Indian Engineering Journal
ISSN: 2984-9047
Vol 4 Issue 1 (2026)

A Literature Survey on Secure and Energy-Efficient Routing Techniques in Manets

M. Selvi[1], Dr. R. Rajesh[2]
[1]Research Scholar, PG and Research Department of Computer Science, Kaamadhenu Arts and Science College Sathyamangalam, Tamilnadu, India.
[2]Assistant Professor, Department of Information Technology, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamilnadu, India.

Abstract:
Mobile Ad Hoc Networks (MANETs) are decentralized wireless networks that enable mobile nodes to communicate without fixed infrastructure. Due to their dynamic topology, limited bandwidth, and lack of centralized administration, MANETs are highly vulnerable to security threats such as black hole attacks, wormhole attacks, Sybil attacks, Distributed Denial of Service (DDoS), sinkhole attacks, and Man-in-the-Middle (MITM) attacks. Researchers have proposed various secure and energy-efficient routing mechanisms to improve network performance, reliability, and protection against malicious activities. This literature survey reviews recent advancements in MANET security, trust management, intrusion detection systems, blockchain integration, machine learning-based attack detection, cryptographic approaches, and energy-aware routing techniques. Several studies emphasize the use of trust-based routing, artificial intelligence, clustering methods, optimization algorithms, and blockchain technologies to enhance packet delivery ratio, throughput, network lifetime, and attack detection accuracy. The survey also highlights the limitations of existing approaches, including computational complexity, scalability issues, dependence on centralized nodes, and lack of real-world validation. Overall, this study provides a comprehensive understanding of current research trends and identifies future directions for developing lightweight, scalable, secure, and energy-efficient MANET frameworks suitable for IoT, VANET, healthcare, and smart city applications.
Keywords:- Mobile Ad Hoc Network (MANET) , Secure Routing, Energy Efficiency , Trust Management , Intrusion Detection System (IDS), Blockchain Technology, Artificial Intelligence, Network Security

Introduction

Mobile Ad Hoc Networks (MANETs) are self-configuring wireless networks composed of mobile nodes that communicate with one another without relying on fixed infrastructure or centralized administration. Each node in a MANET functions both as a host and as a router, forwarding packets to neighboring nodes in a multi-hop communication environment. MANETs are widely used in military communications, disaster recovery operations, healthcare systems, smart transportation, Internet of Things (IoT), and emergency rescue services because of their flexibility, scalability, and rapid deployment capabilities.

Despite their advantages, MANETs face several challenges due to their dynamic topology, limited battery power, bandwidth constraints, and open wireless medium. These characteristics make MANETs highly susceptible to various security threats and routing attacks such as black hole attacks, wormhole attacks, sinkhole attacks, Sybil attacks, packet dropping attacks, Distributed Denial of Service (DDoS), and Man-in-the-Middle (MITM) attacks. Such attacks can significantly degrade network performance by reducing packet delivery ratio, increasing delay, consuming energy, and compromising data confidentiality and integrity.

To address these challenges, researchers have developed several security and routing mechanisms aimed at improving secure communication, energy efficiency, trust management, intrusion detection, and quality of service (QoS) in MANETs. Modern approaches integrate advanced technologies such as machine learning, deep learning, blockchain, fuzzy logic, optimization algorithms, cryptographic schemes, and trust-based routing protocols. Techniques like Energy Efficient Routing Establishment (EERE), Fast Recursive Transmission Algorithm (FRTA), Trust-Based Energy Aware Routing (TEAR), Secure Cryptography-Based Clustering Mechanism (SCCM), and blockchain-enabled routing protocols have shown significant improvements in security, throughput, latency reduction, and attack detection accuracy.

In recent years, Artificial Intelligence (AI) and Machine Learning (ML) techniques have gained attention for identifying malicious nodes and mitigating network attacks in real time. Similarly, blockchain technology has emerged as a reliable solution for ensuring decentralized security, data integrity, authentication, and privacy

preservation in MANETs, VANETs, and IoT environments. Furthermore, optimization algorithms such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Whale Optimization, and Flower Pollination Algorithms have been employed to improve routing efficiency and energy conservation.
This literature survey analyzes various research contributions related to secure and energy-efficient routing protocols, trust management systems, intrusion detection systems, and blockchain-based security frameworks in MANETs. The study evaluates the merits and limitations of different techniques and identifies research gaps for future improvements. The survey aims to provide a detailed understanding of emerging technologies and methodologies that can strengthen the security, reliability, and performance of MANET environments.

Literature Survey

1. Bondada (2022) et.al In terms of security and energy efficiency, the suggested group key management-based routing strategy for MANETs performs better than competing methods. Two specialized nodes, known as the Calculator Key (CK) and the Distribution Key (DK), are employed in asymmetric key cryptography. Secret key generation, verification, and distribution are handled by these two nodes. Consequently, no extra processing is required on the part of other nodes to construct the secret keys. These nodes were chosen based on their trust levels and energy consumption. More energy is dispersed since each node is in charge of creating and distributing its own secret keys in the majority of the routing protocols in use today. Furthermore, there should be security breaches if any node is compromised. The security of the entire network remains unaffected when nodes other than the CK and DK are compromised. Numerous tests are conducted while taking into account both the suggested and current protocols. According to performance analyses, the suggested procedure performs better than the rival methods.

MERITS :
Surpasses current security and energy efficiency requirements.
DEMERITS :
Dependence on specialized nodes could be a single point of failure if compromised.

2. Sheela, M (2024) et.al suggested Fast Recursive Transmission Algorithm (FRTA) is intended to optimize routing, maximize data security, minimize the impact of malicious attacks, and choose the optimal way over the MANET by utilizing the Collision Detection Avoid Algorithm (CDAA). Known as proactive routing protocols, table-driven routing systems require that all network nodes maintain current routing information. Frequent updates to the routing table are sent throughout the network by these protocols, requiring modifications to the network topology in order to maintain consistent routing information for network nodes. These upgrades have a significant overhead. Network energy efficiency is increased and node data loss rates are decreased by the proposed FRTA algorithm.Table-driven routing methods, sometimes referred to as proactive routing protocols, require that all network nodes maintain current routing information. These protocols convey regular updates to the routing table throughout the network, requiring modifications to the network topology in order to maintain consistent routing information for network nodes. These enhancements come with a lot of overhead. The proposed FRTA algorithm improves network energy efficiency and reduces node data loss rates. The suggested approach outperforms other current assessments of the most sophisticated security and routing energy, end-to-end latency, packet transfer rate, and packet loss.

MERITS :
The FRTA algorithm improved network energy efficiency and decreased node data loss rates.
DEMERITS :
FRTA algorithm incurs higher computational complexity due to frequent routing table updates.

3. Jha, A (2023) suggested a hybrid approach that chooses the best path advancement leaps using cat slapped solo algorithms (C-SSA). This method would make it possible for MANETs to transport energy with confidence, security, and efficiency. Initial fuzzy clustering is used, and the number of clusters (CHs) is chosen based on how

important recent, implicit, and direct trust are. Nodes that depended on the trust threshold value were also found. The optimum routes are chosen here depending on lag, performance, and connection across this context, and even the CHs take part in wireless multi-hop routing. The optimal paths in this situation are found using the hybrid method that has been proposed. When compared to current methods, the suggested hybrid algorithm, C-SSA, offers 90% detection rate, secure, energy-efficient, and privacy-aware routing in MANETs.

MERITS :
The suggested approach decreased the energy need to 0.11 m electron volts and increased the detection rate to 90%.
DEMERITS :
C-SSA algorithm may have higher computational overhead due to fuzzy clustering and trust evaluation.

4. Kaur, M (2021) et.al suggested a concept for the Internet of Things (IoT) that is both safe and energy-efficient for e-health. Secure transmission and retrieval of biomedical pictures across IoT networks is the primary goal. To do this, the biological pictures are encrypted using the five-dimensional hyper-chaotic map (FDHC) and compressive sensing. But FDHC has a difficulty with hyper-parameter adjustment. FDHC then uses the adjusted attributes to produce the secret keys. Next, the input biological images are diffused and permuted using the secret keys that were obtained. To conduct encryption, permutation and diffusion procedures are applied to the input biological image row-wise and column-wise. Since the initial scrambled row and column determines the permutation and diffusion of each row and column, the suggested method is sensitive to the input images. Experimental results show that the suggested method performs better than the most advanced image encryption methods. The suggested framework can be utilized to secure communication in green IoT networks because it encrypts and decrypts images more quickly.

MERITS :
The proposed method enhances image encryption speed and security in IoT networks with improved performance over existing methods.
DEMERITS :
FDHC-based method struggles with hyper-parameter tuning, affecting encryption efficiency.

5. Shuaishuai Tan (2015) suggested. A fuzzy Petri net model is used in a trust-based routing system. FPNT-OLSR is created by expanding the OLSR protocol by evaluating the trust values of mobile nodes to choose secure paths with the highest trust value without the need for additional control messages. A fuzzy Petri net-based trust reasoning model is introduced in this technique to assess the trust values of mobile nodes. A trust-based routing algorithm is also suggested to choose a path with the highest path trust value out of all potential routes in order to prevent hostile or hacked nodes. The suggested trust model and trust-based routing algorithm, known as FPNT-OLSR, are then used to expand OLSR. A trust factor collection approach and an effective trust information propagation method that don't produce additional control messages are designed for the FPNT-OLSR implementation. The outcomes of the simulation demonstrate how successful FPNT-OLSR is at creating safe paths. Additionally, it outperforms current trust-based OLSR protocols in terms of overhead, average latency, and packet delivery ratio.

MERITS :
Reduces latency and overhead, increases packet delivery ratio, and is efficient in creating secure routes.
DEMERITS :
Large networks' possible processing overhead and the difficulty of evaluating trust.

6. Ahamed, U (2023) et.al improve the security of data communications between source and destination nodes in a MANET against network layer-based active attacks, a lightweight security mechanism is suggested. Blackhole is an active attack that operates at the network layer. Packet Delivery Ratio (PDR), Average End-to-End Delay

(AEED), Throughput, and Simulation Processing Time at Intermediate Nodes (SPTIN) are used to assess the network's performance. Each network's performance was compared using the controller network. Because of the blackhole assault, the experiment's PDR was 0.28%, AEED was infinity, and throughput was 0.33% when compared to the controller network. The PDR, AEED, Throughput, and SPTIN values of the suggested security mechanism were determined to be 98.0825%, 100.9346%, 99.9988%, and 96.5660%, respectively, when compared to the controller network's performance. Comparing the data packet delivery ratio to the controller network, it was 100.00%. The network that experienced a blackhole assault had the lowest PDR and the highest ADDR compared to the controller network. The network afflicted by the blackhole did worse than the controlling network. Regarding PDR, AEED, and throughput, the recommended security approach performs better than the controller network. The AEED and SPTIN results demonstrate that there are no intricate computations in the suggested approach. The solution's functionality can be extended to include a lightweight intrusion detection system to address various security threats in MANETs.

MERITS :
High throughput and packet delivery ratio, low complexity.
DEMERITS :
Might not provide a thorough response to every assault type.

7. Mohindra, A (2021) et.al created a Clustering Mechanism (SCCM) for MANET based on Secure Cryptography. Secure routing, encryption, signature generation, signature verification, and decryption were its components. The mobile nodes were connected once the network was established. The AOMDV routing protocol was then put into practice, creating secure routing between the source and destination. The original packet was then encrypted using Elliptic Curve Cryptography (ECC) and transformed into an unidentified format. As a result, the encrypted packet's signature was created and sent to the destination through the Region Head (RH) and further gateway nodes. The packet's validity was confirmed by the destination node using the signature verification procedure after it was received. Should it be legitimate, the receiver would accept the information and use the ECC decryption technique to decrypt it; if not, it would reject the packet and notify the base station. Using a variety of metrics, the simulation results assessed the suggested security mechanism's performance and contrasted it with alternative methods to demonstrate its superiority.

MERITS :
SCCM enhances data security with ECC-based encryption and secure routing in MANETs.
DEMERITS :
SCCM increases computational overhead due to encryption and signature verification processes.

8. Merlin, R (2019) provide a brand-new MANET trust-based energy-aware routing (TEAR) technique. The TEAR mechanism's primary features are its ability to mitigate BHs by dynamically generating different detection routes to identify BHs as soon as possible and for improving data route security by gaining nodal trust. More importantly, the TEAR mechanism can efficiently manage the generation and exchange of these multi-detection pathways for BH detection. To increase the energy efficiency and intended data route security, these multi-detection routes in the TEAR mechanism are essentially created by fully utilizing the energy in non-hotspots (i.e., without wasting the energy). The results of the theoretical and experimental study demonstrated that their TEAR mechanism performed better than the previous studies. Because the TEAR mechanism prevents black hole assaults and significantly raises the likelihood of successful data routing, it greatly extends the network's lifespan.

MERITS :
Increases the lifespan of networks and the security of data routes.
DEMERITS :
Complexity in managing multiple detection routes.

9. V. Nivedita (2021) suggested using a cluster-based architecture to increase energy efficiency using the adaptive clustering reputation model (ACRM). The suggested framework is used to address the issues of privacy, policy, and data protection. In order to achieve an efficient service recovery process, the master recovery timer (MRT) and the proposed ACRM-MRT approach—which incorporates both direct and indirect node trust computation—are developed. The service execution process is used to determine the service recovery time. The Sybil assault is the most damaging of the many attack types that might happen during data transmission in MANET. This study suggested a resilient system for Sybil attack detection and prevention in order to solve this issue. Ultimately, the effectiveness of the suggested approach is assessed in terms of time delay, throughput, energy efficiency, control overhead, and detection rate. The simulation results demonstrate that, in comparison to the current approaches, the suggested ACRM-MRT method can successfully improve time delay, throughput, energy efficiency, control overhead, and detection rate.

MERITS :
The suggested approach improves security and energy efficiency, although real-time fault recovery may take longer than expected.
DEMERITS :
ACRM-MRT increases computational complexity due to trust computations and Sybil attack detection.

10. Huda A. Ahmed (2024) et.al Suggests a new deep learning model-based optimized link state routing (OLSR) protocol. First, the Kaggle dataset is used to gather the input videos. Next, a novel twin-attention-based dense convolutional bidirectional gated network (SA_ DCBiGNet) model is used to locate the black-hole node. The extended osprey-aided optimized link state routing protocol (EO_OLSRP) approach is then used to route once the nearby nodes have been examined using trust values. Similar to this, the expanded osprey optimization algorithm (EOOA) chooses the best feature by taking into account variables like link and node stability. In order to enhance the security of MANET data, blockchain storage is incorporated through the use of interplanetary file system (IPFS) technology. Furthermore, a delegated proof-of-stake (DPoS) consensus approach is used to validate the suggested blockchain system. The suggested approach makes use of Python and is tested with data obtained from different mobile simulator models in addition to the NS3 simulator. With a packet-delivery ratio (PDR) of 91.6%, average end delay (AED) of 23.6 s, and throughput of 2110 bytes, the suggested model outperforms the current approaches, which have respective PDRs of 89.1%, AEDs of 22 s, and throughputs of 1780 bytes.

MERITS :
Improves security with deep learning and attains low latency and 99.8% packet delivery.
DEMERITS :
Lack of real-world validation limits scalability and adaptability to various attackers.

11. Bukohwo Michael Esiefarienrhe (2022) uses a network protocol known as the optimal link state routing protocol (OLSR) to provide a security framework that is QoS-aware in MANETs. This framework aims to close the gap between security and QoS objectives, which may not always be equivalent, in order to provide a MANET that operates as efficiently as possible. Via a network sinkhole attack, the framework's throughput, jitter, and delay are assessed. The implementation of a sinkhole attack using OLSR, the design and implementation of a lightweight intrusion detection system using OLSR, and a framework that eliminates phony routes and optimizes bandwidth are the contributions of this study. In terms of network throughput, the simulation results showed that the QoS-aware framework improved network performance by over 70%. Compared to when the network was under attack, there was a nearly 85% decrease in delay and jitter.

MERITS :
The framework enhances QoS and security, optimizing throughput and reducing delays for video streaming.
DEMERITS : The framework overlooks energy efficiency, which is essential for managing battery power in resource-constrained environments.

12. K. Rajkumar (2024) suggested a new security paradigm for mitigating wormholes. To identify an active wormhole attack in MANET, their security architecture makes use of the attack model. Their framework's main idea is that an admin node is selected from a list of reliable nodes. Every so often, a boomerang packet is sent over the network by the admin node. The packet that is meant to return to the admin node itself is known as a boomerang packet. When the boomerang packet returns, the administrator determines if it has been the target of a wormhole attack based on its current condition. If a wormhole attack is possible, precautions are taken to lessen the impact of the attack. They used the NS-3.26 simulator to do extensive trials, and they compared the outcomes with the most advanced systems. With 97% accuracy, our method was able to identify the wormhole nodes. In addition, the packet loss rate during the wormhole attack was lower than that of other cutting-edge systems. This resulted from the early and precise identification of the MANET wormhole attack.

MERITS :
The suggested system reduces packet loss and achieves 97% wormhole attack detection accuracy, improving MANET security.
DEMERITS :
By depending on an admin node for boomerang packet testing, system resilience is at risk in the event that the node is compromised or fails.

13. Tanweer Alam (2020) The Cloud-MANET-IoT Integrated Framework's suggested Efficient and Secure Data Transmission Approach has the potential to be a significant component of several 5G communication systems. This framework was created by the authors to improve interaction efficiency. The cloud architecture is based on such a diverse structure that it acquires several security concerns or precautions related to distributed concepts. Data transmission security problems or barriers that rely on the factors that make cloud computing appealing. Furthermore, a lot of these extra threats have gotten stronger in the majority of cloud frameworks. The authors have examined communication security issues and security needs for all linked devices across cloud services.

MERITS :
In Cloud-MANET-IoT integrated settings for 5G scenarios, the suggested framework enhances data transfer, interaction efficiency, and security.
DEMERITS :
The lack of thorough implementation and evaluation in the research casts doubt on its practical applicability.

14. DhinaharanNagamalai (2020) et al. uses the Optimized Link State Routing Protocol (OLSR) network protocol to provide a QoS-aware security framework for MANETs. This framework aims to close the gap between security and QoS objectives, which may not always be similar, in order to provide a MANET that operates at its best. This article outlines the different security objectives, threats, and issues in MANETs as well as the current security assault defense techniques and designs. A security keying system is also included in this framework to determine QoS. Through its Multi-point Relays (MPRs) capabilities, the keying system is connected to the OLSR protocol's fundamental configuration. The suggested framework maximizes time and network resource utilization.

MERITS :
The framework optimizes security and QoS in MANETs by utilizing OLSR protocol's MPR functionality for efficient resource and time management.
DEMERITS :
The framework's reliance on OLSR protocol limits its compatibility with other routing protocols in MANETs.

15. Khan, D. M.(2020) et.al proposed the Blackhole attack prevention strategy for MinMax Ant Colony Optimization. The Ant Colony Optimization Algorithm λ-MMAS is employed in this study to address precise route finding in mobile ad hoc networks. Extending previous findings with the unusual example of a single MMA, this study focuses on a vertical ideal process that uses all types of ideal state λ nodes. In a fixed number of times

per unit, They have shown that the most dynamic paths can also be handled by the λ-MMAS. Plans for detailed comparisons (by maintaining a proximity of about 0.5 premiums for its effects). The λ-MMAS settings allow you to check changes in brain-boggling challenges. For instance, lowering the outcomes of the malicious routes with a constant phase length, which includes two weight capabilities and malicious route reduction. The route data will be saved in reactive routing protocol formats once the route discovery has been found. Because any device must deliver data, the Reactive Routing Protocol operates on demand. This means that route configuration is repeated based on the nodes' requirement to provide data. Because of their ant colony optimization (MAX-MIN anti-system), If uses reactive routing protocols and has low-end head concerns, the above-the-resolution solution will be removed. The reactive routing strategy will be used to stop Black Hole Attacks and data loss during transfers.

MERITS :
In MANETs, the λ-MMAS algorithm improves route finding, guards against black-hole attacks, and guarantees effective data transfer.
DEMERITS :
The approach's convergence time is dependent on the choice of pheromone parameter, it has trouble with big networks, and it is limited in its ability to initially exclude malevolent hubs.

16. R. Basri (2025) provide a trust method to determine an IoT network's communication trust. The packet delay brought on by MITM attacks during packet transmission is taken into account when calculating each packet-wise instantaneous communication trust (IPCTCM) in the suggested model. The normal distribution is used to replicate the MITM attack-induced delays, which are then injected into the testbed data produced in our IoT lab. They model the delays using a normal distribution since MITM assaults usually follow a random pattern of occurrence. As a result, they assume that delays cluster around the central value of the distribution, increasing the possibility that attackers might successfully hide their malicious activity and making it more difficult to identify them. According to their IPCTCM results, there is a clear correlation between a noticeable drop in trust levels and an increase in packet transmission delays brought on by attacks. Their IPCTCM's ability to identify all active attacks using its instantaneous communication trust values that are sensitive to attack delays (DA) is another important advantage. This is because an active MITM attack adds additional E2E delays. Additionally, IPCTCM outperforms PIE-IDS by having the highest detection accuracy for MITM attacks.

MERITS :
The IPCTCM model excels in MITM attack detection with higher accuracy and sensitivity to delay-induced trust variations.
DEMERITS :
The assumption of normal distribution for MITM attack delays may restrict the model's real-world applicabilit.

17. Sivanesan. Na (2025) et.al compares the use of machine learning (ML) to reduce DDoS attack traffic and separate it from non-threatening traffic. In accordance with certain standards, this is done to mitigate security dangers in the network and prevent multiple attacks. In order to reduce the susceptibility of both conventional and SDN-IoT setups to DDoS attacks, the study employed machine learning-based methodologies. Determining whether SDN and SDN-IoT platform is more adept at identifying DDoS assaults and assessing how effectively both platforms function when paired with machine learning techniques are thus the main objectives of the comparison study. After protecting data packets and transmissions, this study employs a defensive MANET and machine learning to find susceptible nodes. A more effective technique for thwarting DDoS attacks has been achieved by combining ML models with different SDN procedures in WSN. In both a traditional and an Internet of Things context, this study employed three different machine learning approaches using SDN. As a result, EFACNN has a 98% success rate in defending IoT devices against distributed denial of service (DDoS) assaults, outperforming the other two machine learning techniques. Additionally, EFACNN obtains a 98.81% success rate when paired with ETC and hyperparameter modification. The comparison results show that adjusting the

hyperparameter is essential for enhancing the performance of the ML technique in DDoS attack detection and mitigation in SDN.

MERITS :
In both conventional and SDN-IoT contexts, the EFACNN model with hyperparameter change utilizing ETC has a 98.81% success rate in thwarting DDoS attacks.
DEMERITS :
The method's reliance on certain ML models and intricate hyperparameter tuning may provide challenges in real-time IoT networks.

18. Clement Daah (2025) et.al introduces an innovative way to improve financial institution security by combining blockchain technology, a hybrid access control system, and a Zero Trust architecture. Blockchain guarantees data integrity and non-repudiation by securing digital identities and transaction logs through its immutable ledger, while Zero Trust imposes constant authentication and dynamic access limits. Using Ethereum-Ganache-enhanced OMNeT++ simulations, the suggested system demonstrates enhanced resistance to insider threats and other assaults, decreased false positives, and improved detection accuracy. By creating strong audit trails, it also improves adherence to regulatory standards and safeguards sensitive financial data.

MERITS :
For financial institutions, the combination of blockchain technology and Zero Trust architecture improves security, detection precision, and regulatory compliance.
DEMERITS :
Reliance on blockchain and ongoing authentication could result in computational cost that compromises performance and scalability.

19. Moutaz Alazab (2024) et.al provide a thorough picture of the cybersecurity threat landscape by integrating several data sources, such as corporate network logs, open-source intelligence, and dark web surveillance, into a new multi-layered threat intelligence architecture. In contrast to earlier research, In order to incorporate these various features into machine-learning algorithms (XGBoost, Gradient Boosting, LightGBM, Extra Trees, Random Forest, Decision Tree, K-Nearest Neighbor, Gaussian Naive Bayes, Support Vector Machine, Linear Discriminant Analysis, Logistic Regression, AdaBoost, Quadratic Discriminant Analysis, and Gaussian Naive Bayes) in a distinctive manner, their approach employs a range of feature selection algorithms (information gain, correlation coefficient, chi-square, fisher score, forward wrapper, backward wrapper, backward wrapper, backward wrapper, and Ridge classifier). The real-world LITNET-2020 dataset was used to evaluate the proposed architecture. The architecture's resilience was proven by extensive testing against real-world cyberattacks, such as phishing and malware, which produced remarkable outcomes. With a detection accuracy of 99.98%, precision of 99.97%, and recall of 99.96%, XGBoost in particular showed the best performance, greatly outperforming conventional techniques. Additionally, both LightGBM and Gradient Boosting performed exceptionally well, achieving 99.97% recall, accuracy, and precision. Their results highlight how well Their architecture significantly improves an organization's ability to identify and promptly respond to cyber threats. This study contributes to the field of cybersecurity by creating a thorough threat intelligence framework, which offers a strong instrument for boosting organizational resilience against cyberattacks.

MERITS :
The multi-layered architecture with XGBoost uses cutting-edge machine learning algorithms to detect threats in real time with 99.98% accuracy, precision, and recall.
DEMERITS :
The reliance on computationally intensive ML models may hinder scalability in resource-limited environments.

20. Shahbaz Siddiqui (2024) provides a novel framework for adaptive security governance designed for smart cities. This framework ensures data security and privacy during smart service interoperability by utilizing dynamic security regulations that are applied through smart contracts. With the integration of multi-chain blockchain technology, smart services APIs, and SoftwareDefined Networking (SDN), real-world use examples in collaborative smart city environments verify the framework and demonstrate how it can improve security and efficiency in collaborative services. In order to address administrative concerns and prioritize data security and privacy, this study helps create safe and effective collaborative services inside smart cities. Their analysis demonstrates how the suggested security framework is scalable, made possible by essential elements like the Blockchain memory pool and SDN controller. The Blockchain memory pool guarantees the integrity and immutability of security-related transactions and data, while the SDN controller facilitates centralized management and effective communication amongst smart services. In the future, incorporating a privacy management module into smart service interoperability could improve data confidentiality, user privacy, and adherence to privacy laws.

MERITS :
The architecture ensures scalable, privacy-focused collaborative services by utilizing multi-chain blockchain, SDN, and smart contracts to enhance security and efficiency in smart cities.
DEMERITS :
The framework's performance may differ because of resource and environmental requirements, and it lacks real-world validation.

21. Ahmed M (2024) presents a novel method for detecting attacks on the Ad Hoc On-Demand Distance Vector (AODV) routing protocol in MANETs, particularly ones that use malicious nodes that use AODV's sequence numbers to pose as the optimum routing paths. To provide safe communication between various MANET nodes, an addition to the AODV protocol is presented. A signature verification process based on the Edwards digital signature curve (Ed25519), which is illustrated on the Objective Modular Network Testbed in C++ (OMNet++) simulator, is part of the suggested security mechanism. To ensure a high level of security, Their approach creates and verifies digital signatures by introducing asymmetric cryptography into the AODV protocol. To detect rogue nodes in the network, a novel detection method is also added as an extra security layer. The simulation findings demonstrate a high detection rate, accurately identifying between 83% and 100% of malicious nodes based on their presence in the network.

MERITS :
The AODV protocol addition guarantees strong security and high malicious node detection (83–100%) with Ed25519-based digital signature verification.
DEMERITS :
In resource-constrained MANETs, asymmetric cryptography may result in higher processing overhead, which could impact scalability and efficiency.

22. Amit Mittal (2024) et.al presented a successful decentralized Consensus Blockchain technique in light of VANETs' low storage capacity and susceptibility to attacks and their devices. In this proposed solution, blockchain technology is becoming more and more popular because of its decentralized, distributive, cooperative maintenance, and non-tampering nature. This article presents a decentralized VANET consensus architecture based on blockchain technology. The DC blockchain was used to establish the decentralization and node authentication for the car network. The Vehicular Ad-Hoc blockchain is used to achieve network security. The suggested method lowers DoS and false reputation in VANETs, enhances attack detection, and improves the security authentication procedure by 84%. Impersonation, replay, false reputation, denial of service, and device injection have all been assessed and contrasted with the suggested system and current techniques in the security analysis.

MERITS :
VANET security is increased by 84% using the decentralized consensus blockchain technique, which also lowers DoS and fake reputation attacks.
DEMERITS :
Real-time communication may be impacted by the high processing needs and delays that come with integrating blockchain into VANETs.

23. Jun Zhou (2015) et.al The collaboration of mobile patients in the same social group for both hierarchical and dispersed environments proposes a safe and privacy-preserving key management technique that is resistant to time-based and location-based mobile attacks. Additionally, it uses the blinding technique to implant the symmetric structure of the human body into Blom's symmetric key mechanism with modified proactive secret sharing, protecting patient identification, sensor deployment, and location privacy. In particular, the cloud server is contracted to handle the computationally demanding privacy-preserving key material updating, and the energy-constrained WBANs benefit greatly from the unaltered pairwise keys following key material updating. Lastly, the results of the security analysis and simulation demonstrate that our scheme performs significantly better than the others in terms of thwarting mobile attacks and reducing the overhead of computing, storage, and communication.

MERITS :
The suggested key management system uses outsourcing and effective key updates to save resource consumption while improving security and privacy in cloud-assisted WBANs.
DEMERITS :
Cloud trustworthiness vulnerabilities may arise when computationally demanding operations are outsourced to the cloud, thereby impacting the system's overall security.

24. V. Anjana Devi (2024) The Energy Efficient Routing Establishment (EERE) system determines the energy level of nodes in the network and uses hybrid whale positions along with the Flower Pollination Algorithm (WP-FPA) for optimal path allocation. Additionally, in order to guarantee network security, Aggregated Packet Control Trust Protocol (APCTP) has estimated the trust value for each participating node on the network using a trust evaluation factor. Mitigated nodes in the path are recognized and removed by the trust assessment factor and the knowledge about the node's neighbors, improving security. Metrics including average residual energy, packet delivery ratio (PDR), packet latency, and network lifetime are used to compare how well the suggested security-based routing techniques perform. In specified node mobility, the suggested EERE-APCTP techniques increase residual energy by 80%. The network lifetime is extended to 265 milliseconds and the packet delivery ratio is raised to 99%. There is a 0.6% decrease in routing overhead.

MERITS :
The EERE scheme improves network performance, achieving high packet delivery, residual energy, and prolonged lifetime, while ensuring security through trust-based mitigation.
DEMERITS :
In large-scale networks, hybrid algorithms like WP-FPA may impact real-time adaptation by increasing computing complexity.

25. G.R. Rama Devi (2023) et.al A cross-layered routing system that uses a modified contention window technique and is based on particle swarm optimization (PSO). The PSO algorithm uses the traffic index, average energy load, data success rate, and trust value parameters—all of which are calculated from the network layer—to create reliable and energy-efficient routing routes. Following the establishment of routing channels, the network's contentions are monitored using average energy loads and MAC layers for communications.The following constraints are used to calculate node trust: quality trust, which is determined by node QoS, and group trust, which is delivered by neighbor nodes. To improve data security and integrity, dual authentications with EnDA (improved dual authentication) employ key management techniques. Communications security is increased by using Diffie-

Hellman key exchanges with bilinear maps and elliptical curve cryptography (ECC). The proposed protocol performed satisfactorily when evaluated in terms of energy consumption and secure key agreements during network communications.

MERITS :
The ESCL-PSO protocol improves packet delivery and lowers energy consumption by utilizing PSO, dual authentication, and sophisticated encryption to improve energy efficiency and secure routing.
DEMERITS :
Real-time performance may be impacted by increased computational cost resulting from the integration of cross-layer optimizations and sophisticated cryptography algorithms.

26. C. Edwin Singh (2023) et.al suggested the PCA-FELM, a new fuzzy extreme learning machine based on Principal Component Analysis. Fuzzy Extreme Learning Machine is used to classify the features after they have first been extracted using Principal Component Analysis. With MAT LAB, the suggested PCA-FELM is put into practice. Fuzzy Extreme Learning Machine is used to classify the features after they have first been extracted using Principal Component Analysis. Increasing detection rates in this way can enhance network security. With MAT LAB, the suggested PCA-FELM is put into practice. When compared to other current techniques like DBN-IDS, GOA-SVM, and SDAE-ELM, the suggested PCA-FELM gets a greater accuracy of 99.08% from the comparison. Tests conducted on the KDD Cup99 dataset demonstrate that the proposed PCA-FELM model performs better than other methods already in use. The system will soon be enhanced to detect more network assaults by adding more parameters to the suggested attack detection technique. Future research should consider different types of attacks to improve network performance.

MERITS :
The PCA-FELM model achieves 99.08% accuracy in network attack detection, outperforming DBN-IDS, GOA-SVM, and SDAE-ELM.
DEMERITS :
The PCA-FELM model's relevance to contemporary and changing network threats may be limited by the usage of the KDD Cup99 dataset.

27. S Vijayalakshmi (2023) et.al One possible way to overcome vulnerabilities is to create an Intrusion Detection System (IDS) that is appropriate for the security requirements and features of ad hoc networks in order to provide effective and efficient performance against invasions. Because harmful nodes are identified early on and removed from the network, Their method has increased the packet delivery rate by 42% even when hostile nodes are present. Reliability in security can be increased by identifying collisions between different attacking nodes. Their work is AODV-focused and applicable to different routing strategies. This study focuses on partial and total dropping to address various misbehavior patterns in the forwarding phase. To effectively manage the various kinds of traffic, it can be enhanced by dynamically altering the rating policy. Additional strategies are required for future study in order to enable QoS and improve network fairness.

MERITS :
The proposed IDS enhances packet delivery by 42% by detecting and eliminating malicious nodes, ensuring better security and performance.
DEMERITS :
The technique is less successful against other network threats because it is restricted to packet dropping.

28. M. Arun (2023) et.al In order to provide QoS parameters, suggest an adaptive congestion and energy aware multipath routing scheme (ACEAMR) that can dynamically adjust to network changes. In order to estimate connection stability and notify nodes in advance of link failure, ACEAMR takes stable link prediction (SLP) into account. A stable link guarantees the most bandwidth for effective data transfer by being chosen depending on

the channel availability state. When determining a route, ACEAMR takes into account nodes that have enough residual energy, uses the queue occupancy function to evaluate the level of congestion, divides the traffic load over several paths, and increases the network lifetime. Two scenarios of varied mobility speed and varying simulation time are explored in order to conduct various ACEAMR tests on the simulation tool. In terms of throughput, delay, packet delivery ratio, overhead, and energy consumption, experimental results demonstrate that ACEAMR performs better than the current LLECP-AOMDV, OLEADM, and AOMDV routing schemes. Mobile nodes are susceptible to a wide range of security risks and assaults because of their open environment. In the future, secrecy and secure data transfer can be achieved by designing a secure routing scheme that uses a trust assessment model to fight against various kinds of attacks.

MERITS :
ACEAMR optimizes traffic distribution, reducing delays and improving network throughput and lifetime by considering node congestion and residual energy.
DEMERITS :
The scheme's absence of security threat protection leaves nodes open to wormhole and black hole attacks.

29. Deepa Krishnan (2015) a programmable mobile agent-based distributed self-adaptive intrusion detection system (IDS), which can serve as a vital line of defense against significant security breaches. Combining the two IDS trends—rule-based and behavior-based schemes—is how the suggested intrusion detection model is set up. Additionally, this model highlights the advantages of both host-based and network-based intrusion detection systems and deploys them intelligently while taking MANETs' crucial characteristics into account. This is an effective architecture that is self-adaptive and mindful of the inherent limitations of MANETS, in contrast to many proposed and implemented IDSs. Additionally, using lightweight mobile agents offers a minimal overhead technique that is ideally suited to the features of MANETs. This study attempts to improvise the mobile agents by making them tamper obvious, which is crucial because the agents could be compromised, rendering all of the IDS's efforts pointless.

MERITS :
The suggested IDS is perfect for the dynamic and resource-constrained nature of MANETs since it improves adaptability and lowers overhead.
DEMERITS :
In high-threat situations, a hacked mobile agent might compromise the entire IDS, decreasing system dependability.

30. Yulliwas Ameur (2024) provides a novel architecture for enhancing privacy in vehicle ad hoc networks (VANETs) by fusing homomorphic encryption with machine learning algorithms. Due to their dynamic and diversified nature, VANETs—which are essential for Intelligent Transport Systems (ITS)—have numerous privacy and security concerns. Their technology use K-nearest neighbors (KNN), a simple yet effective machine learning technique, to get around these challenges and safeguard the network's security and privacy. The ability to add more machine learning algorithms to the framework increases its flexibility and effectiveness in a variety of VANET settings.
The use of homomorphic encryption (HE), a cryptographic approach that permits calculations on encrypted data without the need for decryption, is essential to this framework. This function protects the privacy of data and enables safe calculations by third parties. The development and varieties of homomorphic encryption are covered in this work, with a focus on the significance of Fully Homomorphic Encryption (FHE) and its capacity to assess complex polynomial functions.

MERITS :
Data leakage hazards in VANETs are reduced and privacy protection is improved when homomorphic encryption and machine learning are combined.

DEMERITS :
Homomorphic encryption ensures privacy but introduces high latency and resource consumption, limiting real-time application feasibility in VANETs.

Conclusion
Mobile Ad Hoc Networks (MANETs) have become an important area of research because of their flexibility, decentralized nature, and applicability in various real-world scenarios such as military operations, disaster management, healthcare systems, smart cities, IoT, and vehicular networks. However, MANETs face major challenges related to routing reliability, energy consumption, security vulnerabilities, and dynamic topology changes. The absence of centralized infrastructure makes these networks highly vulnerable to attacks including black hole, wormhole, sinkhole, Sybil, DDoS, and MITM attacks.
The literature survey reveals that numerous researchers have proposed secure and energy-efficient routing mechanisms to address these issues. Trust-based routing protocols, clustering techniques, cryptographic frameworks, machine learning models, deep learning algorithms, and blockchain-based approaches have significantly improved packet delivery ratio, throughput, attack detection accuracy, network lifetime, and overall communication security. Techniques such as FRTA, TEAR, SCCM, FPNT-OLSR, EERE, ACEAMR, and PCA-FELM demonstrate strong performance in securing MANET communications while optimizing energy utilization.
Recent advancements in Artificial Intelligence and Machine Learning have enabled intelligent detection and mitigation of malicious activities in MANETs. Similarly, blockchain technology and Zero Trust architectures provide decentralized authentication, data integrity, and secure communication frameworks for IoT, VANETs, and smart city applications. Although these methods achieve higher security and efficiency, several limitations still exist, including increased computational overhead, scalability issues, complex trust evaluation, dependency on specialized nodes, and lack of real-time implementation.
Future research should focus on developing lightweight, scalable, and adaptive security mechanisms capable of operating efficiently in resource-constrained MANET environments. Integrating AI-driven intrusion detection systems, blockchain-enabled trust management, and energy-aware routing protocols can further improve network resilience and reliability. Additionally, real-world implementation and performance validation are necessary to ensure the practicality and effectiveness of proposed solutions in dynamic network environments.
Overall, the reviewed studies demonstrate that combining secure routing, trust management, optimization algorithms, and intelligent attack detection mechanisms can substantially enhance the security, efficiency, and reliability of MANETs for next-generation wireless communication systems.

REFERENCES

[1] Bondada, P., Samanta, D., Kaur, M., & Lee, H. (2022). Data Security-Based Routing in MANETs Using Key Management Mechanism. Applied Sciences. https://doi.org/10.3390/app12031041.
[2] Sheela, M., Suganthi, R., Gopalakrishnan, S., Karthikeyan, T., Jyothi, K., & Ramamoorthy, K. (2024). Secure Routing and Reliable Packets Transmission In MANET Using Fast Recursive Transfer Algorithm. Babylonian Journal of Networking. https://doi.org/10.58496/bjn/2024/009.
[3] Jha, A., Vivek, V., Gupta, P., Joshi, R., Singh, P., & Iyengar, N. (2023). Trust aware secure energy efficient hybrid protocol for MANET. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 1105-1109. https://doi.org/10.1109/AISC56616.2023.10085229.
[4] [4]. Kaur, M., Singh, D., Kumar, V., Gupta, B., & El-Latif, A. (2021). Secure and Energy Efficient-Based E-Health Care Framework for Green Internet of Things. IEEE Transactions on Green Communications and Networking, 5, 1223-1231. https://doi.org/10.1109/TGCN.2021.3081616.
[5] Tan, S., Li, X., & Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30, 84-98. https://doi.org/10.1016/j.adhoc.2015.03.004.
[6] Ahamed, U., & Fernando, S. (2023). Lightweight Security Mechanism to Mitigate Active Attacks in a Mobile Ad-hoc Network. International Journal of Electronics and Telecommunications. https://doi.org/10.24425/ijet.2022.139862.
[7] Mohindra, A., & Gandhi, C. (2021). A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET. , 18. https://doi.org/10.48048/WJST.2021.8987.

[8] Merlin, R., & Ravi, R. (2019). Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. Wireless Personal Communications, 104, 1599 - 1636. https://doi.org/10.1007/s11277-019-06120-8.

[9] V. Nivedita and N. Nandhagopal (2021). Trust Management-Based Service Recovery and Attack Prevention in MANET. Intelligent Automation & Soft Computing DOI:10.32604/iasc.2021.017547

[10] Huda A. Ahmed and Hamid Ali Abed AL-Asadi (2024). An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks. J. Sens. Actuator Netw. 2024, 13, 22. https://doi.org/10.3390/jsan13020022.

[11] Bukohwo Michael Esiefarienrhe, Thulani Phakathi and Francis Lugayizi (2022) Node-Based QoS-Aware Security Framework for Sinkhole Attacks in Mobile Ad-Hoc Networks. Telecom 2022, 3, 407–432. https://doi.org/10.3390/telecom 3030022.

[12] K. Rajkumar; S. Mercy Shalinie; Nagarathna Ravi; R. Rajesh Alias Harinarayan (2024). Boomerang Packet Testing to Mitigate Wormhole Attack in MANET, International Conference on Computing Communication and Networking Technologies (ICCCNT) DOI: 10.1109/ICCCNT61001.2024.10725065

[13] Tanweer Alam. Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework. *Journal of Telecommunication, Electronic and Computer Engineering.* Vol 12(1). 2020.

[14] DhinaharanNagamalai et al. (Eds): CSEIT, WiMoNe, NCS, CIoT, CMLA, DMSE, NLPD - 2020 pp. 91-108, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101109

[15] Khan, D. M., Aslam, T., Akhtar, N., Qadri, S., Khan, N. A., Rabbani, I. M., Aslam, M. (2020). Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique. Information Technology and Control, 49(3), 308-319. https://doi.org/10.5755/j01.itc.49.3.25265

[16] R. Basri, G. Karmakar, S.H.S. Newaz et al., Enhancing IoT security: Assessing instantaneous communication trust to detect man-in-the-middle attacks, Future Generation Computer Systems (2025), doi: https://doi.org/10.1016/j.future.2025.107714.

[17] Sivanesan. Na, N. Parthibanb , S. Vijayc , S.N. Sheela (2025), "Comparison of mitigating DDoS attacks in software defined networking and IoT platforms", http://www.keaipublishing.com/en/journals/cyber-security-and-applications/. Publishing Services by Elsevier.

[18] Clement Daah , Amna Qureshi, Irfan Awan, Savas Konur (2025), "Simulation-based evaluation of advanced threat detection and response in financial industry networks using zero trust and blockchain technology", Volume 138, 103027, ISSN 1569-190X, https://doi.org/10.1016/j.simpat.2024.103027.(https://www.sciencedirect.com/science/article/pii/S1569190X24001412).

[19] Moutaz Alazab, Ruba Abu Khurma, Maribel García-Arenas, Vansh Jatana , Ali Baydoun, Robertas Damaševičiusf (2024), "Enhanced threat intelligence framework for advanced cybersecurity resilience", ISSN 1110-8665, https://doi.org/10.1016/j.eij.2024.100521. (https://www.sciencedirect.com/science/article/pii/S1110866524000847)

[20] Shahbaz Siddiqui, Sufian Hameed, Syed Attique Shah, Junaid Arshad, Yussuf Ahmed, Dirk Draheim, A smart-contract-based adaptive security governance architecture for smart city service interoperations, Sustainable Cities and Society,Volume 113,2024,105717, ISSN 2210-6707, https://doi.org/10.1016/j.scs.2024.105717. https://www.sciencedirect.com/science/article/pii/S2210670724005420)

[21] Ahmed M. Eltahlawy, Heba K. Aslan, Mahmoud Said Elsayed, Anca D. Jurcut, Marianne A. Azer, Detection of sequence number attacks using enhanced AODV protocol in MANETs, Computers and Electrical Engineering, Volume 118, Part B, 2024, 109395, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2024.109395. (https://www.sciencedirect.com/science/article/pii/S0045790624003239)

[22] Amit Mittal, Archana Mantri, Rahul Mishra, Vehicular ad-hoc security improvements using decentralised consensus blockchain, Measurement: Sensors, Volume 33, 2024, 101165, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2024.101165. (https://www.sciencedirect.com/science/article/pii/S2665917424001417)

[23] Jun Zhou, Zhenfu Cao, Xiaolei Dong, Naixue Xiong, Athanasios V. Vasilakos, 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks, Information Sciences, Volume 314, 2015, Pages 255-276, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2014.09.003. (https://www.sciencedirect.com/science/article/pii/S0020025514008998)

[24] V. Anjana Devi, Vithya Ganesan, V. Sri Anima Padmini, Shriman k.arun, An energy efficient routing establishment (EERE) mechanism for MANET-IoT security, Franklin Open, Volume 8, 2024, 100150, ISSN 2773-1863, https://doi.org/10.1016/j.fraope.2024.100150. (https://www.sciencedirect.com/science/article/pii/S277318632400080X)

[25] G.R. Rama Devi, M. Swamy Das, M.V. Ramana Murthy, Secure cross-layer routing protocol with authentication key management scheme for manets, Measurement: Sensors, Volume 29, 2023, 100869, ISSN 2665-9174,https://doi.org/10.1016/j.measen.2023.100869. (https://www.sciencedirect.com/science/article/pii/S2665917423002052)

[26] C. Edwin Singh, S. Maria Celestin Vigila,Fuzzy based intrusion detection system in MANET, Measurement: Sensors, Volume 26, 2023, 100578, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2022.100578. (https://www.sciencedirect.com/science/article/pii/S2665917422002124)

[27] S Vijayalakshmi, S Bose, G Logeswari, T Anitha, Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory, Cyber Security and Applications, Volume 1, 2023, 100011, ISSN 2772-9184 , https://doi.org/10.1016/j.csa.2022.100011. (https://www.sciencedirect.com/science/article/pii/S277291842200011X)

[28] M. Arun, R. Jayanthi, An adaptive congestion and energy aware multipath routing scheme for mobile ad-hoc networks through stable link prediction, Measurement: Sensors, Volume 30, 2023, 100926, ISSN 2665-9174,https://doi.org/10.1016/j.measen.2023.100926. (https://www.sciencedirect.com/science/article/pii/S2665917423002623)

[29] Deepa Krishnan (2015), "A Distributed Self-Adaptive Intrusion Detection System for Mobile Ad-hoc Networks using Tamper Evident Mobile Agents", s. Published by Elsevier B.V. Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies.

[30] Yulliwas Ameur, Samia Bouzefrane, Enhancing privacy in VANETs through homomorphic encryption in machine learning applications, Procedia Computer Science, Volume 238, 2024, Pages 151-158, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2024.06.010. (https://www.sciencedirect.com/science/article/pii/S1877050924012468).