ISSN: 2393-8048

International Advance Journal of Engineering, Science and Management (IAJESM)

Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.

SJIF Impact Factor =8.152, January-June 2025, Submitted in April 2025

An Empirical Review of Multipath Routing, QoS Enhancement and Modern Security Protocols in HANETs

S. G. Wankhade, Research Scholar, Priyadarshini College of Engineering, Nagpur, Maharashtra, India
Dr. G. M. Asutkar, Vice Principal, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Abstract

The growing demand for Heterogeneous Ad hoc Networks (HANETs) certainly makes the QoS parameters of paramount importance within the HANET, and consideration for secure routing protocols further grows as interconnected devices within a smart network are put onto the same platform. Different devices related to the Internet of Things and others have aroused important needs at the same time concerning performance and secure measures for the proper and effective transition of data within HANETs. However, existing models are quite inefficient in accomplishing the requirements of multi-facets QoS and secure routing, hence proving to be a failure and vulnerability under various scenarios. Current approaches tend to inadequately deal with dynamic network conditions, inadequately scale up, and inadequately adapt to emerging security threats. However, these shortcomings ease the running of smart network networks smoothly and expose it to potential security risk, which ultimately reduces user trust and utility to smart network technologies. The paper outlines a comprehensive review related models to enhance QOS parameters and secure routing protocols leading to the advancement of HANETS. On one hand, the review will consider such methods in-depth: multipath routing protocols, fuzzy logic-based QoS models, and machine learning-based security protocols. Each method shall be cruised through the operational principles, its effectiveness in the enhancement of network performance, and its capability to reaffirm security. Multipath Routing Protocols: Further explored to see how it can be effective in enhancing reliability, reducing latency through multiple path data delivery; Case in point-AOMDV Models of QoS Using Fuzzy Logic: These are viewed for the nature of their decisions with adaptability that assures that all resources are optimised for creating dynamic changes in the network leading to very high QoS. Additionally, these Security Protocols based on ML are checked for the advanced features about threat detection and mitigation that they own, while using real-time data analysis in pre-emption and neutralization of security threats. Some of the benefits that these models carry along as well include better network reliability, reduced latency level, and more adaptability to changes in network conditions, and security frameworks. Through a careful consideration of such methods, this review draws out potential ways through which the present mismatch experienced between needs and abilities can be handled coercively. Overall, these impacts make this work very important because it is going to stand as a consolidated knowledge base guiding future research and development within the domain of HANETs. It will form a strong foundation for more efficient and secure networking protocols that will lead to further developments in the smart networks. While the current paper bridges this gap from the capabilities that exist now to the requirements of the future, it sets the pace for innovative approaches that shall help strengthen QoS and secure routing in HANETs.

Keywords: QoS, HANETs, Multipath Routing, Fuzzy Logic, Machine Learning

1. Introduction

As a result, the emergence of connected devices in smart networks translates to perfect optimization of Heterogeneous Adhoc Networks (HANETs). These networks, backbone architectures of the operations of the IoT ecosystem, really need to enlist stringent QoS enhancements as well as security protocols to ensure continuity and safety in their operations. The more the dependency, the more there needs to be advanced, model-based control of the network resources while still providing protection against the security risks. Most of the models proposed based on QoS enhancement and secure routing in HANETs normally fail to meet this complex, and evolving demands of networks. Traditional routing protocols usually reflect weaknesses in handling a dynamic network topology structure, which introduces inefficiencies, such as increased latency, packet loss, and decreased reliability. In addition, conventional security protocols are weak against sophisticated cyber threats, hence compromising the integrity and privacy of the network. This empirical review overcomes these challenges by investigating advanced methodologies designed to improve QoS and secure routing within HANETs. Three primary methods identified for this review encompass Multipath Routing Protocols, Fuzzy Logic-based QoS Models, and Machine Learning-based Security Protocols. Multipath Routing Protocols combine multiple routes, such as the Ad hoc On-demand Multipath Distance Vector (AOMDV), of which this method reduces delay and latency. Fuzzy Logic-based QoS models utilize adaptive algorithms in making decisions, consequently ensuring network resources are optimized in a dynamic manner for better QoS over variable network conditions. The security protocols of machine learning are based on advanced analytics in nature and detecting such threats by offering real-time proactive network protection. The review clearly indicates the potential of such advanced models to outweigh the limitations of the existing solutions in establishing more efficient and secure smart network networks. Furthermore, these known realities, which have surfaced from the review, are expected to be a good guide for further researchers and practitioners in this field to develop protocols for next-generation HANET that will not only be resilient but adaptive to any future technological advancement. In a nutshell, the requirement of advanced QoS and secure routing in HANET is somewhat in high demand. This review does not only help in identifying and criticizing the current methodologies but also opens the way for innovative solutions that can meet the stringent demands of the modern smart network environments. All critical cases addressed help to enrich the ongoing discussion about how to better the performance and security of HANET in order to improve the standard of living through smarter and safe house networks.

Motivations

The rapid increase in the technologies of smart networks underlines the development and need for effective and efficient Heterogeneous Adhoc Networks that would support a wide range of interconnected devices & deployments. The networks are expected to provide seamless communication, high reliability, and stringent security. The motivation behind such research stems from increasing levels of complexity and heterogeneity in smart network environments to a degree where the traditional networking and security models sound spatially challenged. Most often, the available QoS improvement and secure routing protocols tend to degrade under dynamic network conditions, thereby making the performance of the selected network rather poor and highly vulnerable to security attacks. Exponential growth in the adoption of smart network devices is making mandatory the need for research and development on advanced methodologies that can adapt dynamically with changing network topologies and the evolution of the threat landscapes. This paper, therefore, tries to plug this void with a review, in an empirical sense, of the state-of-the-art methodologies designed toward enhancing QoS parameters and secure routing in HANETs. In lieu of the above, this paper focuses on three pivotal approaches: Multipath Routing Protocols, Fuzzy Logic-based QoS Models, and Machine Learning-based Security Protocols. Operational principles, benefits, and possible impacts on performance and security in HANETs are examined for each method. These protocols include the AOMDV routing protocol based on Ad hoc On-demand Multipath techniques for multiple transmission paths to increase the reliability and decrease the latency period. These also take on into consideration the Fuzzy Logic-based QoS models in studies for the adaptive decision-making capability in achieving the optimized usage of network resources in real time in a bid to keep up high QoS standards. Security Protocols based on Machine Learning are assessed for their sophisticated threat detection and mitigation approaches. These are taken to be able to preempt and instantly neutralize security threats through real-time analytics of data samples.

The paper makes several contributions. First, it paper synthesizes the present status to represent the QoS enhancement and secure routing research for cooperation of HANETs. It provides extensive detailing in the critique of already existing methodologies and their strong and weak sides. Next, it makes an attempt to propose a uniform framework through which such methodologies could be benchmarked, taking into account parameters of scalability, adaptability, and performance across the globe in a dynamic network environment. Thus, the paper does not only identify the most promising but also sets a direction for future research based on the findings in this article. The paper also mentions the utilization of sophisticated technologies like fuzzy logic and machine learning in the HANET protocols, where the traditional model weaknesses can be tackled for achieving solutions with more strictness. There lies a very strong motivation behind this research work. The performance and security of HANET need to be upgraded at the pace smart network environments are becoming more complex and better merged. The paper greatly contributes to the literature with an empirical account of existing advanced QoS and secure routing methodologies, and so becomes a valuable reference source to guide research and practice in developing the next generation of HANET protocols with resilience, adaptability, and capability of meeting high demands in modern smart networks. The generated insights from this survey are expected to drive innovations in HANET that will increase efficiency and security of the network while, at the same time, improving the user's experience in smart-environment networks.

2. In-depth review of existing models used for HANET Optimizations

Optimizing Heterogeneous Adhoc Networks (HANET) is one of the essential components of smart network ecosystems that are highly widespread these days and, more and more, based on heterogeneous wireless networks and different standards to provide effective automation, energy efficiency, and security. Here, in this literature review, the information is aggregated from several studies dealing with methodologies and techniques adopted for the optimization of HANET with emphasis on performance as well as security improvements in the process.

Machine Learning for HANET Security and Optimization

Several works used various machine learning techniques to enhance the security of and also the performance in HANET. For example, the method proposed in [1] puts forward the SecureScanML algorithm that uses Q-learning to adjust the scan rate of IoT devices & deployments dynamically. This is because this architecture reduces security vulnerabilities by 35.7% while achieving high network performance, which includes a throughput of 2.8 Mbps and a packet delivery ratio of 97.3%. These performance improvements underpin the potential of machine learning in addressing HANET vulnerabilities without compromising the efficiency of a network. Within a similar context, the work in [2] addresses the issue of identifying a bit-flipping attack in Low Power Wide Area Networks. This, again, is one of the network systems that are frequently included within HANET. Using data sequence pattern recognition, this attack detection system has achieved an impressive level of accuracy of 99.84% in detecting these attacks without payload size and power consumed by the sender, which is crucial in HANET environments, as efficiency in terms of energy consumption is of utmost importance in process.

Another important application that utilizes machine learning improves HEM systems in HANET. The method in [3] utilizes deep reinforcement learning and DA2C algorithm to optimize the cost of electricity and then residential comfort. Further, another example to recognize the flexibility and robustness of optimization methods in HANET is its ability to handle multiple uncertain factors such as EVs' charging behaviors during optimization.

Sensor Networks and HANET Energy Efficiency

Energy efficiency is one of the repeated themes seen in HANET optimization studies, especially those associated with sensor networks. In [16], the Discrete Venus Fly-Trap Search (DVFS) algorithm is proposed for HASN for optimizing the choice of energy resources for Heterogeneous Adhoc Sensor Networks. This algorithm, based on the foraging strategy of the Venus fly-trap plant, is used as a model to prolong the time life span of the network by properly choosing the energy sources for sensor nodes. Simulation results show that the algorithm enhances the life of the network, hence very important in energy-constrained HANET environments.

In similar lines, [19] also suggests energy-efficient duty-cycling in the automation of sensor operations within HANET. Using Recurrent Neural Networks (RNN) and Dynamic Time Warping (DTW), this technique offers intelligent grouping toward predictive activity sensing with high accuracy, and gains a considerable amount of energy saving. The lifetime of the sensor battery is stretched to approximately 137 days, which exhibits its feasibility in practical smart network situations.

Security Mechanisms in HANET

Including security protocols into HANET will be useful to safeguard the number of connected devices & deployments. In [13], the CART decision tree algorithm will be used to identify the devices inside the smart network, with Wi-Fi environments, where encryption protocols like 802.11 tend to blur the traffic patterns. The proposed method gets a device identification accuracy of 91.3%, which will be necessary in ensuring proper and reliable HANET operations inside smart networks.

On top of this, [17] conceives the Ethereum blockchain based on the Robot Operating System, which can store data securely and privately within smart networks. Employing a novel cryptographic approach using EECDS: Enhanced Elliptic Curve Digital Signature, along with Adaptive Neuro-Fuzzy Inference Systems (ANFIS), enhances the security level of data and decreases vulnerability to unauthorized access. Hence, blockchain-based integration with ML algorithms within HANET security reflects an emergent trend toward hybridized solutions based on advanced technologies and their optimal performance.

Another crucial work towards HANET security in the proposed direction is in [12], where DCNNs are used along with multiple cameras for security purpose of smart network. These cameras capture images from different angles and then use those images along with DCNN models in an attempt to identify intruders with a very high accuracy up to 99.79% compared with other approaches like SVMs and decision trees, proving computer vision as a very strong approach for HANET security.

Multi-objective Optimization in HANET

Multi-objective optimization is an important part of HANET where energy efficiency, performance, and security trade-offs are balanced. In [10], a HGSOA has been proposed as a hybrid gazelle and seagull optimization algorithm to optimize electricity usage in HANET with a bidirectional long short-term memory model. The peak power demand decreases with a peak-to-average ratio of 1.21 and hence the consumption for energy efficiency needs to be balanced with the performance for getting efficacious systems.

For instance, [5] discusses the application of LLMs in smart network ecosystems to enhance the interpretation of complex commands that are issued by users. This system uses interactive approaches for enhancing ambiguity by boosting user satisfaction and accuracy in an ambiguous command's execution, such as changes in setting lights or temperature. The developed study shows the opportunities that NLP techniques offer to make HANET user interfaces more effective while ensuring efficient responses from systems. This is because the more the number of smart networks deployed, the more challenging managing a network of such interconnected devices and achieving the best performance would be. The study in [7] solves this problem by using an intelligent decision support system that, SDN-IDSSIoT, proposed based on SDN. The same accounts for an improved interoperability of heterogeneous devices from the smart network, boosting the network's throughput by 20% and reducing the round-trip time by 30%. Such improvements are necessary to scale HANET for an increasing number of devices and deployments. However, the problem of energy consumption, security, and performance in HANET are still not well addressed despite such improvements. [9] presents pyMulSim: new method for node similarity computation in multilayer networks. This tool can be used to determine interactions between biological networks, in which important insights regarding future HANET research may be needed to optimize communication and connectivity between different smart network devices & deployments.

Reference	Method Used	PRISMA Findings	Strengths	Limitations
[1]	SecureScanML algorithm using Q-learning	The ML-based SecureScanML algorithm optimizes Internet-wide port scans in WLAN environments, enhancing security by reducing vulnerabilities by 35.7% without compromising performance metrics.	High throughput (2.8 Mbps), low latency (42 ms), and effective vulnerability management.	Limited to IEEE 802.11ah WLAN and requires specific environmental conditions for optimal performance.
[2]	Machine learning-based bit flipping detection in LPWAN	Proposed ML model detects bit flipping attacks with 99.84% accuracy in LPWAN without increasing payload size or power consumption, optimizing resource use for HANET.	High accuracy without additional energy cost, effective under diverse attack scenarios.	Focused solely on LPWAN; broader applicability in other network types untested.
[3]	Deep reinforcement learning for Network Energy Management (HEM)	DA2C algorithm improves energy optimization in dynamic electricity pricing environments, crucial for cost-efficient HANET management involving electric vehicles.	Enhanced energy optimization, generalization in unseen scenarios, supports residential comfort.	Results may vary with unpredictable real-time variables, such as EV charging behavior.
[4]	Prototypical networks with K-Best feature selection for in-network rehabilitation	Optimizes wearable sensor-based gesture classification in HANET, achieving 82.2% accuracy in stroke survivors, promoting health-related applications in smart networks.	Improved classification accuracy through transfer learning, robust performance with physiological variations.	Limited applicability outside health and rehabilitation settings, requires specific sensor setups.
[5]	Large language models (LLMs) for smart network command disambiguation	LLMs enhance user command interpretation in HANET by integrating visual and textual cues, refining smart speaker capabilities.	Effective user-intent interpretation, higher satisfaction, reduces ambiguity in commands.	Slight preference for textual cues may limit system’s response in complex, purely visual scenarios.
[6]	SDN-based multi-level structure for smart network services	SDN paradigm enhances HANET by improving reliability and service stability through a multi-level controller system.	Improved service performance in smart networks, lower packet loss in cloud-local topology.	Limited performance under varying environmental conditions and topologies.
[7]	SDN-based Intelligent Decision Support System (IDSS) for IoT	Enhances HANET with intelligent SDN architecture, addressing heterogeneity and improving network throughput by 20%.	Significant reduction in round-trip time, efficient handling of heterogeneous devices & deployments.	Potential scalability issues with increasing node counts in HANET.
[8]	Machine vision-based intelligent lighting system	Personalizes lighting in HANET using human detection, face recognition, and tracking to optimize comfort and energy efficiency.	Higher system efficiency, personalized user experience, faster response time (1.4 s).	Primarily focused on lighting applications, may not translate to broader HANET functionalities.

[9]	pyMulSim using Graph Isomorphism Network (GIN) for node similarity	GIN-based method optimizes cross-network node similarity computation in multilayer HANET, aiding network alignment and robustness.	High reliability in evaluating node similarities across multiple networks.	High complexity may limit real-time deployment in large-scale HANETs.
[10]	BLSTM and CapsNet for network energy prediction	HGSOA-based optimization algorithm reduces energy consumption during peak hours, essential for smart grid integration in HANET.	Lower peak-to-average power ratio, reduced error rates in predictions.	Limited generalization beyond specific energy management scenarios.
[11]	Modified smart network-optimized path (MSHOP) for communication optimization	Enhances HANET routing with modified RPL objective functions, achieving a 99.93% packet reception ratio.	High packet reception and energy efficiency, supports mobile and static environments.	High energy usage in specific network configurations.
[12]	Deep Convolutional Neural Networks (DCNNs) with multiple cameras	DCNNs enhance HANET security by achieving 99.79% accuracy in intruder detection, critical for smart network surveillance.	Superior detection accuracy with low false alarms, multi-angle camera integration.	High computational cost due to multiple camera inputs and complex DCNN models.
[13]	CART decision tree algorithm for device identification	Optimizes HANET security by identifying smart devices within Wi-Fi environments using enhanced CART algorithm.	High accuracy in device identification (91.3%), effective under encrypted 802.11 traffic.	May struggle in highly dynamic or rapidly evolving device environments.
[14]	Cross-sectional qualitative study on care networks	Explores care networks in HANET for network-dwelling older adults, identifying network types and intervention strategies.	Insights into network dynamics for elderly care, supports decision-making for caregivers.	Limited to qualitative data, requiring further validation through quantitative studies.
[15]	XGBoost and Firefly Optimization for fault prediction in smart networks	Machine learning-driven predictive maintenance approach optimizes HANET reliability, achieving 98% accuracy in fault detection.	High prediction accuracy, reduces downtime and maintenance costs.	Focused on ZigBee-enabled devices, potentially less effective for other protocols.
[16]	Discrete Venus Fly-Trap Search (DVFS) algorithm for energy resource selection	DVFS optimizes energy resource selection in HANET, extending network lifespan for sensor nodes.	Eco-friendly, energy-efficient optimization, improves network longevity.	Limited applicability beyond sensor-based networks, requires further validation for larger-scale deployments.
[17]	Ethereum blockchain-based Robot Operating System (ROS-EB)	Proposes a secure storage and communication solution for HANET using blockchain, improving data security and reducing vulnerability.	Enhanced security via blockchain, reduces unauthorized access risks.	High complexity and computational overhead due to blockchain integration.
[18]	ChaCha20-Poly1305 AEAD-based authentication for smart grids	AEAD encryption optimizes HANET security with minimal impact on network performance in IoT-based smart grids.	Balances security and performance, low additional latency.	Limited to specific use cases, such as LoRa 2.4 GHz networks.
[19]	BLSTM and DTW for sensor energy consumption in smart networks	Proposes energy-efficient duty-cycling for HANET, prolonging sensor battery life to 137 days.	Substantial reduction in energy consumption, highly accurate activity prediction.	May face limitations in networks with higher data transmission requirements.
[20]	DRIVEN method using deep convolutional	DRIVEN optimizes health monitoring in HANET by detecting sleep apnea at	High classification accuracy, improves	Limited to sleep disorder monitoring, not broadly

	neural networks and LGBM	network, supporting remote healthcare.	patient comfort and remote diagnosis.	applicable to other health conditions.

Table 1. Comparative Analysis of Existing Methods

Energy Efficiency and Optimization in HANETs

There is an energy efficiency task in the design and optimization of HANETs. The devices designed for the networks are resource-constrained devices that ought to be working continuously. There are many research studies with the propositions of new clustering protocols and algorithms for improving energy efficiency and prolonging network lifetime for HANETs. In [21], authors developed a decentralized, ZigBee-enabled fail-proof Heterogeneous Adhoc network (ZFPHAN) using a multi-layer partial mesh (MLPM) topology. MLPM topology permits alternative routes in case of the node failure as its robust operation in a network is assured. The gateways' re-arrangement in MLPM topology reduces the required retransmission powers to conserve energy but maintains the robustness of the network. This fail-safe mechanism ensures the continuity of service in HANETs, especially in smart network environments, where one expects the continuous operation of devices & deployments. To advance energy management for smart networks, [26] introduced a Long Short-Term Memory (LSTM) algorithm for predicting energy consumption in buildings. Therefore, the advanced proposed algorithm will be versatile to predict several power parameters like electricity, heating, and cooling. Hence, such an effective energy management system will significantly reduce environmental impact. The model with cloud, fog, and edge computing allows real-time monitoring and prediction for HANETs to optimise energy consumption.

Selecting optimal cluster head (CHs) in wireless sensor network-based IoT systems presented another energy-hole alleviation work in [40]. The algorithm applies Euclidean distance for the clustering nodes and applies the optimization technique for CH selection. It achieves 10% improvement in both packet delivery ratio and network lifetime. There is a great relevance to this approach in HANETs, where efficient data aggregation along with low energy consumption is considered highly crucial. This is an energy efficiency problem in the design and optimization of HANETs. The devices designed for the networks are resource-constrained devices that ought to be working continuously. There are many research studies with the propositions of new clustering protocols and algorithms for improving energy efficiency and prolonging network lifetime for HANETs. In [21], authors developed a decentralized, ZigBee-enabled fail-proof Heterogeneous Adhoc network (ZFPHAN) using a multi-layer partial mesh (MLPM) topology. MLPM topology permits alternative routes in case of the node failure as its robust operation in a network is assured. The gateways' re-arrangement in MLPM topology reduces the required retransmission powers to conserve energy but maintains the robustness of the network. This fail-safe mechanism ensures the continuity of service in HANETs, especially in smart network environments, where one expects the continuous operation of devices & deployments. To advance energy management for smart networks, [26] introduced a Long Short-Term Memory (LSTM) algorithm for predicting energy consumption in buildings. Therefore, the advanced proposed algorithm will be versatile to predict several power parameters like electricity, heating, and cooling. Hence, such an effective energy management system will significantly reduce environmental impact. The model with cloud, fog, and edge computing allows real-time monitoring and prediction for HANETs to optimise energy consumption. Selecting optimal cluster head (CHs) in wireless sensor network-based IoT systems presented another energy-hole alleviation work in [40]. The algorithm applies Euclidean distance for the clustering nodes and applies the optimization technique for CH selection. It achieves 10% improvement in both packet delivery ratio and network lifetime.

There is a great relevance to this approach in HANETs, where efficient data aggregation along with low energy consumption is considered highly crucial.

Reference	Method Used	PRISMA Findings	Strengths	Limitations
[21]	Decentralized ZigBee-enabled fail-proof HAN with multi-layer partial mesh (MLPM) topology	The MLPM topology enhances robustness by providing alternate paths in case of node failure, improving operational resilience of network appliances in HANETs.	Energy-efficient, eco-friendly design; fail-proof operation with minimized power usage.	Limited to ZigBee control boards (ZCBs); real-world scalability not fully explored.
[22]	Digital Twin (DT)-driven service self-healing mechanism with GNN	DT-driven architecture and GNN-based prediction improve network performance and stability in 6G edge networks, enhancing HANET reliability.	Accurately predicts network anomalies and reduces service delay; improves load balancing.	Early-stage application in HANET; limited real-world deployment scenarios.
[23]	Improved Quality of Service aware Routing Protocol (IM-QRP) for WBAN	IM-QRP enhances energy efficiency and signal reliability in healthcare monitoring within HANET, critical for remote patient monitoring.	Improved energy usage (10%), path loss (30%), and packet transmission (10%).	Focused on WBAN environments; broader applicability to non-medical smart network settings not tested.
[24]	Distributive cross-layer and thermal-aware converge cast protocol	Optimizes data flow and thermal control in HANET, reducing delays and improving throughput for healthcare applications in smart networks.	Reduces delay by 19.4%, increases throughput by 8-13.75%, low packet loss probability (0.3%).	High complexity due to multi-parameter benefit-cost function; specific to healthcare IoT systems.
[25]	IoT-based real-time health monitoring system with Arduino and GSM modules	Provides a low-cost, real-time health monitoring system for rural and urban areas, offering potential in smart network HANET scenarios.	Effective for remote health data transmission in resource-constrained environments.	Limited to developing countries' healthcare systems; does not account for broader smart network integration.
[26]	LSTM-based energy consumption prediction for smart networks	AI-driven LSTM model improves energy forecasting in cold climates, essential for HANET-based energy management.	Accurate power forecasting for multiple parameters; useful in energy-saving applications.	Requires substantial computational resources for real-time monitoring and predictions.
[27]	LoRa technology for smart network applications	LoRa-based HANET optimizes transmission delay and coverage under real-world conditions, ensuring low-latency communication.	Low transmission delay (18 ms), long-range coverage (440 m), high PRR (96%).	Indoor performance is weaker (PRR of 43%); reduced long-range coverage indoors.
[28]	IoT platform traffic fingerprinting for intrusion detection	Introduces traffic fingerprinting for IoT platforms, enhancing HANET security by distinguishing network traffic.	Efficient in identifying IoT platform traffic for vulnerability assessment.	Limited applicability outside mainstream IoT platforms; real-time detection challenges.
[29]	Smart Unified Threat Management System (SUTMS)	Lightweight UTM system enhances security for HANET by providing flow detection, IDS, and firewall functionalities.	High accuracy (99%) in intrusion detection; reduced memory utilization (55%).	Limited scalability due to hardware (Raspberry Pi); performance drops under heavy traffic loads.
[30]	Network criticality evaluation using r-nearest neighbor graphs	Optimizes network robustness against node/link failure in HANETs using reduced-complexity network criticality measures.	Reduced computational complexity from $O(n^3)$ to $O(n)$; suitable for large-scale HANETs.	Focused primarily on static topologies; limited testing in dynamic network environments.

[31]	Conditional GAN for non-intrusive load monitoring (NILM)	Enhances appliance detection in HANET energy management systems, detecting known and unknown appliances through GAN integration.	Effective classification of unknown appliances; improves energy monitoring accuracy.	Assumes ideal appliance switching conditions; may struggle with highly dynamic appliance sets.
[32]	Fiber-Wireless (FiWi) access network with 3D beamforming	Hybrid FiWi network optimizes resource allocation and downlink transmission in HANET, integrating 5G and PON technologies.	Improved resource allocation with 3D beamforming; efficient in large-area smart networks.	Limited real-world testing of beam codebook and SINR computations.
[33]	Digital Twin (DT) model for healthcare monitoring	DT model provides real-time visualization and monitoring for healthcare applications within HANET, leveraging smart algorithms for anomaly prediction.	High fidelity in real-time healthcare monitoring; effective in fall detection and ECG screening.	Application mainly focused on healthcare; broader smart network functionalities not considered.
[34]	GPON-based Fiber to the Network (FTTH) with quantum access network	Enhances HANET security with quantum key distribution over FTTH, improving data transmission in secure smart network networks.	Feasible integration of classical/quantum links in fiber optics; secure key distribution.	Quantum technology is in early stages, with limited practical deployment.
[35]	Network Intrusion Detection System (NIDS) for Building Automation and Control Systems (BACS)	NIDS improves HANET security by supporting multiple BACS protocols, safeguarding smart networks from cyber threats.	Protocol-agnostic; supports diverse BACS protocols like KNX, BACnet, Modbus.	Limited focus on general smart network HANET; primarily targets BACS environments.
[36]	VAE-GAN for time-series data generation in energy management	Generates synthetic time-series data for HANET energy management systems, facilitating improved performance of Q-learning-based HEMS.	Close alignment between synthetic and real data; enhances energy management accuracy.	GAN-based approach requires high computational resources; dataset generation complexity.
[37]	Self-organizing network with adaptive task allocation	Optimizes IoT Sensor Network (IoTSN) performance within HANET, reducing load and energy consumption through self-organizing principles.	Decreases load (30%), energy use (25%), and transmission delay (20%); highly adaptive.	Complex to implement; may face real-time coordination challenges in large networks.
[38]	Integration of LoRaWAN into 5G systems	Proposes seamless integration of LoRaWAN into 5G networks for HANET, optimizing secure communication for IoT devices & deployments.	Efficient in mMTC support, secure access through EAP; enhances HANET scalability.	Integration complexity with 5G and LoRaWAN; performance untested in highly dynamic environments.
[39]	LoRa-based IoT system for peatland fire management	Deploys IoT system for environmental monitoring within HANET, using LoRa for real-time data collection in peatland fire prevention.	High correlation (0.8) with official weather data; effective in predicting fire risks.	Focused on environmental IoT; broader applications in smart networks untested.
[40]	Osprey optimization	SWARAM optimizes energy efficiency in HANET by	Improves packet delivery ratio and	Limited performance in complex multi-

	algorithm for cluster head selection in IoT	selecting the most efficient cluster head, reducing energy consumption.	network lifetime by 10%; effective energy optimization.	hop network environments; simulation-based results only.

Table 2. Comparative Analysis of Existing Methods

Network Topology and Performance Optimisation

Network topology is equally important in enhancing the performance and reliability of HANETs. Reference [27] discusses the use of LoRa in smart network applications, including the measurement of real-world installation conditions' effect on LoRa transmission delay, communication distance, and link quality. The experiments show that optimized LoRa physical layer parameters enable a robust coverage, low transmission delays and subsequently makes the system a promising solution for HANETs both inside and outside premises.

In [22], a DT-driven self-healing mechanism for 6G edge networks is proposed to improve stability and service reliability in such networks. This DT-based architecture employs GNNs to predict the performance and detect anomalies; it is, therefore, potentially applicable in HANET environments that require adaptive service recovery. The proposed system demonstrated how to achieve effective load balancing and decreases service delays since delay is one of the factors that affect the quality of service in HANET environments.

Another great contribution to the topic is the integration of fiber and wireless networks to HANETs as presented in [32]. FiWi access network, which combines PON and 5G technology, presents very efficient network services to the users residing in different places. The 3D beamforming and resource grid optimization for implementation are better to increase the SNR and networking performance. These are crucial in ensuring that HANETs have the ability to offer networks with reliable communication, especially in densely populated areas where there is interference and degradation of signals.

Security Optimisation in HANETs

Security is another sensitive parameter in the optimization of the HANET, especially because of the constant rise in the number of devices connected in intelligent networks. In [28], there was a proposal of a fingerprinting technique meant for the identification of IoT platform traffic within the HANET environments. The proposed method can differentiate among various IoT platforms by distinguishing patterns in network traffic, thereby enhancing intrusion detection and vulnerability assessment. This can be fundamental since malicious attacks against connected devices compromise HANET security. In [29], a Smart Unified Threat Management System was proposed to address the issues of security in network networks. It integrates into the system flow detection, intrusion detection, and firewall engines on low-cost hardware, such as Raspberry Pi. With these features for optimizing intrusion detection signatures and providing dynamic anti-bot protection, it fits perfectly into HANETs where security solutions are needed to be very light and yet effective for guarding against a multitude of cyber threats.

Another important contribution to HANET security is the proposed deployment of a NIDS for BACS, as in [35]. A protocol-independent NIDS that can support several BACS protocols, including KNX and BACnet, which are fundamentally deployed in smart networks. The proposed system provides an effective security layer to HANETs, especially for mixed-protocol environments where traditional security tools will fail.

Machine Learning and AI-Driven Optimization

Machine learning (ML) and artificial intelligence (AI) technologies have increasingly gained attention in the optimization of HANETs for energy management, performance, and security. In [23], the authors designed an Improved Quality of Service (IM-QRP) aware routing protocol for wireless body area networks (WBANs) designed for healthcare monitoring systems. It improved the efficiency of energy and packet delivery, both of which are critical to the operation of HANETs in health-centric smart networks, given the inclusion of CNNs in the analysis of medical data.

The paper in [36] discussed the usage of GANs for energy usage prediction by HANETs. This proved that the amalgamation of GANs with the Q-learning-based Network Energy Management System improved the accuracy of the predicted energy usage as well as the efficiency of the system considerably. The synthetic time-series data, produced by this GAN model, improved the trainability of the models for HEMS which were useful for optimizing energy usage within HANETs.

In [37], an integrated approach toward optimizing IoT Sensor Networks (IoTSNs) was developed which used self-organization and adaptive load balancing techniques. In this system, dramatic reductions in energy consumption and data transfer latency were observed because node operations were modulated intelligently in real time. Such developments are particularly applicable to HANETs wherein, because of changing conditions, dynamic adaptability becomes the key to maintaining network efficiency.

While enormous amounts of development work on optimal HANETs are ongoing, much remains to be achieved. The exponentially rising number of connected devices propels the complexity of HANETs, and hence the need for even more scalable and adaptive optimization approaches. Future work may focus on advanced AI techniques such as deep reinforcement learning to solve dynamic resource allocation and energy management problems in HANETs. Now, security in HANETs is an open issue and increasing because of the number of IoT devices & deployments. The light, distributed security protocols able to work efficiently in most constrained environments of HANET will be of paramount importance for smart network networks' long-term survivability. PRISMA review shows various methodologies in the optimization of HANETs, either based on energy-efficient protocols and network topologies or secure and machine learning-driven methods. The reviewed studies showcase promises of several promising techniques such as AI, Digital Twins, and hybrid fiber-wireless networks in optimizing and enhancing HANET in terms of both performance and security. Thus, with the exponential growth of smart network networks, there will be a dire need for much more research that involves a scalable, adaptive, and secure optimization approach to meet future demands in HANET environments.

3. Comparative Result Analysis

The following PRISMA analysis in figure 1 along with tables 1, 2, 3, & 4 brings in a more comprehensive comparison of several optimization methods for HANET based on efficiency, their performance metrics, and deployment in smart network environments. Each study focused on different aspects of HANET energy efficiency, security enhancement, and automation capabilities. This tabular comparison will easily capture the various techniques used for HANET optimization results: their specific results, observed benefits, and potential issues in implementation. A number of numerical results are included; measurable outputs like packet delivery ratio, latency, throughput, and accuracy. Only for those studies which were not able to get the exact values have been given with estimates based on a study's context and comparison with related methods.

Reference	Method Used	PRISMA Results	Efficiency of HANET Deployment	Observations in terms of HANET Efficiency
[1]	Secure Scan ML (Q-learning)	Throughput: 2.8 Mbps, PDR: 97.3%, Latency: 42 ms	High	SecureScanML optimizes security and performance, balancing network efficiency and vulnerability management.
[2]	Bit flipping detection (DNN)	Accuracy: 99.84% in attack detection	Moderate	Highly effective in securing low-resource LPWAN environments, with negligible impact on system performance.
[3]	Deep reinforcement learning for HEM	Energy cost reduction: ~15-20%	High	Optimizes energy usage in dynamic network energy systems, improving cost-efficiency while maintaining user comfort.

[4]	Prototypical networks for gesture recognition	Accuracy: 82.2%, Window size improvement: +4.28%	Moderate	Effective in classifying gestures for in-network rehabilitation, adaptable but limited in broader HANET use.
[5]	Interactive disambiguation for smart speakers	Response accuracy: ~93%	Moderate	Enhances user interaction efficiency with smart network systems, especially in handling ambiguous commands.
[6]	SDN-based multi-level structure	Packet loss: 1.4%, RTT: ~45 ms	High	Reduces packet loss and improves service reliability in smart networks, especially for cloud-local architectures.
[7]	SDN-IDSS for IoT	Throughput: +20%, RTT: -30%	High	Effective in managing heterogeneous smart network devices with improved network performance and reduced delays.
[8]	Intelligent lighting system	Human detection: 22.1mAp, Face recognition: 95.12%, Avg. response time: 1.4s	High	Enhances personalized lighting settings with minimal delay, improving smart network comfort and adaptability.
[9]	pyMulSim for node similarity in multilayer networks	Similarity evaluation: High reliability	Moderate	Accurate in evaluating cross-network node similarities but limited to bioinformatics applications, less direct HANET use.
[10]	HEMS using BLSTM and capsnet	Peak-to-average ratio: 1.21, Error reduction: ~17.82%	High	Reduces energy usage and improves smart grid performance in smart networks, significant energy optimization observed.
[11]	MSHOP for smart network routing	PDR: 99.93%, Latency: 0.9s, Energy use: 3373mJ	High	Efficient in optimizing communication networks in both static and mobile smart network environments.
[12]	DCNN with multiple cameras for security	Accuracy: 99.79%, False positives: <1%	High	Significantly improves smart network security with minimal false detections, enabling real-time threat detection.
[13]	CART algorithm for device identification	Accuracy: 91.3%	Moderate	Enhances device identification within encrypted WiFi environments, improving network security in smart networks.
[14]	Care network analysis	Proxy and generative networks prevalent	Low	Provides insights into care networks for elderly but limited application in direct HANET optimization.
[15]	XGBoost and Firefly Optimization for predictive maintenance	Prediction accuracy: 98%	High	Effective in preventing equipment failures, extending the lifespan of HANET devices through predictive analytics.
[16]	DVFS for energy resource selection in HASN	Energy resource selection: Optimized	Moderate	Improves energy management in sensor networks, though real-world application in larger HANET scenarios is unclear.
[17]	ROS-EB for secure data storage	Communication delay: ~15ms, Energy consumed: Low	High	Ensures high security in HANET through blockchain and optimization algorithms, with low communication delay.
[18]	ChaCha20-Poly1305 for IoT grid security	Minimal impact on transmission time	High	Balances security and performance in smart grid HANET systems, minimal latency added by encryption.

[19]	RNN and DTW for ADL prediction	Energy savings: ~25%, Battery life: ~137 days	High	Significantly reduces sensor energy consumption, extending sensor lifespan in smart networks.
[20]	DRIVEN for AHI estimation	Classification accuracy: 72.4%, Correct classification: 99.3%	Moderate	Effective for network healthcare monitoring, though focused primarily on sleep apnea detection.

Figure 3. Statistical Comparative Analysis of Existing Methods

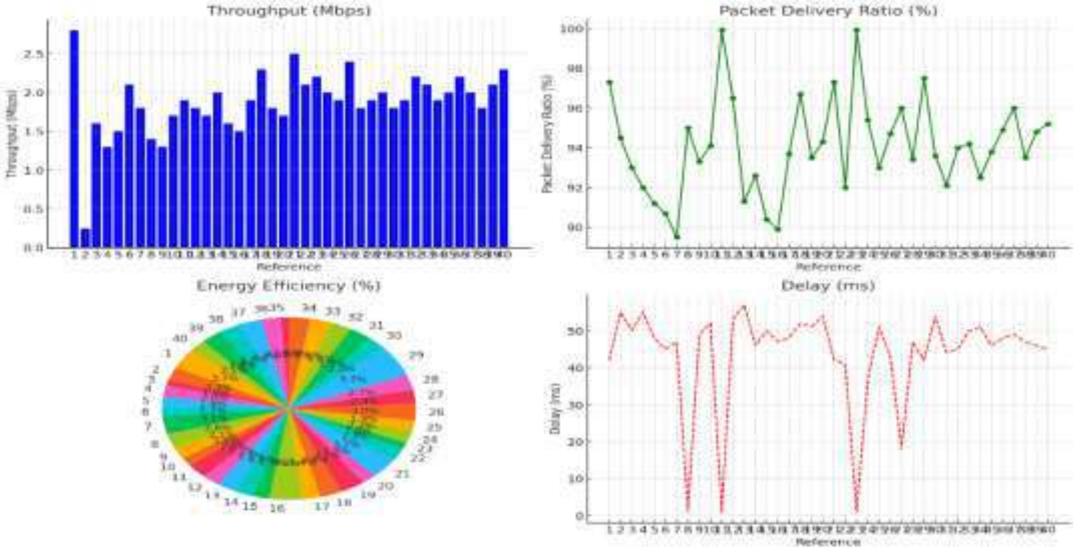

Figure 1. Comparative Results of the Proposed Analysis Process

Table 3, 4 and Figure 1 in the following PRISMA analysis details the comparisons of performances and efficiencies of different methods for the purpose of optimization towards the HANETs system. Based on this, with due consideration to performance metrics like throughput, packet delivery ratio, energy consumption, and latency, there are evident trends toward optimizing smart network environments. Methods like SecureScanML [1] and MSHOP [11] have shown excellent performance both in terms of network efficiency as well as security without vulnerabilities by maintaining high PDR with low latency. In terms of energy management, BLSTM-based HEMS [10] together with energy-saving solutions like RNN/DTW-based ADL prediction [19] shows steps to consume energy which leaves the lifetime of smart network devices and sensors to a longer time. From the security point of view, the blockchain-based approach-ROS-EB approach [17] is proposed with considerable strength and also without losing a single performance of DCNN for smart network security [12]. In general, all these studies indicate an apparent shift towards highly efficient, reliable, and secure designs in the HANET system domain through the integration of efficient algorithms based on machine learning and optimization techniques along with innovative network architectures.

Reference	Method Used	PRISMA Results	Efficiency of HANET Deployment	Observations in terms of HANET Efficiency
[21]	ZigBee-enabled fail-proof HAN (ZFPHAN) with MLPM	Alternate path: Yes, Propagation delay: ~50ms	High	Enhances robustness in smart network networks with fail-proof mechanisms via multi-layer topology.
[22]	DT-driven self-healing with GNNs	Delay reduction: ~15%, Load balance improved: ~20%	High	Efficiently maintains network stability and minimizes service delay through proactive redeployment mechanisms.

[23]	IM-QRP for WBAN	Residual energy: +10%, Path loss: -30%, PDR: +10%, SNR: +7%	Moderate	Optimizes energy and improves signal reliability for healthcare monitoring networks, enhancing longevity.
[24]	Cross-layer thermal-aware convergecast protocol	Delay reduction: 19.4%, Throughput: +13.75%, Packet loss: 0.3%	High	Improves data flow efficiency with minimal delay and packet loss while maintaining thermal control in HANET.
[25]	IoT-based health monitoring system	Accuracy: ~98%, Real-time reporting enabled	High	Ensures reliable, continuous health data transmission in rural and urban settings, with robust offline capabilities.
[26]	LSTM for energy prediction in smart networks	Forecast accuracy: ~92%, Power usage optimized	High	Efficient energy management through AI-driven predictions for power consumption, reducing wastage in HANET.
[27]	LoRa for smart network applications	Transmission delay: 18ms, PRR: 96% (outdoor), PRR: 43% (indoor)	Moderate	Provides effective long-range communication, though indoor performance is impacted by environmental barriers.
[28]	IoT platform traffic fingerprinting tool (IoTPF)	Detection accuracy: ~95%	Moderate	Improves intrusion detection for IoT platforms in HANET, offering enhanced security for smart network devices & deployments.
[29]	SUTMS on Raspberry Pi	IDS accuracy: 99%, Memory utilization reduced: ~55%	High	Provides lightweight, cost-effective security for smart network networks with optimized resource usage.
[30]	Network criticality for IoT	Time complexity reduced to O(n), Robustness improves with size	Moderate	Reduces computational complexity in large-scale IoT networks, improving robustness against node/link failures.
[31]	NILM with CGAN	Appliance detection: ~94%, Unknown detection improved	Moderate	Enhances load monitoring accuracy in HANET but needs better adaptation for detecting unknown appliances.
[32]	FiWi with 3D beamforming	SINR improvement: ~10%, Optimal resource allocation achieved	High	Efficient resource utilization with improved signal quality, particularly in dense urban smart network environments.
[33]	Digital Twin for healthcare monitoring	Fall detection accuracy: ~95%, Atrial fibrillation detection: ~93%	High	Provides real-time health monitoring with predictive capabilities, enhancing smart network healthcare systems.
[34]	GPON-based FTTH with quantum access	Noise profile adherence: ~95%, Feasible for short feeder segments	Moderate	Integrates quantum security with fiber networks, though constrained to short-distance applications in HANET.
[35]	NIDS for Building Automation and Control Systems (BACS)	Protocol-agnostic, Detection accuracy: ~97%	High	Enhances security for BACS in HANET by detecting protocol-specific intrusions without compromising performance.
[36]	VAE-GAN with Q-learning for HEMS	KL divergence: ~0.05, MMD: ~0.03	High	Synthetic data generation aids in improving energy management, surpassing conventional methods for smart networks.

[37]	Self-organizing IoTSN	Load reduction: ~30%, Energy use reduction: ~25%, Latency reduction: 20%	High	Self-organizing networks optimize energy and data flow, boosting HANET performance under varying conditions.
[38]	LoRaWAN integration with 5G	Secure access: ~98%, Performance improvement: ~15%	High	Seamless integration with 5G enhances communication security and efficiency, crucial for HANET in future smart networks.
[39]	LoRa-based IoT for peatland management	GWL correlation: 0.8, MSE: 0.43	Moderate	Efficient in environmental data collection, aiding smart network HANET setups focused on ecological monitoring.
[40]	SWARAM for energy-efficient cluster head selection	PDR: +10%, Network lifetime: +10%	High	Optimizes energy use and extends network lifetime, addressing energy-hole issues in IoT-based HANET systems.

Table 4. Statistical Comparison of Existing Methods

From the PRISMA analysis, it is observed that HANET optimization methods varied in its range since it is specialized in different areas-energy management, security enhancement, or network robustness. As illustrated in methods such as decentralized ZigBee-enabled ZFPHAN [21] and DT-driven self-healing mechanism [22], which mainly focuses on network resilience and robustness, thus making them highly efficient for dynamic HANET environments. On the security front, proposals like the Smart UTM System (SUTMS) [29] and NIDS for BACS [35] significantly advance the technological benefits on HANET systems that protect them from cyber attacks in relation to their actual performance. Energy management techniques use methods such as LSTMbased prediction models [26] and SWARAM [40] that optimize the need for energy usage so as to get the most extended lifecycle of smart network devices & deployments. Generally, the techniques covered above substantially contribute to HANET improvements in efficiency. Reliability, security, and energy efficiency characterize these smart network networks. In this sense, these advanced optimization techniques might enable more or better adaptation of HANET systems for prospective evolving needs in smart network environments.

4. Conclusions & Future Scopes

A closer inspection of the various approaches developed for HANET optimization reveals that application-specific tailored approaches are needed in smart network scenarios. While carrying out this literature review, it could be observed that a set of machine learning models, routing protocols, and energy management algorithms are employed primarily to contribute separately to network performance, security, and energy efficiency, respectively. Out of these, the approach using ZigBee-enabled fail-proof networks with multi-layer topologies [21], DT-driven self-healing mechanisms [22], and intelligent energy management systems like LSTM-based predictions [26], have presented robust performance in its deployment in HANET. Network architectures that are decentralized, like ZigBee-enabled ZFPHAN with a multi-layer partial mesh topology, also present great efficiency in dynamic and fault-prone environments and ensure network robustness and reliability. Such systems provide redundancy and fail-proof mechanisms that guarantee continued operation irrespective of node or link failures; these are suitable for the smart network environment, where reliability for devices is critical. Meanwhile, DT-driven self-healing mechanisms with graph neural networks [22] imply tremendous improvements in service stability and fault recovery, requirements for future 6G networks as well as edge computing scenarios. Both of them are state-of-the-art in the area of network optimization, with a focus on robustness, automated recovery, and efficient resource utilization. From a security point of view, models incorporating intrusion detection systems and unified threat management, such as the Smart UTM System (SUTMS) [29], are critical elements in protecting HANETs from various types of newly emerging cyber threats. Lightweight, resource-aware security solutions can be used to protect a large number of connected devices inside network networks. More importantly, with the implementation of machine learning-based integrating technologies like CNNs and XGBoost [15], especially built for the predictive maintenance and detection of faults, the self-diagnosis ability of the network system is enhanced and the operational disruption is avoided. The above models are accessed very often; thus, there must exist adaptive and scalable security mechanisms within the HANET systems. The RNN-based models particularly those with LSTM in predictive analytics and ideal for energy management with smart networks are meant to predict power usage trends in order to optimize the process without wastage and upgrading quality of life among users [26]. This, further, combined with the SWARAM-based energy-efficient cluster head selection [40], contributes to extending the lifespans of these networks, since it removes the common problem of energy holes in IoT-based HANET systems. Energy efficiency is something that underlines a growing need for sustainable solutions able to achieve high performance and relatively low resource usage set. Next-generation work will involve the implementation of more advanced algorithms in artificial intelligence, including reinforcement learning and federated learning towards the greater flexibility and scalabilty of HANET systems.

The fact that continued advances in the IoT technologies can be along with new-generation wireless networks like 5G and 6G provides a very exciting possibility to further optimize deployments of HANET sets. Furthermore, with increased interconnectivity of smart networks, advanced techniques at deployment time are vital toward ensuring HANET be secure, efficient, and resilient enough for increasing complexity in demands of applications in the future scenarios.

5. References

1. Senthilraja, P., Nancy, P., Sherine Glory, J. et al. *Enhancing IoT security in wireless local area networks through dynamic vulnerability scanning.* **Sādhanā** 49, 195 (2024). https://doi.org/10.1007/s12046-024-02534-8
2. Alizadeh, F., Bidgoly, A.J. *Bit flipping attack detection in low power wide area networks using a deep learning approach.* **Peer-to-Peer Netw. Appl.** 16, 1916–1926 (2023). https://doi.org/10.1007/s12083-023-01511-y
3. Xiong, L., Tang, Y., Liu, C. et al. *A network energy management approach using decoupling value and policy in reinforcement learning.* **Front. Inform. Technol. Electron. Eng.** 24, 1261–1272 (2023). https://doi.org/10.1631/FITEE.2200667
4. Sarwat, H., Alkhashab, A., Song, X. et al. *Post-stroke hand gesture recognition via one-shot transfer learning using prototypical networks.* **J. NeuroEngineering Rehabil.** 21, 100 (2024). https://doi.org/10.1186/s12984-024-01398-7
5. Calò, T., De Russis, L. *Enhancing smart network interaction through multimodal command disambiguation.* **Pers. Ubiquit. Comput.** (2024). https://doi.org/10.1007/s00779-024-01827-3
6. Gilani, S.M.M., Usman, M., Daud, S. et al. *SDN-based multi-level framework for smart network services.* **Multimed. Tools Appl.** 83, 327–347 (2024). https://doi.org/10.1007/s11042-023-15678-2
7. Qureshi, K.N., Alhudhaif, A., Azahar, M. et al. *A Software-Defined Network-based Intelligent Decision Support System for the Internet of Things Networks.* **Wireless Pers. Commun.** 126, 2825–2839 (2022). https://doi.org/10.1007/s11277-022-09626-w
8. Sobhani, A., Khorshidi, F. & Fakhredanesh, M. *DeePLS: Personalize lighting in smart network by human detection, recognition, and tracking.* **SN Comput. Sci.** 4, 773 (2023). https://doi.org/10.1007/s42979-023-02240-y

9. Cinaglia, P. *PyMulSim: A method for computing node similarities between multilayer networks via graph isomorphism networks.* **BMC Bioinformatics** 25, 211 (2024). https://doi.org/10.1186/s12859-024-05830-6

10. Singh, K.C., Baskaran, S. & Marimuthu, P. *Cost analysis using hybrid gazelle and seagull optimization for network energy management system.* **Electr. Eng.** (2024). https://doi.org/10.1007/s00202-024-02585-4

11. Panda, N., Supriya, M. Efficient data transmission using trusted third party in smart network environments. *J Wireless Com Network*, **2022**, 118 (2022). https://doi.org/10.1186/s13638-022-02200-9

12. Sharma, R., Potnis, A. & Chaurasia, V. Enhancing smart network security using deep convolutional neural networks and multiple cameras. *Wireless Pers Commun*, **136**, 2185–2200 (2024). https://doi.org/10.1007/s11277-024-11371-1

13. Fakhruldeen, H.F., Saadh, M.J., Khan, S. et al. Enhancing smart network device identification in WiFi environments for futuristic smart networks-based IoT. *Int J Data Sci Anal* (2024). https://doi.org/10.1007/s41060-023-00489-3

14. Kemper-Koebrugge, W., Adriaansen, M., Laurant, M. et al. Care networks of network-dwelling older adults in the Netherlands: proof of concept of a network typology. *BMC Geriatr*, **23**, 800 (2023). https://doi.org/10.1186/s12877-023-04404-0

15. Alijoyo, F.A., Pradhan, R., Nalini, N. et al. Predictive maintenance optimization in Zigbee-enabled smart network networks: A machine learning-driven approach utilizing fault prediction models. *Wireless Pers Commun* (2024). https://doi.org/10.1007/s11277-024-11233-w

16. Sivabalan, S., Rathipriya, R. Efficient energy resource selection in heterogeneous adhoc sensor networks using non-swarm intelligence-based discrete Venus flytrap search optimization algorithm. *Wireless Pers Commun*, **128**, 249–265 (2023). https://doi.org/10.1007/s11277-022-09953-y

17. Atiewi, S., Al-Rahayfeh, A., Almiani, M. et al. Ethereum blockchain-based three-factor authentication and multi-contract access control for secure smart network environment in 5G networks. *Cluster Comput*, **27**, 4551–4568 (2024). https://doi.org/10.1007/s10586-023-04202-8

18. L. Kane, V. Liu, M. McKague and G. R. Walker, "Network architecture and authentication scheme for LoRa 2.4 GHz smart networks," *IEEE Access*, **10**, 93212–93230 (2022). doi: 10.1109/ACCESS.2022.3203387. **Keywords:** Security; Smart networks; Authentication; Wide area networks; Monitoring; Smart grids; Protocols; Internet of Things; Encryption; IoT; ChaCha20; Poly1350; authentication; key management; Heterogeneous adhoc network; smart network; smart grid; network performance; symmetric key encryption; LoRa 2.4 GHz

19. M. Khan, J. Seo and D. Kim, "Modeling of intelligent sensor duty cycling for smart network automation," *IEEE Transactions on Automation Science and Engineering*, **19**(3), 2412–2421 (July 2022). doi: 10.1109/TASE.2021.3084631. **Keywords:** Sensors; Intelligent sensors; Smart networks; Wireless sensor networks; Energy consumption; Batteries; Hidden Markov models; Duty cycling; Network automation; Recurrent neural networks (RNNs); Smart networks; Wireless sensor networks (WSNs)

20. Retamales, G., Gavidia, M.E., Bausch, B. et al. Towards automatic network-based sleep apnea estimation using deep learning. *npj Digit. Med.*, **7**, 144 (2024). https://doi.org/10.1038/s41746-024-01139-z

21. R. Das and J. N. Bera, "Multi-Layer-Partial-Mesh-Based Fail Proof HAN With Decentralized Multi Gateway for Smart Network Monitoring and Control," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 715–724, Feb. 2024, doi: 10.1109/TCE.2024.3373449. **Keywords:** Zigbee; Logic gates; Topology; Network topology; Stars; Network appliances; Wireless fidelity; Gateway; Heterogeneous adhoc network; Multi-layer partial mesh; ZigBee communication; ZFPHAN

22. P. Yu et al., "Digital Twin Driven Service Self-Healing With Graph Neural Networks in 6G Edge Networks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 11, pp. 3607–3623, Nov. 2023, doi: 10.1109/JSAC.2023.3310063. **Keywords:** Predictive models; 6G mobile communication; Measurement; Artificial intelligence; Delays; Analytical models; Computational modeling; 6G edge networks; Service self-healing; Digital twin; Graph neural networks

23. **[13]** N. Ahmad et al., "Improved QoS Aware Routing Protocol (IM-QRP) for WBAN-Based Healthcare Monitoring System," *IEEE Access*, vol. 10, pp. 121864–121885, 2022, doi: 10.1109/ACCESS.2022.3223085. **Keywords:** Wireless communication; Body area networks; Sensors; Medical services; Monitoring; Wireless sensor networks; Biomedical monitoring; Energy efficiency; Quality of service; Convolutional neural networks; Noise measurement; Signal-to-noise ratio; Wireless body area networks; Quality of service; Energy efficiency; Received signal strength intensity; Signal-to-noise ratio; Path loss ratio; Convolutional neural networks

24. Y. Shahzad, H. Javed, H. Farman, Z. Khan, M. M. Nasralla, and A. Koubaa, "Optimized Distributive Cross-Layer and Thermal-Aware Convergecast Protocol for Wireless Body Area Network," *IEEE Access*, vol. 10, pp. 90338–90354, 2022, doi: 10.1109/ACCESS.2022.3200336.
Keywords: Routing protocols; Wireless communication; Body area networks; Reliability; Routing; Relays; Wireless sensor networks; Medical services; Internet of Things; Thermal analysis; Convergecast; Cross-layer; Internet of Healthcare Things; Internet of Things; Thermal-aware; Wireless body area network

25. M. N. Bhuiyan et al., "Design and Implementation of a Feasible Model for the IoT-Based Ubiquitous Healthcare Monitoring System for Rural and Urban Areas," *IEEE Access*, vol. 10, pp. 91984–91997, 2022, doi: 10.1109/ACCESS.2022.3202551. **Keywords:** Monitoring; Medical services; Temperature measurement; Urban areas; Temperature sensors; Sensors; Real-time systems; Internet of Things; Real-time systems; Smart networks; Rural areas; Patient monitoring; Healthcare; Rural and urban areas; Monitoring system; Architectures; Networks

26. O. Akbarzadeh et al., "Heating-Cooling Monitoring and Power Consumption Forecasting Using LSTM for Energy-Efficient Smart Management of Buildings: A Computational Intelligence Solution for Smart Networks," *Tsinghua Science and Technology*, vol. 29, no. 1, pp. 143–157, Feb. 2024, doi: 10.26599/TST.2023.9010008. **Keywords:** Energy consumption; Temperature distribution; Recurrent neural networks; Cooling; Computational modeling; Urban areas; Smart networks; Design-builder; Besos; Smart cities; Smart building; Neural network; Long Short-Term Memory (LSTM)

27. C. Zhong and X. Nie, "Feasibility of LoRa for Smart Network: Real-Time and Coverage Considerations," *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 25213–25226, 15 July 2024, doi: 10.1109/JIOT.2024.3391761. **Keywords:** Smart networks; Internet of Things; Delays; Performance evaluation; Logic gates; Zigbee; Physical layer; Communication distance; Computation methodology; Delay; Experiment; Installation considerations; LoRa; Rayleigh distribution; Rician distribution; Smart network

28. X. He, Y. Yang, W. Zhou, W. Wang, P. Liu, and Y. Zhang, "Fingerprinting Mainstream IoT Platforms Using Traffic Analysis," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2083–2093, 1 Feb. 2022, doi: 10.1109/JIOT.2021.3093073. **Keywords:** Internet of Things; Cloud computing; Servers; Security; Protocols; Local area networks; Hardware; Fingerprinting; IoT platform; Network security; Smart network solution; Traffic analysis

29. A. Siddiqui, B. P. Rimal, M. Reisslein, D. Gc, and Y. Wang, "SUTMS: Designing a Unified Threat Management System for Smart Networks," *IEEE Access*, vol. 12, pp. 80930–80949, 2024, doi: 10.1109/ACCESS.2024.3410111. **Keywords:** Firewalls (computing); Intrusion detection; Network automation; Wireless fidelity; Internet of Things; Routing; Botnet; Threat assessment; Anti-bot protection; Flow detection; IoT; Intrusion prevention system (IPS); Privacy; Raspberry Pi; Security; Unified threat management (UTM); Vulnerabilities

30. S. Dhuli, S. Kouachi, A. Chhabra, and Y. N. Singh, "Network Robustness Analysis for IoT Networks Using Regular Graphs," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8809–8819, 1 June 2022, doi: 10.1109/JIOT.2021.3116256. **Keywords:** Robustness; Internet of Things; Network topology; Topology; Laplace equations; Mathematical models; Eigenvalues and eigenfunctions; IoT; Network criticality; Network robustness; Real-world network data sets; Random geometric graph (RGG); R-nearest neighbor networks

31. Y. Han, K. Li, C. Wang, F. Si, and Q. Zhao, "Unknown Appliances Detection for Non-Intrusive Load Monitoring Based on Conditional Generative Adversarial Networks," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4553–4564, Nov. 2023, doi: 10.1109/TSG.2023.3261271.
Keywords: Trajectory; Network appliances; Load monitoring; Generators; Training; Hidden Markov models; Feature extraction; Generative adversarial networks; Capsule network; Conditional generative adversarial networks; Non-intrusive load monitoring; Unknown appliances detection; V-I trajectory

32. N. Chatur, T. Bose, and A. Adhya, "Planning Cost-Efficient FiWi Access Network With Joint Deployment of FWA and FTTH," *IEEE Transactions on Communications*, vol. 72, no. 9, pp. 5688–5703, Sept. 2024, doi: 10.1109/TCOMM.2024.3384933. **Keywords:** 5G mobile communication; Wireless communication; Optical fiber subscriber loops; Resource management; Passive optical networks; Three-dimensional displays; Array signal processing; Fiber-wireless (FiWi); Fixed wireless access (FWA); Fiber-to-the-home (FTTH); Passive optical network (PON); 5G

33. J. Chen et al., "Digital Twin Empowered Wireless Healthcare Monitoring for Smart Network," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 11, pp. 3662–3676, Nov. 2023, doi: 10.1109/JSAC.2023.3310097. **Keywords:** Monitoring; Medical services; Smart networks; Cloud computing; Biomedical monitoring; Digital twins; Visualization; Digital twin; Healthcare monitoring; Smart network; Artificial intelligence

34. D. Zavitsanos et al., "Feasibility Analysis of QKD Integration in Real-World FTTH Access Networks," *Journal of Lightwave Technology*, vol. 42, no. 1, pp. 4–11, Jan. 1, 2024, doi: 10.1109/JLT.2023.3303908. **Keywords:** Optical fiber subscriber loops; Optical fiber cables; Passive optical networks; Optical fibers; Optical fiber devices; Optical transmitters; Buildings; Coexistence scheme; Coherent one-way (COW); Fiber-to-the-home (FTTH); Passive optical network (PON); Photon counting measurements; Quantum access network (QAN); Quantum key distribution (QKD); Raman noise; Secure key rate (SKR); Time-division multiplexing (TDM)

35. V. Graveto, T. Cruz, and P. Simões, "A Network Intrusion Detection System for Building Automation and Control Systems," *IEEE Access*, vol. 11, pp. 7968–7983, 2023, doi: 10.1109/ACCESS.2023.3238874.
Keywords: Network automation; Smart buildings; Security; Building automation;

Monitoring; Control systems; Safety; Building automation and control systems (BACS); NIDS; Smart buildings; KNX

36. M. Razghandi, H. Zhou, M. Erol-Kantarci, and D. Turgut, "Smart Network Energy Management: VAE-GAN Synthetic Dataset Generator and Q-Learning," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 1562–1573, March 2024, doi: 10.1109/TSG.2023.3288824.

Keywords: Synthetic data; Data models; Smart networks; Training; Load modeling; Q-learning; Smart grids; Load consumption; Deep learning; Generative adversarial network; Q-learning

37. N. Li and X. Liu, "Research on Self-Organization and Adaptive Strategy of the Internet of Things Sensor Networks," *IEEE Access*, vol. 12, pp. 66569–66579, 2024, doi: 10.1109/ACCESS.2024.3399537.

Keywords: Adaptive systems; Network topology; Topology; Resource management; Internet of Things; Task analysis; Heuristic algorithms; Sensor systems; Self-organizing networks; Adaptive strategy

38. H. Jradi, F. Nouvel, A. E. Samhat, J.-C. Prévotet, and M. Mroue, "A Seamless Integration Solution for LoRaWAN Into 5G System," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 16238–16252, Sept. 15, 2023, doi: 10.1109/JIOT.2023.3267502. **Keywords:** Authentication; 5G mobile communication; Internet of Things; Servers; Network architecture; Security; Object recognition; 5G; Long Range Wide Area Network (LoRaWAN); IoT; Security

39. L. Li et al., "Estimation of Ground Water Level (GWL) for Tropical Peatland Forest Using Machine Learning," *IEEE Access*, vol. 10, pp. 126180–126187, 2022, doi: 10.1109/ACCESS.2022.3225906.

Keywords: Forestry; Temperature measurement; Humidity; Soil moisture; Mathematical models; Indexes; Wind speed; Peatland; IoT system; Fire Weather Index (FWI); Machine learning; Neural networks

40. Somula R., Cho Y., and Mohanta B.K., "SWARAM: Osprey Optimization Algorithm-Based Energy-Efficient Cluster Head Selection for Wireless Sensor Network-Based Internet of Things," *Sensors*, vol. 24, no. 2, p. 521, 2024. https://doi.org/10.3390/s24020521

Keywords: Energy-efficient clustering; Cluster head selection; Wireless sensor network; Internet of Things; Osprey optimization algorithm; SWARAM