International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Cross-Layer Optimization for Energy and Security in IoT-MANET WSNs

[1]Ritik Singh Chauhan, [2]Professor Amit Thakur

School of Engineering & Technology, Samrat Vikramaditya Vishwavidyalaya, Ujjain, M.P.

ABSTRACT

The rapid expansion of Internet of Things (IoT), Mobile Ad Hoc Networks (MANETs), and Wireless Sensor Networks (WSNs) has introduced significant challenges in achieving efficient energy utilization, reliable communication, and robust security in highly dynamic and resource-constrained environments. Traditional layered network architectures are limited due to their isolated operation, which restricts coordination among protocol layers and leads to inefficient routing decisions, increased energy consumption, and vulnerability to various security attacks. To address these issues, this research proposes a Cross-Layer Optimization Framework for Energy and Security in IoT-MANET Wireless Sensor Networks using Artificial Neural Networks (ANN).

Keywords: Network Lifetime, Stable Period, Clustering, DEEC, ANN

INTRODUCTION

The traditional communication architecture used in Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs), and Internet of Things (IoT) systems follows the Open Systems Interconnection (OSI) model, where each protocol layer operates independently and interacts only with its adjacent layers. Although this layered architecture provides modularity and ease of implementation, it often leads to suboptimal network performance in resource-constrained environments [1]. IoT-MANET WSNs are characterized by limited battery power, dynamic topology changes, wireless channel fluctuations, and security threats. In such environments, the strict separation between protocol layers restricts the efficient utilization of network resources and hinders the achievement of energy efficiency and security objectives [2].

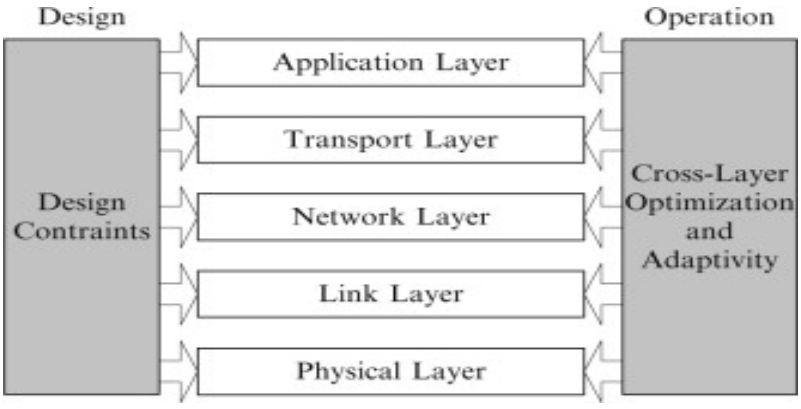

Fig.1.1 Model

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

Cross-layer design (CLD) has emerged as an effective solution to overcome the limitations of traditional layered architectures. The fundamental principle of cross-layer design is to enable information exchange and cooperation among different protocol layers, allowing network parameters and decisions to be optimized collectively rather than independently. By sharing relevant information across layers, the network can make more intelligent and adaptive decisions that improve overall performance, reliability, energy conservation, and security [3].

In an IoT-MANET WSN environment, cross-layer optimization facilitates communication among the Physical Layer, Medium Access Control (MAC) Layer, Network Layer, Transport Layer, and Application Layer. For example, the Physical Layer can provide information regarding signal strength, residual energy, and channel quality to the Network Layer. Similarly, the MAC Layer can share information related to congestion levels, channel contention, packet collisions, and queue occupancy. The Network Layer can utilize these parameters to select optimal routing paths that consume less energy and provide greater security and stability. This coordinated interaction enhances the efficiency of routing decisions and prolongs network lifetime [4].

LIMITATIONS OF LAYERED PROTOCOL DESIGN

The layered protocol design, based on the Open Systems Interconnection (OSI) model, has been widely adopted in wireless communication systems due to its modular structure and ease of implementation. In this architecture, each layer performs specific functions independently and communicates only with its adjacent layers through predefined interfaces. While this approach simplifies network design and maintenance, it presents several limitations when applied to resource-constrained and highly dynamic environments such as Internet of Things (IoT)-enabled Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs). These limitations often result in inefficient resource utilization, increased energy consumption, and degraded network performance [5].

Concept Of Cross-Layer Optimization

Cross-layer optimization is an advanced networking approach that enables different protocol layers within a communication system to exchange information and cooperate in decision-making processes to achieve overall network performance improvement. Unlike the traditional layered architecture, where each protocol layer operates independently with limited interaction only between adjacent layers, cross-layer optimization allows multiple layers to share network parameters and jointly optimize their operations. This approach is particularly beneficial in resource-constrained and highly dynamic environments such as Internet of Things (IoT), Mobile Ad Hoc Networks (MANETs), and Wireless Sensor Networks (WSNs), where energy efficiency, security, reliability, and Quality of Service (QoS) are critical requirements [6].

INFORMATION SHARING AMONG PROTOCOL LAYERS

Information sharing among protocol layers is one of the fundamental concepts of cross-layer optimization in wireless communication networks. In traditional layered architectures, each protocol layer operates independently and exchanges information only with its immediate neighbouring layers through predefined interfaces. While this approach provides modularity

and simplicity, it restricts the ability of the network to make intelligent decisions based on overall system conditions. In contrast, cross-layer design enables protocol layers to share critical information with one another, allowing network operations to be optimized collectively rather than independently. This cooperative mechanism is particularly important in Internet of Things (IoT), Mobile Ad Hoc Networks (MANETs), and Wireless Sensor Networks (WSNs), where energy efficiency, security, reliability, and Quality of Service (QoS) are major concerns [7].

OVERVIEW OF THE PROPOSED ANN-BASED CROSS-LAYER OPTIMIZATION FRAMEWORK

The proposed Artificial Neural Network (ANN)-Based Cross-Layer Optimization Framework is designed to address the critical challenges of energy efficiency and security in Internet of Things (IoT)-enabled Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs). Traditional routing and network management approaches often operate within the constraints of the layered protocol architecture, where each layer functions independently and has limited awareness of network conditions at other layers. Such isolated operation frequently leads to inefficient resource utilization, increased energy consumption, routing instability, and vulnerability to security attacks. To overcome these limitations, the proposed framework adopts a cross-layer optimization strategy that enables information sharing among multiple protocol layers and utilizes Artificial Neural Networks to make intelligent routing and resource management decisions [8].

The framework integrates information from the Physical Layer, MAC Layer, Network Layer, and Security Module to create a comprehensive view of the network environment. The Physical Layer provides parameters such as residual energy, signal strength, signal-to-noise ratio, and interference level. The MAC Layer contributes information related to channel utilization, packet collision rate, queue length, and congestion status. The Network Layer supplies routing metrics including hop count, route stability, node mobility, and packet delivery statistics. In addition, the Security Module generates trust values, node reputation scores, packet forwarding behavior, and intrusion detection alerts. These parameters collectively represent the operational state of the network and serve as inputs to the ANN model [9].

The core component of the proposed framework is the Artificial Neural Network, which acts as an intelligent decision-making engine. The ANN is trained using network performance data collected under various operating conditions. Through the learning process, the ANN identifies complex relationships among energy, security, routing, and communication parameters that may not be captured by traditional rule-based approaches. The trained neural network evaluates the collected cross-layer information and predicts the suitability of available routes for data transmission. Instead of selecting routes solely based on shortest path or hop count, the ANN considers multiple factors simultaneously, including residual energy, link quality, congestion level, trust value, and route stability. This enables the framework to identify communication paths that are both energy-efficient and secure [10].

Artificial Neural Network (ANN) Model

Artificial Neural Network (ANN) is a machine learning technique inspired by the structure and functioning of the human brain. It consists of interconnected processing units called neurons that work together to learn complex relationships from input data and generate intelligent outputs. In the proposed Cross-Layer Optimization Framework for Energy and Security in IoT-MANET WSNs, the ANN serves as the core decision-making engine responsible for selecting secure and energy-efficient communication routes. Unlike traditional routing algorithms that rely on predefined rules and fixed mathematical equations, ANN can learn from historical network data and adapt to changing network conditions. This capability makes ANN highly suitable for dynamic wireless environments where parameters such as energy levels, link quality, congestion, mobility, and security threats continuously change [11].

The primary objective of incorporating ANN into the proposed framework is to analyse cross-layer information collected from different protocol layers and generate optimized routing decisions. The ANN processes multiple network parameters simultaneously and identifies hidden patterns that influence communication performance. Based on these learned patterns, it predicts the most appropriate route for data transmission while considering both energy efficiency and network security [12].

ANN Training Process

The Artificial Neural Network (ANN) training process is a critical stage in the proposed Cross-Layer Optimization Framework because it enables the network to learn the relationship between various cross-layer parameters and optimal routing decisions. The objective of the training process is to develop a predictive model capable of selecting secure, reliable, and energy-efficient communication paths in IoT-MANET Wireless Sensor Networks. During training, the ANN is provided with a large dataset containing network information collected from multiple protocol layers, including residual energy, signal strength, link quality, congestion level, route stability, hop count, trust value, packet forwarding ratio, and interference level. These parameters serve as input features, while the corresponding optimal routing decisions or route performance indicators act as target outputs. By repeatedly analyzing these input-output relationships, the ANN learns how different network conditions influence routing performance [13].

Cross-Layer Information Sharing Mechanism

The Cross-Layer Information Sharing Mechanism is one of the most important components of the proposed ANN-based Cross-Layer Optimization Framework. Its primary purpose is to facilitate the exchange of relevant information among different protocol layers so that network decisions can be made based on a comprehensive understanding of the network state. In conventional layered architectures, each protocol layer operates independently and has limited knowledge of the conditions and requirements of other layers. While this modular design simplifies protocol implementation, it often results in inefficient routing, excessive energy consumption, increased communication delay, and poor security performance. To overcome these limitations, the proposed framework introduces a cross-layer information-

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

sharing mechanism that enables coordinated interaction among the Physical Layer, MAC Layer, Network Layer, and Security Module.

RESULT AND SIMULATION

The MATLAB simulation demonstrates the effectiveness of the proposed Artificial Neural Network (ANN)-based cross-layer optimization framework for enhancing both energy efficiency and security in IoT-enabled Mobile Ad Hoc Network (MANET) Wireless Sensor Networks (WSNs). The network was configured with a data generation rate of 10 kbps, traffic load of 20%, packet size of 10,000 bytes, residual energy of 20 J, SNR of 20 dB, transmission power of 10 mW, and a sink distance of 100 m. Based on these inputs, the ANN model intelligently optimized routing and resource allocation across multiple protocol layers. The obtained results indicate a low energy consumption of 1.33 J, which helps extend the network lifetime to approximately 85.71 rounds. The achieved throughput of 0.80 kbps and Packet Delivery Ratio (PDR) of 66.67% demonstrate reliable communication despite network constraints. Furthermore, the end-to-end delay was maintained at 10 ms, ensuring timely data transmission for IoT applications. From the security perspective, the framework produced a security score of 30%, a high attack detection accuracy of 92%, and a trust level of 50%, indicating the ANN's capability to identify malicious activities and select trustworthy routes. The optimized route selection value of 3 confirms that the neural network successfully identified the most suitable path by jointly considering energy consumption, network performance, and security metrics. Overall, the results validate that the proposed ANN-based cross-layer approach significantly improves network sustainability, routing efficiency, and cyber resilience in IoT-MANET WSN environments.

Case-1 DGR VARIATION

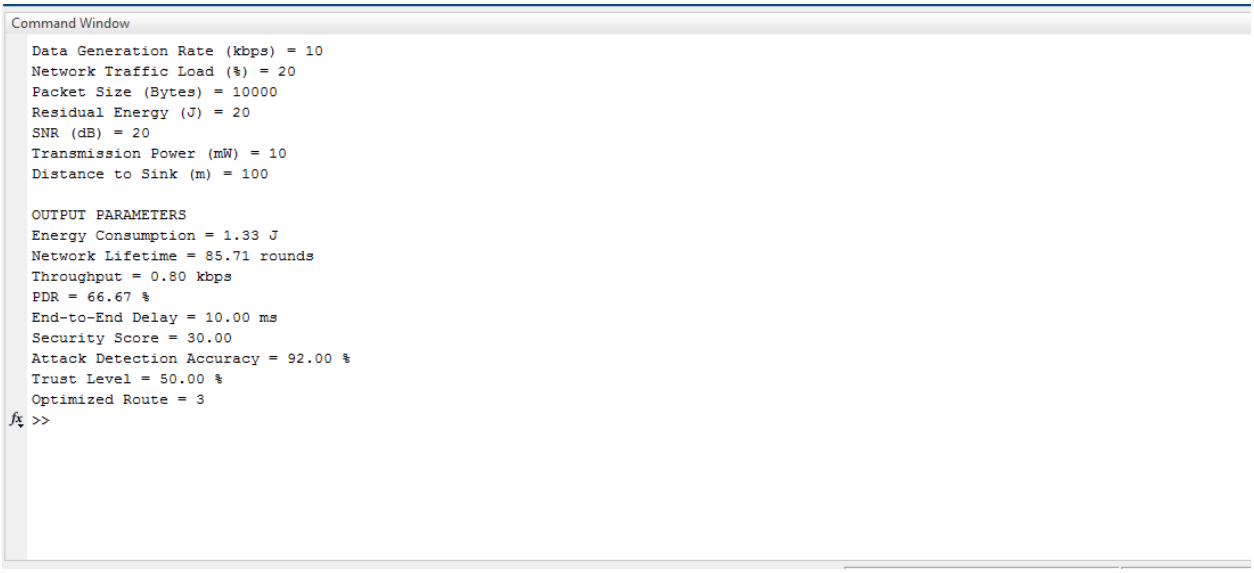

Fig.5.1 Parameters evaluation Case-1

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

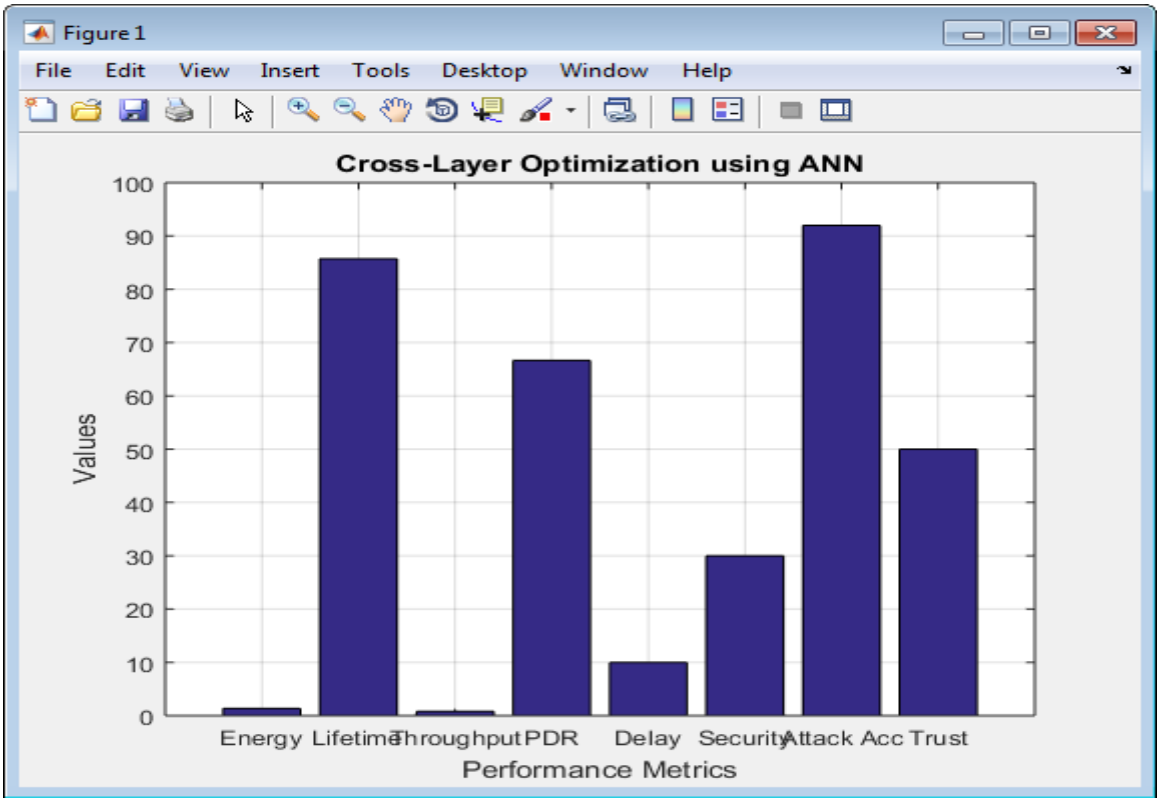

Fig.5.2 Output Parameters evaluation Case-1

Fig.5.3 Output Parameters evaluation Case-1

CONCLUSION AND FUTURE SCOPE

Conclusion

The proposed research on Cross-Layer Optimization for Energy and Security in IoT-MANET Wireless Sensor Networks using Artificial Neural Networks (ANN) presents an intelligent and adaptive framework designed to overcome the limitations of conventional layered network architectures. Traditional routing and communication approaches generally operate in isolation within individual protocol layers, which leads to inefficient energy utilization, poor security management, increased latency, and reduced network lifetime. In contrast, the proposed cross-layer framework integrates information from the Physical Layer, MAC Layer, Network Layer, and Security Module to enable coordinated decision-making. By incorporating ANN as the core optimization engine, the system is capable of learning complex nonlinear relationships among multiple network parameters such as residual energy, signal strength, congestion level, link quality, route stability, and trust values.

The proposed framework significantly improves network performance by enabling intelligent route selection based on multiple objectives rather than a single metric. The ANN-based decision-making process ensures that communication routes are not only energy-efficient but also secure and stable. The inclusion of trust-based security mechanisms enhances the detection and mitigation of various network attacks such as Black Hole, Gray Hole, Wormhole, and Selective Forwarding attacks. Furthermore, energy-aware optimization strategies help in balancing energy consumption across nodes, thereby extending the overall network lifetime. The framework also reduces routing overhead, improves packet delivery ratio, minimizes end-to-end delay, and enhances Quality of Service (QoS), making it highly suitable for dynamic and resource-constrained environments like IoT, MANETs, and WSNs.

Future Scope

Although the proposed framework demonstrates significant improvements in energy efficiency, security, and routing performance, there are several directions for future enhancement and research expansion. One important future scope is the integration of advanced deep learning models such as Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks to further improve prediction accuracy and enable time-series analysis of network behavior. These models can help in predicting node mobility, energy depletion trends, and future network congestion more effectively than traditional ANN.

REFERENCES

1. Shinde, N. K., & Patil, V. H. (2024). Secured and energy efficient cluster based routing in WSN via hybrid optimization model, TICOA. Sustainable Computing: Informatics and Systems, 44, 101052
2. Lakshmi, G. V., & Vaishnavi, P. (2024). A trusted security approach to detect and isolate routing attacks in mobile ad hoc networks. Journal of Engineering Research, 12(3), 379-386.
3. Mishra, R. (2024). Raspberry Pi Performance analysis across its Operating System in LED Control Operation. International Journal of Advanced Research and Multidisciplinary Trends (IJARMT), 1(2), 01-11.

4. Mishra, R. (2025). IOT and DSP (combination of hardcore Virtex-5 FPGA and soft core DSP processor) OFDM System PAPR Reduction Using Artificial Intelligence Algorithm. International Journal of Advanced Research and Multidisciplinary Trends (IJARMT), 2(1), 135-149.
5. Mishra, R., & Sharma, A. (2026). Enhanced Trajectory Tracking of a 6-DOF Robotic Manipulator Using GA–PID and ANN–PID Controllers. International Journal of Research & Technology, 14(2), 53-70.
6. Devi, G. R., Das, M. S., & Murthy, M. R. (2023). Secure cross-layer routing protocol with authentication key management scheme for manets. Measurement: Sensors, 29, 100869.
7. Gopalan, S. H., Vignesh, V., Rajkumar, D. U. S., Velmurugan, A. K., Deepa, D., & Dhanapal, R. (2024). Fuzzified swarm intelligence framework using FPSOR algorithm for high-speed MANET-Internet of Things (IoT). Measurement: Sensors, 31, 101000.
8. Vincent, S. S. M., & Duraipandian, N. (2024). Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm. Expert Systems with Applications, 249,123765.
9. Changazi, S. A., Bakhshi, A. D., Yousaf, M., Mohsin, S. M., Akber, S. M. A., Abazeed, M., & Ali, M. (2024). Optimization of network topology robustness in IoTs: A systematic review. Computer networks, 250, 110568.
10. Chandra, A., & Chakravarthy, A. S. N. (2025). EAURP: An Energy-Efficient and Trust-Aware Unobservable Routing Protocol for Secure Mobile Ad Hoc Networks. Sustainable Computing: Informatics and Systems, 101285.
11. 7.Mostafa, R. R., Vijayan, D., & Khedr, A. M. (2025). EGBCR-FANET: Enhanced genghis Khan shark optimizer based Bayesian-driven clustered routing model for FANETs. Vehicular Communications, 100935.
12. 8.Ananth, C. A., & Krishnaraj, N. (2023). Detection of intrusions in clustered vehicle networks using invasive weed optimization using a deep wavelet neural networks. Measurement: Sensors, 28, 100807.
13. 9.Savithri, G., & Sai, N. R. (2024). Dynamic Deep Learning for Enhanced Reliability in Wireless Sensor Networks: The DTLR-Net Approach. Computers, Materials & Continua, 81(2).