RESEARCH ARTICLE OPEN ACCESS

Enhancing Wireless Sensor Network Security: Exploring Machine Learning Solutions and Challenges

Nand Kishor Dhakar
Department of Computer Science & Engineering
Global Institute of Technology, Jaipur, Rajasthan

Abstract:
Energy efficiency and security are two critical yet conflicting challenges in wireless sensor networks (WSNs). As security mechanisms become more complex, they consume more energy, leading to faster battery depletion. Due to the ever-changing network architecture and communication limitations among sensors WSNs sometimes lack the resources to rely only on conventional security measures such as encryption and key management due to their power constraints. Intelligent monitoring and decision-making made possible by machine learning (ML) approaches is an intriguing new avenue for enhancing WSN security. The requirement for large amounts of training data and processing resources are two additional difficulties introduced by ML approaches. If you're looking for a reference on the topic of WSN security issues and how ML algorithms can help, this is it. By enhancing the network's capacity to identify threats, attacks, and harmful behaviors, it investigates how ML might optimize security costs. Additionally, the study discusses challenges in integrating ML with WSNs, along with potential solutions for enhancing sensor intelligence and adaptability. Finally, open research issues related to aligning ML models with the constraints of WSN infrastructure are examined.

Keywords: topics covered include data transfer, wireless sensor networks, clustering routing, and cluster formation

.

I INTRODUCTION

Some shortcomings in man-made progress are inevitable [1]. The ingenuity of humans is the origin of all communication advancements, including WSN, the IoT, embedded systems, ad hoc networking, and associated technologies. Smart housing, transportation, and remote communication are just a few examples of how technology is advancing to better people's lives. When it comes to sensing and managing applications from a distance, WSNs are currently all the rage. The term "wide area network" (WSN) refers to a network that uses a number of sensor nodes spread out across a wide area to keep track of different physical variables. Several locations record a wide range of variables, including temperature, wind speed, pressure, humidity, and many more. Most importantly, WSN sensor nodes run on batteries and can potentially function in inaccessible or otherwise difficult-to-reach areas [2].

Wide area networks (WSNs) rely on a constant flow of data captured by a large number of sensor nodes and sent to a predetermined sink node. The information can be sent directly between nodes or it can go via middlemen called cluster chiefs. Nodes in the cluster act as relays, receiving data transmissions from the sensor nodes and relaying them to the base station (BS) [3,4]. Each layer in a WSN is responsible for a certain function that is essential to the network's operation and the transfer of data efficiently. For WSNs to function reliably and securely, each of these layers physical, data-link, network, transport, and application is essential [5].

Threats to the network's security arise at the physical layer, the foundational layer of WSN design. Here, fundamental jamming, eavesdropping, compromised node, and replicating node assaults take center stage. Nodes and communication routes are the primary targets of these threats, which could compromise the security and integrity of data. Assaults including intelligent jamming, collision assaults, unfairness attacks, and denial of service (DoS) are major worries at the data-link layer. In addition to managing communication between neighboring nodes, this layer is responsible for addressing issues with data packet collision and channel access. Preserving the reliability of the network depends on keeping the data-link-layer protocols intact. Emergence of threats such as Sybil at the network layer sinkhole, spoofing, and black-hole, gray-hole, and wormhole, further complicating security These assaults pose serious risks to the operation of the network because they take use of loopholes in the routing protocols in order to mimic valid nodes, hijack routing paths, or interrupt data transfer. Service dependability and quality are both affected by assaults on the transport layer, such as flooding and resynchronization. This layer ensures data integrity

and controls end-to-end communication; it is an integral aspect of WSN security.

The data collected by WSNs is processed and used by the application layer, the last layer It is critical to guarantee the confidentiality of this data. Data at the application layer is vulnerable to manipulation and interceptions, thus strong security measures are required to keep critical information safe.

Many industries, such as healthcare, environmental monitoring, and industrial automation and surveillance, have come to rely on WSNs. In these networks, a number of tiny, autonomous sensor nodes work together to wirelessly communicate data, allowing for efficient data collection and distribution. The network layer is particularly vulnerable to the particular vulnerabilities, topological changes, and resource constraints that characterize wireless sensor networks (WSNs). Data routing in a WSN is the job of the network layer, which is also in charge of creating and maintaining connections between sensor nodes.

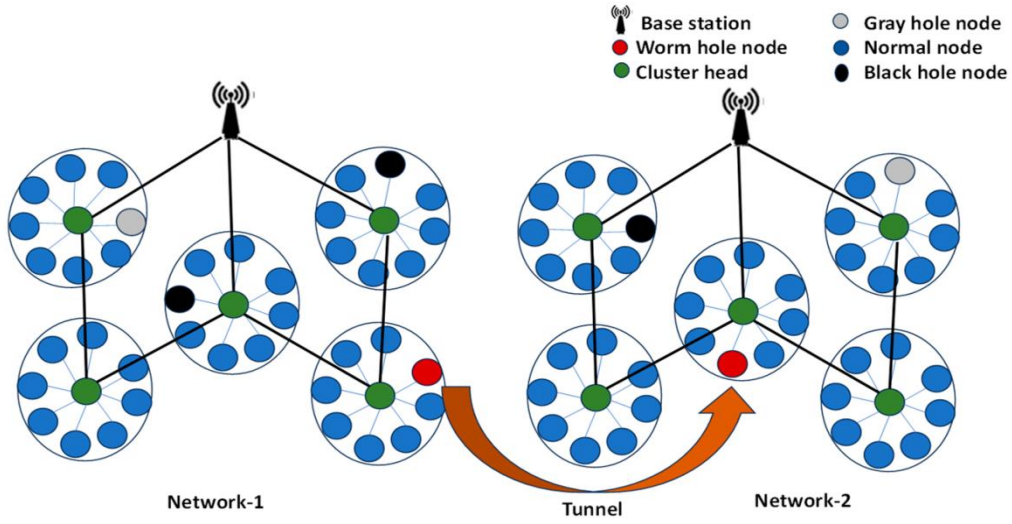

Figure 1. Attacks on wireless sensor networks' routing protocols.

Despite its critical importance, the network layer faces a number of security risks that put data accessibility, integrity, and confidentiality at risk. The ideal path, which involves the fewest hops to the destination, is always preferred by nodes in hop-to-hop communication in WSNsTaking the shortest and most efficient route has many advantages, such as less energy use, packet loss, and transmission overhead. In multi-hop communication, an attacker node can pose as a node that is geographically closest to the target and ask for the route to the destination. Optimal path selection causes the asking node to choose the way that the attacking node has suggested, which results in a routing attack in the WSN. In order to cause congestion, data loss, or even denial of service in networks, attacks on the routing mechanism might modify it such that it hinders accurate data transfer. Several types of attacks target the network layer, such as flooding, spoofing, sybil, black-hole, gray-hole, sink-hole, and wormhole assaults [6]. In Figure 1 we can see a few examples of these attacks. When a network receives an overwhelming amount of route requests, it is known as a flooding assault. Depleting network resources, lowering availability, and overwhelming nodes to the point that they can't complete their tasks these assaults can do serious damage [7].

By manipulating routing tables, spoofing attacks aim to build a recursive path between source and destination nodes in WSNs. This kind of attack can change routing information. Node partitioning, wrong path redirection, reduced network lifetime, and inaccurate routing information dissemination are some of the serious repercussions that might arise from this type of attack [8].

An attacker can launch a sybil attack by sending numerous messages to different nodes with different identifiers, creating the illusion that the messages are coming from different places. Because of this assault, nodes in the network are compelled to seek out different paths in order to avoid collisions. Because of the attacker's manipulation of the circumstance, nodes are confused and unable to choose the correct path for data transfer. By modifying the data flow's routing

path, this sort of attack can compromise data integrity [9].

The network tricks users into thinking it has the fastest route to their destination by routing all traffic through itself. an attacker can create a black-hole attack in a network. At the same time, the malicious node either absorbs or drops the packets, stopping them from reaching their destination. Making a "black hole" in the network is the aim in order to stop data from getting where it needs to go and communication from being stopped. In more complex gray-hole attacks, sometimes called selective forwarding attacks, infected nodes falsely advertise better paths to collect data packets, which they then alter or discard before they reach their final destination. The routing procedure is compromised in this assault, which could lead to critical information falling into the wrong hands.

A wormhole assault involves a group of malicious nodes that join forces via a tunnel formed by high-speed wireless connection, ethernet, or fiber-optic cables. By rapidly transmitting data packets across the network, the tunnel gives the impression that nodes are physically closer together than they actually are. In order to disrupt communication, the attackers want to create a loophole in the network that nodes would take the wrong way. Wormhole nodes are able to evade detection by other nodes in the network due to their transparent operation. Consequently, they function flawlessly and don't necessitate network IDs or cryptographic keys [10].

Weak network layer security in WSNs has prompted several proposals for preventative measures [11,12]. These plans incorporate a wide range of methods, such as secure routing protocols, intrusion detection systems, and authentication. To stop unauthorized nodes from joining the network, authentication procedures make sure that nodes only communicate with other authenticated and trustworthy nodes. In order to quickly identify assaults and implement suitable countermeasures, intrusion-detection systems keep an eye on network traffic, looking for unusual patterns of behavior.

Ensuring safe and efficient data transmission paths is the primary goal of secure routing protocols, which play a crucial role in prevention. Security measures are incorporated into protocols such as ad hoc on-demand distance vector (AODV) and low-energy adaptive clustering hierarchy (LEACH) to protect against a multiplicity of assaults. The security of the network layer in WSNs is enhanced by this protection, which guarantees the confidentiality, integrity, and validity of data throughout the routing process. When it comes to WSNs' network layer intrusion detection, ANN-based approaches offer the optimal answer, in contrast to these conventional methods.

For WSNs, ANN-based solutions provide a better way to identify intrusions at the network layer than conventional methods. Options such as the convolution neural network (CNN) model and the feed-forward ANN approach stand out among these solutions. To identify routing attacks in WSNs, we will first assess different ANN-based models and then choose the best one.

II WSN SECURITY

The Triangle of Confidentiality, Integration, and Authentication (CIA) has been the focus of extensive study on WSN management protocols' security. Any network can't be considered secure until it meets all three criteria, which are represented by this triangle. Data privacy is the process of ensuring that sensitive information transmitted between WSN nodes remains private. Typically, crucial packet parts are encrypted before transmission from the sending node and subsequently decoded at the receiving node [13]. If the network is to maintain its integrity, it must be ready to prevent tampering with sent communications. The attackers can alter their polarity by creating interference beams. Evil routing nodes can also change critical packet data before sending it on. Finally, availability must be met in order for the security triangle to be completed. Accessibility refers to how readily the WSN Services are available at all times. Any given scenario can lead to attacks that impair or completely destroy a network. Wireless interference, protocol manipulation, and other forms of depletion of WSN nodes can all lead to a Denial of Service (DoS) attack, which can render a network unworkable [14]. As far as network availability is concerned, this is the biggest risk. We will address this type of assault at a later time.

To further ensure the safety of data transfers, the widely used 6LoWPAN transport layer protocol UDP can be upgraded using Datagram Transport Layer Security (DTLS) [15]. Run over TCP, TLS employs the AES-128 technique for link-layer authentication and encryption .But if you want to keep using advanced encryption procedures with TLS/DTLS, more encryption hardware [16]. Transport Layer Security (TLS) and Internet Protocol Security (IPSec), both of which are widely utilized at the network layer, are notoriously difficult to incorporate into such networks' applications due to the high resource consumption and high overhead costs associated with these protocols [17]. Additionally, these solutions do not

provide the full Security Triangle (CIA) because WSN devices use public communication channels for wireless communication. Protocols need to work together for these networks to be secure and work well in their environments. There are various types of hostile attacks in the realm of WSN security [18], and the impact on sensor nodes varies depending on the level. The distribution of these groups is shown in Figure 4 for each level of the WSN model. Figure 2 shows that while the DoS attack uses all layers, there are distinct malicious attacks in each tier. Denial of Service (DoS), Jamming, Exhaustion, and Collision all lower network availability and connectivity. In contrast, selective forwarding, Sybil, hole, spoofing, session hijacking, eavesdropping, and man-in-the-middle all pose risks to privacy and security [19]. Furthermore, certain assaults might be in either an active or passive state; others specifically target connectivity and availability.

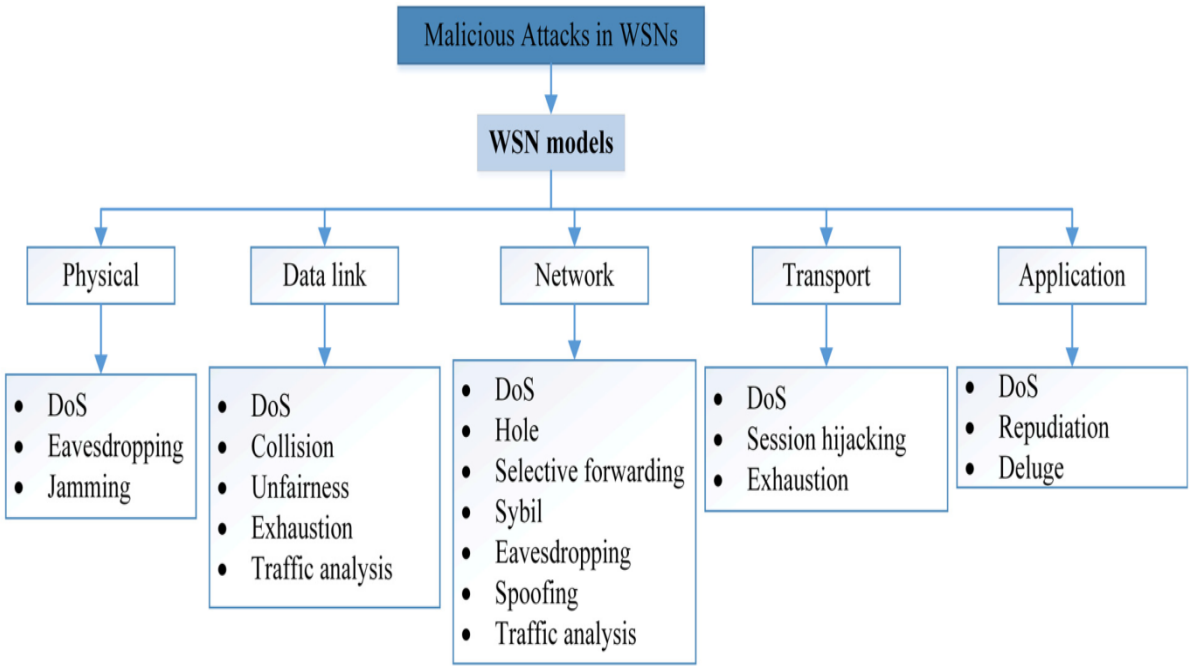

Figure 2. Malicious attacks classifications.

Attacks on WSNs

Figure 2 shows that there are many different kinds of malicious WSN assaults, and that these attacks lead to problems with power and CPU usage in addition to security. Consequently, unlike traditional networks, these ones should prioritize the discovery of practical and workable solutions. They go over the effects of each assault type on WSNs in depth.

Eavesdropping

Due to the nature of WSNs' security constraints—including unpredictable nodes, inconsistent connectivity, and potentially dangerous environments—hackers can easily intercept data transmitted between nodes, which in turn increases the impact of radio fading and frequency transmission/scattering.

Jamming

When it comes to private wireless networks, this is one of the most deadly forms of attack. Neglecting security measures to prevent it, despite the dangers it poses, might lead to major issues following the deployment of wireless networks. One major effect of jamming is the interference it causes with radio frequencies, which in turn hinders user service or availability.

Collision

Given the dispersed nature of the sensors, node replacement corruption by hostile actors could be the source of this assault. Malicious nodes can disrupt other broadcasts by sending a short noise packet that does not follow the Intermediate Access Control Protocol. Although this attack does not consume much energy from the attacker, it can lead to major network outages .Moreover, due to the characteristics of wireless communication, it is difficult to determine the origin node

Unfairness

By exploiting the specifications for the contract's connection time, this kind of attack prevents authorized users from gaining access to the network and thereby avoids the submission deadline. Attacks like these can leverage techniques like random exploitation of cooperative media access control layer priority algorithms or perhaps just plain old collisions.

Exhaustion

This assault keeps launching collisions with the WSN nodes until their energy is completely depleted. That is to say, resource depletion attacks cause nodes to lose power because they cause packet transfers to become more complicated and longer due to routing loops and path lengthening.

Traffic monitoring

The purpose of traffic analysis in WSNs is to discover how the nodes are communicating with one another. In order to conduct the analysis, data was collected via listening in on conversation between nodes. Any node that stores sensitive information or knows the location of the access point or sink node is fair game for this attack. When an assault succeeds, it reveals a lot of information. This could potentially cause the system to fail.

Hole attack

Black hole or sink attacks are vulnerabilities in the network layer that happen when messages are being routed. This devastating bombardment is aimed for cluster heads. By designating an adversarial node as the cluster head, this attack can cause all member nodes to lose their transaction processing capabilities. A sinkhole may form as a consequence.

Selective forwarding

When compromised nodes wilfully trash packets, a selective redirection threat becomes even more difficult to detect. With the help of selective redirection, hackers can set up route discovery, which allows them to add or remove network traffic. Further, they can change the range of primary routers, send out misleading signals, and ignore critical messages.

Sybil

The Sybil attack generates many node IDs from a single live node in order to make it look like a sensor node is present. Problems with allocating resources and other factors also contribute to system failure. It has far-reaching consequences for load-balancing technologies such server protocols, structure management, and shared computing.

Spoofing

Root path expansions and compression, network segmentation, heightened end-to-end latency, routing loops, and fake error messages are all possible outcomes of this assault, which targets routing data sent between nodes.

Session hijacking

An additional form of man-in-the-middle attack is a cookie side takeover, which grants the hacker complete control over the system account. In order to sign in to a service like Facebook or Twitter, for example, the app will transmit a "session cookie"—a small bit of data that identifies you to the server and grants you access to that account. Access to the app will be granted by the server as long as the session token is retained on the user's device.

Repudiation

When a system or program doesn't have proper controls in place to track and record user actions, it opens the door to repudiation attacks, which involve hostile manipulation or the fabrication of extra stages. Taking use of this flaw could lead to malevolent users logging the erroneous data in their log files since they changed the data writing. Just with email spoofing, it can be used to handle data in general while pretending to be someone else. The results of this attack could be misleading or incorrect information saved in log files.

Deluge

Try to reconfigure dispersed nodes—also called a reprogramming assault. A significant chunk of the network could fall under the attacker's control if the attack succeeds. It was possible to carry out this attack because most of the sensors were placed in dangerous areas and could be operated remotely through a wireless network. The use of robust authentication could make this impossible to happen.

DoS

Any layer of a WSN may be targeted by this attack type because it was employed across all layers. The objective of a denial-of-service (DoS) assault is to make a system or network unavailable to the people who need it. For a distributed denial of service assault to succeed, the target must either be inundated with traffic or given knowledge that causes them to fail. A denial of service attack targets real individuals by removing their access to services or assets.

Why Is Machine Learning Needed in WSN Security?

Certain WSNs engage in unsupervised interactions with security-sensitive data under malicious conditions. In such cases, WSN security precautions are of the utmost importance. The security measures can help with data freshness, authenticity, integrity, and confidentiality. Because of their low processing power and restricted resources, WSNs aren't a good fit for traditional network security solutions like user permission. Hence, the access gateway developed by the authors of [20] to assess the activities of IoT malware networks employing ML classification techniques such as k-NN, Random Forest, and Naive Bayes illustrates this point. Among these strategies, k-Nearest Neighbor (k-NN) proved to be the most accurate in performance evaluations. A privacy-preserving Support Vector Machine (SVM) training strategy was also suggested by the authors of [21] for IoT data; this method does not depend on a trustworthy third party and requires only two transactions per iteration. Comparing this method to traditional SVM, the computing complexity is drastically reduced. So, ML technology is a great example of how to cut costs in various security domains. For instance, anomaly detection performed admirably when protecting against DoS attacks, monitoring packets through analysis, and other forms of malicious activities [22] Additional ML-based procedures include increasing network availability, error detection [24], and traffic congestion [23]. Aside from the physical layer's authentication processes, it could be an effective solution [25]. Hence, ML approaches applied to WSNs should alleviate a lot of these issues while also offering great benefits in terms of accuracy and adaptability. **Challenges of WSN Security**

Networks of wireless sensors are an efficient system for gathering data and transmitting it in real-time via the perception layer. On the other hand, the network's reliance on public wireless channels is severely constrained by this layer. Many obstacles exist, particularly in the realm of security. Concerns with data privacy and security in WSNs compound the problems with applying network security standards to these networks, as previously mentioned. They will discuss the main concerns highlighted in Figure 3, which illustrate the main challenges to WSN security:

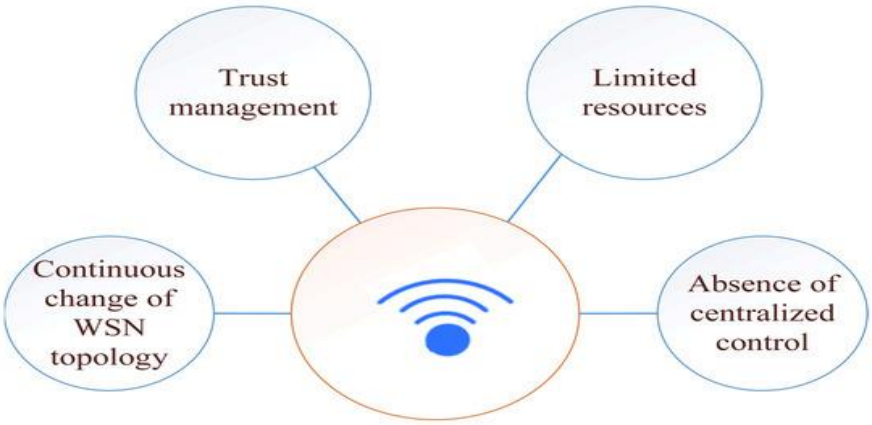

Figure 3. WSN's main security challenges.

Absence of Centralized Control

For instance, authentication activities will occur independently between neighboring WSN nodes because the perception layer is not centralized. Consequently, a workable option is to implement protocols that group WSN nodes into clusters and allow neighboring nodes to share authentication.

WSNs Topology Changes

The topology of a WSN network is always changing because nodes in the network can move

around, the environment can change, and nodes can be added or removed from the network [26]. Because of the need of handling these topological changes, authentication and routing systems that provide multi-hop communication are essential. All nearby (receiving) WSN nodes within the transmitter's broadcast range, for example, get the signal when the network's architecture is renewed.

Scalable Trust Management

In WSNs, trust management is the difficulty of identifying legitimate nodes from illegitimate nodes. The occurrence of a breach and the need to withdraw trust when it is detected, power limitations, the number of nodes to consider, and the difficulty of rebuilding trust when breaches occur are all unique challenges to trust in sensor network management. Furthermore, due to the performance/energy limits of several of the WSN nodes, it may not be able to accomplish complex key generation methods or pairs between them. It might not be feasible to do something frequently, even if it is feasible on an individual occasion. Assuming that some WSN nodes would inevitably have their shared keys physically compromised, It is wise to restrict the amount of nodes that can exchange keys to lessen the impact of an attack. Simple methods of key management can do this [27].

Limited Resources

Another issue stemming from the little effort required by the WSN node to get the data this sensor is meant to provide is a lack of resources. Since these gadgets aren't strong enough to secure even the most basic degree of protection for themselves, bringing their prices down to meet customer demands is a major concern when it comes to security. Weak reliance on connections, processing, or storage should characterize security management in WSNs if it is to be compatible with other network administration operations.

Challenges of Using ML Algorithms in WSN Security

Regardless, machine learning techniques are crucial for training WSN nodes to identify security flaws and hostile intrusions. This form of wireless network has numerous obstacles because of its low power and processing capacity. Predictions made in the present moment by machine learning algorithms—which include learning from past data—are erroneous. The effectiveness of the algorithm is set by the quantity of extra data. Energy costs are directly proportional to the size of the data set. Put another way, the WSN's power constraints and the ML algorithm's heavier computational load are not mutually exclusive. This trade-off can be avoided by centrally implementing ML algorithms. As a result, environments using wireless sensor networks are vulnerable to these algorithms. The security needs of WSNs cannot be met only by machine learning methods. When it comes to authentication and integrity, for example, they can be tricky to implement. Processing and power consumption are significant for providing such actions between WSN nodes. For example, this can be shown through authentication between the car and the driver, but it's not easy to show between different WSN nodes. Conversely, ML algorithms have been employed in certain research to authenticate users by exploiting physical channels [28].

There is always some degree of inaccuracy in any machine learning algorithm, no matter how tiny. Consequently, secret information should be as secret as possible. To improve case-based risk management of sensitive healthcare data using ML technology, the authors collaborated by delivering a Mathematical Encryption Standard (MES). Fuzzy inference systems combined with neural networks improved decision-making about MES's risk control strategy. Their aim to raise security concerns is supported by the results showing an accuracy rate of 97% and a MES error rate of less than 0.05. Even with the writers' best efforts, there will always be some degree of mistake, no matter how small.

ML-Based WSN Diversified Security

the role of ML algorithms in wireless sensor network security in different areas other than those discussed in the previous subsection, including the man in the middle, espionage, and selective forward.

In [29], the authors employed a neural network approach that includes three types of neurons: devices, sensing, and delay. Additionally, they utilized five hidden neurons with three levels of sensitivity. Each node's health is monitored by the proposed algorithm through those inputs to the network packets. Values that aren't where they should be suggest either erroneous information or

the existence of a human intervening in the assault. In a different method that use an ML algorithm to recognize WSN devices, the authors of [30] introduced a unique model to classify newly allocated devices in the house or office as reliable, strict, or limited. An Internet of Things security provider takes the fingerprints that the gateway creates and uses a machine learning classification model to determine the device's kind and the data it sends and receives. The gateway must also keep an eye on the traffic that freshly assigned devices produce. Furthermore, ML was employed by the writers of [31] to distinguish between data traffic emanating from WSN and non-WSN devices. Classification is being accomplished with the use of session data and device-specific properties.
.

Furthermore, to ascertain whether a benign node had become malicious, the method detailed in [32] employed an ML algorithm. You can also employ bio-inspiration as a defense mechanism against harmful nodes. It is necessary to divide the normal and faulty data sets before the k-means method can begin. Subsequently, support vector machines (SVMs) are used to create a decision block that has normal, defect, and critical boundaries. With the use of an anomaly detection method, they calculate the WSN node's mean and standard deviation from the SVM dataset. In response to a detected anomaly, the immune system goes into action. By mimicking biological processes, virtual antibodies ultimately eradicate dangerous nodes

Table 1 Summary of reviewed ML algorithms in WSN diversified security.

Refs.	ML Technique	Processing Cost	Attack	Accuracy	Limitations
[33]	ANN	High	Man in the Middle	99%	Needs huge datasets
[34]	Random Forest	Low	Traffic monitoring (identification)	96%	Not expandable
[35]	Binary Classifier	Low	Traffic monitoring (identification)	95%	Centralization of classification
[36]	k-mean + SVM	Moderate	Malicious node	NA	Centralization of classification
[37]	Random Forest	Low	Privacy	NA	Requires large memory for storage
[38]	Random Forest + SVM	Moderate	Channel identification	NA	Not effective for large networks

III RELATED WORKS

Research in wireless sensor networks is now centered on clustering and routing protocols with the goals of improving network efficiency, extending the lifespan of sensor nodes, and optimizing data transfer. Here, we highlight developments in a variety of fields by classifying recent academic research into three separate parts. They begin with a discussion of fuzzy logic-based methods for routing and clustering. Finally, it looks at how to improve the performance of routing and clustering by using intelligent computing approaches, most especially Particle Swarm Optimization algorithms. Finally, to effectively tackle the intrinsic problems of WSNs, they take a look at techniques that combine intelligent algorithms with fuzzy logic.

A region-centric method is used to defuzzify the output linguistic variables in order to achieve a clear value. Once the CH election is finished, nodes that aren't CHs join the cluster that has the closest CH. Clustering is completed when non-CH nodes communicate sensed data to their corresponding CHs; thereafter, each CH compiles all the received data and sends it on to its recipient. To get a more accurate view of the CH's energy usage, E-FUCA looks at the average distance to the communication node rather than the node density. Selecting the

mean distance provides an accurate depiction of the communication expense experienced by the CH. Cluster formation in FUCA is marred by greedy decisions made by non-CH nodes, which pick the nearest CH regardless of the CH's load. With E-FUCA, non-CH nodes pick CHs smartly by considering the rank of the CH, how close the node is to the CH, and how many nodes are in the cluster radius that was determined when the node was chosen. In order to further improve energy efficiency, E-FUCA chooses its CHs according to the next hop rank, proximity to the next hop, and distance reduced to basis station. Strategies for routing and clustering that rely on intelligent computing Reliability, load balancing, and fault tolerance are all made easier with traditional clustering-based routing techniques. Nevertheless, they shorten the lifespan of CHs. New ideas for WSN routing and clustering protocols have emerged with the meteoric rise of intelligent computing techniques. A method for selecting CH that uses less energy was presented in [39]. This approach uses an improved GWO algorithm to pick CHs while taking into account convergence distance, residual energy, balancing factor, and average intra-cluster distance, among other characteristics, to prolong the WSN's life.

When designing the fitness function for CH selection, we take into account things like residual energy and the distance between nodes and the BS in terms of standard geometry. The goal of this design is to increase the lifetime of the network and promote energy balance by selecting CH uniformly in each round. The PSO algorithm is another popular smart optimization method that relies on population data. An approach to choosing appropriate sensor nodes as CHs in order to extend the lifetime of the network is presented in CASICPSO.This method makes use of PSO. At the outset, CASIC-PSO generates a random starting point for every particle, determining its speed and location by converting particle encoding to sensor node coordinates. The next step is to calculate the fitness values of the particles using a fitness function that accounts for the transmission energy usage between the BS and the sensor nodes as well as the remaining energy of the nodes themselves. Then, we find out each particle's optimal personal fitness value and the optimal global fitness value. At last, the particles keep changing their positions until the predetermined number of iterations has passed, at which point they will have achieved the optimal solution based on the position and velocity vectors globally. To further improve search quality relative to iteration number, acceleration coefficients are adaptively tuned. [40]

In [41], It offered a method to strengthen network defenses against intrusions that could occur through unauthorized internet traffic. Finding a happy medium between the need for security and the limitations caused by things like trust and available resources was the goal of the suggested solutionA ranking-based route mutation mechanism that selects optimal network flows using the bafflement technique was employed in the study to achieve this. Strong security at the base station level is ensured by taking into account numerous factors while picking these routes, such as route overlap, energy utilization, and link cost. Along with inspection methods designed for completely centered WSNs, this approach also enables numerous changed paths that can confound possible attackers. The method is picking out a number of imposter sink nodes in advance so that attackers can't tell which one is the real one. The remaining energy of surrounding nodes associated with the selected intruder sink nodes is taken into consideration by using an appropriate value. The predicted extra cost of communication within the associated region is taken into account by this parameter. Notably, this technique can still be implemented in large-scale sensor networks at a reasonable cost.

IV CONCLSUION

The optimizing communication in Wireless Sensor Networks (WSNs) is crucial for enhancing network efficiency, energy conservation, and prolonging the network's lifespan. The review of clustering algorithms and routing protocols demonstrates that clustering plays a pivotal role in reducing energy consumption, minimizing communication overhead, and improving scalability in WSNs. Effective clustering algorithms such as LEACH, HEED, and DEEC optimize the selection of cluster heads and enhance intra-cluster communication, contributing to extended network longevity.Additionally, the integration of advanced routing protocols, including hierarchical, flat, and location-based approaches, enables more efficient data transmission. These protocols, especially when combined with energy-aware mechanisms, help in reducing latency, conserving energy, and improving the overall throughput of the network. By leveraging clustering and routing protocols, future WSN implementations can achieve more reliable communication, reduced power consumption, and better adaptability to changing network dynamics.

However, ongoing challenges like load balancing, node mobility, and handling of large-scale networks still require further research to fully optimize communication in WSNs for diverse applications. The integration of machine learning, energy harvesting, and hybrid techniques holds promise for further advancements in this field.

Table 2 literature study on WSN application with ML

Author(s) & Year	Focus Area	Key Contributions
Rami Ahmad et al. (2022)[42]	Security & ML in WSNs	Explores challenges of energy vs. security in WSNs, highlights ML for security enhancement, discusses attack detection & mitigation techniques.
Shereen Ismail et al. (2023)[43]	Cybersecurity in WSNs	Reviews 164 articles on WSN security, explores ML & Blockchain for security, proposes a BC-ML framework for attack detection and prevention.
Tahesin et al. (2024)[44]	ML in WSNs Security	Discusses ML algorithms for improving WSN security, identifies challenges like QoS, anomaly detection, and congestion control.
Shereen Ismail et al. (2022)[45]	ML-based Intrusion Detection	Proposes Weighted Score Selector (WSS), a lightweight ML ensemble for WSN attack detection, evaluates against boosting, bagging, and stacking.
Himanshu Sharma et al. (2021)[46]	Smart City WSN-IoT Optimization	Reviews ML approaches for optimizing WSN-IoT nodes, finds 61% supervised, 27% reinforcement, 12% unsupervised learning used in smart city applications.
Ponnusamy Chinnasamy et al. (2024)[47]	6G & WSN Security	Explores blockchain and ML for 6G WSN security, proposes optimization methods, reports 97% throughput, 95% energy efficiency, 96% accuracy.
Liyazhou Hu et al. (2024) [48]	Energy Efficiency & Security in WSNs	Introduces DeepNR, a DRL-based approach for adaptive security & energy efficiency in WSNs, improves network speed (25%), lifespan (30%), security (20%).
Hasan Alkahtani et al. (2024))[49]	ICS Cyber security	Proposes ML-based attack detection for ICS, tests KNN, DT, CNN-LSTM on real-world datasets, achieves 100% accuracy in binary and multiclass classification.
Ahmad Alzahrani et al. (2023) [50]	IoT & Medical Cyber-Physical Systems	Discusses AI-powered IoT sensor data processing for healthcare, integrating DSS for real-time decision-making.

REFERENCES

[1]. Chijioke, W., Jamal, A.A.,Mahiddin, N.A. Wireless Sensor Networks, Internet of Ma, G.; Yang, Y.; Qiu, X. Fault-tolerant topology control for heterogeneous wireless sensor networks using multi-routing tree. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017, pp. 620–623.

[2]. Babita Jain, Gaurav Soni, Shruti Thapar, M Rao, "A Review on Routing Protocol of MANET with its Characteristics, Applications and Issues", International Journal of Early Childhood Special Education, Vol. 14, Issue. 5, pp. 2950-2956, 2022.

[3]. Sandhya, R., Sengottaiyan, N. S-SEECH secured scalable energy efficient clustering hierarchy protocol for wireless sensor network. In Proceedings of the International Conference on Data Mining and Advanced Computing (SAPIENCE), Ernakulam, India, 16–18 March

2016.
[4]. Cohen, R., Kapchits, B. Energy-delay optimization in an asynchronous sensor network with multiple gateways. In Proceedings of the 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Salt Lake City, UT, USA, 27–30 June 2011.
[5]. Sharma, N., Kaushik, I.; Bharat, A.V.B., Aditya, K. Attacks and Security Measures in Wireless Sensor Network. In Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques, and Applications; Wiley: Hoboken, NJ, USA, 2021.
[6]. Farahani, G. Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks. Secur. Commun. Netw. 2021, 2021, 8814141.
[7]. Akyildiz, I.F. Su, W. Sankarasubramaniam, Y. Cayirci, E. Wireless sensor networks: A survey. Comput. Netw. 2002, 38, 393–422.
[8]. Rawat, P. Singh, K.D. Chaouchi, H. Bonnin, J.M. Wireless Sensor Networks: Recent developments and potential synergies. J. Supercomput. 2013, 68, 1–48.
[9]. Akyildiz, I.F. Pompili, D. Melodia, T. Challenges for efficient communication in underwater acoustic sensor networks. ACM Sigbed Rev. 2004, 1, 3–8.
[10]. Heinzelman, W.B.,Chandrakasan, A.P., Balakrishnan, H. Application-specific protocol architecture for wireless micro sensor networks. IEEE Trans. Wirel. Commun. 2002, 1, 660–670.
[11]. Swetha, R., Santhosh Amarnath, V.,Anitha Sofia, V.S. Wireless Sensor Network: A Survey. Int. J. Adv. Res.Comput. Commun. Eng. 2018, 7, 114–117.
[12]. Perrig, A.,Szewczyk, R., Tygar, J.D.; Wen, V. Culler, D.E. SPINS: Security protocols for sensor networks. Wirel. Netw. 2002, 8, 521–534.
[13]. Shi, E., Perrig, A. Designing secure sensor networks. IEEE Wirel. Commun. 2004, 11, 38–43.
[14]. Geetha, V.A., Kallapur, P.V., Tellajeera, S. Clustering in wireless sensor networks: Performance comparison of leach & leach-c protocols using ns2. Procedia Technol. 2012, 4, 163–170.
[15]. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. Comput. Netw. 2008, 52, 2292–2330.
[16]. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. Computer 2002, 35, 54–62.
[17]. Zhu, Q., Wang, R.; Chen, Q., Liu, Y.; Qin, W. Iot gateway: Bridging wireless sensor networks into internet of things. In Proceedings of the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010; pp. 347–352.
[18]. Kuo, Y.W.; Li, C.L.; Jhang, J.H.; Lin, S. Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications. IEEE Sens. J. 2018, 18, 5187–5197.
[19]. Pirbhulal, S., Zhang, H.; E Alahi, M.E., Ghayvat, H., Mukhopadhyay, S.C., Zhang, Y.T.; Wu, W. A novel secureIoT-based smart home automation system using a wireless sensor network. Sensors 2017, 17, 69.
[20]. Messaoud, S., Bradai, A., Bukhari, S.H.R., Quang, P.T.A., Ben Ahmed, O.,Atri, M. A survey on machine learning in Internet of Things: Algorithms, strategies, and applications. Internet Things **2020**, 12, 100314.
[21]. Yang, Y., Zheng, X., Guo, W., Liu, X., Chang, V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Inf. Sci. **2019**, 479, 567–592.
[22]. Ahmad, R.H., Pathan, A.-S.K. A Study on M2M (Machine to Machine) System and Communication. In Security Solutions and Applied Cryptography in Smart Grid Communications; IGI Global: Hershey, PA, USA, 2016; pp. 179–214. ISBN 9781522518310.
[23]. Glissa, G., Meddeb, A. 6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 264–269.
[24]. Mamdouh, M., Elrukhsi, M.A.I., Khattab, A. Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; pp. 215–218.
[25]. Karakaya, A., Akleylek, S. A survey on security threats and authentication approaches in wireless sensor networks. In Proceedings of the 2018 6th International Symposium on

Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–4.
[26]. Gebremariam, G.G., Panda, J., Indu, S. Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network. Wirel. Commun. Mob. Comput. **2023**, 2023, 2744706
[27]. Miettinen, M.; Marchal, S.; Hafeez, I.; Asokan, N.; Sadeghi, A.R.; Tarkoma, S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 2177–2184.
[28]. Sirajuddin, M. Enhancing Security in Wireless Sensor Networks Using Trust-Based Path Selection. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 2023, 9, 329–337.
[29]. rasad, R.; Baghel, R.K. A novel fault diagnosis technique for wireless sensor network using feedforward neural network. IEEE Sens. Lett. **2021**, 6, 1–4.
[30]. Ahmad, R., Wazirali, R., Bsoul, Q.; Abu-Ain, T., Abu-Ain, W. Feature-Selection and Mutual-Clustering Approaches to Improve DoS Detection and Maintain WSNs' Lifetime. Sensors **2021**, 21, 4821.
[31]. Wazirali, R., Ahmad, R. Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime. Comput. Mater. Contin. **2022**, 70, 4922–4946.
[32]. Ioannou, C., Vassiliou, V. An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression. In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Montreal, QC, Canada, 28 October–2 November 2018; pp. 259–263.
[33]. Ul Islam, R., Hossain, M.S., Andersson, K. A novel anomaly detection algorithm for sensor data under uncertainty. Soft Comput. **2018**, 22, 1623–1639.
[34]. Tama, B.A., Comuzzi, M.,Rhee, K.H. TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System. IEEE Access **2019**, 7, 94497–94507.
[35]. Gulganwa, P., Jain, S. EES-WCA: Energy efficient and secure weighted clustering for WSN using machine learning approach. Int. J. Inf. Technol. **2022**, 14, 135–144
[36]. Wu, D.; Jiang, Z., Xie, X.; Wei, X., Yu, W., Li, R. LSTM Learning with Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. IEEE Trans. Ind. Informat. **2020**, 16, 5244–5253.
[37]. Wazirali, R., Ahmad, R., Alhiyari, S. SDN-OpenFlow Topology Discovery: An Overview of Performance Issues. Appl. Sci. **2021**, 11, 6999.
[38]. Canedo, J., Skjellum, A. Using machine learning to secure IoT systems. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 219–222.
[39]. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.R.,Tarkoma, S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 2177–2184.
[40]. Meidan, Y, Bohadana, M.,Shabtai, A, Guarnizo, J.D.,Ochoa, M., Tippenhauer, N.O.,Elovici, Y. ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017.
[41]. O'Mahony, G.D., Harris, P.J.; Murphy, C.C. Detecting Interference in Wireless Sensor Network Received Samples: A Machine Learning Approach. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020.
[42]. Rami Ahmad,Raniyah Wazirali,Tarik Abu-Ain (2022) "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues" 2022, 22(13), 4730; https://doi.org/10.3390/s22134730, 23 June 2022
[43]. Shereen Ismail,Diana W. Dawoud,Hassan Reza (2023) "securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review" 2023, 15(6), 200; https://doi.org/10.3390/fi15060200, 30 May 2023
[44]. Tahesin,Samira,Delwar,Unal,Aras,Sayak,Mukhopadhyay,Akshay,Kumar,Ujwala,,shirsagar,Yangwon Lee,Mangal Singh,Jee-Youl Ryu (2024) "The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection: A Detailed Analysis" 2024, 24(19), 6377; https://doi.org/10.3390/s24196377, 1 October 202

[45]. Shereen Ismail,Zakaria El Mrabet,Hassan Reza (2023) "An Ensemble-Based Machine Learning Approach for Cyber-Attacks Detection in Wireless Sensor Networks" . 2023, 13(1), 30; https://doi.org/10.3390/app13010030, 20 December 2022

[46]. Himanshu Sharma.Ahteshamul Haque,Frede Blaabjerg (2021) "Machine Learning in Wireless Sensor Networks for Smart Cities: A Survey" 2021, 10(9), 1012; https://doi.org/10.3390/electronics10091012, 23 April 2021

[47]. 6. Ponnusamy Chinnasamy,G. Charles Babu,Ramesh,Kumar,Ayyasamy,S. Amutha,Keshav Sinha,Allam Balaram (2024) "Blockchain 6G-Based Wireless Network Security Management with Optimization Using Machine Learning Techniques" 2024, 24(18), 6143; https://doi.org/10.3390/s24186143, 23 September 2024

[48]. Liyazhou Hu,Chao Han,Xiaojun Wang,Han Zhu,Jian Ouyang (2024) "Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks" 2024, 24(6), 1993; https://doi.org/10.3390/s24061993, 21 March 2024

[49]. Hasan Alkahtani,Theyazn H. H. Aldhyani (2022) "Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems" 2022, 11(11), 1717; https://doi.org/10.3390/electronics11111717, 27 May 2022

[50]. Ahmad Alzahrani,Mohammed Alshehri,Rayed AlGhamdi,Sunil Kumar Sharma (2023) "Improved Wireless Medical Cyber-Physical System (IWMCPS) Based on Machine Learning" 2023, 11(3), 384; https://doi.org/10.3390/healthcare11030384, 29 January 2023

[51]. Juan Parras,Maximilian Hüttenrauch,Santiago Zazo,Gerhard Neumann (2021) "Deep Reinforcement Learning for Attacking Wireless Sensor Networks" 2021, 21(12), 4060; https://doi.org/10.3390/s21124060, 12 June 2021.