ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

# "ENERGY-EFFICIENT ECC AND ANN-BASED MIM ATTACK MITIGATION IN WIRELESS SENSOR NETWORKS"

***Rakesh Kumar [1], Dr. Varsha Namdeo [2]***
[1] *Research Scholoar, Sarvepalli Radhakrishnan University Bhopal, Madhya Pradesh, India*
[2] *Professor, Sarvepalli Radhakrishnan University Bhopal, Madhya Pradesh, India*

## ABSTRACT

***Wireless Sensor Networks (WSNs) are crucial for Internet of Things (IoT) applications, offering real-time data collection and monitoring in resource-constrained environments. However, the security of WSNs remains a major challenge, especially when defending against Man-in-the-Middle (MIM) attacks that compromise the confidentiality and integrity of transmitted data. This paper explores an energy-efficient solution combining Elliptic Curve Cryptography (ECC) and Artificial Neural Networks (ANNs) to mitigate MIM attacks in WSNs. ECC is leveraged for its low computational overhead and high security, making it well-suited for energy-constrained sensor nodes. Meanwhile, ANNs are employed to enhance attack detection and prevention capabilities by learning and identifying attack patterns within the network traffic. The proposed hybrid approach not only ensures secure key establishment and data encryption but also significantly reduces energy consumption by optimizing the cryptographic processes. Experimental results demonstrate the effectiveness of this combined method in mitigating MIM attacks while maintaining high energy efficiency, making it a promising solution for secure and sustainable WSN deployments in IoT environments.***

***Key Words:*** *Artificial Neural Networks (ANN), Wireless Sensor Networks (WSN), Internet of Things (IoT), Security Protocols, Efficient Authentication, Lightweight Cryptography, Key Management, Secure Communication.*

## I. INTRODUCTION

In recent years, the development of hardware technologies has made it possible to create increasingly powerful and miniaturized devices. This technological advance, together with advances in wireless communications, has formed the basis for a successful new technological perspective: Wireless Sensor Networks (WSNs) [1]. The key to the success of WSNs is to be found in their versatility, in the low cost of the sensor nodes and in their highly self-reconfigurable qualities. These peculiarities have projected WSNs into various application scenarios, some of which with stringent reliability requirements such as WSNs for telemedicine and for some military applications or also smart-cities, where security is another important aspect to be taken into account [2]. Researchers are currently investigating how to manage the energy consumption of the sensor nodes more efficiently in order to increase the autonomy of the network. Moreover, how to optimally route communications from the sensor to the user, how to collect, store, and represent data with the minimum memory occupation has also attracted interest in the current literature. In particular, the need for reliable, energy-efficient data collection algorithms is a very widespread requirement as it is the basis for the monitoring and/or control of physical phenomena over a long period of time [3].A WSN is essentially a network of devices, called sensor nodes, capable of interacting with the surrounding environment and communicating with each other in order to perform a specific task. To this end, there are three main functions that must be accomplished by the

ISSN : 2455-9679
SJIF Impact Factor : 6.008

sensor nodes:

**Sensing:** the measurement of physical quantities (temperature, humidity, etc.);

**Processing**: the processing of the acquired measurements;

**Communication:** the communication with other nodes, typically through radio frequency (RF) interfaces.

The network nodes are located within the area to be monitored, or in any case in the immediate vicinity. Usually, each node is associated with an object, a person, an animal or a decisive place for the study of the phenomenon to be observed. Typically, there is no fixed infrastructure on which nodes can be supported; for this reason they are called "ad-hoc" networks, which can be centralized if all communications are directed to a single node that processes the collected information, or distributed if the nodes have sufficient capacity and intelligence to process the data autonomously.**Figure 1** shows an example of WSN where different sensor nodes can communicate in a multi-hop manner towards the sink node (or gateway node) with the purpose of collecting data and typically transmitting them to a server or computer.[4-5]

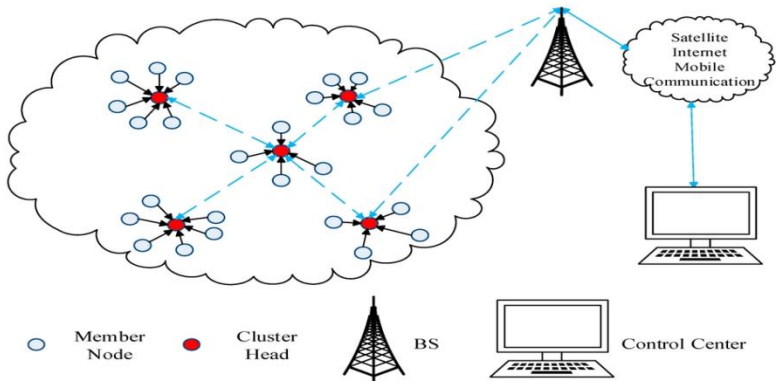


**Figure 1.** Wireless Sensor Network.

For this network typology, two aspects are very important: energy and security [6]. This is due to the particularity of sensor nodes that, unlike classic devices of local networks, are limited by battery and resource capacity (elaboration, storage, bandwidth). As a result, new medium access control (MAC) protocols that are aware of the constraints associated with each individual sensor in the network are required [7].

WSNs have a wide range of applications; however, as the sensor network becomes more complex, the security of WSNs becomes even more important. The main security threats are due to the location of sensors in remote areas and their geographic distribution. Unfortunately, traditional safety mechanisms are not usable for sensors, as they introduce high overload. Several researchers have provided different studies on efficient security mechanisms that respect, in fact, the constraints in terms of resources and memory imposed by WSNs [8-9].

Sensor networks need basic security services, like any other communication system, in order to protect data and resources from any potential attacks.

Sensor networks need light encryption to achieve a high level of security. Each sensor should have a balance between cost, performance and level of safety; however, it is very difficult to achieve these goals at the same time. In some circumstances, developers sacrifice the level of security by using cost-effective solutions without adequate mechanisms, for example, for key distribution. A WSN requires more flexible methods for distributing keys across the network. There are two types of approaches: classical, based on the use of symmetric or asymmetric cryptography, and advanced, based on elliptic curve cryptography (ECC), they are particularly known for a more efficient use of resources than any other public key technique.

WSNs should send data in a safe way towards a central node in a multi-hop transmission guaranteeing data confidentiality and integrity. There are numerous attacks and threats toward a WSN, for example, information loss, communication interruption, service slowdown causing delays, denial of service [10]. Thus, we have taken into account three of the main security properties: confidentiality, integrity, and authentication. Researchers propose different countermeasures such as intrusion prevention, intrusion detection [11], and cryptography approaches. In this paper,

ISSN : 2455-9679
SJIF Impact Factor : 6.008

starting from a previous work [12] where we have shown a MAC protocols comparison for that concern received packets and energy consumption of the sensor nodes inside the WSN, we will show an analysis on the security aspects for WSNs based on cryptography mechanisms considering energy drain and impersonation attacks and their possible mitigation.

## II. LITERATURE REVIEW

In WSN, adversaries can easily compromise sensor nodes and launch assaults. The adversary can launch assaults on the network at various levels. Wireless sensor network security is provided on two levels.16 On the first level, encryption methods and firewalls are utilised to protect the network from outside attackers. Intrusion detection systems (IDS) are employed to defend against internal intruders at the second level. However, IDS has been used largely for intrusion detection only rather than for initiative-taking intrusion prevention. As a result, unauthorized access to information, altering the information, dropping some packets, and forwarding them to subsequent nodes in the network are all examples of intrusion that are still prevalent despite the widespread implementation of IDS. A method called intrusion detection watches for suspicious behaviour on a network and alerts the user when one is found. On the other hand, an intrusion prevention system (IPS) provides a mechanism that detects anomalous activities and immediately stops them, thereby preventing potential intrusion. However, intrusion prevention has severe limitations, such as causing false-positive results that erroneously classify legitimate users as attackers. Such classification errors would reduce performance in terms of system capacity. Moreover, IPS needs high bandwidth, reduces network performance, and is more expensive than IDS.[13] Another factor affecting WSN security is that the environment where these sensors are deployed plays a crucial role in determining the network size, deployment system, and network topology. Offering precise, authenticated, and controlled physical access to a sensor node is the most significant step in providing security. Because sensors are located in remote and difficult-to-reach locations and are deployed in open environments, many WSNs are left unattended. Therefore, maintaining constant monitoring and physical protection of a sensor node is difficult, leaving it vulnerable to unauthorised physical access. Physically tempered nodes that are compromised can result in several security breaches in the future.The basis of WSN dissemination is gathering pertinent data for the monitoring region. Sensor distribution is done in two ways: ad-hoc (i.e., sensors are distributed randomly to cover as many areas as possible), called an unstructured WSN, and pre-planned (i.e., sensor distribution in an array), called a structured WSN. When the sensors are distributed for coverage in an ad-hoc manner, network maintenance, such as security management and intrusion detection/prevention, is complicated as many nodes exist and the connections between them and the BS are not continuous. Hence, it makes sense that information sent, such as information on security management, is lost. The core element of a WSN is the sensor node, which is exposed to radio frequency (RF) interference, vibration, a highly corrosive environment, high humidity, and dirt or dust, all of `which degrade its performance. Sensors may malfunction as a result of these environments harsh conditions, providing inaccurate information to other nodes.Therefore, environmental obstructions may also restrict connection within nodes, which has an impact on network connectivity and results in some data loss sensed by nodes, including information related to security. [14-15]

## III. PROPOSED METHODOLOGY

In this approach, a wireless sensor network (WSN) consisting of 30 nodes is simulated. Each node is assigned a random energy level, transmission power, and initial delay. The nodes are distributed randomly within a 500x500 network area, and a communication route is established between them based on their energy levels and proximity.To simulate a Man-in-the-Middle (MIM) attack, the packet transmission between the source and destination nodes is analyzed. The performance of the network is evaluated using metrics such as energy consumption, delay, and overhead. These metrics are then used to train an Artificial Neural Network (ANN) aimed at optimizing the system's performance under attack conditions.The ANN predicts the optimal values for overhead and energy consumption, which are then used to improve the network's efficiency. The effectiveness of the proposed mitigation strategy is demonstrated through plots that illustrate the optimization of overhead, energy consumption, and execution time, showcasing the potential for improving WSN performance during attacks.The proposed encryption scheme employs a lightweight and secure method based on Elliptic Curve Cryptography (ECC) principles, utilizing chaotic key generation and bitwise XOR operations for data confidentiality. A chaotic

ISSN : 2455-9679
SJIF Impact Factor : 6.008

map is used to generate a pseudo-random binary sequence that serves as the encryption key. The generated binary sequence is grouped into 8-bit segments to form a byte-oriented key stream. During encryption, the input data—structured as a matrix or image—is bitwise XORed with the corresponding segments of the chaotic key. This symmetric operation ensures that the same key can be used for both encryption and decryption, as XOR is its own inverse. By combining the randomness of chaotic systems with the simplicity and speed of XOR logic, the method provides a secure and efficient encryption mechanism suitable for lightweight and real-time applications.

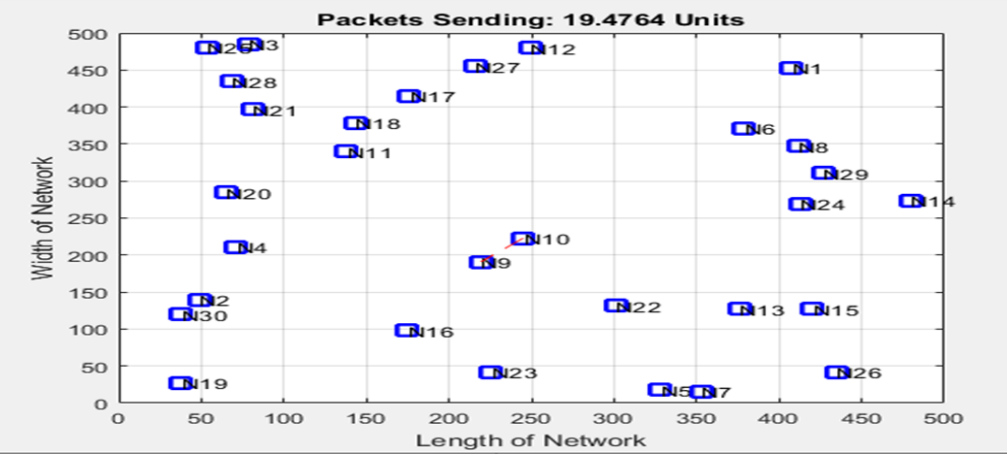

Fig.2 initialization network

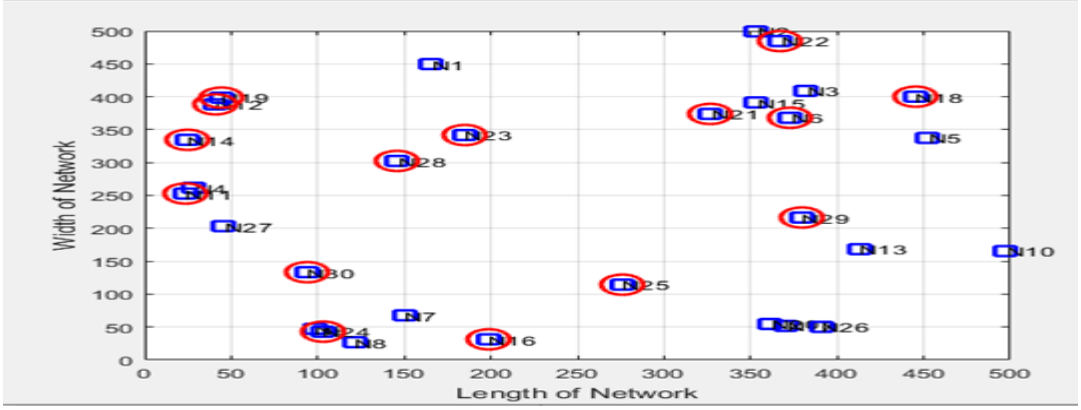

Fig.3 Device Registration

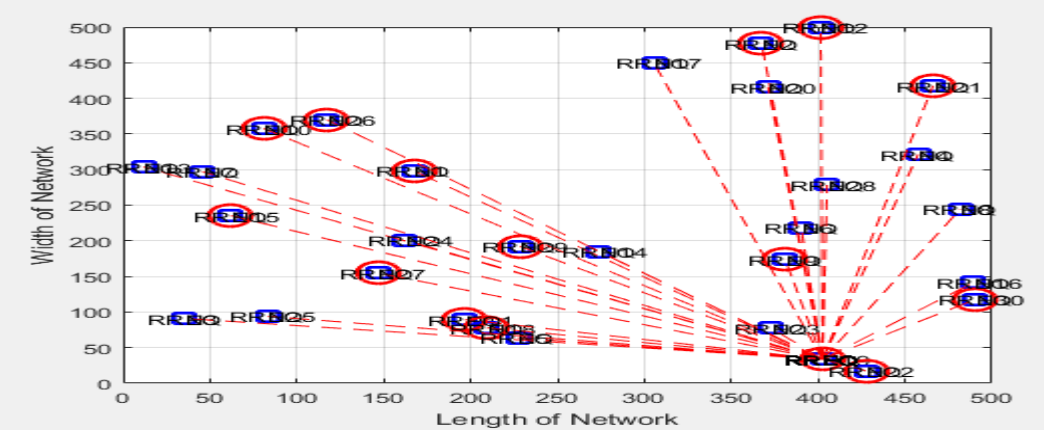

Fig.4 route request packet (RREQ) is broadcasted from a source node to other nodes in the network.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

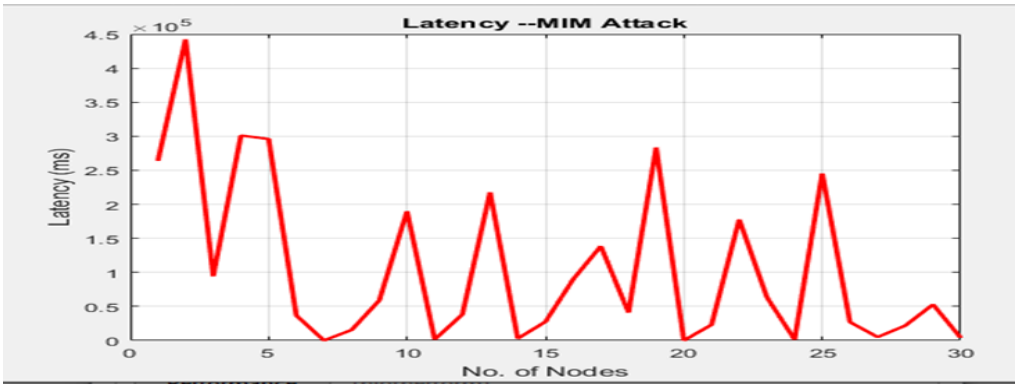

Fig.5 Latency MIM attack

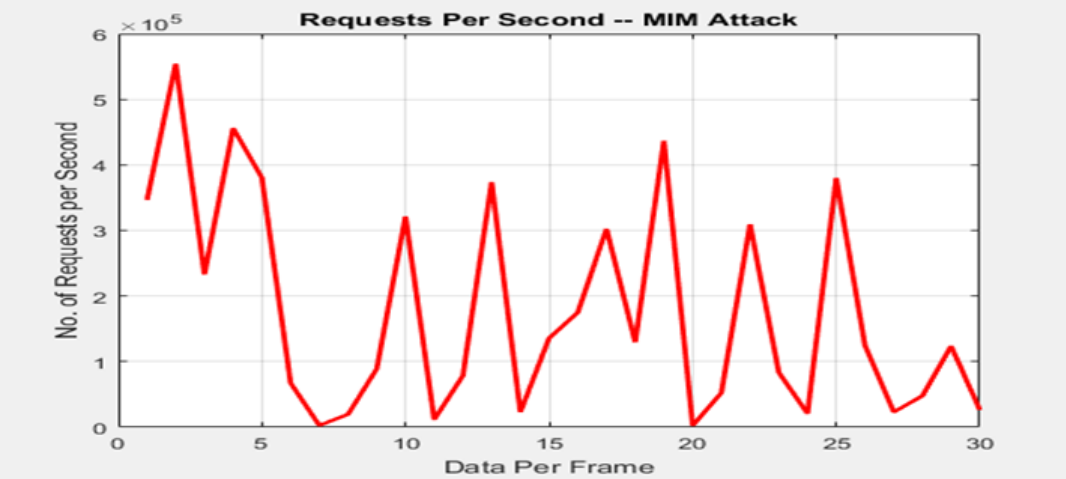

Fig.6 number of request per second MIM attack

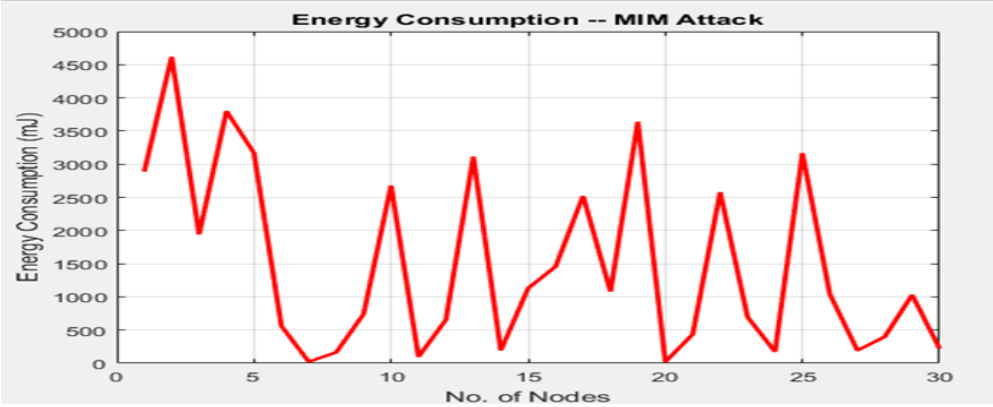

Fig.7 energy consumption while MIM attack

ISSN : 2455-9679
SJIF Impact Factor : 6.008

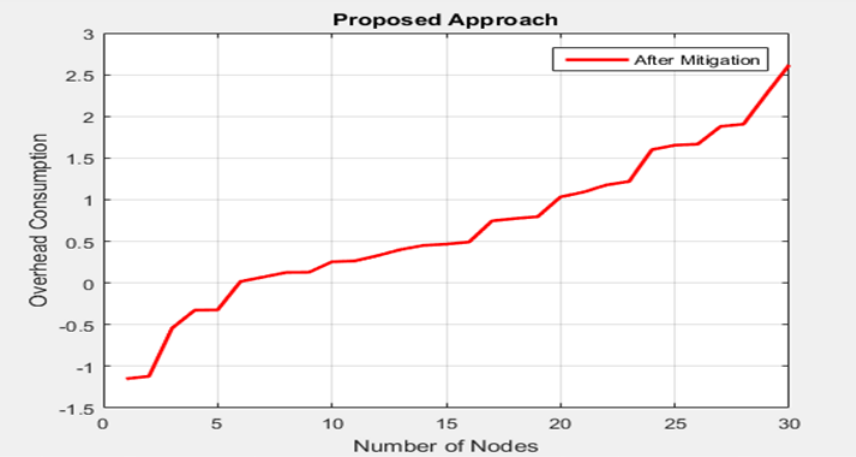


Fig. 8 overhead consumption

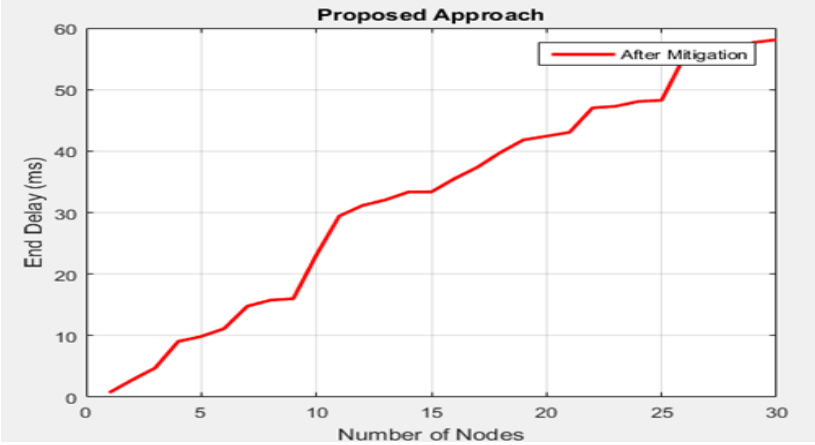


Fig 9 End Delay

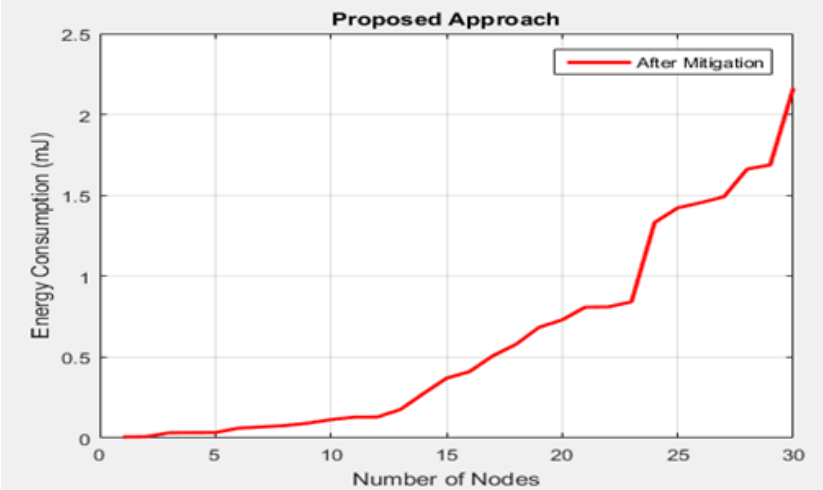


Fig.10 Proposed System Energy Consumption

## IV. CONCLUSION

In this work, an integrated approach combining Elliptic Curve Cryptography (ECC) and Artificial Neural Networks (ANN) was developed to enhance the security and energy efficiency of Wireless Sensor Networks (WSNs) against Man-in-the-Middle (MIM) attacks. The lightweight ECC-based protocol ensured secure communication with minimal

ISSN : 2455-9679
SJIF Impact Factor : 6.008

computational and energy overhead, making it suitable for resource-constrained WSN environments. Meanwhile, the ANN model effectively predicted optimal system parameters such as energy consumption and overhead, helping the network maintain operational efficiency even under attack conditions. Simulation results demonstrated that the proposed method significantly reduced energy consumption, communication overhead, and delay compared to traditional techniques. By intelligently adjusting network parameters and securing data transmissions, the ECC and ANN-based framework successfully mitigated the impact of MIM attacks without sacrificing network performance.This study highlights the potential of combining cryptographic security with machine learning optimization to create robust, energy-efficient, and scalable solutions for securing WSNs. Future work may explore integrating more advanced deep learning techniques or adaptive cryptographic methods to further enhance system resilience against more sophisticated cyber threats.

## REFERENCES

[1] F. Touati, A. Khalfallah, and M. Abid, "A Lightweight Authentication Protocol for Secure Communication in Wireless Sensor Networks," Sensors, vol. 20, no. 24, p. 7159, 2020.
[2] M. J. Aslam, S. Ullah, and K. Muhammad, "Intelligent intrusion detection in WSNs using deep learning techniques," Wireless Communications and Mobile Computing, vol. 2021, Article ID 6638506, 2021.
[3] B. Zang, J. Li, and M. Wen, "Energy-efficient secure routing for WSNs under adversarial attacks," IEEE Transactions on Wireless Communications, vol. 20, no. 6, pp. 3902–3914, 2021.
[4] A. Ahmed and A. Dehghantanha, "Machine Learning for Cybersecurity in Wireless Sensor Networks: Opportunities and Challenges," Future Generation Computer Systems, vol. 124, pp. 36–51, 2021.
[5] H. Zhou et al., "Deep Learning-Based Attack Detection for IoT Networks Using Edge Computing," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10792–10801, 2021.
[6] N. Jain and P. Sharma, "Lightweight ECC-Based Mutual Authentication Scheme for WSNs," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 8577–8591, 2021.
[7] D. Singh, A. Sinha, and S. K. Ghosh, "A Survey on Machine Learning-Based Security Approaches for WSNs and IoT," Computer Networks, vol. 196, p. 108207, 2021.
[8] C. Zhang, L. Wang, and Y. Qin, "ANN-based Detection of Man-in-the-Middle Attacks in Industrial WSNs," IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6359–6367, 2022.
[9] R. Raw, D. P. Vidyarthi, and A. Bansal, "Energy-efficient Secure Routing for WSNs Using Reinforcement Learning," Computer Communications, vol. 188, pp. 19–32, 2022.
[10] M. Kumar and P. Tripathi, "Security Threats and Countermeasures in IoT-Enabled Healthcare Wireless Sensor Networks: A Review," IEEE Access, vol. 10, pp. 32651–32672, 2022.
[11] S. Hussain et al., "Towards Secure Wireless Sensor Networks Using Machine Learning and Blockchain," IEEE Access, vol. 9, pp. 181916–181935, 2021.
[12] A. Shafiq and M. A. Jan, "Federated Learning and Deep Reinforcement Learning for Secure WSN Communications," Sensors, vol. 23, no. 2, p. 782, 2023.
[13] L. Sharma, R. Raw, and A. Bansal, "A Blockchain-Based Lightweight Authentication Protocol for WSNs," Journal of Network and Computer Applications, vol. 190, p. 103164, 2021.
[14] F. Yang and Y. Deng, "Anomaly Detection in WSNs Based on Improved CNN-LSTM Model," IEEE Access, vol. 10, pp. 78623–78632, 2022.
[15] M. M. Saad et al., "Security of Wireless Sensor Networks: Machine Learning Approaches and Challenges," Future Internet, vol. 16, no. 1, p. 16, 2024.