MRS Journal of Multidisciplinary Research and Studies
ISSN *(Online) 3049-1398*
Vol-3, Iss-1 (January-2026)
Journal homepage: https://mrspublisher.com/journals

Machine Learning-Driven Optimization and Security in IoT Ubiquitous Sensor Networks: A Comprehensive Review

Tammineni Anil Kumar[1*], Dr. R. Rajeswara Rao[2]

[*1]Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Vizianagaram, Andhra Pradesh, India

[*2]Supervisor & Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Vizianagaram, Andhra Pradesh, India

Corresponding Author: ***Tammineni Anil Kumar*** *(Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Vizianagaram, Andhra Pradesh, India)*

Received: 15 / 12 / 2025	Accepted: 11 / 01 / 2026	Published: 30 / 01 / 2026

Abstract: Internet of Things Ubiquitous Sensor Networks (IoT-USNs) represent a significant paradigm shift in technological infrastructure, enabling the development of intelligent applications across various sectors, including healthcare, smart urban settings, precision agriculture, and industrial automation. Notwithstanding their widespread implementation, IoT-USNs face enduring challenges that hinder their scalability, operational efficiency, and security. This systematic review investigates cutting-edge solutions through an exhaustive analysis of 19 peer-reviewed articles published from 2018 to 2024. The identified critical limitations encompass an increased vulnerability to cyber threats, severe constraints in energy and computational resources, and complexities associated with the management of real-time data via effective aggregation and routing mechanisms. The decentralized architecture exacerbates challenges pertaining to data integrity and security enforcement, rendering networks susceptible to various attack vectors. The analysis delineates three primary research trajectories: optimization techniques driven by machine learning that achieve energy efficiency improvements of up to 40%; trust management systems that enhance authentication protocols; and adaptive routing protocols that significantly mitigate congestion issues. This review provides a critical assessment of existing methodologies, identifies notable deficiencies in integrated security-energy optimization frameworks, and underscores the limited real-world implementation of cross-layer solutions. The contribution of this work lies in synthesizing contemporary research trajectories and proposing future research directions that emphasize integrative strategies incorporating advanced security mechanisms, energy-aware protocols, and intelligent data management frameworks to fully harness the potential of IoT-USNs.

Keywords: *Internet of Things, Ubiquitous Sensor Networks, Machine Learning, Trust Management, Energy Efficiency, Adaptive Routing, Network Security, Optimization Algorithms.*

Cite this article: Kumar, T. A. & Rao, R. R. (2026). Machine Learning-Driven Optimization and Security in IoT Ubiquitous Sensor Networks: A Comprehensive Review. *MRS Journal of Multidisciplinary Research and Studies, 3(1),43-54.*

Introduction

The Internet of Things (IoT) has emerged as one of the most transformative technological paradigms of the contemporary era, facilitating seamless interconnectivity among billions of intelligent devices, sensors, and systems. This interconnected ecosystem enables sophisticated communication between physical and digital environments, driving innovations across diverse domains, including smart homes, industrial automation, precision agriculture, healthcare systems, and environmental monitoring. Within this expansive IoT framework, Ubiquitous Sensor Networks constitute a pivotal component by deploying extensive arrays of distributed sensor nodes that collaboratively collect, process, and transmit environmental data. These networks form the foundational infrastructure of IoT ecosystems, delivering real-time insights and enabling control over geographically dispersed infrastructures.

Despite their growing significance and widespread deployment, IoT-USNs encounter persistent challenges that fundamentally limit their scalability, operational efficiency, and security. The dense and heterogeneous composition of these networks introduces substantial security vulnerabilities, as the proliferation of interconnected devices exponentially increases the attack surface, making it vulnerable to potential intrusions and malicious activities. Furthermore, resource constraints, including limited energy capacity, restricted bandwidth, and constrained computational power, significantly restrict the performance capabilities and operational lifetime of sensor nodes. Another critical challenge involves data management complexities, wherein the enormous volume of sensory data generated in real time necessitates intelligent routing mechanisms, congestion control algorithms, and efficient storage solutions to maintain network reliability while minimizing latency. Successfully addressing these

interconnected challenges is essential for realizing the full operational potential of IoT-USNs in mission-critical applications.

Recent advances in Machine Learning have demonstrated considerable promise in addressing the inherent complexities characterizing IoT-USNs. ML algorithms possess the capability to analyze large-scale datasets, predict network behavioral patterns, and

automates decision-making processes without requiring explicit programming. Their inherent adaptability facilitates the dynamic optimization of critical network parameters, including routing efficiency, load balancing, trust management, and energy consumption, all of which are key determinants for sustaining efficient and secure IoT-USN operations. For instance, predictive ML models can anticipate the mobility patterns of sink nodes, thereby reduce redundant transmissions and substantially improve energy efficiency. Similarly, trust-aware learning models can continuously evaluate the reliability of sensor nodes, thereby strengthening the network's resilience against malicious attacks and faulty node behavior. The integration of ML with optimization algorithms further enables the development of self-organizing and self-healing network architectures capable of real-time adjustment to environmental changes and workload variations.

This review encompasses the critical aspects of ML-driven optimization and management techniques for IoT-USNs, with particular emphasis on three fundamental research domains. First, energy efficiency and routing optimization encompass techniques that utilize ML and metaheuristic algorithms to extend the network lifetime. Second, trust management and security enhancement involve models that employ ML-based trust assessment, anomaly detection, and secure routing mechanisms. Third, adaptive and predictive network control includes methods that integrate ML for mobility prediction, data aggregation, and dynamic resource allocation. Through a systematic analysis and comparative evaluation of state-of-the-art studies across these domains, this study presents a comprehensive perspective on how machine learning contributes to resolving core operational challenges in IoT-USNs.

The remainder of this paper is organized as follows. Section II provides an overview of the IoT- USN architecture and identifies common challenges. Section III presents a comprehensive literature review of existing solutions. Section IV analyzes the research gaps identified in the current literature. Section V proposes a conceptual framework for optimizing performance. Section VI discusses the expected outcomes. Section VII concludes with directions for future research.

OVERVIEW OF IOT-UBIQUITOUS SENSOR NETWORKS

The Internet of Things fundamentally relies on Ubiquitous Sensor Networks as its core infrastructure, facilitating the seamless integration of physical environments with digital systems. IoT-USNs comprise spatially distributed sensor nodes that continuously gather, process, and transmit environmental or contextual data, thereby enabling intelligent real-

time decision-making. Their pervasive nature ensures uninterrupted sensing and communication capabilities across extensive or heterogeneous environments, including smart cities, healthcare systems, industrial facilities, and environmental monitoring frameworks.

Architecture and Components

A typical IoT-USN architecture exhibits a hierarchical and multilayered design optimized for efficient data flow and energy conservation across network entities. The primary architectural components are sensor nodes, cluster heads, sink nodes, gateways, cloud servers, and end-user applications.

Sensor nodes are compact, energy-constrained devices equipped with sensing, processing, and wireless communication capabilities. These devices are tasked with detecting environmental changes, including temperature variations, humidity levels, atmospheric pressure, motion detection, and chemical presence, and subsequently transmitting the sensed data to higher architectural layers. Owing to their limited computational capacity and restricted power resources, sensor nodes are the most critical yet vulnerable components of the network infrastructure.

In large-scale deployments, the sensor nodes are organized into clusters that are managed by designated cluster heads. These cluster heads aggregate data from their member nodes, perform local processing or compression operations, and forward the summarized information to subsequent layers, thereby reducing redundant transmissions and conserving energy resources. Sink nodes, which function as data collection hubs, receive aggregated data from the cluster heads or directly from the sensor nodes. In certain network configurations, mobile sinks traverse the network field to efficiently collect data from multiple locations, thereby minimizing the communication overhead and energy consumption. However, mobility introduces additional challenges related to route prediction and synchronization.

Gateways connect local IoT-USNs to external networks or cloud platforms, where large-scale data analytics, storage, and visualization operations are performed. They facilitate the integration of machine learning models and decision-making frameworks that enhance network intelligence. The top architectural layer represents end-user applications that utilize processed data to generate actionable insights, including precision agriculture systems that automate irrigation, healthcare systems that monitor patient vitals, and industrial systems that optimize production lines.

Common Challenges in IoT-USNs

Despite their versatility, IoT-USNs encounter several fundamental challenges that affect their reliability, scalability, and operational efficiency.

Energy constraints represent a primary limitation, as sensor nodes are typically battery-powered and deployed in remote or inaccessible environments, rendering energy efficiency crucial for sustained operation. Frequent communication and data transmission activities can precipitate rapid battery depletion, potentially fragmenting network connectivity, and reducing the overall network lifespan.

Data loading and network congestion are significant challenges. The substantial volume of data generated by distributed sensors can overwhelm the network capacity, resulting in congestion, packet loss, and increased latency. Efficient data aggregation and sophisticated routing protocols are required to maintain real-time responsiveness and reliability of the system.

Scalability and topological dynamics add to the complexity. As the number of connected devices increases, managing

communication and maintaining synchronization across dynamic and heterogeneous nodes is increasingly challenging. Network topologies may evolve continuously because of node mobility, component failures, or environmental variations, necessitating adaptive management strategies.

Security and trust issues remain paramount. The open and distributed nature of IoT-USNs exposes them to various security risks, including data tampering, node compromise, and denial-of-service attacks. Trust management among nodes is essential for ensuring data integrity and maintaining reliable communication channels in a network.

Resource heterogeneity introduces additional complexity because IoT networks frequently comprise devices with varying capabilities, communication protocols, and computational resources. This diversity creates substantial challenges in terms of standardization, compatibility assurance, and unified network management.

Existing Network Models and Architectures

Several architectural models have been proposed to enhance the performance and manageability of IoT-USNs, each offering distinct advantages and limitations.

The flat architecture represents the simplest configuration, wherein all sensor nodes perform similar roles and communicate directly with sink nodes or through multi-hop routing. Although conceptually simple, this architecture suffers from high energy consumption and limited scalability, rendering it unsuitable for large-scale deployments.

A hierarchical or cluster-based architecture organizes nodes into clusters, each managed by a designated cluster head. This structural approach improves energy efficiency and scalability by substantially reducing communication overhead. Protocols such as LEACH, HEED, and EE-LEACH exemplify this architectural paradigm.

A mobile sink-based architecture incorporates one or more mobile sinks that traverse the network to collect data. This model reduces the data transmission distance and balances the energy consumption across the network. However, intelligent prediction and routing mechanisms are required to effectively manage mobility patterns and maintain communication reliability.

Heterogeneous architectures combine nodes with varying energy capacities, transmission ranges, and processing abilities to optimize performance in complex environments. These architectures often integrate machine learning-based optimization to manage device diversity and resource allocation efficiently.

Fog and edge-enhanced architectures represent recent advancements in integrating fog or edge computing capabilities with IoT-USNs, bringing computation and analytics closer to data sources. This approach reduces latency, enhances scalability, and supports real-time machine learning-driven decision-making.

IoT-Ubiquitous Sensor Networks form the foundational backbone of smart and connected environments. However, their performance remains constrained by factors such as energy efficiency limitations, trust management requirements, and scalability challenges. The incorporation of machine learning and optimization algorithms has recently emerged as a transformative approach to overcome these limitations, providing adaptive, secure, and energy-aware solutions for the evolving Internet of Things (IoT) landscape.

PROBLEM STATEMENT

Despite significant advancements in the realm of Internet of Things Ubiquitous Sensor Networks (IoT-USNs) and their increasing integration across various sectors, several crucial challenges hinder their complete realization. These challenges mainly focus on security weaknesses, resource constraints, and the complexities associated with data governance. IoT-USNs often face issues in protecting the integrity and security of the data

They transmit data primarily because of their vast and decentralized structure, which makes them vulnerable to a wide range of security threats. In addition, IoT devices functioning within these networks are typically limited by strict energy and computational resources, thus requiring the development of highly efficient resource management strategies to sustain their effectiveness and performance. Moreover, the large amount of data generated by these sensor networks necessitates sophisticated algorithms for effective aggregation, processing, and routing to alleviate network congestion and ensure timely data transmission.

LITERATURE REVIEW

This section provides a comprehensive analysis of existing research addressing challenges in IoT-USNs through machine learning-driven approaches, optimization techniques, and security mechanisms.

Veeranjaneyulu et al. investigated Data Synchronized–Machine Learning (DS-ML) for IoT-connected networks, focusing on seamless adaptation to network changes by minimizing disruptions and enhancing overall network efficiency. Despite its strengths, this approach is significantly constrained by its reliance on high-quality synchronized data, which is often unavailable in dynamic or resource-limited IoT environments. The approach also requires precise temporal synchronization across distributed nodes, a condition that becomes increasingly difficult to maintain as network heterogeneity and scale expand.

In the realm of energy-efficient routing, Ramesh et al. introduced the Energy Efficient Routing Protocol (EERP) for IoT-based networks. Employing a TDMA-based MAC protocol, EERP optimizes energy consumption by allocating time slots for data transmission and utilizing multi-hop routes. Although the protocol improves network coverage and efficiency, it suffers from the inherent limitation of TDMA systems—the need for strict synchronization among nodes. This dependency is particularly challenging in dynamic environments, affecting communication reliability when node mobility or irregular topologies are present.

Nourildean et al. employed the Riverbed Modeler Simulation Program to evaluate IoT network performance across diverse topologies using ZigBee end devices. While this simulation-based assessment offers valuable insights into efficiency and reliability factors, the exclusive reliance on ZigBee devices limits transmission range and data rate. These constraints hinder scalability and throughput, especially in large or high-bandwidth IoT applications.

Srinivasa et al. explored routing complexities in mobile IoT scenarios, incorporating Convolutional Neural Networks (CNNs) into the clustering process. However, CNN performance is influenced heavily by the representativeness of training data,

posing challenges in dynamic mobile IoT contexts. Additionally, the computational complexity of CNNs may hinder real-time deployment in resource-constrained IoT devices.

Tan et al. proposed a distributed tree-based clustering routing protocol emphasizing energy efficiency by selecting cluster heads based on remaining energy, node density, and location. Despite these advantages, scalability and flexibility remain significant concerns. The heterogeneous nature of IoT devices and evolving network dynamics may reduce the efficiency and consistency of the EE-DTC protocol.

Banimelhem et al. utilized Principal Component Analysis to generate fixed paths for mobile sinks, offering a feasible data collection mechanism. However, the method is tailored primarily for single mobile sink prediction, limiting its applicability in more complex scenarios involving multiple mobile sinks.

Jothikumar et al. introduced an Optimal Cluster-Based Routing technique employing k-means for node clustering and a multihop chain-routing approach. While effective, performance depends on the initial selection of cluster centers, and the k-means algorithm's sensitivity to outliers becomes problematic in highly dynamic environments. Variations in node mobility and density further influence multihop efficiency.

Ahmad et al. proposed the Zone Routing Protocol, demonstrating improvements in packet delivery and throughput. Nevertheless, its performance is highly sensitive to zone boundary selection and specific environmental conditions. Structural or size changes in the network may impact protocol consistency across diverse IoT scenarios.

Sethi employed sink mobility to address energy disparities and prolong network lifetime by integrating multiple sojourn-location route patterns with centralized static sinks. While beneficial, the inclusion of various mobile sinks and route patterns introduces additional network overhead, such as increased control of traffic and routing messages, which can offset energy gains.

Bharathi et al. presented the Energy Efficient Particle Swarm Optimization (EEPSO) technique for optimizing cluster-head selection under diverse IoT conditions. Although effective, EEPSO faces scalability challenges as network size and device heterogeneity increase. Furthermore, convergence speed and susceptibility to local optima may hinder application in dynamic scenarios.

Vahabi et al. proposed a hybrid method combining hierarchical and geographic techniques with mobile sinks to improve energy efficiency and network lifespan. However, in highly mobile scenarios, hierarchical and geographic strategies may become less effective. Adaptability to dynamic topologies and dependence on accurate location information also affects overall performance.

Wang et al. developed a distance-aware routing algorithm incorporating multiple mobile sinks for energy conservation. Practical deployment challenges arise due to the need for synchronization and coordination among mobile sinks. Scalability and adaptability to real-world variations, such as changing mobility patterns and node densities, must therefore be carefully considered.

Kaur and Kumar introduced a PSO-based fault-tolerant clustering technique addressing unequal clustering and energy heterogeneity within sensor nodes. While enhancing resilience to node failures, the protocol may face scalability issues as network size increases, and parameter sensitivity remains a critical factor for effective real-world implementation.

Wen et al. proposed a cooperative data collection algorithm (CDCA) that groups nodes and assigns a mobile sink to each group to optimize transmission. Although the algorithm improves performance, experimental results show that network lifetime declines after extended operational rounds. This outcome may stem from increased energy expenditure or inefficiencies in grouping and routing strategies, indicating the need for further investigation to refine the CDCA approach.

REVIEW METHODOLOGY

This review adopts a systematic approach to ensure comprehensive coverage of research related to IoT-based Ubiquitous Sensor Networks (IoT-USNs). The methodology follows established guidelines for systematic literature reviews to maintain transparency, reproducibility, and rigor throughout the selection and analysis process.

Relevant literature was collected from five major scholarly databases: IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and MDPI. The search was conducted in October 2024, covering publications primarily from 2014 to 2024 to capture the modern era of IoT-WSN integration, while including earlier foundational works where necessary for theoretical context. Keywords were combined using Boolean operators: ("IoT" OR "Internet of Things" OR "Ubiquitous Sensor Network") AND ("wireless sensor network" OR "WSN") AND ("routing" OR "clustering" OR "energy efficiency" OR "mobile sink" OR "optimization" OR "metaheuristic" OR "machine learning"). The search was limited to peer-reviewed articles published in English.

Studies were included if they proposed novel routing, clustering, optimization, or machine learning techniques for IoT-WSNs; were published in reputable journals (impact factor ≥ 1.0) or recognized conferences; presented experimental results or simulation analyses with performance comparisons; or were highly cited foundational works (≥ 50 citations). Studies were excluded if they focused solely on hardware implementation without algorithmic contributions, lacked technical depth or performance evaluation, were duplicate publications or reviews, or addressed topics outside the IoT-USN domain.

The selection process followed a multi-stage screening approach. Initial database searches identified approximately 120 papers. Two independent reviewers screened titles and abstracts, resolving disagreements through discussion, resulting in 48 papers for full-text examination. Primary exclusion reasons included works outside scope (28 papers), insufficient technical depth (18 papers), duplicates (15 papers), and review articles (11 papers). Full-text assessment of the 48 papers evaluated methodological rigor, technical contribution, and alignment with review objectives, yielding 26 relevant studies. Further exclusions included marginal contributions (9 papers), inadequate experimental validation (7 papers), and significant overlap with selected works (6 papers). Final quality assessment based on methodology clarity, contribution significance, experimental rigor, and relevance to current challenges resulted in 19 key papers for comprehensive analysis and synthesis.

For each selected paper, information was systematically extracted including problem addressed, proposed solution,

methodology, performance metrics (energy consumption, network lifetime, throughput, latency, packet delivery ratio), evaluation parameters, and key findings. The 19 studies were organized into six thematic categories through iterative analysis: machine learning and deep learning-based solutions, energy-efficient routing protocols, clustering and cluster head selection techniques, mobile sink-based routing strategies, hybrid metaheuristic optimization approaches, and simulation and performance analysis studies. This classification, developed by identifying common methodological patterns and complementary contributions, forms the structural foundation for the literature discussion in subsequent sections.

Table 1. Gap Identification through literature review

S. NO	AUTHORS	TITLE OF THE PAPER	YEAR OF PUBLICATION	MECHANISMS USED	OBSERVATIONS	GAPS
1.	Veeranjaneyulu et al.	Data Synchronized-Machine Learning in IoT Connected Networks	2024	Data Synchronized-Machine Learning (DS-ML)	Enhances network efficacy by minimizing disruptions	Dependency on high-quality synchronized data
2.	Pedditi, Ramesh Babu, and Kumar Debasis. 2023.	"Energy Efficient Routing Protocol for an IoT-Based WSN System to Detect Forest Fires"	2023	EERP	Used TDMA MAC protocol	limitation of the TDMA-based MAC protocol is its reliance on precise synchronization among nodes, which can be difficult to maintain in dynamic and resource-constrained environments.
3.	Nourildean, Shayma W. and Mohammed, Yousra A. and Abdulhadi, May T.,	Investigating the Impact of Network Topologies on the IoT-Based WSN in Smart Home Monitoring System	2023	Zigbee based	IoT Wireless Sensor Network (WSN) platform utilizing the Riverbed Modeler Simulation Program to investigate network performance across diverse topologies	ZigBee end devices is their limited transmission range and data rate
4.	SrinivasaBabu Kasturi, P. Venkateswarlu Reddy,K VenkataNagendra, M. Radha MadhavSudhanshu	An Improved Energy Efficient Solution for Routing in IoT	2022	incorporation of Convolutional Neural Networks (CNNs) into	gives insight on the complexity of routing in mobile IoT	success is strongly dependent on the diversity and relevancy of the data it

	Kumar Jha			the cluster proce ss[8]	scenarios	learns from
5.	Tan, Nguyen Duy, and Hong-Nhat Hoang.	Energy-Efficient Distributed Cluster-Tree Based Routing Protocol for IoT-Based Wireless Sensor Networks	2022	presented the distributed tree-based clustering routing protocol [9]	with an emphasis on energy efficiency	heterogeneous nature of IoT devices, as well as dynamic changes in network circu mstances over time, may have an impact on the efficiency
6.	Banimelhem,O.;Taqied din, E.; Shatnawi	An Efficient Path Generation Algorithm Using Principal Component Analysis for Mobile Sinks in Wireless Sensor Network	2021	uses principal component analysis (PCA) to build a fixed path for mobi le sinks [10]	provides a feasible data collection solution	Its restriction is that it is only applicable to cases with a single mobile sink forecast.
7.	Li, Zengpeng, C. Jothikumar, Kadiyala Ramana, V. Deeban Chakravarthy, Saurabh Singh, and In-Ho Ra	An Efficient Routing Approach to Maximize the Lifetime of IoT-Based Wirel ess Sensor Networks in 5G and Beyond	2021	Optimal Clust er-Based Routing [11]	uses the k-means method for node clustering	may be influenced by the initial cluster center selection
8.	I. Ahmad	Performance Assessment of QoS Using AODV, TORA and ZRP Routing Proto col in MANET	2020	The Zone routing protocol [12]	achieves noteworthy results in packet delivery ratio and throughput	may be influenced by the zone boundary selection
9.	Sethi D.	An approach to optimize homogeneous and heterogeneous routing proto cols in WSN using sink mobility	2020	4-or 8-sojourn-location route patterns [13]	utilizes sinks node mobility in wireless sensor networks to reduce the ener gy gap	may result in additional network overhead
10	Bharathi, R.; Abirami, T.; Dhanasekaran, S.; Gupta, D.; Khanna, A.; Elhoseny, M.; Shankar	Energy effici ent clustering with disease	2020	Energy Effici ent Particle Swarm	goal of optimizing Cluster Head (CH) selection	scalability and adaptability to large-scale IoT networks may

		diagnosis model for IoT based sustainable healthcare systems.		Optimization (EEPSO) [14]	in various IoT device scenarios	be limited
11	Vahabi, S.; Eslaminejad, M.; Dashti, S.E	Integration of geographic and hierarchical routing protocols for energy saving in wireless sensor networks with mobile sink	2019	hybrid of hierarchical and geographic approaches [15]	to improve energy efficiency and network lifespan	may be hampered when dealing with rapidly changing network topologies
12	Gao, Y.; Wang, J.; Wu, W.; Sangaiah, A.K.; Lim, S.	A Hybrid Method for Mobile Agent Moving Trajectory Scheduling using ACO and PSO in WSNs	2019	distance-aware routing algorithm using ACO and PSO [16]	uses numerous mobile sinks to reduce network energy usage.	may be influenced by synchronization and coordination issues among the mobile sinks.
13	Kaur, T.; Kumar, D.	Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks	2018	PSO based clustering [17]	consists of applying PSO to optimize the clustering process	scalability concerns as the network grows, as well as potential parameter sensitivity.
14	W. Wen, C.-Y. Chang, S. Zhao, and C. Shang	Cooperative Data Collection Mechanism Using Multiple Mobile Sinks in Wireless Sensor Networks	2018	cooperative data collection algorithm (CDCA) [18]	for grouping sensor nodes and assigning a mobile sink to each group	it was discovered that after a certain number of rounds, the lifetime was shortened

Table2: Strengths and Limitations of Existing Studies

Papers	**Strengths**	**Limitations**
Veeranjaneyulu et al.	Smooth ML-based adaptation; improves stability	Requires highly synchronized data; not suitable for heterogeneous networks

Srinivasa et al.	CNN improves clustering accuracy	High computational load; needs large training data
Ramesh et al.	Reduces energy through TDMA; good for static networks	Strict synchronization requirement; poor for high mobility
Tan et al.	Energy-aware clustering; simple decisions	Not scalable; limited flexibility in dynamic networks
Ahmad et al.	Higher packet delivery and throughput	Sensitive to zone boundaries; environment dependent
Kaur & Kumar	Fault tolerance; adaptive clustering	Parameter-sensitive; scalability issues
Bharathi et al.	Improved CH selection using PSO	May fall into local optima; convergence speed issues
Wang et al.	Balanced energy consumption using mobile sinks	Coordination among sinks is complex
Vahabi et al.	Extends lifetime via mixed methods	Ineffective in rapidly changing mobility patterns
Banimelhem et al.	Efficient PCA-based sink path	Works only for single sink; not scalable
Sethi	Reduces hotspot problem	High control overhead in multi-sink settings

RESEARCH GAPS AND OPPORTUNITIES

The comprehensive analysis of existing literature reveals several critical research gaps that must be addressed to advance IoT-enabled underwater sensor networks. These gaps can be broadly categorized into protocol-level limitations, intelligent system challenges, and sustainability concerns, each presenting distinct opportunities for scholarly contribution.

At the protocol level, the predominant reliance on TDMA-based MAC protocols requiring precise temporal synchronization represents a fundamental constraint. The variable propagation delays and resource limitations characteristic of underwater environments render strict synchronization both difficult to achieve and costly to maintain. This dependence creates operational bottlenecks that compromise system robustness,

particularly in dynamic aquatic settings. The development of asynchronous or loosely coupled synchronization mechanisms emerges as a priority of research direction. Similarly, current communication technologies exhibit significant limitations; while ZigBee devices offer energy efficiency, their restricted transmission ranges and reduced data rates constrain scalability in large deployments where signal attenuation is already pronounced. Hybrid communication architectures capable of dynamic protocol adaptation based on real-time network conditions represent a promising yet underexplored avenue that could optimize the energy-coverage trade-off essential for extended underwater operations.

The integration of intelligent systems, particularly machine learning approaches, introduces additional challenges that current research has not adequately resolved. Convolutional Neural Networks and similar techniques demonstrate potential for network management, yet their performance remains tightly coupled to training data characteristics. The marked degradation observed when models encounter deployment scenarios differing from training conditions highlights a critical gap in generalization capabilities. Advanced methodologies including transfer learning, federated learning, and domain adaptation warrant systematic investigation to enable effective operation across heterogeneous

device configurations and evolving environmental parameters. Furthermore, mobility management for multiple mobile sinks presents coordination complexities that existing path optimization approaches, largely limited to single-sink scenarios, fail to address comprehensively. The communication overhead and synchronization requirements associated with multi- collector systems necessitate novel protocol designs that balance data collection efficiency with energy conservation.

Sustainability and scalability concerns constitute the third major gap category. Contemporary routing protocols, whether zone-based, hierarchical, or hybrid, exhibit performance degradation under frequent topological changes resulting from node mobility, failures, or environmental disturbances. The predominance of reactive adaptation strategies proves insufficient; predictive methodologies that anticipate network evolution and adjust parameters proactively remain underdeveloped. Additionally, clustering algorithms demonstrate sensitivity to initialization parameters without robust systematic solutions for optimal configuration. Most critically, the accelerated network lifetime degradation observed across multiple operational cycles reveals fundamental inadequacies in energy management paradigms. While energy harvesting technologies and ultra-low-power communication systems offer potential solutions, their integration into practical underwater deployments remains nascent. Scalability limitations in optimization- based approaches further compound these issues, as centralized methods become computationally prohibitive, and distributed algorithms encounter convergence difficulties in large-scale networks.

These interconnected gaps underscore the necessity for holistic research approaches that transcend isolated technical improvements. Future investigations should prioritize integrated frameworks that simultaneously address protocol efficiency, intelligent adaptation, and sustainable operation, recognizing that advances in individual domains may prove insufficient without considering system-level interactions and trade-offs inherent to underwater sensor network deployments.

PROPOSED CONCEPTUAL FRAMEWORK FOR PERFORMANCE OPTIMIZATION

This section presents a comprehensive conceptual framework designed to enhance operational performance, security, and resilience of IoT-USNs through integration of predictive analytics, evolutionary optimization, and trust-aware mechanisms.

Framework Overview

The proposed conceptual framework aims to enhance operational performance, security, and resilience of IoT-USNs by integrating predictive analytics, evolutionary optimization, and trust-aware mechanisms into a unified architecture supporting intelligent decision- making in dynamic and resource-constrained environments. The framework comprises two interdependent modules. The first module focuses on mobility prediction and adaptive routing for performance optimization. The second module introduces a trust-aware secure communication model to strengthen the reliability of data exchange. Collectively, these modules constitute a hybrid system capable of learning, adapting, and securing network behavior in response to mobility and environmental uncertainty.

Module I: Mobility Prediction and Adaptive Routing

The mobility prediction and adaptive routing module address the challenge of maintaining energy-efficient and reliable communication within IoT-USNs characterized by mobile sinks and dynamically changing topologies. The module proceeds through a sequence of computational stages beginning with network initialization and culminating in iterative adaptation and optimization.

At the outset, the IoT-USN environment is initialized through definition of essential parameters including the number and spatial distribution of sensor nodes, communication range, initial energy levels, and underlying network topology. These parameters establish the simulation baseline upon which predictive and optimization processes operate.

Subsequently, future trajectories of mobile sinks are estimated using a deep learning-based predictive model. Recurrent Neural Networks or Long Short-Term Memory architectures are particularly suitable for this task, as they possess capability for modeling sequential dependencies in mobility patterns over time. The predictor leverages historical position sequences together with contextual variables including node density, link reliability, and residual energy to estimate future sink positions. Accurate sink prediction enables proactive adaptation of routing decisions, reducing link failures, and minimizing unnecessary retransmissions.

Once mobility has been predicted, the framework employs a multi-objective optimization algorithm to improve network performance with respect to energy consumption, throughput, and lifetime. Evolutionary techniques such as Particle Swarm Optimization or Genetic Algorithms are applied to search for optimal configurations of routing paths and cluster- head selection. The optimization process formulates a composite fitness function that simultaneously minimizes energy expenditure and delay while maximizing data delivery and lifetime extension. Through iterative evaluation of candidate solutions against this objective, the optimizer converges toward a balanced network configuration that harmonizes performance and sustainability.

Based on outcomes of prediction and optimization, an adaptive routing mechanism is executed. This routing algorithm dynamically adjusts communication paths according to predicted sink positions, current node energy, and real-time traffic conditions. Through continuous monitoring and reconfiguration, it maintains efficient energy utilization and reliable packet delivery even under rapidly evolving network conditions. The system is designed to operate as a closed feedback loop wherein predicted mobility information is continuously supplied to optimization and routing layers. As network conditions fluctuate, the loop iteratively refines routing structure, thereby preserving network efficiency and stability. This feedback-driven architecture allows the IoT-USN to exhibit self-adaptive behavior, an essential feature for large-scale deployments where manual reconfiguration is infeasible.

Module II: Trust-Aware Secure Communication

The second module focuses on enhancing security, reliability, and trust management of the IoT-USN. In distributed sensing environments, nodes may exhibit faulty or malicious behavior due to energy depletion, compromise, or transmission errors. To mitigate these risks, the proposed framework incorporates a dynamic trust-based evaluation mechanism that

quantifies node reliability and integrates this measure into the routing decision process.

During initialization, trust parameters are assigned to all nodes, forming the basis for subsequent trust computation. Each node maintains a local trust table that records both self-observed and peer-reported behavioral metrics. Trust evaluation is performed using a dual approach combining direct and indirect observations. Direct trust is derived from the node's own behavioral record including packet forwarding success, energy efficiency, and compliance with routing protocols, while indirect trust is inferred from neighboring nodes through probabilistic inference mechanisms including Bayesian reputation modeling.

The overall trust value for each node is defined as a weighted combination of direct and indirect trust components, where the weighting factor determines the relative influence of local and collective assessments. This formulation provides a balanced and resilient measure of trustworthiness that accounts for both individual and social behaviors within the network.

The computed trust values are then classified into distinct reliability categories including trusted, uncertain, and malicious nodes using dynamic thresholds. Nodes with trust values below the threshold are restricted from participating in forwarding or cluster formation activities, thereby isolating potential adversaries. Based on these classifications, routing decisions are guided by a hybrid metric that integrates trust, energy, and topological distance. The optimal forwarding route is selected by maximizing the combined measure considering node trustworthiness, residual energy, and hop distance to the sink. This strategy ensures that data are routed preferentially through nodes that are both trustworthy and energetically stable, thereby enhancing overall integrity and endurance of the network.

The trust system operates adaptively with periodic updates of trust decay rates, reliability counters, and communication statistics. This dynamic adjustment enables the framework to respond promptly to behavioral shifts, environmental fluctuations, and emergent threats, maintaining an accurate representation of network trust states. Performance evaluation of the trust-aware module is conceptually based on metrics including throughput, residual energy, and trust accuracy, which together provide indication of communication reliability, energy sustainability, and security robustness. The trust-aware mechanism therefore not Only protects the network from malicious interference but also contributes to long-term performance stability by preventing resource exhaustion and routing misbehavior.

Implementation Considerations

Although this study presents a conceptual synthesis, the proposed framework is implementable within standard simulation environments including MATLAB or Python-based IoT toolkits. Simulation scenarios can be constructed to assess network performance under varying densities, mobility models, and attack conditions. Key parameters including energy consumption, latency, throughput, and trust accuracy can be quantitatively analyzed to evaluate the effectiveness of predictive and trust-aware mechanisms. The use of evolutionary and deep learning algorithms in tandem facilitates reproducibility and allows fine-tuning of algorithmic parameters for empirical validation.

Framework Contributions

The integration of predictive modeling, optimization, and trust management is expected to yield significant improvements in energy efficiency, network lifetime, and security assurance. By predicting sink mobility, the system minimizes redundant transmissions and prolongs node longevity. The trust-aware component enhances data integrity by isolating unreliable nodes, reducing risk of data corruption, or routing attacks. Moreover, adaptive optimization of resources promotes efficient load distribution and mitigates congestion, enabling the network to maintain high throughput even under mobility or attack scenarios. The modular design of the framework ensures scalability across diverse IoT domains including smart cities, precision agriculture, healthcare monitoring, and industrial automation. The framework provides a foundational model for future empirical research, offering a structured approach for integrating machine learning and trust-aware routing within intelligent IoT-USNs.

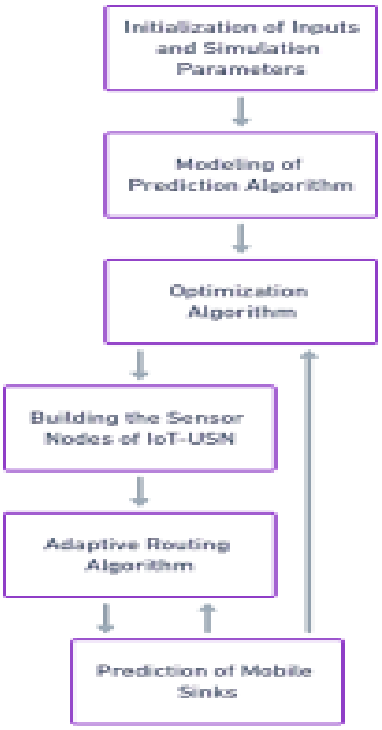

Figure 1 High-level conceptual workflow of IoT-USN routing and mobile sink prediction

KEY INSIGHTS FROM THE SURVEY

The proposed framework is projected to deliver substantial and multifaceted advancements in the performance, security, and operational sustainability of IoT-based Ubiquitous Sensor Networks (IoT-USNs). By integrating mobility prediction, evolutionary optimization, and trust-aware secure communication, the system is designed to significantly enhance network efficiency while comprehensively addressing critical challenges associated with reliability, scalability, and security.

First, the incorporation of a predictive mobility model for mobile sinks is expected to markedly improve routing efficiency. By accurately forecasting node movements, routing protocols can proactively adjust data transmission paths, thereby minimizing redundant communications, reducing packet loss, and lowering

energy consumption. This proactive adaptation not only optimizes network traffic flow but also extends the operational lifespan of sensor nodes, which is vital for reducing maintenance and deployment costs in large-scale sensor networks. Moreover, the predictive capabilities facilitate better load balancing across the network, preventing bottlenecks and ensuring smoother data delivery even in highly dynamic environments.

Second, the integration of a trust-aware assessment mechanism is anticipated to significantly enhance network security and communication reliability. This mechanism continuously evaluates both direct and indirect trust metrics, enabling real-time identification and isolation of untrustworthy or malicious nodes. By safeguarding the confidentiality, integrity, and authenticity of transmitted data, the framework mitigates risks posed by common security threats such as data tampering, node impersonation, and unauthorized access. The trust model also supports adaptive trust recalibration based on network behavior, which strengthens resilience against evolving attack strategies. Consequently, this approach fosters a secure communication environment that is essential for sensitive IoT applications requiring high data fidelity.

Third, the deployment of adaptive evolutionary optimization techniques is expected to facilitate dynamic resource management, enabling the network to maintain stable and optimal performance under varying traffic loads, mobility patterns, and threat conditions. This adaptive architecture allows for continuous learning and fine-tuning of network parameters, which contributes to robust defense mechanisms against denial-of-service attacks, node capture, and data manipulation. By optimizing resource allocation such as bandwidth, energy, and computational power in real time, the framework ensures sustained network operability and responsiveness. Furthermore, the evolutionary algorithms support scalability by efficiently managing the increased complexity and heterogeneity of expanding IoT-USN deployments.

Fourth, the modular and extensible design of the proposed framework is expected to demonstrate exceptional scalability and adaptability across a wide range of IoT application domains. Whether implemented in dense urban smart city infrastructures, industrial automation, or sparse agricultural monitoring systems, the framework is engineered to maintain reliable and consistent performance irrespective of environmental complexity or deployment scale. This flexibility enables seamless integration with existing IoT platforms and facilitates customization to meet specific operational requirements. The modularity also supports incremental upgrades and incorporation of emerging technologies, thereby future proofing the network architecture against rapid technological evolution.

Finally, the study is projected to yield comprehensive documentation encompassing detailed methodology, implementation procedures, and rigorous performance evaluations of the proposed system. The development of associated simulation tools, algorithmic libraries, and software modules is anticipated to provide valuable resources for researchers and practitioners, thereby accelerating innovation and practical adoption in IoT network management and intelligent sensing technologies. These resources will support reproducibility, benchmarking, and continuous improvement, fostering a collaborative ecosystem for advancing IoT-USN capabilities.

Collectively, these anticipated outcomes underscore the framework's potential to address pivotal challenges in energy efficiency, security, reliability, scalability, and long-term sustainability. By combining predictive analytics, adaptive optimization, and trust-based security within a scalable architecture, the framework lays a robust foundation for the next generation of intelligent, resilient, and efficient IoT-USN systems capable of supporting diverse real-time data collection and processing applications across multiple sectors.

CONCLUSION AND FUTURE WORK

This study advances a comprehensive and intelligent framework for optimizing performance, security, and operational sustainability of IoT-USNs. By addressing critical gaps identified in existing literature including synchronization challenges, limited scalability, insufficient trust mechanisms, and inefficient handling of mobility, this study integrates machine learning-driven prediction, adaptive optimization, and trust-aware decision systems into a unified architecture. The proposed methodology, structured around predictive mobility modeling, evolutionary optimization, and trust computation, provides a multilayered solution capable of addressing the dynamic, resource-constrained, and security-sensitive nature of modern IoT-USNs.

The mobility prediction module introduces a deep learning framework capable of forecasting sink trajectories and enabling proactive routing decisions, thereby reducing redundant transmission and improving energy efficiency. Additionally, the optimization layer refines routing structures and resource allocation using evolutionary algorithms, ensuring sustained performance under varying network conditions. The trust-aware module further enhances communication reliability by evaluating node behavior using combined direct and indirect trust metrics and incorporating these trust levels into routing decisions. Together, these components form a closed-loop system that continuously adapts to environmental changes, mobility patterns, and evolving security challenges.

The expected outcomes of this study including enhanced routing efficiency, strengthened trust management, dynamic resource optimization, and broad scalability underscore the potential of the proposed framework to serve as a foundational model for next-generation IoT architectures. The modularity of the framework ensures its applicability across diverse IoT domains including precision agriculture, smart cities, healthcare monitoring, and industrial automation where energy sustainability, secure communication, and resilient routing are essential.

Future Research Directions

Although the conceptual framework demonstrates strong potential, several avenues for future exploration have emerged. First, extensive simulation-based validation using MATLAB or platforms such as NS-3 or IoT-Sim is required to quantify performance benchmarks across varying node densities, mobility patterns, and attack scenarios. Second, integration of real-world datasets and heterogeneous hardware configurations will enable more robust evaluation of model generalizability and scalability. Third, future extensions may incorporate federated learning or edge intelligence paradigms, enable decentralized prediction and trust computation while reduce communication overhead.

Additionally, the dynamic trust model can be enhanced through reinforcement learning to autonomously adjust trust decay rates, anomaly thresholds, and behavioral patterns in real time. Similarly, multi-sink mobility prediction using multi-agent

learning approaches can be explored to address limitations identified in prior studies that relied on single-sink predictions. Finally, practical implementation in testbeds or real-time IoT deployments is crucial for validating the framework under operational constraints including intermittent connectivity, physical security vulnerabilities, and environmental variability.

The proposed framework establishes a strong foundation for intelligent, secure, and energy-aware IoT-USNs. This study provides a pathway for future research that leverages machine learning and optimization to create resilient and autonomous IoT infrastructures capable of supporting the growing demands of ubiquitous sensing environments.

REFERENCES

1. J. Kharel, H. T. Reda, and S. Y. Shin, "Fog computing-based smart health monitoring system deploying LoRa wireless communication," IETE Technical Review, vol. 36, no. 1, pp. 69-82, 2019.
2. V. Hayyolalam and A. A. P. Kazem, "Black widow optimization algorithm: A novel meta-heuristic approach for solving engineering optimization problems," Engineering Applications of Artificial Intelligence, vol. 87, p. 103249, 2020.
3. Badshah, A. Ghani, M. A. Qureshi, and S. Shamshirband, "Smart security framework for educational institutions using Internet of Things (IoT)," Computers, Materials & Continua, vol. 61, no. 1, pp. 81-101, 2019.
4. Aravind and P. K. R. Maddikunta, "Dingo optimization based cluster based routing in Internet of Things," Sensors, vol. 22, no. 20, p. 8064, 2022.
5. R. Nagaraju, V. C., K. J., M. G., S. B. Goyal, C. Verma, C. O. Safirescu, and T. C. Mihaltan, "Secure routing-based energy optimization for IoT application with heterogeneous wireless sensor networks," Energies, vol. 15, no. 13, p. 4777, 2022.
6. V. K., L. M., S. Venkateswara Swamy, S. K., N. N., and A. S., "Enhancing wireless sensor network routing strategies with machine learning protocols," in Proc. 2nd International Conference on Networking and Communications (ICNWC), Chennai, India, 2024, pp. 1-7.
7. R. B. Pedditi and K. Debasis, "Energy efficient routing protocol for an IoT-based WSN system to detect forest fires," Applied Sciences, vol. 13, no. 5, p. 3026, 2023.
8. S. B. Kasturi, P. V. Reddy, K. V. Nagendra, M. R. Madhavi, and S. K. Jha, "An improved energy efficient solution for routing in IoT," Journal of Pharmaceutical Negative Results, pp. 1683-1691, Oct. 2022.
9. N. D. Tan and H.-N. Hoang, "Energy-efficient distributed cluster-tree based routing protocol for IoT-based wireless sensor networks," in Proc. Seventh International Conference on Research in Intelligent and Computing in Engineering, vol. 33, 2022, pp. 213-218.
10. O. Banimelhem, E. Taqieddin, and I. Shatnawi, "An efficient path generation algorithm using principle component analysis for mobile sinks in wireless sensor networks," Journal of Sensor and Actuator Networks, vol. 10, no. 4, p. 69, 2021.
11. Z. Li, C. Jothikumar, K. Ramana, V. D. Chakravarthy, S. Singh, and I.-H. Ra, "An efficient routing approach to maximize the lifetime of IoT-based wireless sensor networks in 5G and beyond," Mobile Information Systems, vol. 2021, Article ID 9160516, 2021.
12. Ahmad, "Performance assessment of QoS using AODV, TORA and ZRP routing protocol in MANET," Mehran University Research Journal of Engineering and Technology, vol. 39, no. 4, pp. 744-750, 2020.
13. D. Sethi, "An approach to optimize homogeneous and heterogeneous routing protocols in WSN using sink mobility," MAPAN, vol. 35, no. 2, pp. 241-250, 2020.
14. R. Bharathi, T. Abirami, S. Dhanasekaran, D. Gupta, A. Khanna, M. Elhoseny, and K. Shankar, "Energy efficient clustering with disease diagnosis model for IoT based sustainable healthcare systems," Sustainable Computing: Informatics and Systems, vol. 28, p. 100453, 2020.
15. S. Vahabi, M. Eslaminejad, and S. E. Dashti, "Integration of geographic and hierarchical routing protocols for energy saving in wireless sensor networks with mobile sink," Wireless Networks, vol. 25, pp. 2953-2961, 2019.
16. Gao, J. Wang, W. Wu, A. K. Sangaiah, and S. Lim, "A hybrid method for mobile agent moving trajectory scheduling using ACO and PSO in WSNs," Sensors, vol. 19, no. 3, p. 575, 2019.
17. T. Kaur and D. Kumar, "Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks," IEEE Sensors Journal, vol. 18, no. 11, pp. 4614-4622, 2018.
18. W. Wen, C.-Y. Chang, S. Zhao, and C. Shang, "Cooperative data collection mechanism using multiple mobile sinks in wireless sensor networks," Sensors, vol. 18, no. 8, 2018.
19. S. W. Nourildean, Y. A. Mohammed, and M. T. Abdulhadi, "Investigating the impact of network topologies on the IoT-based WSN in smart home monitoring system," Eastern-European Journal of Enterprise Technologies, vol. 6, no. 9, pp. 6-14, 2022.