Review Of Literature Machine Learning Approach For Detection Of Attacks In Wireless Sensor Networks

*Deepak Kumar Gupta and **Dr. Praveen Kumar

*Research Scholar, Department of Computer Science & Engineering, SunRise University, Alwar, Rajasthan (India)
**Professor, Department of Computer Science & Engineering, SunRise University, Alwar, Rajasthan (India)
Email: deepakmtechcs@gmail.com

Abstract: This study provides a thorough examination of the important intersection of Wireless Sensor Networks (WSNs) with machine learning (ML) for improving security. WSNs play critical roles in a wide range of applications, but their inherent constraints create unique security challenges. To address these problems, numerous ML algorithms have been used to improve WSN security, with a special emphasis on their advantages and disadvantages. Notable difficulties include localisation, coverage, anomaly detection, congestion control, and Quality of Service (QoS), emphasising the need for innovation. This study provides insights into the beneficial potential of ML in bolstering WSN security through a comprehensive review of existing experiments. This study emphasises the need to use ML's potential while expertly resolving subtle nuances to preserve the integrity and dependability of WSNs in the increasingly interconnected environment.

[Gupta, D.K. and Kumar, P. **REVIEW OF LITERATURE MACHINE LEARNING APPROACH FOR DETECTION OF ATTACKS IN WIRELESS SENSOR NETWORKS**. *Researcher* 2025;17(1):9-12]. ISSN 1553-9865 (print); ISSN 2163-8950 (online). http://www.sciencepub.net/researcher. 02. doi:10.7537/marsrsj170125.02

Keywords: Wireless Sensor Networks (WSNs); machine learning (ML); Quality of Service (QoS); Path Planning (PP); Sensor Node Deployment (SND)

Introduction

Wireless sensor network (WSN) is a talented technology for practical applications since its size, inexpensive also simply distributed environment. By reason of several exterior otherwise interior components, WSN can update dynamically. Thus it necessitates reform the network. In traditional WSN, intrusion detection (ID) approaches based on trust management. The Trust management procedure is measuring trust with properties which manipulate trust. It creates several problems, for example, limitation of necessary valuation data, require of big data procedure, the demand of easy trust correlation appearance as well as expectation of automation. To solve these issues, machine learning (ML) techniques can be functional to respond accordingly. In this review, we explain different Trust management algorithm for WSNs with their benefits, limitations and complexity. In addition, we discuss the ML, classification, and several machine learning approaches.

The realisation of artificial intelligence (AI) across multiple fields is currently the focus of worldwide interest. Within this broader framework, Wireless Sensor Networks (WSNs) emerge as a strong facilitator, conspicuously exercising their effect across diverse industries such as healthcare facilities, smart infrastructure, precision agriculture, and industrial ecosystems [**1**].

Notably, the deployment of a large and dynamically dispersed array of sensor nodes is inevitably required for these expanding applications. As a result, they become the focal point of a complex web of rigorous limitations, including imperatives like minimising packet loss, extending network lifetime, increasing data throughput, optimising energy utilisation, and reducing transmission delays. As a result of this complex terrain, network managers are constantly faced with the onerous chore of fine-tuning a suite of stack settings to meet the rigorous expectations imposed by these many network situations.

The recent trajectory of technological development has been considerably altered by the convergence of micro-electro-mechanical system (MEMS) technology, mobile communications, and digital electronics. This convergence has ushered in a new age marked by the introduction of small but powerful sensor nodes with cost-efficiency, energy frugality, multifunctionality, and compact form factors. These sensor nodes, which include a slew of critical components such as the ability to sense, interpret data, and communicate wirelessly, serve as the foundation for the notion of sensor networks [**2**].

This paradigm change is dependent on the collaborative synergy generated by a slew of these small nodes, which pool their resources to create a disruptive technological environment. Sensor networks, in contrast to conventional sensors, which generally function in two independent deployment modes, result in a paradigm change with substantial implications.

Conventional sensors are frequently limited to places far from the direct source of the phenomenon they aim to detect, relying on complicated procedures to

separate the intended signal from the cacophony of ambient noise that surrounds it. To accomplish its discerning purpose, this strategy needs the deployment of considerably bigger sensors endowed with complicated signal processing capabilities.

An alternate technique is the deployment of many sensors that are primarily concerned with perceiving the physical environment but lack comprehensive signal processing capabilities. To arrange both the physical location of these sensors and the extensive web of communication topologies that connects them in this situation, rigorous engineering is necessary. This complex interplay culminates in the transfer of time series data containing detected events to central nodes, where computational alchemy occurs and data fusion transforms raw data into useful insights. This contrast between the old sensor paradigm and the transformational sensor network ethos emphasises the latter's seismic shift in strategy and technical innovation.

Energy and security are major challenges in a wireless sensor network, and they work oppositely. As security complexity increases, battery drain will increase. Due to the limited power in wireless sensor networks, options to rely on the security of ordinary protocols embodied in encryption and key management are futile due to the nature of communication between sensors and the ever-changing network topology. Therefore, machine learning algorithms are one of the proposed solutions for providing security services in this type of network by including monitoring and decision intelligence. Machine learning algorithms present additional hurdles in terms of training and the amount of data required for training. This paper provides a convenient reference for wireless sensor network infrastructure and the security challenges it faces. It also discusses the possibility of benefiting from machine learning algorithms by reducing the security costs of wireless sensor networks in several domains; in addition to the challenges and proposed solutions to improving the ability of sensors to identify threats, attacks, risks, and malicious nodes through their ability to learn and self-development using machine learning algorithms. Furthermore, this paper discusses open issues related to adapting machine learning algorithms to the capabilities of sensors in this type of network.

Review of literature

A WSN is a complex network of tiny sensor nodes strategically deployed throughout a geographical area, creating a harmonic symphony of cooperative data exchange via wireless conduits. These sensor nodes act as diligent data collectors inside the monitored landscape, reporting their results to a centralised repository known as a sink. This sink, in turn, is responsible for data processing, either locally or by connections with larger networks, including the enormous expanse of the Internet, supported by gateways [**4**].

A typical sensor node or mote, which is the fundamental building element of a WSN, is a multidimensional entity that includes a variety of critical components. These nodes house processors that manage mote operations and perform data processing functions. Sensors attached to the device can detect environmental characteristics such as temperature, humidity, and light. However, it is critical to recognise that these motes function under rigorous limits, such as limited computing capacity and limited sensing capabilities due to bandwidth and battery constraints [**8**].

Memory resources are critical for storing programme instructions as well as the wide range of sensor data, from raw measurements to processed insights. The motes communicate with one another using a low-rate (10–100 kbps) and short-range (less than 100 m) wireless radio, which is commonly based on IEEE 802.15.4 radio standards. Given wireless communication's ravenous thirst for power, effective energy-conscious communication strategies are required to maintain mote operation. Rechargeable batteries develop as a widespread power source in this environment. Motes contain energy-harvesting technologies like solar cells to enhance their durability in distant and harsh situations, allowing for years of unattended deployment [**9**].

A WSN's Sensor Node Deployment may be divided into two paradigms: ad hoc and preplanned. Ad hoc installations are useful in large, open areas where a large number of nodes may be spread for autonomous monitoring and reporting. However, because of the vast number of nodes involved, this strategy complicates network maintenance and failure detection. Preplanned deployments, on the other hand, are appropriate for scenarios requiring restricted coverage, where a prudent selection of nodes is strategically positioned, resulting in lower network maintenance and administration costs [**20**].

A WSN is a complex ecosystem made up of multiple sensor nodes engaged in intricate inter-node communication over a wide range of radio frequencies, capable of performing a variety of critical tasks such as sensing, surveillance, measurement, and tracking [**10**]. These wireless nodes are absolutely resource-bound while being essential to their tasks, as seen by their confined processor power, bandwidth, battery life, and memory capacity [**1**].

Wireless Sensor Network (WSN) is one of the most effective methods for many real-time applications, due to its compactness, cost-effectiveness, and ease of deployment [**1**]. The

function of the WSN is to monitor the field of interest, collect the data, and transmit it to the base station (Access point) for post-processing analysis [2]. A large number of sensor nodes are used in some WSN implementations. In addition, these wireless nodes have a limited battery life and memory capacity [3]. Therefore, to obtain the most out of these WSNs, there must be a management system for these WSN nodes capable of regulating the relationship among themselves and with the access point as well.

For example, the ZigBee [4] and 6LoWPAN [5] are two protocols that support management in WSNs developed by the Internet Engineering Team (IETF) for standard transmission over IEEE 802.15.4. These protocols support modern management systems to use IEEE 802.15.4 in the 2.4 GHz band and support short transmission [6]. For example, 6LoWPAN IPv6 provides a connection between WSNs based on IP addresses on different layers. It also uses the 6LoWPAN Low Power and Loss Network (RPL) standard to map the network topology and uses the AES encryption algorithm to secure the WSN connection [7]. However, as the topology of these types of networks is constantly changing, it will have an impact on network routing strategies, delay, multi-layer design, coverage, Quality of Services (QoS), and fault detection [8]. Therefore, it is necessary to reconsider the management of WSNs by designing or incorporating new protocols to deal with the nature of the environments for which these embedded devices are designed.

Security and energy consumption are among the most important challenges in WSNs, as each one negatively affects the other. The increased security complexity of a WSN increases the power consumption of a node and vice versa. Given the challenging environments in which these sensors can operate, the need for both (reducing security and energy consumption) is one of the challenges that recent studies in this field are addressing [9,10]. Furthermore, the use of the traditional methods for providing security, which is known by the Triangle and defined by Confidentiality, Integration, and Authentication (CIA) [1], needs to be reconsidered. The process of encryption of data between two communication devices (two nodes) and associated operations, such as key exchange and encryption, are also considered traditional [2]. Moreover, these technologies are energy-intensive methods, especially as we mentioned in the previous paragraph, in the constant change in network topologies due to the constant movement of WSN nodes. Therefore, finding alternative methods that are simpler and faster is what is being sought. Thus, for example, artificial intelligence algorithms are one of the methods that can be used for this purpose. A node can develop skills to interact with nearby WSN nodes, detect viruses, analyze incoming and outgoing packets, authenticate between nodes, and maintain availability [3].

Machine learning (ML) is one of the most famous branches of artificial intelligence that has been developed, where its algorithms build a mathematical model based on a sample of data [4], known as "training data" to make predictions or decisions without being explicitly programmed to do so [5]. For the reasons listed, the ML nature of WSNs is appropriate: WSN ecosystems are complicated and mathematical frameworks cannot be constructed. Furthermore, some programs use data sets that must be combined to function properly. In addition, WSNs have unexpected dynamics and behaviors, and finally, in line with the nature of WSNs, ML algorithms do not require human intervention [6]. However, there are two main challenges to ML in WSNs: the resources and computational limitations of nodes, and the need for large data sets for learning. As for the security of the WSN networks, one of the most important challenges faced by ML algorithms is the difficulty in applying them to the integrity and confidentiality of security requirements. Therefore, machine learning algorithms can help increase security in wireless networks, reduce all forms of congestion problems [9], and help authentication processes through the physical layer [2], and error detection [5]. Furthermore, ML algorithms have a great advantage in analyzing packets as they travel between WSN nodes and detecting suspicious nodes [6].

Many surveys discussed the role of machine learning algorithms in various fields of wireless sensor networks and the Internet of Things (IoT). For example, authors in [7] discussed ML algorithms in different WSN applications. Moreover, other authors in [5] discussed ML algorithms in sub-domains security, such as congestion traffic and intrusion detection in IoT and WSN. Others discussed security requirements in WSNs, such as [3]. However, none of these reviewed studies discussed the use of ML algorithms to provide security requirements for WSNs in all layers. Therefore, this study provides a detailed description of the security requirements of the WSN and the role of ML algorithms in providing these requirements in all WSN layers. ML algorithms can provide a better method for the security of wireless sensor networks than the traditional methods represented by encryption algorithms.

References

1. Eljakani, Y.; Boulouz, A.; Ben Salah, M.; El Hachemy, S. Performances prediction in Wireless Sensor Networks: A survey on Deep learning based-approaches. In *ITM*

Web of Conferences; EDP Sciences: Les Ulis, France, 2022; Volume 43, p. 01010.
2. Intanagonwiwat, C.; Govindan, R.; Estrin, D. Directed diffusion: A scalable and robust communication paradigm for sensor networks. In Proceedings of the ACM Mobi-Com'00, Boston, MA, USA, 6–11 August 2000; pp. 56–67.
3. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless Sensor Networks: A survey. *Comput. Netw.* **2002**, *38*, 393–422.
4. Rawat, P.; Singh, K.D.; Chaouchi, H.; Bonnin, J.M. Wireless Sensor Networks: A survey on recent developments and potential synergies. *J. Supercomput.* **2014**, *68*, 1–48.
5. Mitchell, T.M. *Machine Learning*, 1st ed.; McGraw-Hill, Inc.: New York, NY, USA, 1997.
6. Alsheikh, M.A.; Lin, S.; Niyato, D.; Tan, H.-P. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1996–2018.
7. Fu, S.; Zhang, Y.; Jiang, Y.; Hu, C.; Shih, C.-Y.; Marron, P.J. Experimental study for multi-layer parameter configuration of wsn links. In Proceedings of the 2015 IEEE 35th International Conference on Distributed Computing Systems, Columbus, OH, USA, 29 June–2 July 2015; pp. 369–378
8. Vinayakumar, R.; Alazab, M.; Soman, K.P.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* **2019**, *7*, 41525–41550
9. Ma, X.; Yao, T.; Hu, M.; Dong, Y.; Liu, W.; Wang, F.; Liu, J. A Survey on Deep Learning Empowered IoT Applications. *IEEE Access* **2019**, *7*, 181721–181732.
10. Ahmad, R.; Wazirali, R.; Abu-Ain, T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors* **2022**, *22*, 4730.

12/2/2024