focuses on intrusion detection techniques using a dataset specifically designed for cybersecurity. Reference [28] utilizes the CICIDS2017 dataset, released by the Canadian Institute for Cybersecurity (CIC). This dataset includes both benign network activity and malicious attacks, such as denial-of-service (DoS), probing, and malware distribution. Additionally, the UNSW-NB15 dataset, created by researchers at the University of New South Wales (UNSW), contains network traffic data from a simulated environment. Both datasets are used for evaluating and refining intrusion detection systems. Reference [32] applies machine learning techniques to the IoT (Internet of Things) attack dataset to enhance IoT security. Reference [37] explores cognitive and behavioral research using eye tracking, synchronized video, and think-aloud protocols. Reference [38] employs simulation techniques from SUMO (Simulation of Urban Mobility) and NS-3 (Network Simulator-3) to study vehicular networks. Reference [41] uses experimental measurements to investigate lanthanide oxide nanoparticles to check hydrogen peroxide levels present in water, while reference [43] analyzes routing metrics to improve network algorithms. Reference [47] leverages the Gawk Data Extraction Tool for text processing and data analysis. Reference [49] works with Databases for ToN-IoT (ToN-IoT dataset is obtained from a practical and large-scale network developed by the UNSW Canberra Cyber IoT Lab) and InSDN (dataset covers many scenarios and attack classes, including Probe, DoS application, web attacks, brute force attack, password guessing, U2R, and DDOS attacks) for network security in IoT and software-defined networking. Reference [51] focuses on IoT security with the IoTR-DS (IoTR-DS used as a use case to classify three known security attacks (DIS, Rank, and Wormhole)) dataset, while reference [62] uses the Bot-IoT (Bot-IoT is a realistic network environment created by UNSW Canberra that includes normal and botnet traffic) dataset for studying botnet attacks. Reference [65] employs the NSLKDD (NSLKDD dataset is the benchmark dataset we use in our research for Intrusion Detection System) dataset for network intrusion research, and reference [76] analyzes network data using RIPE (Reseaux IP Europeens) and BCNET (a not-for-profit organization). Reference [77] investigates wireless body area networks (WBANs) for health monitoring, while reference [79] uses flow data to model network behaviors. Reference [80] works with non-IID (independent and identically distributed) datasets to address data dependency challenges, reference [84] develops bespoke datasets for specific research needs, and reference [87] uses the RPL-NIDS17 dataset for network intrusion detection in constrained networks. Reference [83] generates synthetic data for specific research purposes.

Table 4: The Literature depiction of datasets for routing protocols and machine learning

S.No.	Number	Dataset
1	[24]	Intrusion detection dataset specifically designed for cybersecurity
2	[28]	CICIDS2017 and UNSW NB15 for evaluating and refining intrusion detection systems
3	[32]	IoT attack dataset to increase IoT security
4	[37]	Tracking Data of Eye, Synchronizing Video Data, Think Aloud Protocols, Logging of Data for tracking of user's position

(Continued)

Table 4 (continued)

S.No.	Number	Dataset
5	[38]	Vehicular Mobility Traces (SUMO), Simulated Environment Data (NS-3) for studying vehicular network
6	[41]	Experimental Measurements of Lanthanide Oxide Nanoparticles in water for hydrogen peroxide
7	[43]	ML method used to train Routing Metrics Dataset
8	[47]	Gawk Data Extraction Tool for text processing and analyzing of data
9	[49]	ToN-IoT and InSDN for network security
10	[51]	IoTR-DS was implemented as a use case for attacks like rank, wormhole, and DIS
11	[64]	Bot-IoT dataset to implement various types of attack
12	[65]	NSLKDD Dataset for network intrusion research
13	[71]	Simulation data from SUMO and NS-3
14	[76]	RIPE and BCNET for analyzing network data
15	[77]	WBANs (Wireless Body Area Networks) for health monitoring
16	[79]	Flow Data Datasets for model network behavior
17	[80]	Non-id (not independent and identically distributed) dataset for data dependency challenge
18	[83]	Generated Dataset for specific research
19	[84]	Bespoke dataset for specific research needs
20	[87]	RPL-NIDS17 Dataset for network intrusion detection in constrained networks

3.3 Literature Depiction Routing Techniques for Routing Protocols and Machine Learning

The literature review covers a wide spectrum of works aiming at many facets of routing protocols and machine learning applied using different Routing techniques and approaches are presented in Table 5. Reference [24] focuses on Routing Protocol for Low-Power and Lossy Networks (RPL) and 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), targeting energy-efficient and low-power network environments. Reference [26] utilizes GPSR (Greedy Perimeter Stateless Routing), a geographical-based routing method designed for efficient packet delivery. References [29,30] explore *Ad Hoc* On-Demand Vector Routing protocol (AODV), which supports robust route discovery in *ad hoc* networks. References [31,34] also examine RPL, emphasizing its application in low-power settings. Reference [33] develops a machine learning-based forwarding algorithm for VANETs to enhance routing decisions. Reference [35] implements online-sequential Extreme Learning Machine Q-network (OS-ELM QN) which works on replay buffer prioritization to reduce learning time. Reference [37] investigates the A* Algorithm, known for its heuristic-based shortest path calculations. Reference [38] introduces a hybrid algorithm combining Software-Defined Vehicular Network (SDVN) modes, AODV, and Dijkstra's Algorithm using software-defined networks for versatile vehicular routing. Reference [39] reviews intelligent-Software-Defined Vehicular Network (iSDVN) protocol for intelligent vehicular network routing. Reference [40] presents the Watch Dog Routing Algorithm, which incorporates monitoring for security enhancements. References [41,49] apply the Low Energy Adaptive Clustering Hierarchy (LEACH) for energy-efficient clustering. Reference [43] proposes ML-RPL (Machine Learning-enhanced RPL) to improve routing with machine learning techniques. References [45,51] focus on IPv6-based RPL for low-power network environments. Reference [46] introduces e-RLRP (Enhanced Routing Protocol based on Reinforcement Learning), comparing it to Optimized Link State Routing Protocol Optimized Link State Routing Protocol (OLSR) and a Better Approach to Mobile *Ad hoc* Networking (BATMAN) for routing optimization. Reference [47] combines DTN (Delay-Tolerant Networking) with Greedy Perimeter Stateless Routing (GPSR) for scenarios involving intermittent connectivity. Reference [50] proposes Group'n Route (GnR) for group-based routing strategies.

Table 5: The literature depiction of routing techniques for routing protocols and machine learning

S. No.	Number	Routing techniques
1	[24]	6LoWPAN and RPL: targeting energy-efficient and low-power network environments
2	[26]	Greedy perimeter stateless routing (GPSR) for efficient packet delivery
3	[29]	AODV supports robust route discovery in <i>ad hoc</i> networks
4	[31]	RPL to work well in low power setting
5	[33]	ML-based forwarding algorithm for vehicular <i>ad hoc</i> networks (VANETs) to enhance routing
6	[34]	RPL for low power-setting
7	[35]	Online-Sequential Extreme Learning Machine Q-network (OS-ELM QN) which works on replay buffer prioritization to reduce learning time
8	[36]	RPL for black-hole attacks and suspicious nodes
9	[37]	A* Algorithm, known for its heuristic-based shortest path calculations
10	[38]	Hybrid Algorithm for SDVN (Highest Stable Least Delay Mode, Highest Stable Shortest Path Mode), AODV, Dijkstra's Algorithm for versatile routing of vehicle
11	[39]	State-of-the-art iSDVN Routing Protocols
12	[40]	Watch Dog Routing Algorithm for enhancing the security
13	[41]	LEACH for decision for monitoring the water quality
14	[42]	Various V2X (vehicle to any device) Routing Protocols
15	[43]	ML-RPL (Machine Learning-enhanced RPL) to improve decision of routing
16	[45]	IPv6-RPL for low-power network environment
17	[46]	Enhanced Routing Protocol based on Reinforcement Learning (e-RLRP), with comparisons to OLSR, BATMAN, and RLRP
18	[47]	DTN (Delay-Tolerant Networking) and GPSR (Geographic Source Routing) for scenarios involving intermittent connectivity
19	[48]	Routing Algorithm
20	[49]	Energy Harvesting Real-Time Routing Protocol (EHRT) and Low-LEACH for energy-efficient clustering
21	[50]	Group'n Route (GnR): novel clustering technique for message passing
22	[51]	RPL for low-power network
23	[52]	Cooperative Routing (CR) which emphasizes collaborative strategies among nodes to enhance routing performance
24	[53]	Enhanced Hybrid Ant Colony Optimization Routing Protocol (EHACORP) and Rider Integrated Cuckoo Search (RI-CS) to improve route discovery
25	[54]	Routing Protocol for Low-power and Lossy Networks (RPL) and WOABC (Whale Optimization Algorithm-Based Clustering) to optimize routing in low power scenario
26	[55]	SDN-resilience manager (SDN-RM) to delay the attack, so that loss was less, and Delay-based attack detection and isolation scheme (DA-DIS) to prevent unknown node from being a participant
27	[56]	IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) for low power supply network
28	[57]	KOCED protocol works on a cluster which is based on K-means and k-medoids
29	[58]	Information-Centric Networking (ICN) based on content-based routing
30	[59]	Hybrid Protocol (MDC-K) combining multiple routing techniques for adaptive performance
31	[60]	<i>Ad hoc</i> On-Demand Distance Vector (AODV), emphasizing its use in dynamic network scenarios
32	[61]	Routing Protocol for Low-power and Lossy Networks (RPL) for efficient data routing
33	[62]	Medium Access Control (MAC) Protocols to improve throughput while reducing delay and consumption of energy
34	[63]	Routing Protocol for Low power and Lossy Networks (RPL) and Destination Oriented Directed Acyclic Graph (DODAG) for efficient routing
35	[64]	<i>Ad Hoc</i> On-Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) compare their working in various conditions related to attacks
36	[65]	LEACH (Low-Energy Adaptive Clustering Hierarchy) and Sub-cluster LEACH for energy efficiency of network
37	[66]	Hierarchical Routing Protocol (QFHR), for layered network structure
38	[67]	Penicillium Reproduction-based Online Learning Adaptive Routing (POLAR) a novel adaptive routing
39	[68]	Low Energy Adaptive Clustering Hierarchy (LEACH) for energy-efficient clustering
40	[69]	WiCHORD+ enhanced protocol in the non-wired network

(Continued)

Table 5 (continued)

S. No.	Number	Routing techniques
41	[70]	Energy-efficient control and routing protocol focus on an energy-efficient control and routing protocol to balance energy consumption and routing efficiency
42	[71]	<i>Ad hoc</i> On-Demand Distance Vector (AODV) for its current applicability
43	[73]	Combining the Biomimicry Buzz Algorithm and Bellman-Ford-Dijkstra Algorithm for better performance
44	[74]	Reconfigurable CRN-based Cross-Layer Routing Protocol for cognitive radio network
45	[77]	AODV (<i>Ad hoc</i> On-Demand Distance Vector) further enhances its adaptability
46	[78]	Optimal routing protocol to achieve the best performance under various conditions
47	[81]	Backpressure Algorithm which optimizes network throughput by managing congestion
48	[82]	RPL Protocol emphasizes its role in energy-efficient networking
49	[83]	RPL (Routing Protocol for Low Power and Lossy Networks) for low power supply
50	[84]	IPv6 with Neighbor Discovery Protocol (NDP) enhancing address resolution and node discovery in IPv6 networks
51	[85]	Cluster Routing focuses on organizing nodes into clusters for efficient communication
52	[86]	Expanding Ring Search (ERS) and random Early Detection (RED) for dynamic and congestion-aware routing
53	[87]	RPL showing effectiveness in low-power and lossy environments
54	[88]	Trust-Based Multipath Routing Protocol (TBSMR) to enhance reliability through trust evaluation
55	[89]	Epidemic, Prophet, and PPHB++, which use different strategies for data dissemination
56	[90]	Federated Deep Reinforcement Learning (FDRL) leveraging advanced machine learning techniques for routing decisions
57	[91]	ML-based Intelligent Routing Algorithm (ML-RA) which incorporates machine learning for adaptive routing
58	[92]	Clustering and Multi-hop Routing combining these approaches for efficient communication
59	[93]	Link Quality Estimation to improve routing decisions based on link performance
60	[94]	Authentication Routing Protocol for enhancing security
61	[95]	Multi-hop routing which optimizes communication over multiple hops
62	[96]	Cluster Formation to improve network organization
63	[97]	Hybrid Energy Efficient Learning Protocol (HELP) for energy conservation in routing
64	[98]	Routing Protocol for Low-Power and Lossy Networks (RPL) focusing on its adaptations for specific network conditions
65	[99]	Logistic Chaotic Algorithm for routing optimization
66	[100]	Balanced Routing Protocol based on Machine Learning (BRP-ML) for balanced routing using ML techniques
67	[102]	RPL (Routing Protocol for low-power and Lossy Networks) for low-power network
68	[103]	RPL for low-power network
69	[104]	Ant Colony Optimization (ACO) to implement ant behavior in the network

Reference [52] introduces Cooperative Routing (CR), which emphasizes collaborative strategies among nodes to enhance routing performance. Reference [53] develops the paper introduces the Enhanced Hybrid Ant Colony Optimization Routing Protocol and Rider Integrated Cuckoo Search, which integrate ant-colony optimization with cuckoo methods of search to improve routing discovery. Reference [54] focuses on RPL integrated with WOABC (Whale Optimization Algorithm-Based Clustering) to optimize routing in low-power scenarios. Reference [55] presents the Software Defined Networking (SDN)(-resilience manager (SDN-RM) and Delay-based attack detection and isolation scheme for enhancing security and resilience in software-defined networks. Reference [56] explores IPv6-based RPL, continuing the trend of low-power network optimization. Reference [57] proposes the K-means with Optimal clustering for Wireless sensor network (WSN) considering Centrality, Energy, and Distance (KOCED) protocol, which works for energy management in clusters using K-means and K-medoid. Reference [58] examines Information-Centric Networking (ICN), which focuses on content-based routing rather than traditional address-based

methods. Reference [59] introduces a Hybrid Protocol Mobile Data Collector with a K-mean machine learning clustering algorithm (MDC-K), combining multiple routing techniques for adaptive performance. Reference [60] also studies AODV, emphasizing its use in dynamic network scenarios. References [61,63] explore variations of RPL, including its integration with DODAG (Destination Oriented Directed Acyclic Graph) for efficient data routing. Reference [64] compares AODV with Optimized Link State Routing (OLSR), highlighting their performance in different network conditions of attacks. Reference [65] works on LEACH and Sub-cluster LEACH to enhance energy efficiency in clustering. Reference [66] proposes the Q-learning and fuzzy logic-based hierarchical Routing Protocol (QFHR) for layered network structures. Reference [67] introduces Penicillium reproduction-based Online Learning Adaptive Routing scheme (POLAR), a novel adaptive routing approach. Reference [68] continues the exploration of LEACH for energy-efficient clustering. Reference [69] presents WiCHORD+, works on enhancement of protocol named WiCHORD in non-wired networks. Reference [70] focuses on an energy-efficient control and routing protocol to balance energy consumption and routing efficiency. Reference [71] revisits AODV, assessing its current applicability. Reference [73] propose the Biomimicry Buzz Algorithm and Bellman-Ford-Dijkstra Algorithm, blending bio-inspired methods with classic algorithms. Reference [74] develops a Reconfigurable CRN-based (Cognitive Radio Network) Cross-Layer Routing Protocol for cognitive radio networks. Reference [77] also investigates AODV, further exploring its adaptability. Reference [78] focuses on an Optimal Routing Protocol, aiming for the best performance under various conditions.

Reference [81] investigates the Backpressure Algorithm, which optimizes network throughput by managing congestion. Reference [82] examines RPL, emphasizing its role in energy-efficient networking. Reference [84] explores IPv6 with Neighbor Discovery Protocol (NDP), enhancing address resolution and node discovery in IPv6 networks. Reference [85] proposes Cluster Routing, focusing on organizing nodes into clusters for efficient communication. References [86,87] both analyze RPL, highlighting its effectiveness in low-power and lossy environments. Reference [86] addresses Expanding Ring Search (ERS) and Random Early Detection (RED) for dynamic and congestion-aware routing. Reference [88] develops the Trust-Based Multipath Routing Protocol (TBSMR), which enhances reliability through trust evaluation. Reference [96] focuses on Cluster Formation strategies to improve network organization. Reference [89] evaluates Epidemic, Prophet, and Privacy-Preserving History-Based routing in the opportunistic networks (PPHB++) routing protocols, which use different strategies for data dissemination. Reference [90] introduces Federated Deep Reinforcement Learning (FDRL), leveraging advanced machine learning techniques for routing decisions. Reference [91] proposes the ML-based Intelligent Routing Algorithm (ML-RA), which incorporates machine learning for adaptive routing. Reference [92] explores Clustering and Multi-hop Routing, combining these approaches for efficient communication. Reference [93] focuses on Link Quality Estimation to improve routing decisions based on link performance. An Authentication Routing Protocol enhances security in routing processes [94]. Reference [95] works on a Multi-Hop Routing Protocol, which optimizes communication over multiple hops. Reference [97] proposes the Hybrid Energy Efficient Learning Protocol (HELP) for energy conservation in routing. Reference [98] continues the study of RPL, focusing on its adaptations for specific network conditions. Reference [99] introduces the Logistic Chaotic Algorithm, which applies chaos theory to routing optimization. Reference [100] presents the Balanced Routing Protocol based on Machine Learning (BRP-ML), integrating machine learning for balanced routing. Reference [102] also investigates RPL, reinforcing its application in low-power networks. Reference [104] utilizes Ant Colony Optimization (ACO) for routing, inspired by ant behavior.

3.4 Literature Depiction Optimization Techniques for Routing Protocols and Machine Learning

The review of the literature covers a wide spectrum of works aiming at many facets of routing protocols and machine learning applied using different optimization techniques and approaches presented in Table 6. Reference [26] employs the linear additive weighting method to balance multiple criteria in decision-making. Reference [27] proposes the Hunger Games Search (HGS) algorithm, for redesigning the new IP address every time, which simulates competitive scenarios to find optimal solutions. Reference [30] utilizes the Ant Colony Algorithm (ACA), inspired by the foraging behavior of ants, for solving optimization problems. Reference [35] applies the Prioritized Experience Replay Buffer to improve reinforcement learning by prioritizing critical experiences. Reference [38] develops a Network Link Entropy Formulation and Link Lifetime Threshold to optimize network resource allocation. Reference [39] focuses on Stochastic Modeling and Performance Analysis to evaluate system performance under uncertainty. Reference [41] enhances the LEACH-based Clustering Algorithm with modifications for improved operation on water and improved quality. Reference [43] utilizes Gradient Boosted Decision Trees (GBDT) for predictive modeling and optimization tasks. Reference [48] explores AI-controlled algorithms that leverage artificial intelligence for optimized decision-making. Reference [49] introduces a Modified Artificial Fish Swarm Algorithm, which enhances swarm-based optimization techniques. Reference [53] presents the Hybrid Whale Dragonfly Optimization Algorithm, combining whale and dragonfly optimization strategies. Reference [54] investigates the Whale Optimization Algorithm (WOA), a nature-inspired method for global optimization [57] to develop the Optimal cluster K-means algorithm (KOCED) for efficient clustering. Reference [58] focuses on Stretch Optimization (ISO), addressing system performance optimization. Reference [59] works on Energy Optimization, targeting improvements in energy consumption. Reference [61] proposes the RL Intelligent Adaptive Trickle-Timer Algorithm (RLATT), combining reinforcement learning with adaptive timing strategies. Reference [62] applies Synthetic Minority Over-sampling Technique (SMOTE), Random Under-Sampling (RUS), and Modified Honey Badger Algorithm (MHBA) to enhance data handling and optimization. Reference [63] utilizes Q-Learning for reinforcement learning-based optimization. Reference [65] employs Levenberg-Marquardt Neural Network (LMNN) and Moth-Flame Optimization (MFO) to refine neural network training and optimization processes.

Reference [67] introduces the Penicillium Reproduction Algorithm (PRA), inspired by the reproduction process of penicillium fungi for optimization. Reference [68] refines the Modified K-means algorithm to improve clustering performance. Reference [72] focuses on Fitness Computing, a method for evaluating and optimizing solutions based on fitness levels. Reference [74] proposes the Spotted Hyena Optimizer (SHO), a nature-inspired algorithm mimicking the behavior of spotted hyenas [75] explores Feature Selection Methodologies for enhancing the relevance of features in predictive models. Reference [76] utilizes Affinity Propagation, a clustering technique based on message passing between data points. Reference [80] develops the DisBezant Mechanism, focusing on dynamic and efficient optimization strategies. Reference [81] addresses Power Control and Modulation and Coding Scheme (MCS) Adaptation for optimizing communication systems. Reference [82] uses the Probability-based Attestation Scheme (PROB_ATT) and Trickle Time to ensure reliable and efficient data transmission. Reference [84] applies locally Weighted Learning Techniques to improve model accuracy. Reference [85] employs Multilayer Estimations for enhanced prediction and optimization. Reference [87] combines Grey Wolf Optimization (GWO) and Dipper Throated Optimization (DTO) with Locality-Sensitive Hashing and Synthetic Minority Oversampling Techniques for robust and accurate optimization learning. Reference [90] utilizes Federated Learning to enhance distributed model training. Reference [97] introduces Hybrid Whale-Dragonfly Algorithms, merging whale and dragonfly optimization strategies. Reference [99] explores Deep Reinforcement Learning-based Extreme Learning Machines (DRLELM) to integrate reinforcement learning with extreme learning for improved performance.

Reference [103] focuses on Multiclass Classification, a technique for handling multiple classification tasks simultaneously. Reference [105] focuses on two rays and shadow fading, and Reference [106] uses the Firefly algorithm for balancing the load and improvising congestion.

Table 6: The literature depiction of optimization techniques for routing protocols and machine learning

S. No.	Number	Optimization techniques
1	[26]	linear additive weighting method to stabilize the link between nodes and increase the delivery of packets
2	[27]	Hunger Games Search (HGS) algorithm, to generate new IP address
3	[30]	Ant Colony Algorithm (ACA) for optimizing the path between ground and space
4	[35]	Prioritized Experience Replay Buffer to improve reinforcement learning by prioritizing critical experiences
5	[38]	Network Link Entropy Formulation, Link Lifetime Threshold to optimize the resource for allocation
6	[39]	Stochastic Modeling and Performance Analysis under uncertain conditions
7	[41]	Modified LEACH-based Clustering Algorithm for monitoring water quality
8	[43]	Gradient Boosted Decision Trees (GBDT) for predictive modeling and optimization tasks
9	[48]	AI-Controlled Algorithms for optimizing decision
10	[49]	Modified Artificial Fish Swarm Algorithm to enhance the swarm techniques
11	[53]	The hybrid Whale Dragonfly Optimization Algorithm (H-WDFOA) is a technique used for the allocation of bandwidth and checking the impact of a DDoS attack
12	[54]	Whale Optimization Algorithm (WOA) for global optimization
13	[57]	Optimal cluster K-means algorithm (KOCED) for clustering
14	[58]	Stretch Optimization (ISO), works on system performance optimization
15	[59]	Energy Optimization targeting improvements in energy consumption
16	[61]	RL Intelligent Adaptive Trickle-Timer Algorithm (RLATT)
17	[62]	SMOTE, Random Under-sampling (RUS), Modified Honey Badger Algorithm (MHBA) for data handling and optimization
18	[63]	Q-Learning for routing optimization
19	[65]	Levenberg-Marquardt Neural Network (LMNN) and Moth-Flame Optimization (MFO) for neural network training and optimization
20	[67]	Penicillium Reproduction Algorithm (PRA)
21	[68]	Modified K-means algorithm to improve clustering performance
22	[72]	Fitness Computing is the method for evaluating and optimizing solutions based on fitness levels.
23	[74]	Spotted Hyena Optimizer (SHO)
24	[75]	Feature Selection Methodologies for enhancing the relevance of features in predictive models
25	[76]	Affinity Propagation is a clustering technique based on message passing between data points.
26	[80]	DisBezant Mechanism focuses on dynamic and efficient optimization strategies
27	[81]	Power control, MCS adaptation for optimizing communication systems
28	[82]	Probability-based Attestation Scheme (PROB_ATT), Trickle Time to ensure reliable and efficient data transmission
29	[84]	Locally Weighted Learning Techniques to Improve Model Accuracy
30	[85]	Multilayer Estimations for enhanced prediction and optimization
31	[87]	Grey Wolf Optimization (GWO) and Dipper Throated Optimization (DTO); Locality-Sensitive Hashing (LSH) combined with SMOTE for robust and accurate optimization learning
32	[90]	Federated Learning to enhance distributed model training
33	[93]	Particle Swarm Optimization (PSO)
34	[96]	Improved Beetle Swarm Optimization (IBSO) algorithm for communication and backup route from the head of the cluster to the base station
35	[97]	Hybrid Whale-Dragonfly Algorithms for Optimization
36	[99]	Deep Reinforcement Learning-based Extreme Learning Machines (DRLELM) for improved performance
37	[103]	Multiclass Classification, is a technique for handling multiple classification tasks simultaneously.
38	[106]	Firefly Algorithm for balancing load and improvising congestion

3.5 Literature Analysis for Feature Extraction Techniques Used for Routing Protocols and Machine Learning

The review of the literature covers a wide spectrum of works aiming at many facets of routing protocols and machine learning applied using different Feature Extraction techniques and approaches, collected in Table 7. Reference [24] employs node-based feature extraction through sliding time windows to capture dynamic network data. Reference [30] leverages node type, energy, and location information as heuristic data for better network analysis. Reference [37] utilizes gaze tracking and automatic classification of landmarks for improved human-computer interaction. Reference [38] predicts link lifetime, channel delay, and network contention to optimize network performance. Reference [39] explores Digital Twins Capabilities for simulating network behaviors. Reference [40] applies the Watch Dog approach to enhance network security. Reference [41] analyzes the fluorescence quenching mechanism for the optical detection of peroxide. Reference [44] investigates nodes' properties to inform network decisions. Reference [46] applies the E-model algorithm for network quality assessment. Reference [47] quantifies coordinate information and performance indicators for GPSR routing. Reference [48] utilizes the Discovery of Functions and Services Protocol (DFSP) for service discovery. Reference [49] uses MRMR (Minimum Redundancy Maximum Relevance) for the selection of features.

Table 7: The authors and the major features of routing protocols

S. No.	Number	Feature extraction
1	[24]	Node-based feature extraction using sliding time windows to capture dynamic network data
2	[37]	Gaze Tracking and automatic Classification of Landmarks to improve the interaction between user and computer
3	[38]	Link Lifetime Prediction, Channel Delay Prediction, and Network Contention Estimation for network performance
4	[39]	Digital Twins' Capabilities for Simulating Network Behaviors
5	[40]	Watch Dog approach for monitoring of security
6	[41]	Fluorescence Quenching Mechanism for detection of peroxide in water
7	[44]	Nodes' Properties for making decision
8	[46]	E-model Algorithm for checking the data link quality
9	[47]	Coordinate Information and performance indicators quantified for GPSR routing
10	[48]	Discovery of Functions and Services Protocol (DFSP) for delivering services
11	[49]	MRMR (Minimum Redundancy Maximum Relevance) to improve performance of intrusion detection system
12	[50]	Graph Metrics for finding the relation between the nodes
13	[53]	QoS Factor Data Preprocessing, Network Quality Measurement
14	[57]	Distances between Cluster Centers, Nodes, and Residual Energies
15	[58]	Stretch Profile for network optimization
16	[59]	Clustering-based features like selection of cluster head and Mobile Data Collector (MDC) (node between head cluster and base station)
17	[60]	Sequence Number Analysis for data integrity
18	[61]	Trickle Timer data for efficient communication protocols
19	[62]	Reformed Histogram Equalization Method in case of pre-processing of data and Modified Honey Badger Algorithm (MHBA) for selection of feature optimally
20	[67]	Geohash
21	[68]	Euclidean distance formula for spatial calculation
22	[69]	MAC address for network management
23	[76]	Fisher Feature Selection Algorithm, MIQ Feature Selection Technique for efficient data analysis
24	[81]	Autoencoder for Spectrum Features
25	[82]	Probability Estimation for data analysis
26	[83]	Trust Values
27	[89]	Real-Time GPS Coordinates for location-based applications

(Continued)

Table 7 (continued)

S. No.	Number	Feature extraction
28	[90]	Cluster Pairing for improving network efficiency
29	[92]	Node mobility, energy utilization rate, and bandwidth for performance assessment
30	[93]	Link Quality Indication (LQI), Received Signal Strength Indication (RSSI), and Signal-to-Noise Ratio (SNR)
31	[97]	Sub-Area Division Algorithm for improved network management
32	[102]	Trust factors and mobility-based metrics for security and efficiency
33	[105]	Two rays and shadow fading

Reference [50] analyzes graph metrics for network analysis. Reference [53] preprocess Quality-of-service (QoS) factor data and measure network quality. Reference [57] calculates distances between cluster centers, nodes, and residual energies for clustering algorithms. Reference [58] uses the stretch profile for network optimization. Reference [59] focuses on clustering-based features and mobile data collector (MDC) metrics. Reference [60] analyzes sequence numbers for data integrity. Reference [61] uses trickle-timer data for efficient communication protocols. Reference [62] applies the reformed histogram equalization method and modified Honey Badger Algorithm (MHBA) for feature enhancement. Reference [67] employs Geohash for spatial data encoding. Reference [68] uses the Euclidean distance formula for spatial calculations. Reference [69] extracts features from MAC addresses for network management. Reference [71] focuses on VANET nodes for vehicular network analysis. Reference [76] uses the Fisher Feature Selection Algorithm and Mutual Information Quotient (MIQ) feature selection technique for efficient data analysis. Reference [81] applies autoencoder techniques for extracting spectrum features. Reference [82] estimates probabilities for data analysis. Reference [89] uses real-time GPS coordinates for location-based applications. Reference [90] focuses on cluster pairing for network efficiency. Reference [92] analyzes node mobility, energy utilization rate, and bandwidth for performance assessment. Reference [93] measures link quality indication (LQI), received signal strength indication (RSSI), and signal-to-noise ratio (SNR) for network performance. Reference [97] uses the sub-area division algorithm for improved network management. Reference [102] evaluates trust factors and mobility-based metrics for security and efficiency.

4 Discussion

Recent advancements in the systematic analysis of routing protocols reflect a significant evolution driven by advancements in Machine Learning techniques, as highlighted by several key studies. Reference [22] asserts that the UAV capabilities and functionalities have grown. Advanced processors, sensors, communications, and networking make robotic systems attractive in military and commercial settings. Technology reduces UAV development and maintenance expenses. One big UAV is giving way to goal-oriented teams. New networking architectures on UAVs are needed for fleet coordination. UAV *ad hoc* networks are harder to set up than MANETs and VANETs because they employ different criteria. Criteria include mobility of nodes, connection, packet routing, quality of service, and applications.

5 Research Challenges and Opportunity

Here, we perform a comparison with some known protocols such as RPL, GPSR, and AODV, the paper discusses UAV network models, *ad hoc* relay node difficulties, and current and future research concerns. In contrast, References [24,31] focus on RPL and its applications in low-power networks, underscoring the protocol's importance for energy-efficient operations. RPL is good in terms of energy saving of the nodes but it will suffer from re-routing issues.

Likewise, GPSR's geographic-based routing is based on still nodes, which is quite difficult to maintain in FANET. References [26,47] demonstrate GPSR and its integration with Delay-Tolerant Networking (DTN) for efficient routing in scenarios with intermittent connectivity, to solve the above, but requires more research for more transfer of packets while nodes are moving. Whereas, Reference [32] leverages machine learning techniques on IoT attack datasets to improve threat detection, illustrating the need for specialized data in addressing IoT-specific vulnerabilities, which raise an issue of network reliability as nodes are moving and any malicious node can participate in this network. In the upcoming implementation paper, we will work on various performance parameters like latency, data loss, Packet Delivery Ratio (PDR), average delay, etc. Large drone networks communicate *ad hoc* in FANETs [107]. This network provides new military, industrial, and civilian purposes. FANETs struggle with high-speed nodes, limited users, and fast topological changes. In these networks, routing is massive. FANET routing techniques that enhance energy efficiency are illustrated. Whereas, Reference [108] demonstrates that the MANETs have issues with shifting topologies, intermittent communication, and unexpected traffic. This research indicates that machine learning increases Mobile *Ad hoc* Network community visitor performance. The proposed approach classifies visitors using SVM, analyzes their correctness, and optimizes efficiency via community optimization. Findings suggest the system may properly identify visitor preferences and enhance community performance. The method may be used in real life to improve the conventional system. In contrast, Reference [78] applies SVM, Ensemble Models, Gaussian Process Regression, and ANFIS for various ML tasks. The technique enhances node pathways by considering energy economy and connection dependability. The routing approach is tested using NS3. Optimized OLSR and greedy optimal link state routing (G-OLSR) simulation results are systematically compared. The technique beats G-OLSR and OLSR in latency, packet delivery, data throughput, and energy usage. The routing solution costs more than G-OLSR.

6 Conclusion

In conclusion, routing algorithms using machine learning in flying *ad hoc* networks mainly emphasize overcoming the issues caused by aerial networks' dynamic and unpredictable character. FANETs, which employ UAVs for various purposes, face challenges such as fast node mobility, frequent topology changes, and intermittent connection. These properties render typical routing techniques ineffective. The work stresses the capacity of ML approaches, notably supervised learning, unsupervised learning, and reinforcement learning, to improve routing efficiency and flexibility in FANETs. Unlike conventional techniques, ML-based protocols use predictive modeling and real-time data to optimize routing choices, enhance network resource management, and resolve connection faults. Reinforcement learning, in particular, is praised for its capacity to deal with dynamic settings by learning from encounters and adjusting without needing pre-existing data. The PRISMA method is used to review the literature from 2021 to 2023 for this study, which focuses on how machine learning can be used in FANET. It compiles current study data, analyzes the advantages and limitations of algorithms based on machine learning, and suggests future research areas. The evaluation emphasizes the need for strong, scalable, and adaptive routing methods that can manage the complexity of FANETs. By outlining current research trends and breakthroughs, the study provides significant insights for designing more effective and intelligent routing techniques in aerial networks, with the ultimate goal of bridging gaps and driving future innovation in this field. In future work, more machine learning techniques can be implanted in the FANET such as deep reinforcement learning, fuzzy logic, and neural networks. Also, Clustering-based reinforcement learning and deep reinforcement learning techniques can be implemented to reduce overhead and provide more stability in the FANET by reducing the action and state spaces.

FANET can be integrated with VANET, which provides robustness in both the network while enhancing connectivity and operational efficiency. The VANET provides communication between the roadside units

and vehicles, which is best for ground-based operations such as transport management, autonomous vehicle coordination, and smart-city development. Extending VANET with the aerial network helps in finding the shortest/fastest route selection, avoiding accidents, better guidance on road safety. All this is possible because FANET behaves as a relay node for reducing latency, processing data locally, and offloading from a central server.

FANET has properties like self-organized, self-managed, and self-healing which make it popular. As it covers a large geographical area in a remote area, will make it a good choice for smart city development in an isolated place. These outskirts lack the basic network infrastructure to support various activities like logistics and delivery, transportation, medical facilities, waste management, disaster management, etc. By implementing FANET in this area, one can develop a smart city.

FANET can be implemented as a pilot deployment. As FANET is easy and quick to deploy and become operational. It can be used in disaster management, surveillance, and logistics. FANET shares real-time data while maintaining the connection in disrupted areas. FANET based on ML-based decisions, can make it an innovative step, as new areas can be explored. For example, in a pharmacy, using FANET, doctors can check the patient sitting far away in a remote area and provide medicine with logistics, using FANET.

Acknowledgement: This work is supported by the Computer Science Department of Lovely Professional University, Phagwara, Punjab, India.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Priyanka, Manjit Kaur: Conceptualization, methodology, Software, formal analysis, resources, data curation, original draft preparation, visualization. Deepak Prashar, Arfat Ahmad Khan, Leo Mrcic: Conceptualization, methodology, validation, formal analysis, investigation, review, supervision. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are openly available in (Scopus database) at www.scopus.com (accessed on 07 January 2025).

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Supplementary Materials: The supplementary material is available online at <https://doi.org/10.32604/cmc.2025.059043>.

References

1. Fadel E, Faheem M, Gungor VC, Nassef L, Akyildiz IF. Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications. *Comput Commun.* 2017;101(6):106–20. doi:10.1016/j.comcom.2016.12.020.
2. Bekmezci I, Sahingoz OK, Temel S. Flying *ad-hoc* networks (FANETs): a survey. *Ad Hoc Netw.* 2013;11(3):1254–70. doi:10.1016/j.adhoc.2012.12.004.
3. Siddiqi MA, Iwendi C, Jaroslava K, Anumbe N. Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. *Math Biosci Eng.* 2022;19(3):2641–70. doi:10.3934/mbe.2022121.
4. Yousefpoor MS, Barati H. DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks. *Wirel Netw.* 2020;26(4):2515–35. doi:10.1007/s11276-019-01980-1.
5. Lakew DS, Sa'ad U, Dao NN, Na W, Cho S. Routing in flying *ad hoc* networks: a comprehensive survey. *IEEE Commun Surv Tut.* 2020;22(2):1071–120. doi:10.1109/COMST.9739.

6. Faheem M, Tuna G, Gungor VC. QERP: quality-of-service (QoS) aware evolutionary routing protocol for underwater wireless sensor networks. *IEEE Syst J*. 2017;12(3):2066–73. doi:10.1109/JSYST.2017.2673759.
7. Faheem M, Gungor VC. Energy efficient and QoS-aware routing protocol for wireless sensor network-based smart grid applications in the context of Industry 4.0. *Appl Soft Comput*. 2018;68(1):910–22. doi:10.1016/j.asoc.2017.07.045.
8. Anubha N, Bedi RPS, Khan AA, Haq MA, Alhussen A, Alzamil ZS. Efficient optimal routing algorithm based on reward and penalty for mobile adhoc networks. *Comput Mater Contin*. 2023;75(1):1331–51. doi:10.32604/cmc.2023.033181.
9. Devi Murugavel K, Ramadass P, Mahendran RK, Khan AA, Haq MA, Alharby S, et al. Maintaining effective node chain connectivity in the network with transmission power of self-arranged ad hoc routing in cluster scenario. *Electronics*. 2022;11(15):2455. doi:10.3390/electronics11152455.
10. Lee SW, Ali S, Yousefpoor MS, Yousefpoor E, Lalbakhsh P, Javaheri D, et al. An energy-aware and predictive fuzzy logic-based routing scheme in flying *ad hoc* networks (FANETs). *IEEE Access*. 2021;9:129977–30005. doi:10.1109/ACCESS.2021.3111444.
11. Mukherjee A, Keshary V, Pandya K, Dey N, Satapathy SC. Flying *ad hoc* networks: a comprehensive survey. In: *Information and Decision Sciences: Proceedings of the 6th International Conference on FICTA*; Singapore: Springer; 2018. p. 569–80.
12. Rahmani M, Ali S, Yousefpoor E, Yousefpoor MS, Javaheri D, Lalbakhsh P, et al. OLSR+: a new routing method based on fuzzy logic in flying *ad-hoc* networks (FANETs). *Veh Commun*. 2022;36:100489. doi:10.1016/j.vehcom.2022.100489.
13. Oubbati OS, Lakas A, Zhou F, Güneş M, Yagoubi MB. A survey on position-based routing protocols for Flying *Ad hoc* Networks (FANETs). *Veh Commun*. 2017;10:29–56. doi:10.1016/j.vehcom.2017.10.003.
14. Srivastava A, Prakash J. Future FANET with application and enabling techniques: anatomization and sustainability issues. *Comput Sci Rev*. 2021;39(2):100359. doi:10.1016/j.cosrev.2020.100359.
15. Zafar W, Khan BM. Flying *ad-hoc* networks: technological and social implications. *IEEE Technol Soc Mag*. 2016;35(2):67–74. doi:10.1109/MTS.2016.2554418.
16. Tareque MH, Hossain MS, Atiquzzaman M. On the routing in flying *ad hoc* networks. In: *2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*; Łódź, Poland: IEEE; 2015. p. 1–9.
17. Saif A, Dimiyati K, Noordin KA, Alsamhi SH, Hawbani A. Multi-UAV and SAR collaboration model for disaster management in B5G networks. *Internet Technol Lett*. 2024;7(1):e310. doi:10.1002/itl2.310.
18. Agrawal J, Kapoor M. A comparative study on geographic-based routing algorithms for flying ad-hoc networks. *Concurrency Comput Pract Exper*. 2021;33(16):e6253. doi:10.1002/cpe.6253.
19. Sang Q, Wu H, Xing L, Xie P. Review and comparison of emerging routing protocols in flying ad hoc networks. *Symmetry*. 2020;12(6):971. doi:10.3390/sym12060971.
20. Arafat MY, Moh S. Routing protocols for unmanned aerial vehicle networks: a survey. *IEEE Access*. 2019;7:99694–720. doi:10.1109/ACCESS.2019.2930813.
21. Khan MF, Yau KLA, Noor RM, Imran MA. Routing schemes in FANETs: a survey. *Sensors*. 2019;20(1):38. doi:10.3390/s20010038.
22. Sahingoz OK. Networking models in flying *ad-hoc* networks (FANETs) Concepts and challenges. *J Intell Robot Syst*. 2014;74(1–2):513–27. doi:10.1007/s10846-013-9959-7.
23. Malhotra A, Kaur S. A comprehensive review on recent advancements in routing protocols for flying ad hoc networks. *Trans Emerg Telecomm Technol*. 2022;33(3):e3688. doi:10.1002/ett.v33.3.
24. Örs FK, Levi A. Data-driven intrusion detection for 6LoWPAN based IoT systems. *Ad Hoc Netw*. 2023;143(4):103120. doi:10.1016/j.adhoc.2023.103120.
25. Sharma T, Mohapatra AK, Tomar G. SDBMND: secure density-based unsupervised learning method with malicious node detection to improve the network lifespan in densely deployed WSN. *Wireless Commun Mob Comput*. 2022;2022(1):9494476. doi:10.1155/2022/9494476.
26. Ji B, Zhang M, Xing L, Li X, Li C, Han C, et al. Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digit Commun Netw*. 2023;9(1):47–55. doi:10.1016/j.dcan.2022.06.012.

27. Gupta A, Pavani M, Kant Dargar S, Dargar A, Singh Chohan A. Improved extreme learning machine-based hunger games search for automatic IP configuration and duplicate node detection. *J Commun.* 2024;19(3):152–60. doi:10.12720/jcm.19.3.152-160.
28. Gebremariam GG, Panda J, Indu S. Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models. *Alexandria Eng J.* 2023;82(1):82–100. doi:10.1016/j.aej.2023.09.064.
29. Sengan S, Khalaf OI, Rao GRK, Sharma DK, Amarendra K, Hamad AA. Security-aware routing on wireless communication for E-health records monitoring using machine learning. *Int J Reliab Quality E-Healthc.* 2022;11(3):1–10. doi:10.4018/IJRQEH.289176.
30. Nie W, Chen Y, Wang Y, Wang P, Li M, Ning L. Routing networking technology based on improved ant colony algorithm in a space-air-ground integrated network. *EURASIP J Adv Signal Process.* 2024;2024(1):34. doi:10.1186/s13634-024-01131-5.
31. Pasikhan AM, Clark JA, Gope P. Incremental hybrid intrusion detection for 6LoWPAN. *Comput Secur.* 2023;135:103447. doi:10.1016/j.cose.2023.103447.
32. Yassein HT, Mesbah S, Madbouly MM. IoT routing attack detection using deep neural network. *Webology.* 2021;18:149–63. doi:10.14704/WEB/V18SI05/WEB18220.
33. Cárdenas LL, Mezher AM, Bautista PAB, León JPA, Igartua MA. A multimetric predictive ANN-based routing protocol for vehicular *ad hoc* networks. *IEEE Access.* 2021;9:86037–53. doi:10.1109/ACCESS.2021.3088474.
34. Kannimuthu P, Thangamuthu J. Decision tree trust (DTTrust)-based authentication mechanism to secure RPL routing protocol on the internet of battlefield thing (IoBT). *Int J Bus Data Commun Netw.* 2021;17(1):1–23. doi:10.4018/IJBDCN.2021010101.
35. Nemoto K, Matsutani H. A lightweight reinforcement learning-based packet routing method using online sequential learning. *IEICE Trans Inf Syst.* 2023;106(11):1796–807. doi:10.1587/transinf.2022EDP7231.
36. Rutravigneshwaran P, Anitha G. Security model to mitigate black hole attack on internet of battlefield things (IoBT) using trust and K-means clustering algorithm. *Int J Comput Netw Appl.* 2023;10(1):95–106. doi:10.22247/ijcna/2023/218514.
37. Ludwig B, Donabauer G, Ramsauer D, Subari KA. Urwalking: indoor navigation for research and daily use. *KI-Künstliche Intelligenz.* 2023;37(1):83–90. doi:10.1007/s13218-022-00795-1.
38. Wijesekara PADS, Gunawardena S. A machine learning-aided network contention-aware link lifetime-and delay-based hybrid routing framework for software-defined vehicular networks. *Telecom.* 2023;4(3):393–458. doi:10.3390/telecom4030023.
39. Ravi B, Varghese B, Murturi I, Donta PK, Dustdar S, Dehury CK, et al. Stochastic modeling for intelligent software-defined vehicular networks: a survey. *Computers.* 2023;12(8):162. doi:10.3390/computers12080162.
40. Hemalatha S, Trupthi M, Vaneeta M, Narayan Das N, Krishna RVV, Suresh Thangakrishnan M. Comparing watch dog algorithm and classification techniques with machine learning technique to detect the various attackers in mobile adhoc network. *J Theor Appl Inf Technol.* 2024;102(14):5469–81.
41. Tadros CN, Shehata N, Mokhtar B. Unsupervised learning-based WSN clustering for efficient environmental pollution monitoring. *Sensors.* 2023;23(12):5733. doi:10.3390/s23125733.
42. Chatterjee T, Karmakar R, Kaddoum G, Chattopadhyay S, Chakraborty S. A survey of VANET/V2X routing from the perspective of non-learning and learning-based approaches. *IEEE Access.* 2022;10:23022–50. doi:10.1109/ACCESS.2022.3152767.
43. Santos CLD, Mezher AM, León JPA, Barrera JC, Guerra EC, Meng J, et al. Machine learning-based routing protocol for wireless smart grid networks. *IEEE Access.* 2023;11:57401–14. doi:10.1109/ACCESS.2023.3283208.
44. Abdan M, Seno SAH. Machine learning methods for intrusive detection of wormhole attack in mobile *Ad Hoc* network (MANET). *Wirel Commun Mob Comput.* 2022;2022(1):2375702.
45. Garcia Ribera E, Martinez Alvarez B, Samuel C, Ioulianou PP, Vassilakis VG. An intrusion detection system for RPL-based IoT networks. *Electronics.* 2022;11(23):4041. doi:10.3390/electronics11234041.
46. Militani DR, de Moraes HP, Rosa RL, Wuttisittikulij L, Ramírez MA, Rodríguez DZ. Enhanced routing algorithm based on reinforcement machine learning—a case of VoIP service. *Sensors.* 2021;21(2):504. doi:10.3390/s21020504.

47. Liang H, Shang Y, Wang S. Study on DTN routing protocol of vehicle *Ad Hoc* network based on machine learning. *Wirel Commun Mob Comput*. 2021;2021(1):7965093. doi:10.1155/2021/7965093.
48. Ramírez PLG, Lloret J, Tomás J, Hurtado M. IoT-networks group-based model that uses ai for workgroup allocation. *Comput Netw*. 2021;186:107745.
49. Elsayed R, Hamada R, Hammoudeh M, Abdalla M, Elsaid SA. A hierarchical deep learning-based intrusion detection architecture for clustered internet of things. *J Sens Actuator Netw*. 2022;12(1):3.
50. Magaia N, Ferreira P, Pereira PR, Muhammad K, Ser JD, de Albuquerque VHC. Group'n route: an edge learning-based clustering and efficient routing scheme leveraging social strength for the internet of vehicles. *IEEE Trans Intell Transp Syst*. 2022;23(10):19589–601. doi:10.1109/TITS.2022.3171978.
51. Al Sawafi Y, Touzene A, Hedjam R. Hybrid deep learning-based intrusion detection system for RPL IoT networks. *J Sens Actuator Netw*. 2023;12(2):21. doi:10.3390/jsan12020021.
52. Shi Z, Peng T, Zhang L, Gao B, Wang H. An efficient cooperative routing with ml based energy efficiency model for distributed underwater WSN electricity meter warning system. *Scalable Comput Pract Exp*. 2023;24(4):1031–40.
53. Marwah GPK, Jain A, Malik PK, Singh M, Tanwar S, Safirescu CO, et al. An improved machine learning model with hybrid technique in VANET for robust communication. *Mathematics*. 2022;10(21):4030. doi:10.3390/math10214030.
54. Golla K, PallamSetty S. An efficient machine learning optimization model for route establishment mechanism in IoT environment. *Int J Comput Netw Commun (IJCNC)*. 2022;14(4):137–56. doi:10.5121/ijcnc.
55. Ramani S, Jhaveri RH. ML-based delay attack detection and isolation for fault-tolerant software-defined industrial networks. *Sensors*. 2022;22(18):6958. doi:10.3390/s22186958.
56. Sahay R, Nayyar A, Shrivastava RK, Bilal M, Singh SP, Pack S. Routing attack induced anomaly detection in IoT network using RBM-LSTM. *ICT Express*. 2024;10(3):459–64. doi:10.1016/j.ict.2024.04.012.
57. Park S, Hwang CG, Lee D. Performance evaluation of k-means and k-medoids in WSN routing protocols. *J Inf Commun Converg Eng*. 2022;20(4):259–64. doi:10.56977/jicce.2022.20.4.259.
58. Ahmad H, Zubair Islam M, Ali R, Haider A, Kim H. Intelligent stretch optimization in information-centric networking-based tactile internet applications. *Appl Sci*. 2021;11(16):7351. doi:10.3390/app11167351.
59. Gantassi R, Ben Gouissem B, Cheikhrouhou O, El Khediri S, Hasnaoui S. Optimizing quality of service of clustering protocols in large-scale wireless sensor networks with mobile data collector and machine learning. *Secur Commun Netw*. 2021;2021(1):5531185. doi:10.1155/2021/5531185.
60. Abadleh A, Btoush A, Alkawasbeh AA, Mahadeen A, Al-Hawari E, Tareef A, et al. Mitigating the effect of blackhole attacks in MANET. *J Eng Sci Technol Rev*. 2022;15(6):107–14. doi:10.25103/jestr.
61. Tan H, Ye T, Rehman S, Rehman O, Tu S, Ahmad J. A novel routing optimization strategy based on reinforcement learning in perception layer networks. *Comput Netw*. 2023;237(2):110105. doi:10.1016/j.comnet.2023.110105.
62. Nayak NKS, Bhattacharyya B. MAC protocol based IoT network intrusion detection using improved efficient shuffle bidirectional COOT channel attention network. *IEEE Access*. 2023;11:77385–402. doi:10.1109/ACCESS.2023.3299031.
63. Jeanita TJ, Sarasvathi V. A multi-agent reinforcement learning-based optimized routing for QoS in IoT. *Cybern Inf Technol*. 2021;21(4):45–61.
64. Sbai O, Elboukhari M. Mobile *Ad Hoc* networks intrusion detection system against packet dropping attacks. *Indones J Electr Eng Comput Sci*. 2022;26(2):819–25.
65. Mittal M, Kobielnik M, Gupta S, Cheng X, Wozniak M. An efficient quality of services based wireless sensor network for anomaly detection using soft computing approaches. *J Cloud Comput*. 2022;11(1):70. doi:10.1186/s13677-022-00344-z.
66. Rahmani AM, Naqvi RA, Yousefpoor E, Yousefpoor MS, Ahmed OH, Hosseinzadeh M, et al. A Q-learning and fuzzy logic-based hierarchical routing scheme in the intelligent transportation system for smart cities. *Mathematics*. 2022;10(22):4192. doi:10.3390/math10224192.
67. Zhao L, Zhao W, Hawbani A, Al-Dubai AY, Min G, Zomaya AY, et al. Novel online sequential learning-based adaptive routing for edge software-defined vehicular networks. *IEEE Trans Wirel Commun*. 2020;20(5):2991–3004. doi:10.1109/TWC.2020.3046275.

68. Ramesh S, Rajalakshmi R, Dwivedi JN, Selvaknmani S, Pant B, Bharath Kumar N, et al. Protocol in wireless sensor network using machine learning. *Comput Intell Neurosci.* 2022;2022(1):5393251.
69. Balatsouras CP, Karras A, Karras C, Karydis I, Sioutas S. WiCHORD+: a scalable, sustainable, and P2P chord-based ecosystem for smart agriculture applications. *Sensors.* 2023;23(23):9486. doi:10.3390/s23239486.
70. Abadi AFE, Asghari SA, Marvasti MB, Abaei G, Nabavi M, Savaria Y. RLBEED: reinforcement-learning-based energy efficient control and routing protocol for wireless sensor networks. *IEEE Access.* 2022;10:44123–35. doi:10.1109/ACCESS.2022.3167058.
71. Ajjaj S, El Houssaini S, Hain M, El Houssaini MA. Incremental online machine learning for detecting malicious nodes in vehicular communications using real-time monitoring. *Telecom.* 2023;4(3):629–48. doi:10.3390/telecom4030028.
72. Islam N, Haseeb K, Ali M, Jeon G. Secured protocol with collaborative IoT-enabled sustainable communication using artificial intelligence technique. *Sustainability.* 2022;14(14):8919. doi:10.3390/su14148919.
73. Dhinakaran D, Udhaya Sankar SM, Raja SE, Jasmine JJ. Optimizing mobile *Ad Hoc* network routing using biomimicry buzz and a hybrid forest boost regression-ANNs. *Int J Adv Comput Sci Appl.* 2023;14(12):92–104.
74. Dhiman G, Sharma R. SHANN: an IoT and machine-learning-assisted edge cross-layered routing protocol using spotted hyena optimizer. *Complex Intell Syst.* 2022;8(5):3779–87. doi:10.1007/s40747-021-00578-5.
75. Jeevaraj D. Feature selection model using naive bayes ML algorithm for WSN intrusion detection system. *Int J Electr Comput Eng Syst.* 2023;14(2):179–85. doi:10.32985/ijeces.14.2.7.
76. Verma RD, Samaddar SG, Samaddar AB. Securing BGP by handling dynamic network behavior and unbalanced datasets. *Int J Comput Netw Commun.* 2021;13:41–52. doi:10.5121/ijcnc.2021.13603.
77. Yıldırım E, Cicioğlu M, Çalhan A. Fog-cloud architecture-driven internet of medical things framework for healthcare monitoring. *Med Biol Eng Comput.* 2023;61(5):1133–47. doi:10.1007/s11517-023-02776-4.
78. George AM, Kulkarni SY, Kurian CP. Gaussian regression models for evaluation of network lifetime and cluster-head selection in wireless sensor devices. *IEEE Access.* 2022;10(4):20875–88. doi:10.1109/ACCESS.2022.3152804.
79. Crespo-Martínez IS, Campazas-Vega A, Guerrero-Higuera ÁM, Riego-DelCastillo V, Álvarez-Aparicio C, Fernández-Llamas C. SQL injection attack detection in network flow data. *Comput Secur.* 2023;127:103093. doi:10.1016/j.cose.2023.103093.
80. Ma X, Jiang Q, Shojafar M, Alazab M, Kumar S, Kumari S. Disbezant: secure and robust federated learning against byzantine attack in IoT-enabled MTS. *IEEE Trans Intell Transp Syst.* 2022;24(2):2492–502. doi:10.1109/TITS.2022.3152156.
81. Davaslioglu K, Soltani S, Erpek T, Sagduyu YE. DeepWiFi: cognitive WiFi with deep learning. *IEEE Trans Mob Comput.* 2019;20(2):429–44.
82. Golla K, Setty SP. A novel approach for enhancing the network lifetime of secure ML_RPL routing protocol in internet of things by using PROB_ATT_SCHEME. *Int J Emerg Technol Adv Eng.* 2022;12(4):115–29. doi:10.46338/ijetae0422_15.
83. Burange AW, Deshmukh VM. Trust based secured routing system for low power networks. *J Integr Sci Technol.* 2023;11(1):nema431–431.
84. Alsadhan A, Hussain A, Liatsis P, Alani M, Tawfik H, Kendrick P, et al. Locally weighted classifiers for detection of neighbor discovery protocol distributed denial-of-service and replayed attacks. *Trans Emerg Telecomm Technol.* 2022;33(3):e3700. doi:10.1002/ett.3700.
85. Karne RK, Sreeja TK. PMLC-predictions of mobility and transmission in a lane-based cluster VANET validated on machine learning. *Int J Recent Innov Trends Comput Commun.* 2023;11(5s):477–83. doi:10.17762/ijritcc.v11i5s.7109.
86. Zafar MH, Altalbe A. Prediction of scenarios for routing in MANETs based on expanding ring search and random early detection parameters using machine learning techniques. *IEEE Access.* 2021;9:47033–47. doi:10.1109/ACCESS.2021.3067816.
87. Alkanhel R, Khafaga DS, El-kenawy ESM, Abdelhamid AA, Ibrahim A, Amin R, et al. Hybrid grey wolf and dipper throated optimization in network intrusion detection systems. *Comput Mater Contin.* 2023;74(2):2695–709. doi:10.32604/cmc.2023.033153.

88. Sirajuddin M, Rupa C, Iwendi C, Biamba C. TBSMR: a trust-based secure multipath routing protocol for enhancing the QoS of the mobile *Ad Hoc* network. *Secur Commun Netw.* 2021;2021(1):5521713. doi:10.1155/2021/5521713.
89. Rashidibajgan S, Hupperich T. Improving the performance of opportunistic networks in real-world applications using machine learning techniques. *J Sens Actuator Netw.* 2022;11(4):61. doi:10.3390/jsan11040061.
90. Sebastin SS, Prabhu V, Parthasarathy V, Senthilkumar G, Gundu V. Intelligent data routing strategy based on federated deep reinforcement learning for IoT-enabled wireless sensor networks. *Meas: Sens.* 2024;31:101012. doi:10.1016/j.measen.2023.101012.
91. Ridwan MA, Radzi NAM, Azmi KHM, Abdullah F, Ahmad WSHMW. A new machine learning-based hybrid intrusion detection system and intelligent routing algorithm for MPLS network. *Int J Adv Comput Sci Appl.* 2023;14(4):94–107. doi:10.14569/IJACSA.2023.0140412.
92. Reddy VSN, Mungara J. Machine learning-based efficient clustering and improve quality of service in MANET. *Indian J Comput Sci Eng.* 2021;12(5):1392–9. doi:10.21817/indjcse/2021/v12i5/211205072.
93. Liu L, Lv H, Xu J, Shu J. A link quality estimation method based on improved weighted extreme learning machine. *IEEE Access.* 2021;9:11378–92. doi:10.1109/Access.6287639.
94. Satyanarayana RK, Selvakumar K. Bi-linear mapping integrated machine learning based authentication routing protocol for improving quality of service in vehicular *Ad-Hoc* network. *e-Prime-Adv Electr Eng, Electron Energy.* 2023;4:100145. doi:10.1016/j.prime.2023.100145.
95. Mertens JS, Panebianco A, Surudhi A, Prabagarane N, Galluccio L. Network intelligence vs. jamming in underwater networks: how learning can cope with misbehavior. *Front Commun Netw.* 2023;4:1179626. doi:10.3389/frcmn.2023.1179626.
96. Mahantesh HM, Guptha MN, Hema MS. Energy-QoS-aware data communication and optimal path selection in software-defined networks using EOMBA and IBSO. *SN Comput Sci.* 2023;4(6):813. doi:10.1007/s42979-023-02253-7.
97. Sampathkumar J, Malmurugan N. HELP-WSN-a novel adaptive multi-tier hybrid intelligent framework for QoS aware WSN-IoT networks. *Comput Mater Contin.* 2022;71(2):2107–23. doi:10.32604/cmc.2022.019983.
98. Wakili A, Bakkali S, Alaoui AEH. Machine learning for QoS and security enhancement of RPL in IoT-enabled wireless sensors. *Sens Int.* 2024;5(1):100289. doi:10.1016/j.sintl.2024.100289.
99. Lavanya K, Devi KV, Bapu BR. Deep reinforcement extreme learning machines for secured routing in internet of things (IoT) applications. *Intell Autom Soft Comput.* 2022;34(2):837–48. doi:10.32604/iasc.2022.023055.
100. Alsalmán L, Alotaibi E. A balanced routing protocol based on machine learning for underwater sensor networks. *IEEE Access.* 2021;9:152082–97. doi:10.1109/ACCESS.2021.3126107.
101. Adhikary S, Choudhury S. Mitigate inter-WBAN interference in body-to-body network to restrain epidemic spread. *SN Comput Sci.* 2022;4(1):68. doi:10.1007/s42979-022-01459-5.
102. Muzammal SM, Murugesan RK, Jhanjhi NZ, Humayun M, Ibrahim AO, Abdelmaboud A. A trust-based model for secure routing against RPL attacks in internet of things. *Sensors.* 2022;22(18):7052. doi:10.3390/s22187052.
103. Zahra F, Jhanjhi NZ, Brohi SN, Khan NA, Masud M, AlZain MA. Rank and wormhole attack detection model for RPL-based internet of things using machine learning. *Sensors.* 2022;22(18):6765. doi:10.3390/s22186765.
104. Wang Y, Han Z. Ant colony optimization for traveling salesman problem based on parameters optimization. *Appl Soft Comput.* 2021;107:107439. doi:10.1016/j.asoc.2021.107439.
105. Kaur M, Prashar D, Rashid M, Khanam Z, Alshamrani SS, AlGhamdi AS. A novel approach for securing nodes using two-ray model and shadow effects in flying *Ad-Hoc* network. *Electronics.* 2021;10(24):316. doi:10.3390/electronics10243164.
106. Kaur M, Prashar D, Rashid M, Khanam Z, Alshamrani SS, AlGhamdi AS. An optimized load balancing using firefly algorithm in flying *Ad-Hoc* network. *Electronics.* 2022;11(2):252. doi:10.3390/electronics11020252.
107. Lansky J, Rahmani AM, Malik MH, Yousefpoor E, Yousefpoor MS, Khan MU, et al. An energy-aware routing method using firefly algorithm for flying *Ad Hoc* networks. *Sci Rep.* 2023;13(1):1323. doi:10.1038/s41598-023-27567-7.
108. Goel M, Singh K, Jain S. The impact of machine learning based framework on network traffic performance in mobile *Ad Hoc* Networks. In: 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); Uttar Pradesh, India: IEEE; 2024. p. 1–6.