Journal of Al-Azhar University Engineering Sector

Vol. 18, No. 69, October 2023, 914 - 938

A REVIEW OF SECURITY CHALLENGES AND SOLUTIONS IN WIRELESS SENSOR NETWORKS

Khaled M. A. Hassan*, Mohamed A. Madkour, Sayed A. Nouh

Computers and Systems Engineering Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt.

***Correspondence:** khaledhassan22@azhar.edu.eg

Citation:

K. M. A. Hassan, M. A. Madkour, S. A. .Nouh " A Review of Security Challenges and Solutions in Wireless Sensor Networks", Journal of Al-Azhar University Engineering Sector, Vol. 18, No. 914- 938, 2023

Received: 11 June 2023
Accepted: 04 August 2023

DoI:10.21608/auej.2023.217015.1380

ABSTRACT

Wireless Sensor Networks (WSNs) are a vital component of the Internet of Things (IoT) since it is a viable technology for a variety of real-time applications. This is mainly because WSNs are naturally distributed, low-cost, fault-tolerant, self-organizing, easily deployable, scalable, and function without a predefined infrastructure. Their applications include surveillance, smart power grids, traffic networks, telecommunications systems, smart cities, intelligent transportation, industrial quality control, and the military, to mention a few. However, the security of WSNs is a major concern due to their vulnerability to various types of attacks, including node compromise, eavesdropping, and denial-of-service.

This paper covers the security issues in WSNs and discusses the security challenges faced by these networks and the existing solutions. It illustrates the possible attacks and explores the different security mechanisms that can be used to protect WSNs, including encryption, authentication, and key management. Trust and reputation management are presented being effective techniques for mitigating routing attacks, and the role of machine learning techniques in enhancing WSN security is outlined. The paper concludes by discussing future research directions in WSN security. The findings of this paper are valuable for researchers, network administrators, and policymakers who are involved in the design and implementation of secure WSNs.

KEYWORDS: Wireless Sensor Networks (WSNs), Security of WSNs, Machine Learning (ML), Internet of Things (IoT), Trust and Reputation, Intrusion Detection System (IDS), Malicious Node, Denial of Service (DoS)

مراجعة شاملة للتحديات الأمنية والحلول في شبكات الاستشعار اللاسلكية

خالد محمد علي حسان*، محمد أشرف مدكور، سيد عبدالهادي نوح

قسم هندسة النظم والحاسبات، جامعة الأزهر، القاهرة، مصر

*** البريد الاليكتروني للباحث الرئيسي:** khaledhassan22@azhar.edu.eg

الملخص العربي: -

تعد شبكات الاستشعار اللاسلكية (WSNs) جزءًا أساسيًا من إنترنت الأشياء (IoT) نظرًا لأنها تقنية قابلة للتطبيق لمجموعة متنوعة من تطبيقات الوقت الفعلي. ويرجع ذلك أساسًا إلى أن شبكات WSNs موزعة بشكل طبيعي، ومنخفضة التكلفة، ومتسامحة مع الأخطاء، كما ان لها القدره على التنظيم الذاتي، وقابلة للنشر بسهولة، وقابلة للتطوير، وتعمل بدون بنية أساسية محددة مسبقًا. تشمل تطبيقات شبكات الاستشعار

اللاسلكية كلا من أنظمة المراقبة وشبكات الطاقة الذكية وأنظمة المرور الذكية وأنظمة الاتصالات والمدن الذكية والنقل الذكي ومراقبة الجودة الصناعية والتطبيقات العسكرية، وذلك على سبيل المثال لا الحصر. ومع ذلك، فإن أمان الشبكات الاستشعار اللاسلكية يعد مصدر قلق كبير نظرًا لضعفها أمام أنواع مختلفة من الهجمات، بما في ذلك اختراق عقدة الاستشعار والتنصت وهجوم تعطيل الخدمة . يتناول هذا البحث مشكلات الأمان في شبكات الاستشعار اللاسلكية ويناقش التحديات الأمنية التي تواجه هذه الشبكات والحلول الحالية للمشكلات. كما يوضح البحث الهجمات المحتملة ويستعرض آليات الأمان المختلفة التي يمكن استخدامها لحماية شبكات الاستشعار اللاسلكي ، بما في ذلك التشفير والمصادقة وإدارة توزيع مفاتيح التشفير. بالاضافة الى ذلك يتم عرض تقنية إدارة الثقة والسمعة باعتبارها تقنية فعالة للتخفيف من هجمات التوجيه ، كما تم التنويه عن دور تقنيات التعلم الآلي في تعزيز أمان شبكات الاستشعار اللاسلكية . ويختتم البحث بمناقشة اتجاهات البحوث المستقبلية في أمن شبكات الاستشعار اللاسلكية. تعتبر نتائج هذا البحث ذات قيمة للباحثين ومسؤولي الشبكات وواضعي السياسات الذين يشاركون في تصميم وتنفيذ شبكات الاستشعار اللاسلكية الآمنة.

الكلمات المفتاحية : شبكات الاستشعار اللاسلكية (WSNs) ، أمن شبكات الاستشعار اللاسلكية ، التعلم الآلي (ML) ، إنترنت الأشياء (IoT) ، أنظمة الثقة والسمعة ، نظام كشف التطفل (IDS) ، عقدة الاستشعار الضارة ، تعطيل الخدمة (DoS).

1. INTRODUCTION

WSNs are an essential component of the future networked world, also commonly known as the Internet of Things (IoT), which is going to be extensively utilized for control, connectivity, security, and general awareness of things large or small, close or far, wired or wireless [1, 2, 3]. WSNs are a type of network composed of small, low-power devices called sensors that are used to collect data from the environment. They have an expansive field of applications in areas such as healthcare, environmental monitoring, and military surveillance. However, the use of wireless communication in WSNs presents a significant challenge to security. Because WSNs are often deployed in uncontrolled environments, they are vulnerable to attacks from malicious nodes that may attempt to compromise the confidentiality, availability, and integrity of the network. Therefore, security is a critical concern in the design and implementation of WSNs. A comprehensive security framework should be established to ensure the protection of the network against attacks [1– 9].

WSNs have become the most popular networks, and their applications have grown widely in recent years, offering solutions that are flexible, low-cost, and easy to set up and run [4 – 9]. Sensor nodes measure environmental conditions and then communicate with each other to send the data they collect to a destination to process it more efficiently. WSNs operate in an infrastructure-less, ad hoc manner, and communication relies on cooperation among sensor nodes. However, the deployment of WSNs faces significant obstacles, such as energy consumption and security issues [9]. Since these networks are designed to operate in a self-organized manner, a malicious node may enter the network [1, 2]. Therefore, the objective of WSN security services is to protect resources and information from threats and inappropriate behavior [10].

Security is a critical issue in WSNs because of their unique characteristics, such as limited resources, wireless communication, deployment in hostile environments, and the sensitive and confidential nature of the data they collect and transmit. Unauthorized access, tampering, and interception of data can lead to serious consequences, such as compromising privacy, disrupting critical operations, and causing physical damage. Therefore, the main objective of security in WSNs is to provide confidentiality, integrity, and availability of data and services [3, 4, 6, 7]. Many attacks that threaten a network's operation could be launched against WSNs, causing harm to either communication stability or sensitive data [9, 11]. Attacks can be classified into insider (internal) and outsider (external) attacks. In insider attacks, the attackers have access to sensor nodes in a network and may be able to add false packets that threaten the integrity of the data system. On the other hand, before an outsider can launch an attack, he or she must first break the network's security [12, 13]. Most attacks focus on routing protocols because they are so important for network operation. Such attacks include a gray hole or selective forwarding, a black hole, a sinkhole,

replayed routing information, a wormhole, a hello flood, acknowledgment spoofing, Sybil attacks, and so on [7, 14–19].

The objective of this paper is to provide a comprehensive understanding of the security challenges in WSNs and to suggest possible solutions that can be employed to enhance the security of these networks. The paper provides an overview of the WSN's infrastructure and classifications, routing issues, and the classification of routing protocols in WSNs. Next, it provides an overview of security issues in WSNs and highlights the various types of attacks that WSNs are vulnerable to, the measures that can be taken to mitigate these attacks, and the trust and reputation management systems in WSNs. Finally, the most important open issues and future directions in the security of WSNs are discussed.

The remainder of this paper is structured as follows: Section 2 discusses an overview of wireless sensor networks, and Section 3 gives a detailed overview of security in WSNs. Section 4 discusses the most important open issues and future directions in the security of WSNs. Finally, Section 5 concludes the paper.

2. Overview of WSNs

2.1. WSNs and the IoT

WSNs are the backbone component of the IoT, which is widely used for universal connectivity, security, control, and general awareness of things. Low-powered, small-sized sensors can efficiently monitor and collect data from any environment [1, 2, 14, 20, 21, 22, 23]."Things" in the IoT refer to tiny embedded physical sensing devices (i.e., sensor nodes) that are connected to the Internet to achieve a specified task [4]. WSN contains many small sensor nodes, which are composed of processing, detecting, communicating, and powering components. These sensor nodes work together to collect data and send it to a destination. However, WSNs have energy, processing, memory, topology, mobility, and lifetime constrain [6, 10, 19, 20, 24]. The sensor nodes in WSNs facilitate efficient data collection and communication in various applications. These sensor nodes connect over a short range through a wireless medium and cooperate to achieve a common task. In many applications, sensor nodes are deployed in an ad hoc manner without engineering or careful planning. After deployment, the sensor nodes should be able to organize themselves autonomously into WSN [4 – 8, 25]. Each sensor node in a WSN can have one or more sensor modules that can sense various physical parameters such as temperature, humidity, light, sound, pressure, etc. Additionally, each sensor node has four components, namely a battery, memory, processing, and communication modules. The lifetime of a sensor is very restricted based on its very limited power source. Thus, saving energy consumption at its lowest level is one of the essential requirements. In general, there are four communication modes at the sensor nodes: transmit, receive, idle, and sleep modes. Idle mode is different from sleep mode. In sleep mode, all the radio components within the sensor nodes are completely shut down (for greater energy savings). Whereas, in idle mode, the sensor nodes switch off all their components except the receive radio antenna [26]. Two sensor nodes can directly communicate if they are within radio range of each other. If they are not, they can use other sensor nodes as routers (intermediary nodes) for data transmission. Anyway, WSNs are the start of a "smart space" revolution in which small devices will connect wireless information technology to our daily lives [5, 6, 7]. Sensor nodes typically rely on batteries and are often deployed in environments where battery replacement may be impossible. Therefore, a primary objective in the design of WSNs is to prolong their lifetime by reducing energy consumption as much as possible. Thus, energy efficiency is the most important issue in all facets of WSN operations [27, 28]. WSNs are widely used in environmental conditions

where approaches depend on sensing and monitoring methods. As a result, because WSNs are in such an open environment, they can be attacked by many malicious attacks. Fig. 1 depicts a WSN that is made up of many independent nodes. Each sensor node gathers data from the environment and sends it to the destination (sink). So that the user can analyze it.

WSNs can be classified into different categories based on various criteria [30], as follows:

- Static and mobile networks.
- Deterministic and non-deterministic networks.
- Static-sink and mobile-sink networks.
- Single-sink and multi-sink networks.
- Single-hop and multi-hop networks.
- Self-reconfigurable and non-self-configurable networks.
- Homogeneous and heterogeneous networks.

New revolutionary techniques of Artificial Intelligence (AI) and Machine Learning (ML) are becoming the future of totally automated IoT applications. In smart cities, low-data-rate WSNs are employed for monitoring and controlling various applications. The sensor nodes serve as the foundational technology infrastructure in the IoT [4, 31]. However, there are challenges such as power management, security, and data management that researchers are developing new techniques and technologies to address [4, 31].

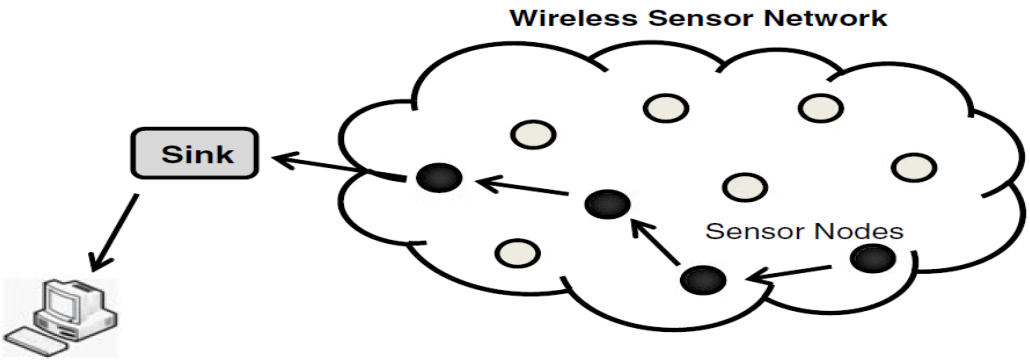

Fig. 1: Collection of data in a scenario of a wireless sensor network [29].

2.2. Routing Protocols in WSNs

WSNs suffer from the restrictions of many network resources, for example, CPU, memory, bandwidth, energy, and storage. Consequentially, the routing protocols that are designed for WSNs are considered a challenge because of the network constraints mentioned above. The main target of a WSN routing protocol is to establish a correct and effective route between a pair of sensor nodes so that packets can be delivered in due course. In WSNs, route construction must be done with a minimum of overhead and bandwidth. Furthermore, the routing protocols for WSNs are responsible for maintaining the routes in a network and must guarantee reliable multi-hop connections under these conditions [32]. WSN's routing protocols are different than the conventional routing protocols in wireless networks because there is no infrastructure, wireless channels are unreliable, and sensor nodes may fail. In addition, the routing protocol must meet stringent requirements to save energy [32]. There are many classifications of the current routing protocols in WSNs. All of the main routing protocols proposed for WSNs can be classified into seven groups, as shown in Table 1 [32].

2.3. Trust and Reputation in WSNs

In WSNs, trust and reputation play an important role in ensuring the reliability and security of the network. Trust in WSNs involves evaluating the behavior and reliability of sensor nodes based on their past actions and interactions. On the other hand, reputation is a measure of the perceived trustworthiness of a sensor node based on the opinions or feedback of other nodes in the network. The concepts of trust and reputation are important in our daily lives, as all relationships are based on trust. This concept has been applied to trust and reputation management models for WSNs, where each sensor node observes the behavior of its neighbors for the purpose of establishing trusting relationships between each other. Thus, the trust and reputation concepts can be used to determine which sensor nodes to trust and which sensor nodes to avoid in the network. Trust and reputation are mathematical tools that represent a sensor node's opinion of another sensor node [16, 19, 31, 33]. However, trust and reputation management models are divided into three types: distributed, centralized, and hybrid [13, 31, 34, 35]. In WSNs, trust and reputation models can be used for various purposes, such as:

- Routing: trust and reputation can be used to select the most reliable and trustworthy paths for routing data in the network.
- Security: trust and reputation can be used to detect and prevent malicious nodes from disrupting the network or compromising its security.
- Resource management: trust and reputation can be used to allocate resources such as bandwidth, power, and memory among nodes in the network.

There are three main approaches to implement trust and reputation management in WSNs, namely, direct, indirect, and hybrid trust. In the direct trust approach, sensor nodes directly evaluate the behavior of other nodes based on their interactions and past experiences. Alternatively, indirect trust may be obtained when sensor nodes evaluate the behavior of other nodes based on the opinions or feedback of other nodes in the network. Hybrid trust is a combination of direct and indirect trust mechanisms. Trust and reputation models are important for making sure that WSNs are reliable, secure, and efficient [13, 31, 34, 35, 36].

3. Security in WSNs

Information security in WSNs is critical as they play a significant role in information sensing and aggregation for big data, cloud computing, and the IoT [7]. WSNs have been successful due to their simplicity, but this simplicity requires a resource limitation, which means additional challenges to the protocol design and security of the network [37]. However, security is a significant concern for WSNs, as they are often deployed in hostile environments without physical protection, allowing them to be easily captured and compromised. Since WSNs rely on wireless communication, malicious attackers can exploit vulnerabilities to disrupt network operations and compromise data confidentiality, integrity, and availability. In addition, the limited resources of the sensor nodes make it unsuitable to apply traditional security solutions; thus, it is essential to use lightweight encryption algorithms that do not consume too much power or memory. Therefore, extensive research has been conducted to address these security challenges in WSNs [7, 37, 38]. There have been many techniques developed to provide security for WSNs. Trust and reputation models and intrusion detection systems are considered important issues in the security of WSNs [7, 37].

Table 1: Routing protocol categories for WSNs [32]

Group	Examples for Protocols
Location-based Protocols	GEAR, GAF, CPSR, BVGF, TBF, GeRaF, MECN, SMECN, GPSR, ATSR.
Data-centric Protocols	SPIN, DD, RR, ACQUIRE, Cougar, EAD, Gradient-Based Routing, Energy-Aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent-Based Information Dissemination, Information-Directed Routing
Hierarchical Protocols	LEACH, HEED, APTEEN, PEGASIS, TEEN, EEHCA
Mobility-based Protocols	Joint Mobility and Routing Protocol, Data Mule-Based Protocol, SEAD, DPTBDD.
Multipath-based Protocols	Braided Multipath, Sensor-Disjoint Multipath, N-to-1 Multipath Discovery
Heterogeneity-based Protocols	CHR, IDSQ, CADR
Quality of Service (QoS)-based protocols	SPEED, SAR, Energy-Aware Routing Protocol.

3.1. Challenges of Security Protocols in WSNs

WSNs provide special challenges for security protocol designers due to the following unique characteristics [6, 7, 8, 15, 19, 21, 22, 23, 26, 36, 37, 39, 40, 41]:

1. All wireless channels use the same frequency band and have the same radio interface.
2. Most protocols for WSNs do not consider necessary security techniques in their design stage, as in the case of the Internet.
3. Because of their complexity and the limited resources of sensor nodes, it is very difficult to implement strong security algorithms on a sensor node platform.
4. Stronger security protocols require more resources at sensor nodes.
5. WSNs are generally deployed in unfriendly regions (unguarded environments) without any fixed infrastructure.
6. Dynamic topology changes and low communication bandwidth.
7. Random deployment and large-scale use of WSNs require security mechanisms that must be adapted to cope with dynamic deployment environments and ensure sensor effectiveness.
8. Data aggregation is an optimization technique used to reduce data transfer to the sink node, but it requires access to the exchanged data, creating a challenge for security mechanisms.
9. Absence of Centralized Control: Protocols dividing sensor nodes into clusters and sharing the same authentication mechanism are acceptable due to a lack of centralization.
10. Scalable trust management in WSNs is difficult due to difficulty identifying legitimate nodes from illegitimate nodes, power limitations, and the difficulty of rebuilding trust when attacks occur.
11. Challenges of using ML algorithms in WSN security due to limited resources in sensor nodes.

3.2. Security Services for WSNs

The objective of WSN's security services is to protect information and resources from threats and misbehavior. The following is a brief illustration of the needed WSN's services [14, 16, 21, 22, 29, 31, 35, 36, 37, 39, 42, 43]:

- **Data Confidentiality:** The goal of confidentiality is to keep information from being used or shared without permission while it is being sent from one place to another. In other words, it ensures that only authorized users have access to the data. This task can be accomplished by using encryption. Because WSNs are resource-constrained, most security protocols use symmetric cryptosystems to secure sensitive data.
- **Data Integrity:** To guarantee that received data is not altered in transit, either by attackers or by accident. In other words, it makes sure that data and routing information don't get tampered with as they move across a network where sensor nodes are often exposed and unattended and the communication channel between sensor nodes is open, making data vulnerable to interference.
- **Data Authentication** is the process of verifying the identities of sensor nodes to ensure the authenticity and integrity of exchanged messages in hostile environments. In other words, it aims to validate an end-user's or a device's claimed identity. It is necessary when sensor nodes exchange control information in a network. A standard approach to maintaining authenticity is through a symmetric-based cryptography mechanism called the message authentication code (MAC).
- **Data Availability:** To ensure that the data is accessible when needed, authorized users should be able to get to the information quickly and reliably. Additionally, it guarantees the safety and availability of sensor nodes even in the presence of specific attacks. Enhancing network availability can be achieved through techniques such as intrusion detection, error detection, and congestion control.
- **Access control:** This service is needed to ensure that authorized users can securely access and utilize the network's provided resources. Prior to accessing the network, the permissions or permission groups of the members should be clearly defined.
- **Authorization** is the act of granting access rights to a user.
- **Accountability** is the act of being explained and justified.
- **Data Freshness:** Data freshness in WSNs is crucial to maintaining the up-to-date and accuracy of sensing data, enabling it to accurately represent the current situation. By incorporating sequence numbers into packets, outdated and invalid information from malicious nodes can be filtered out, ensuring the integrity of the data.
- **Robustness:** It makes sure that the network works and can handle errors and attacks in places where disasters are likely to happen. Robustness is used to express this quality attribute.
- **Self-Organization:** Each sensor node must be flexible and independent enough to be able to fix itself and organize itself depending on the situation.
- **Non-repudiation:** The term "non-repudiation" refers to the fact that neither the transmitting nor the receiving sensor nodes can deny the authenticity of the data packets they have transmitted or received. To improve traceability, a security system must restrict repudiation.
- **Location Security:** For reliable functioning, WSNs necessitate the automatic location of each sensor node within the network. However, the presence of malicious nodes introduces the chance of compromising location information. Consequently, ensuring location security becomes a vital objective for security systems.
- **Forward and Backward Secrecy:** Sensor nodes in a WSN must maintain forward and backward secrecy to prevent attackers from breaking and hacking confidential information, especially for new nodes joining the network.

3.3. Security Mechanisms in WSNs

The limited resources available in WSNs often constrain the development of effective security mechanisms. To secure sensor networks in sensitive fields, robust and resource-intensive security approaches are commonly used, while lightweight security approaches with low resource consumption are suitable for superficial WSNs. Various countermeasures have been suggested, primarily focusing on either preventing security breaches using cryptosystems or detecting them using intrusion detection and trust models. However, these mechanisms may not always be sufficient against high-capacity attackers. Therefore, a combination of these approaches is necessary to fulfill all security requirements. The subsequent sections outline the diverse types of countermeasures that have been proposed for securing WSNs [22, 37]. Fig. 2 represents the types of security mechanisms in WSNs.

3.3.1. Encryption Mechanism

To implement security countermeasures, it is crucial to set up a cryptosystem that uses secure keys to encrypt and authenticate the messages exchanged among sensor nodes. However, the cryptographic algorithms employed must consider the limited resources available at sensor nodes. These algorithms should require low computing power and storage capacity while also being energy-efficient to be compatible with the resource constraints of the sensor nodes [37]. In general, the optimum key management protocol must be selected based on the application field [37].

- **Keys Management:** Keys management refers to the activities involved in establishing and maintaining keys based on a security policy. It is crucial that keys management satisfies security requirements, including authenticity, confidentiality, integrity, scalability, and flexibility, while also considering the resource limitations of the system. These constraints include battery reserve, radio transmission range, bandwidth, available memory, and the random deployment of nodes.
- **Keys Establishment:** Symmetric key cryptography provides more attractive characteristics in terms of speed and low energy costs. However, a common challenge that arises is the problem of key exchange, which involves the need to securely inform communicating entities about the shared key prior to establishing secure communication. A commonly used solution is to utilize a pre-distribution method, whereby keys are loaded into the sensor nodes prior to deployment. However, some studies suggest the potential application of public-key cryptography to reduce computational complexity and the amount of transmitted and stored data.
- **Distribution of Keys:** Key distribution is a key management process that involves distributing cryptographic keys efficiently and securely over all legitimate nodes. There are three essential models for this process: network keying, pair-wise keying, and group keying. The network keying approach is a simple distribution model that consists of using a unique key shared among all sensor nodes within the network. Pair-wise keying is a distribution model where a key is shared only between a pair of sensor nodes. Group keying is a model that combines the characteristics of network keying and pair-wise keying, allowing for a balance between resilience, scalability, robustness, and resource cost.

3.3.2. Authentication Mechanism

Authentication is a security mechanism used in wireless sensor networks. It uses a symmetric-based cryptography mechanism called the message authentication code (MAC). The transmitter creates a unique identifier or authentication code using a shared symmetric key with the receiver node. The receiver subsequently computes the MAC code using the identical key and

compares it with the received MAC code to determine whether the source is authentic [22, 36, 37, 44].

3.3.3. Trust and Reputation Mechanism

Many studies suggest that security techniques rely on trust and reputation to enhance the level of security in WSNs. The development of trust and reputation between sensor nodes can be enhanced by observing the behavior of a sensor node and assigning "trustworthy" nodes with a good reputation. These approaches protect the network from malicious attacks but can consume a lot of resources due to the periodic exchange of control packets. This makes it difficult to develop a trust model with low resource consumption [22, 36, 37].

3.3.4. Intrusion Detection Systems

The security mechanisms implemented to prevent malicious nodes from infiltrating the network are insufficient to ensure optimal network security. To guarantee a high level of security, an intrusion detection system (IDS) is necessary to detect and prevent malicious infiltrations. IDS is responsible for monitoring the suspicious behavior and activities of sensor nodes in the network, assuming there is a noticeable difference between legitimate and malicious nodes. The implementation of an IDS adapted to the limitations of WSNs is a challenge due to the physical limitations of sensor networks. The installation and initialization of an IDS with pre-knowledge before deployment is impractical, and post-deployment learning and intrusion detection activities are expensive in terms of computing overhead and energy consumption. Therefore, current IDSs are not suitable for wireless sensor networks [13, 22, 23, 36, 37].

3.3.5. Machine Learning Mechanisms

ML techniques are essential for WSNs to help sensor nodes make intelligent decisions to detect attacks, risks, threats, and malicious nodes. However, there are challenges due to limited energy and CPU capabilities. Therefore, ML algorithms are recommended to find simpler and faster methods to interact with sensor nodes, analyze packets, detect viruses, maintain availability, and authenticate between sensor nodes [22, 45, 46].

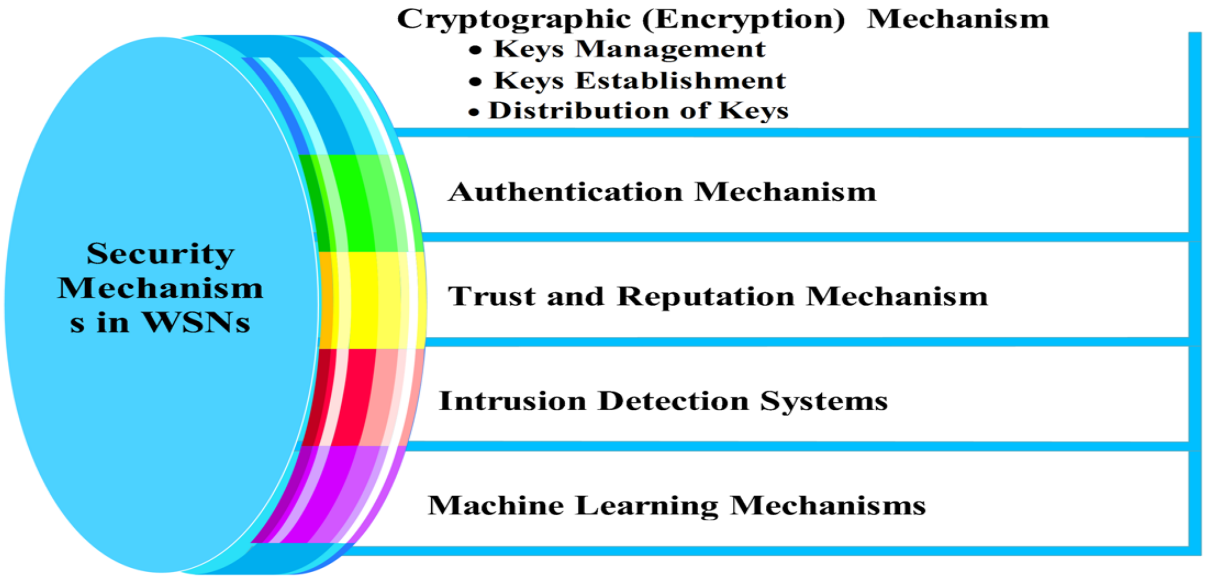

Fig. 2: Security mechanisms in WSNs.

3.4. Attacks in WSNs

Attacks on WSNs may be launched at all layers of the OSI networking model. Fig. 3 outlines such attacks, starting from the physical layer up to the application layer. Moreover, there are other attacks based on the attacker's capabilities and on the information in transit, as shown in Fig. 3. The following reviews these attacks in more detail, and Table 2 concludes this section by providing a summary of the most important routing attacks [11, 47].

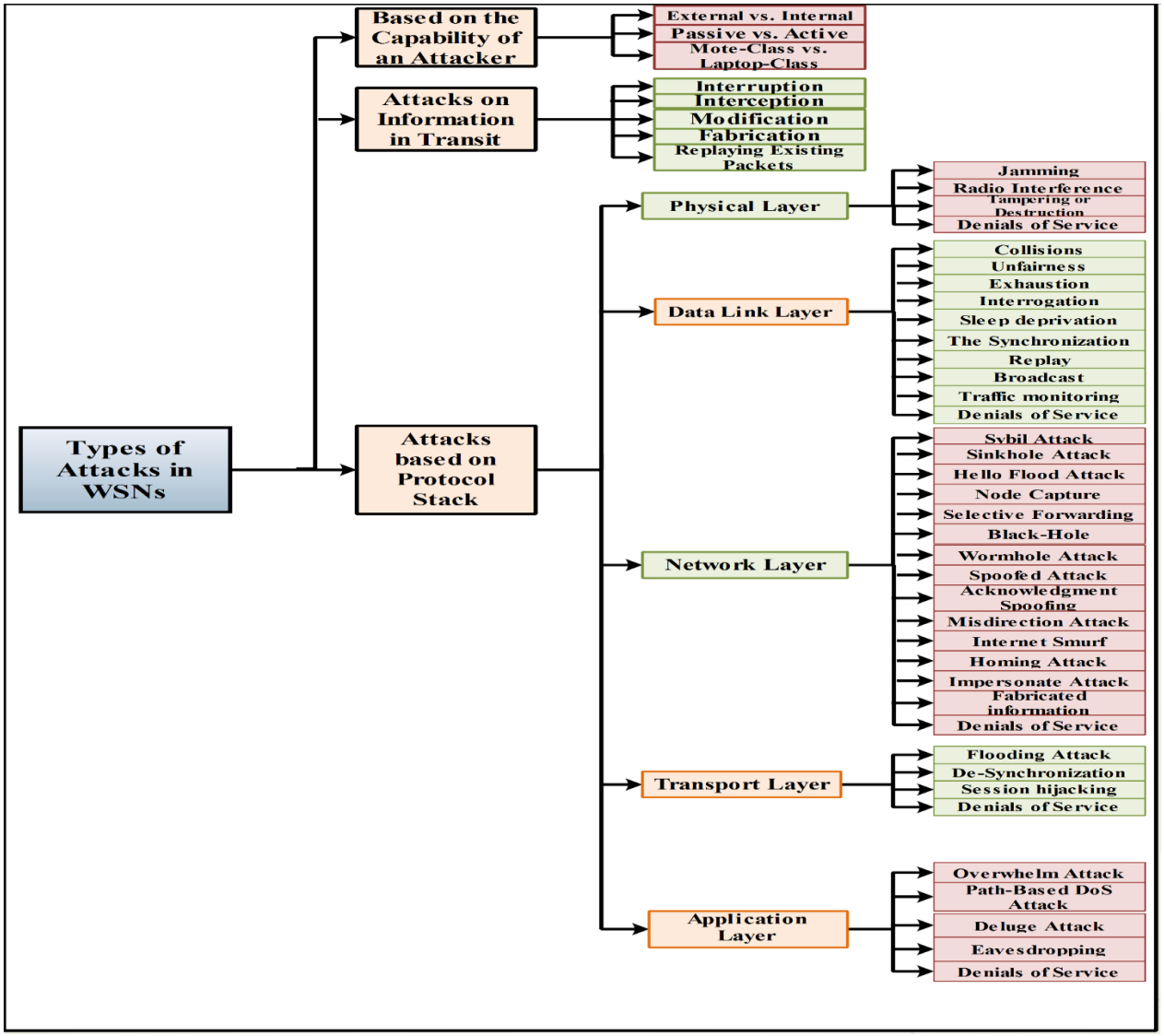

Fig. 3: Types of attacks in WSNs

3.4.1. Attacks Based on the Capability of an Attackers

- **External vs. Internal Attacks**: An outside (external) attack has no specific access to a WSN, such as passive eavesdropping on data transmissions by injecting fake information into a network to exhaust the resources, such as Denial of Service (DoS) attacks. However, external attackers have limited impact. Inside (internal) attacks are more difficult to detect and control, more destructive, and have access to the encryption keys or other codes that a network uses. This is because captured sensor nodes have the ability to steal sensitive information, transmit false information, and manipulate routing information [29, 36, 39, 42].

- **Passive vs. Active Attacks:** A passive attack is the act of monitoring or eavesdropping on the communication between sensor nodes without modifying any data packets. Eavesdropping, traffic analysis, and monitoring of network traffic are all examples of passive attacks in WSNs. While an active attacker's goal is the modification of data packets, as a result, the functions of a WSN collapse and its performance degrades. Jamming, packet injection, and selective forwarding are all types of active attacks that can happen in WSNs [29, 35, 36, 37, 39, 42, 43].
- **Mote-Class vs. Laptop-Class Attacks:** In a mote-class attack, attackers have access to a small number of sensor nodes with the same capabilities as other sensor nodes in a WSN. On the other hand, in a laptop-class attack, attackers can use more powerful devices such as a capable CPU, battery power, and a high-power radio transmitter to eavesdrop on a whole network [29, 42, 48].

3.4.2. Attacks on Information in Transit

- **Interruption:** WSN communication links may become unavailable or lost. This process threatens the availability of services. The major objective is to launch a DoS attack. This process is usually targeted at all layers [29].
- **Interception:** Unauthorized access to sensor nodes or information in WSNs compromises their security. An example of such an attack is the sensor node capture attack, which specifically aims to compromise message confidentiality within the network. The major objective of this attack is to intercept and eavesdrop on the data contained in the messages. Typically, this attack targets the application layer of the WSNs [29, 37, 49].
- **Modification:** Unauthorized sensor nodes pose a dual threat by not only gaining access to information but also tampering with it, thereby threatening the integrity of messages. The major objective is to mislead or confuse sensor nodes that participate in the communication protocol. Such activities typically target the application layer and the network layer [29, 35, 48].
- **Fabrication:** An attacker injects fake information and compromises the reliability of the information. This process threatens message authentication. So, the major objective is to mislead or confuse sensor nodes that participate in the communication protocol. In addition, this process can help with DoS attacks by flooding a network with traffic [29, 49].
- **Replaying Existing Packets:** This process threatens packet freshness, and the major objective of this process is to mislead or confuse sensor nodes that participate in the communications protocol without being conscious. This can lead to false data injection, unauthorized access, and the depletion of network resources. To prevent replay attacks in WSNs, various techniques can be used, such as timestamping, sequence number generation, Message Authentication Codes (MACs), and digital signatures [29, 35, 48, 49].

3.4.3. Attacks based on Protocol Stack

In the OSI model, attacks can be categorized according to the targeted protocol layer. A classification and review of the attacks on the communication layers of WSNs is given next [22, 37, 39, 42, 43, 49, 50].

3.4.3.1 Physical Layer Attacks : The responsibilities of the physical layer are selecting the frequency, modulation, carrier frequency generation, data encryption, and signal detection. Sensor nodes are using Radio Frequency (RF) to communicate wirelessly with each other. Because the communication medium is open, there are high risks that must be faced [22, 37, 39, 42, 48, 50, 51]. Some of these threats are:

- **Jamming Attack :** A jamming attack uses a jamming device to transmit a high-power signal that interferes with communication between the nodes in the network. The goal of the attacker is to disrupt the normal operation of the network and prevent legitimate communication from occurring. Jamming attacks can be harmful to WSNs due to their limited power and processing capabilities. To protect WSNs against jamming attacks, various countermeasures can be employed, such as frequency hopping techniques, spread spectrum techniques, directional antennas, intrusion detection systems, and automatic action [29, 37, 43, 43, 51,52].
- **Radio Interference Attack :** Attackers either create large amounts of interference continuously or intermittently. Thus, to address this problem, symmetric key algorithms are used, which delay the detection of keys for some time [39, 52].
- **Tampering or Destruction Attack :** When someone physically accesses a sensor node, an attacker can extract sensitive data, such as encryption keys or other information, from the sensor. The defense against this attack involves tamper-proofing the sensor node's physical package. In self-destruction packages, when someone physically accesses a sensor, the sensor node’s memory contents evaporate, which prevents any leakage of data [37, 39, 42, 43, 48, 51].

3.4.3.2 Data Link Layer Attacks : The responsibilities of the data link layer are medium access, the multiplexing of data streams, error control, and data frame detection. It guarantees reliable point-to-point and point-to-multipoint connections in a communication network. Moreover, it deals with issues such as synchronization, time scheduling between sensor nodes, and energy control [37, 39, 48]. Some of these threats are:

- **Collisions Attack :** A collision happens when two sensor nodes try to send on the same frequency at the same time, not adhering to the Intermediate Access Control Protocol. When packets collide, a change will possibly happen in the data part, which will cause a checksum mismatch at the receiving end. So, the packet will be discarded as invalid, and the source node will ask for retransmission of the same packet. It also happens in particular packets, such as ACK control packets. An attacker can repeat collisions to cause resource exhaustion. To overcome this attack by using error-correcting codes [22, 37, 42, 43, 51, 52].
- **Exhaustion (Continuous Channel Access) Attack :** An attacker damages the media access control protocol by continuing requests or transmitting over a channel by creating routing loops and path lengthening. A network can overcome this by reducing the MAC acceptance rate and using time-division multiplexing. In addition, each sensor node is allocated a time slot in which it can transmit by using time-division multiplexing [22, 37, 42, 43, 51, 52].
- **Unfairness Attack** : Unfairness can result if an attacker attempts to replicate this collision- or exhaustion-based MAC layer or misuses collective MAC layer priority techniques. The attack is considered a partial DoS attack but results in marginal degradation of performance. To overcome this attack, use small frames, where any individual sensor node seizes a channel for a shorter period only [22, 42, 43, 48, 49].
- **Interrogation Attack :** An attacker can exploit the request-to-send/clear-to-send (RTS/CTS) messages that are used for a handshake. Many MAC protocols use these messages to mitigate the hidden node problem. An attacker sends RTS messages constantly to a targeted sensor node while ignoring CTS reply messages, so he consumes resources for a neighboring sensor node.

To overcome this attack, each sensor node can limit itself to accepting connections from the same identity or by using anti-replay protection and strong link-layer authentication [50].

- **Sleep deprivation Attack :** The sleep deprivation attack is a type of denial-of-service attack that targets the node's energy reserves and hacks into the power management system to reduce transition possibilities in the low-power state. It is difficult to detect due to interactions that appear innocent. It can drastically reduce the victim's lifetime [37].
- **The Synchronization Attack :** The synchronization attack is a difficult to detect attack that causes synchronization problems at the MAC layer. Sensor nodes maintain a wake-up schedule and exchange it with neighboring nodes to synchronize their clocks. In order to stay in synchronization with the sensor node that sent the sync packet, the receiving sensor node must recalculate its sleep duration. Anyway, by sending a compromised synchronization message, the attacker can cause the targeted node to remain awake for a further fraction of the listening cycle [37].
- **Replay Attack :** Replay attacks use messages exchanged between sensor nodes to be retransmitted, causing energy waste and diverting the network from its original purpose. Without an anti-replay mechanism, retransmission can be broadcast across the network, causing energy waste [11, 37].
- **Broadcast Attack :** The broadcast attack is a malicious node that broadcasts unauthenticated traffic, which must be received by all nodes before it is rejected due to authentication failure [37].
- **Traffic monitoring :** Traffic analysis is a tool for detecting patterns of communication among nodes, targeting those that store confidential data and have the position information of an access point or sink node [11, 22].

3.4.3.3 Network Layer (Routing Layer) Attacks*:* Every sensor node acts as a router in WSNs. The network layer is most targeted by attacks due to its role in network functioning. The major aim of the network layer is to provide reliable end-to-end transmission [36, 37, 42]. There are various kinds of attacks at the network layer, as follows:

- **Sybil Attack** : One sensor node can introduce itself to other sensor nodes with multiple forged identifications (either IP addresses or MACs), where attackers can claim fabricated or stolen identities from good sensor nodes. Thus, an attacker may appear in multiple places in a network at the same time. There are many solutions that are suggested to overcome the Sybil attack, as follows:
  1) Key pre-distribution at random that associates a sensor node's identity with the keys attached to it and validates the keys to know if the sensor node is truly who it claims to be.
  2) Choose a radio resource that depends on the assumption that each sensor node has only one radio.
  3) Verification of position that assumes that a WSN is static.
  4) Recording of the identities of a sensor node at a central sink. Each of these solutions has a weakness.

  Each of these solutions has a weakness. For example, the key pre-distribution is challenging because it revokes keys if sensor nodes leave a network and assigns new keys to sensor nodes joining a network or when some of the keys expire. Some of the MAC protocols depend on every sensor node having more than one radio. So, there is no guarantee that every sensor node is going to have only one radio. While there is no guarantee that the network topology is static, sensor nodes do not change their locations. Many WSN deployments require mobile sensor

nodes. So, this solution may fail in the case of dynamic topologies [7, 11, 15, 22, 29, 35, 37, 42].

- **Sinkhole Attack :** Many routing protocols in WSNs need sensor nodes to broadcast "Hello messages" after deployment. That is a sort of neighbor discovery that relies on the radio range of a sensor node. An attacker manages to attract all traffic that is destined for a sink by announcing that it has the shortest path with higher trust and a short-delayed path to the sink. Geographic routing protocols are one of the classes of routing protocols that are resistant to sinkhole attacks [7, 11, 15, 29, 35, 37, 39, 42, 43, 51, 52].
- **Hello Flood Attack :** It uses hello messages as a weapon to persuade sensor nodes in WSNs. A sensor node that receives these messages may assume that it is in the sender's radio range. For example, a laptop-class attacker can transmit this type of message to every sensor node in a network, so they think an attacker belongs in their one-hop radio communication range, which leads to energy waste and data loss. Authentication is the best solution to defend against this attack [11, 15, 29, 35, 37, 42, 48, 52].
- **Node Capture Attack :** An attacker can observe and analyze the victim sensor node, where a single sensor node capture is enough to take control of a whole network. The best solution to this attack, which we mentioned previously, is self-destruction [42, 48].
- **Selective Forwarding (Gray-Hole) Attack :** A malicious node receives packets to forward them to the next hop, but it can selectively drop packets coming from a specific sensor node or a group of sensor nodes. This attack is the most difficult to detect due to conflicting behaviors [11, 15, 22, 29, 35, 37, 39, 42, 48, 52]. Selective forwarding can take the following forms:
    1) Selectively dropping packets from all sensor nodes.
    2) Selectively dropping packets from certain sensor nodes only.
- **Black-Hole Attack :** A malicious node receives packets to forward them to the next hop, but instead of forwarding them, it drops them. This attack is easier to detect due to its uniform behaviors [11, 15, 19, 22, 29, 35, 37, 42, 48, 52]. The black hole can take any of the following forms:
    1) Discards all incoming packets from any sensor node.
    2) Discards all incoming packets from specific sensor nodes.
- **Wormhole Attack :** An attacker often convinces sensor nodes that they are neighbors, so this leads to the quick depletion of their energy resources. This attack can be performed by an outsider or an insider. So, a wormhole is active even if the routing information is encrypted or authenticated. To overcome this attack, packets are routed to the sink along a path, which is always geographically the shortest, or by using very tight time synchronization between sensor nodes, which is impossible in practical environments [15, 29, 37, 42, 43, 50, 52, 53].
- **Spoofed, Altered, or Replayed Routing Information Attacks :** An attacker can change, spoof, or respond by routing fake information to collapse traffic in a network. Such as creating routing loops, repelling or attracting traffic on the network, partitioning a network, shortening and extending source routes, generating false error messages, and increasing end-to-end latency. To defend against these attacks, each message must include a message authentication code (MAC). Also, to overcome spoofing attacks by using efficient authentication and encryption mechanisms [11, 15, 37, 42, 48].
- **Acknowledgment Spoofing Attack :** An attacker can spoof the acknowledgment (ACK) of overheard packets destined for neighboring nodes to provide misleading information to neighboring sensor nodes. In other words, malicious nodes can easily mimic the acknowledgments exchanged between sensor nodes, leading to false information and poor data transmission. To overcome this attack by using encryption via authentication of every sent packet, including the packet headers [11, 15, 22, 37, 42, 48].

- **Misdirection Attack :** An attack where packets are sent in an incorrect direction or to an unreachable destination is known as a flood attack. To overcome this issue, temporarily schedule a victim sensor node in sleep mode if its link is flooded with unhelpful information [50].
- **Internet Smurf Attack :** This is a type of Distributed Denial of Service (DDoS) attack where attackers could flood the victim node's network link. The attackers tamper with the victim's address, broadcast echo messages in a network, and also route all the replies to the victim sensor node. To overcome this attack, if a sensor node's link is getting flooded without any helpful information, the victim sensor node can be scheduled into sleep mode for some time [50].
- **Homing Attack :** An attacker analyzes a traffic pattern to identify and target sensor nodes that have responsibilities, such as encryption key managers or cluster heads. Then it achieves DoS attack by destroying or jamming these keys on the sensor nodes. To overcome this attack, header encryption is used. Also, by using dummy packets throughout a network to achieve equal traffic volume, traffic analysis is prevented. Unfortunately, that wastes energy significantly, so it is used only when preventing traffic analysis is of maximum importance [29].
- **Impersonate Attack :** Where a node's identity is impersonated by an attacker to build a connection with or launch other attacks on a victim node, the attacker may also use the node's identity to build a connection with other sensor nodes or launch other attacks on behalf of the victim node [52].
- **Fabricated information attacks :** This is difficult to detect because of the attacking node's compliance with the routing protocol, leading to false measurement values that do not reflect the reality of their environment. This can be dangerous in scenarios such as monitoring hostile environments and battlefields. [37].

3.4.3.4 Transport Layer Attacks *:* The responsibility of the transport layer is to manage end-to-end communications for various applications in WSNs. Attackers constantly request to establish a connection with the neighboring sensor node, depleting its resources and causing legitimate requests to be ignored, so the protocols of WSNs are commonly simplified to suit the requirements of energy efficiency, such as low energy usage [37, 39, 48]. The main transport-layer attacks are as follows:

- **Flooding Attack :** Attackers may repeatedly initiate new connection requests until the resources needed for each connection reach their maximum capacity or are completely depleted. To overcome this attack, it requires each connecting client to prove its commitment to the connection by solving a puzzle. It can also put a limit on the number of connections to a special sensor node [11, 37, 39, 48].
- **De-Synchronization Attacks :** The de-synchronization attack disrupts existing connections by intercepting messages intended for another node, causing the attacked node to waste energy trying to repair transmission errors that never existed. To overcome this attack, it requires authentication of all packets, including control fields, to communicate between hosts, so header or full packet authentication can overcome it [37, 48, 50].
- **Session hijacking Attack :** A cookie-side takeover attack is a type of man-in-the-middle attack that allows the attacker full access to an online account by sending a session cookie to the server [22].

3.4.3.5 Application Layer Attacks : The application layer's role involves determining the manner in which data is requested and delivered, both for individual sensor nodes and when interacting with an end user [48]. The main attacks on this layer are as follows:

- **Overwhelm Attack :** An attacker may try to overwhelm network sensor nodes with sensory stimuli, which causes a network to send large volumes of traffic to a sink. So, this attacker depletes sensor node energy and network bandwidth. It can decrease the effects of this attacker by carefully tuning the sensor nodes. Also, it can decrease effects by using rate-limiting and efficient data aggregation algorithms [50].
- **Path-Based DoS Attack :** An attacker tries to inject false information or replay packets into a network at sensor nodes' leaves. An attacker can starve a network of legal traffic since it exhausts resources on a path to a sink, so it prevents other sensor nodes from transmitting packets to the sink. So, combining anti-replay protection with packet authentication prevents these attacks [50].
- **Deluge (reprogramming) Attack :** An attacker can reprogram a network remotely if the reprogramming operation is not secure, so it can kidnap this operation and take control of large part of a network. Most sensors were placed in a hostile area and controlled remotely over a wireless network, making this assault successful. It is possible to overcome this attack by using authentication streams to secure the reprogramming operation [22, 50].
- **Eavesdropping attack :** An attacker tries to collect information from a network by snooping on transmitted packets, so hackers use eavesdropping to gain access to information exchanged between sensor nodes, increasing the influence of radio fading and frequency transmission. In this process, information remains the same, but its privacy is compromised. This type of attack is executed on both the physical and application layers [22, 49, 52].
- **Denial of Service (DoS) Attack :** A DoS attack is an attack that attempts to disrupt, corrupt, or destroy a network, making it unreachable to the intended audience. It works by overwhelming the target with an excessive amount of traffic or delivering disruptive information that leads to the target's failure, depriving users of the services or assets they intended to use. DoS attacks can be executed on all layers in the OSI model [22, 37].

3.4.4. Trust and Reputation Attacks

Trust and reputation are important factors in ensuring the security and reliability of WSNs. In recent years, researchers have focused on developing trust- and reputation-based models to address the challenges of security and reliability in WSNs. Several studies have proposed trust-based routing protocols that take the trustworthiness of nodes into account when making routing decisions. Reputation-based models have also been proposed for WSNs, which involve the use of feedback from other sensor nodes to evaluate the reputation of a sensor node. Additionally, researchers have explored the combination of trust and reputation-based models to improve the security and reliability of WSNs. These models use both trust and reputation metrics. The trust and reputation models themselves are threatened by several types of attacks. Understanding these attacks is important to ensure that the integration between the trust and reputation models and WSNs does not open doors for more threats [7, 11, 16, 19, 47, 54]. Fig. 4 represents the types of attacks in the trust and reputation models. These attacks will be reviewed next in more detail [7, 11, 16, 19].

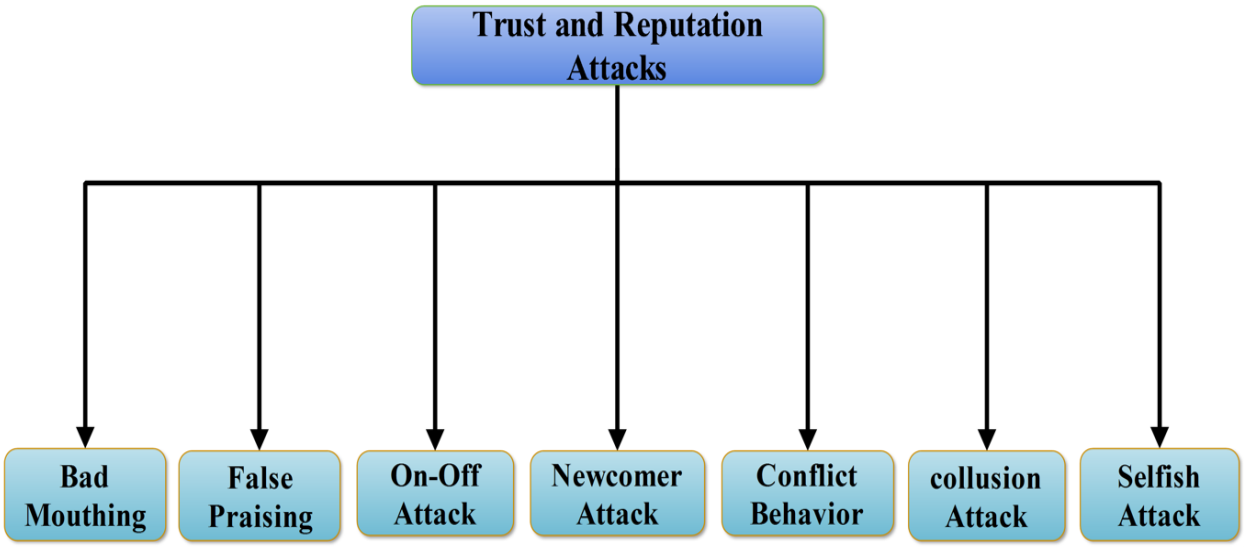

Fig. 4: Types of attacks in trust and reputation models.

3.4.4.1 Bad Mouthing Attack (BM) : This type of attack is most common in a trust and reputation management system that takes recommendations into account. When a few attackers collude to spread false information about a good sensor node, this may lead to a decrease in the trust rating of that sensor node. The trust and reputation management system can be negatively impacted when a sensor node is compromised during an attack, as the compromised node may provide false negative feedback based on its observations of well-behaved neighboring nodes. This attack is visible in scenarios where indirect information is considered and sensor nodes are permitted to share their negative feedback with their neighbors [7, 11, 19].

3.4.4.2 Ballot Stuffing Attack (BS) or False Praising : When a few attackers collude to spread false positive information about another attacker, this may assist attackers in maintaining higher trust ratings and remaining in a network for a longer period of time. This attack is visible in scenarios where indirect information is considered and sensor nodes are permitted to share their positive feedback with their neighbors [7, 16, 19].

3.4.4.3 On-Off Attack (OO) : The objective of an attack is to disrupt the overall performance of a system without being detected or excluded from the network. To delay the recognition of their malicious actions, the attackers employ a strategy of showing both abnormal and normal behavior. This attack can be launched against either trust and reputation activities or general activities in WSNs to keep the trust or reputation of an attacker above a certain threshold. It works well for a period so that its neighbors consider it trustworthy, but it starts acting badly later [7, 11, 16, 19].

3.4.4.4 Newcomer Attack (NC) or Whitewashing : Once the trust and reputation value of the attacker drops below a certain threshold, the sensor node will transition from a trusted mode to a malicious mode. Thus, the attacker will explore alternative methods to increase its trust and reputation value. An approach to achieve this involves rejoining the network using a new ID and erasing all negative past history. If the attacker can launch this attack, then detecting the attacker's misbehavior is not an issue from the attacker’s perspective because all the old history can be wiped out at any stage. In other words, attackers with very low trust and reputation discard their existing identity and, as newcomers, hide their bad history and reenter the system [7, 16, 19].

3.4.4.5 Conflict Behavior Attack : When the attackers carry out contradictory behaviors at various times or domains, they can cause conflicts with normal sensor nodes, thus damaging their ability to provide accurate recommendations [7, 11, 16, 19].

3.4.4.6 A collusion Attack : This situation arises when a group of attackers come together and agree to form a collaborative entity with the aim of manipulating the evaluation results related to trust and reputation for a specific target by systematically submitting fabricated feedback [7, 16, 19].

3.4.4.7 Selfish Attack : After receiving the trust request, a selfish node may refuse to participate in packet forwarding to save its battery energy. Thus, it will simply delete the request and not reserve the resource to transmit the trust reply [7, 11, 16, 19].

Table 2: Summary of the most important routing attacks and their descriptions.

Type of Attack	Attack Behavior
Black hole attack	An attacker tries to drop the received packets (it rejects forwarding any packet).
Gray hole attack	Attackers try to drop part of the received packets (selectively drop packets).
Sink hole attack	Attackers try to make a traffic announcement with fake routing information, but they do not forward it.
Replay attack	Attackers try to deceive routing functionality by repeatedly sending the original routing packets.
Link spoofing attack	An attacker can convince the sender that the packet was sent successfully through spoof link layer acknowledgment for overheard packets.
Modification attack	An attacker tries to modify information or route packets that are forwarding.
Sybil attack	An attacker presents multiple identities to appear on more than one sensor node.
Colluding nodes attack	Distrust may arise between two groups of sensor nodes when a sensor node exhibits inconsistent behavior, functioning perfectly with one group but behaving misbehaving with the other.
Traffic analysis	An attacker monitors a flow of traffic to locate, identify, and attack critical sensor nodes (usually a sink).
Flooding attack	An attacker crashes a victim's limited resources (memory and energy) by flooding a network with messages, which could be either data or routing packets.
Routing loop (Replayed Routing Information)	A network may encounter congestion and denial-of-service issues when an attacker modifies the route information of a message, potentially causing routing loops.
Wormhole	A group of attackers may collude to redirect packets to a slow connection that may cause congestion and raise latency in a network. This is known as tunneling.
Packet injection	A packet may be injected with fake (false) data, such as false source and destination identifiers.
Packet delay	An attacker has the capability to arbitrarily delay packets received for forwarding, employing a random approach. This unpredictable behavior enables the attacker to maintain their trust rating above a specific threshold, making it challenging to detect their malicious activities.
Bad mouth attack	A few attackers might collude to spread incorrect information about a good sensor node. So, the trust rating of a well-respected node might decrease.
Ballot stuffing attack (False praising)	In contrast to the bad-mouthing attacks, attackers collude to spread incorrect positive information about other attackers. As a result, this collusion allows the attackers to maintain higher trust ratings and remain on the network for longer periods of time.
On-off attack (Transient behavior)	An attacker works well for a period to maintain the reputation of the attacker above a certain threshold so that its neighbors consider it trusted while it starts bad behavior later.
Conflicting behavior attack.	An attacker is a contradictory behavior where an attacker behaves differently towards different neighbors or tries to deceive a trust model.
Selfishness attack	A sensor node with a low battery can participate in the route discovery process but may refuse to participate in packet forwarding, resulting in the node behaving maliciously by dropping packets.

3.5. Use of Machine Learning to Secure WSNs

ML techniques can be used to improve the security of WSNs by detecting and mitigating malicious node attacks. Fig. 5 depicts some of the most important ML applications for securing WSNs. These applications are reviewed next in more detail. Generally, the use of ML techniques can enhance the security of WSNs and enable them to detect and respond to attacks in real-time.

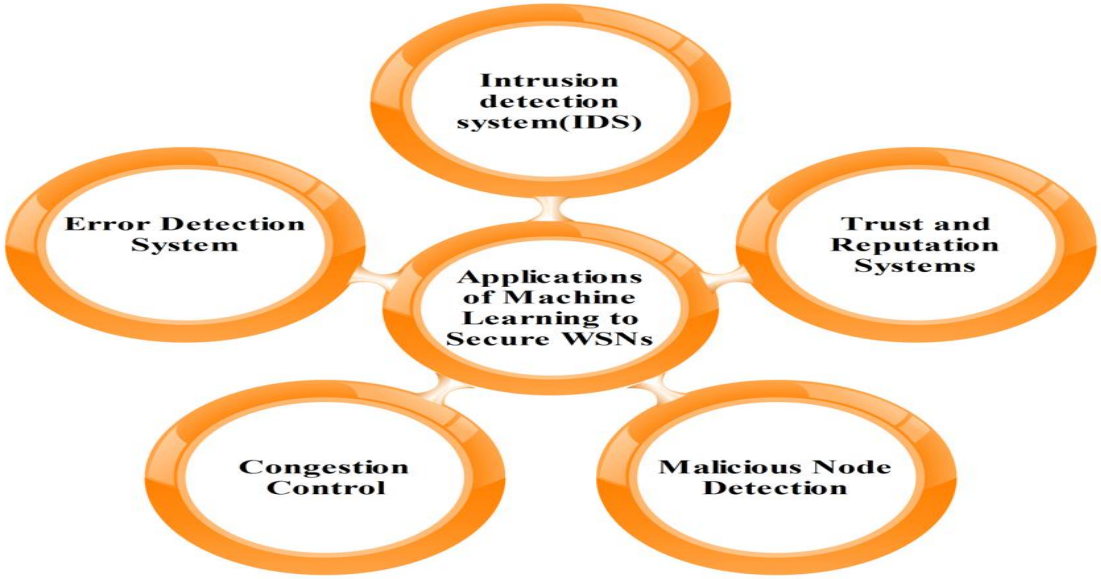

Fig. 5: The Most Important Applications of Machine Learning in Securing WSNs.

3.5.1. Intrusion detection system (IDS)

This is a critical component for protecting WSNs from security threats. By analyzing the network traffic and behavior of the nodes, ML models can identify patterns that indicate an ongoing attack. A well-trained ML model is a powerful tool for developing an effective IDS that can help detect and prevent attacks in WSNs. ML techniques have been successfully used to develop accurate and reliable intrusion detection systems for WSNs. Here are some approaches for intrusion detection using ML in WSNs: Support Vector Machines (SVMs), k-Nearest Neighbor algorithm (KNN), hybrid detection, reinforcement learning, and transfer learning. However, the problem remains with the machine learning training process, so many studies have attempted to improve it by decreasing training time, depending on a small data set, and enhancing accuracy [1, 5, 14, 15, 22, 23, 37, 44, 53].

3.5.2. Error Detection System

In WSNs, error detection is crucial to ensure reliable communication and accurate data transmission. ML is a powerful tool for developing effective error detection mechanisms that can help detect and correct errors in WSNs. By using supervised and unsupervised learning and reinforcement learning, it is possible to develop accurate and reliable error detection mechanisms that can help ensure reliable communication and accurate data transmission in WSNs [22].

3.5.3. Congestion Control

This is an essential aspect of WSNs to ensure trustworthy and efficient communication. ML algorithms can help by evaluating network traffic and identifying the most efficient path. Thus, ML is a powerful tool for developing effective congestion control mechanisms that can help prevent congestion and improve network performance. By using supervised and unsupervised learning and

reinforcement learning, it is possible to develop accurate and reliable congestion control mechanisms that can help prevent congestion and improve network performance in WSNs [22].

3.5.4. Malicious Node Detection

This is an important issue for WSNs due to their vulnerability to security attacks. Thus, ML is a powerful tool for developing effective malicious node detection mechanisms that can help detect and prevent such attacks in WSNs. Several ML techniques have been suggested to detect malicious nodes in WSNs, including algorithms for supervised and unsupervised learning, reinforcement learning, swarm intelligence, ANN, and reputation-based models. It is possible to develop accurate and reliable malicious node detection mechanisms that can help detect and prevent attacks by malicious nodes in WSNs. All these techniques aim to improve the security and reliability of WSNs and prolonging the network's lifespan [23, 31, 36, 44, 55].

3.5.5. Trust and Reputation Systems

Trust and reputation are critical routing issues in achieving secure and reliable communication for WSNs. ML can be used to develop effective trust and reputation mechanisms that can help maintain the integrity of network communications. By using Artificial Neural Networks (ANNs), decision trees, Bayesian networks, reinforcement learning, and game theory, it is possible to identify trustworthy nodes and flag potentially malicious nodes, improving the overall security and reliability of WSNs [14, 16, 36, 53, 56, 57].

4. Future Directions in WSN Security

The current challenges in securing WSNs include resource constraints such as computational power, memory, and limited energy. In addition, sensor nodes are often deployed in uncontrolled, hostile, and unreachable areas, making it difficult to recharge or replace the battery and making them more vulnerable to various attacks. Malicious nodes are also a concern, and various techniques are employed to detect and mitigate them. However, security plays a crucial role in WSNs and is a main issue for several essential applications. Because of the unique constraints and limited resources involved in deploying the sensor nodes, security in WSNs poses additional challenges than in conventional wireless networks. Thus, the security issue is one of the major concerns with WSNs, and several research studies have been conducted to address it [1, 14, 21,22, 23, 25, 36, 37, 38, 44]. Here are the most important open issues and future directions in the security of WSNs, as depicted in Fig. 6

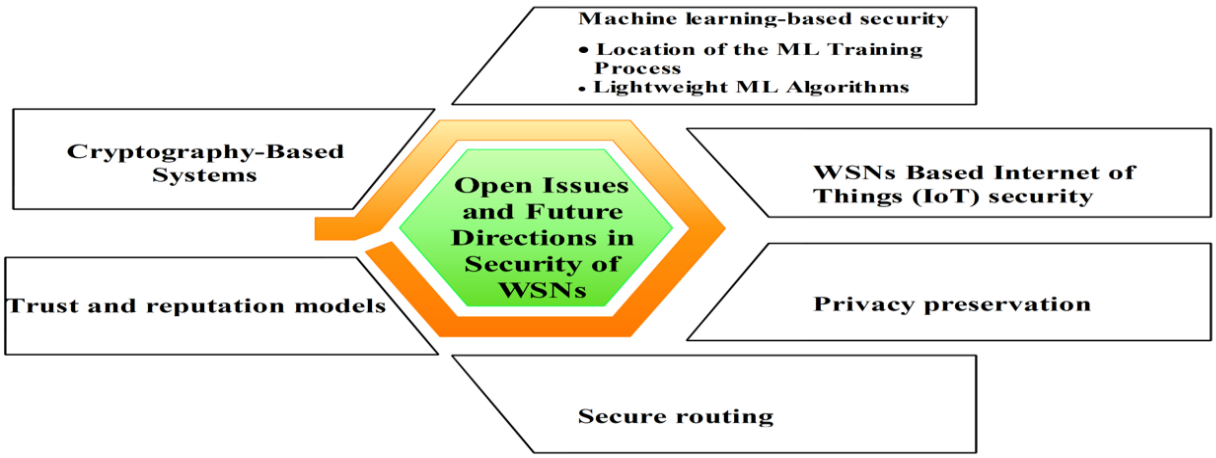

Fig. 6: The Most Important Open Issues and Future Directions in Security of WSNs.

4.1. Cryptography-Based Systems

Cryptography-based systems are used to protect data, but due to resource constraints, they are not appropriate for WSNs. In order to address this issue, security protocols for WSNs incorporate lightweight cryptography algorithms to minimize computing load and memory consumption. However, the current security level is still inadequate to defend against strong and malicious attacks. Thus, researchers suggest combining cryptography-based defenses with intrusion detection systems and security trust models to protect against cyberattacks [22, 37]. Cybersecurity systems must adapt to emerging WSN generations and consider additional constraints, such as underground, underwater, mobile, flying, and space-based sensor networks [37].

4.2. Trust and reputation models

Trust and reputation models can identify and isolate malicious nodes in a way that lightweight security cryptosystems cannot. This can be done by improving the management of WSNs and using ML algorithms to analyze the behavior of adjacent nodes. Additionally, studies have proposed combining trust models with key distribution algorithms and authentication as a means to enhance the level of security [22, 37]. However, the trust and reputation mechanisms using ML algorithms can lead to decreased energy consumption and enhance security protection efficiency compared to conventional trust evaluation schemes [23]

4.3. Secure routing

Routing protocols designed for secure WSNs are an important research area due to the resource-constrained nature of sensor nodes and the potential for routing attacks to disable WSNs. Trust and reputation mechanisms have been presented to improve security and enhance collaboration among nodes, but there are still open research issues such as energy consumption and attack resiliency [6, 11, 14, 15, 36, 37, 48, 58]. Researchers have proposed various secure routing protocols for WSNs, including those that use ML and secure clustering algorithms [16, 22, 23, 36, 41, 44, 53, 57]. Future trends and challenges in secure routing protocols for WSNs include addressing security issues associated with mobile sensors and developing efficient and secure data aggregation and intrusion detection mechanisms [22, 37]. In conclusion, the development of secure routing protocols for WSNs is an active research area with open issues that need to be addressed to ensure the secure and efficient operation of WSNs.

4.4. Privacy preservation

Privacy preservation is critical to protecting the sensitive data collected by WSNs. Future research should focus on developing privacy-preserving mechanisms that can protect the confidentiality and integrity of the data while maintaining its utility. However, an open issue is the privacy requirements, which are an open domain for researchers to research ways to maintain the privacy of sensor nodes from being hacked by peers [22].

4.5. Machine learning-based security

Sensor self-development is essential to maintaining the security of WSNs, and ML techniques are the most suitable option for their self-learning capability. These technologies can detect malicious nodes that are not contained in the existing database list. Thus, ML can be used to develop effective security mechanisms for WSNs, where ML algorithms provide amazing outputs in some fields of security, such as authentication, availability, and analysis of the signal channel [22]. However, they are unable to meet all security requirements in WSNs because they must comply with the limited resource constraints of WSNs when designing routing protocols. However,

future research should focus on developing ML-based approaches for intrusion detection, malware detection, and attack prevention in WSNs [2, 16, 22, 25, 38, 59, 60]. Here are some of the WSN security open issues that require further research using ML algorithms:

- **Location of the ML Training Process:** The most significant issues for WSNs are where to implement ML in the training process, as it is scattered and all its embedded devices are equal in CPU and energy. Existing studies have improved the accuracy of detecting attacks or malicious nodes, but the optimal location for training those algorithms remains unclear. Some authors have utilized Software-Defined Networking (SDN) technology to send training operations to WSN nodes through SDN switches, which is assumed to be a successful idea but requires special protocols to deal with sensor nodes [22]. SDN is a network architecture that separates the control and data planes, providing a centralized controller to manage network resources dynamically. ML can be used to enable automated and intelligent decision-making in network management [22]. The authors in [22] believe SDN technology will be an ideal choice in the future for developing the application of ML algorithms, as it can enhance sensor nodes' competence and lower the cost of use.
- **Lightweight ML Algorithms:** It is not a correct idea to implement complicated ML algorithms to enhance efficiency and accuracy without paying attention to constraint requirements. It is possible to create lightweight hybrid types of ML algorithms that are suitable for operating on embedded devices or to improve the capacity of sensor nodes to differentiate between various types of ML algorithms and autonomously choose the most suitable option based on data type, volume, and remaining energy [22].

4.6. WSNs Based Internet of Things (IoT) security

While WSN-based IoT security has made significant strides, there are still open issues and challenges that need to be addressed. WSN-based IoT security faces several open issues and challenges. Vulnerabilities in the wireless medium and resource constraints make it challenging to design secure WSNs. Conventional security approaches may prove ineffective when applied to WSNs, and the integration of IoT and WSNs has introduced new obstacles in the field of secure network design. However, WSN-based IoT security faces several open issues and challenges, including scalability, energy efficiency, standardization, heterogeneity, privacy protection, and cybersecurity threats. Addressing these issues requires a collaborative effort from researchers, industry, and policymakers to develop secure and reliable WSN-based IoT systems [1, 4, 7, 21, 22, 23, 31, 38].

Conclusions

WSNs are becoming increasingly important, and they are a critical component of the IoT. They have numerous applications in various fields, but their limitations make them difficult to use, making them essential for research. Security is a significant concern in WSNs due to their vulnerability to various types of attacks and the resource-constrained nature of the sensor nodes.

The present work provided a comprehensive overview of WSNs, focusing on their current security issues, the needed security requirements, and the current solutions available to address them. This overview considered the infrastructure, classification, routing issues, and routing protocols of WSNs, as well as the use of trust and reputation approaches for enhancing their routing security. The challenges of security protocols in WSNs are presented, and the available security services and mechanisms are explained. Next, the paper presented a detailed review of the various types of

attacks that can occur in WSNs and investigated the role of machine learning techniques to detect and mitigate malicious node attacks. A discussion of the most important open issues and future directions in the security of WSNs concludes the paper.

CONFLICT OF INTEREST

The authors have no financial interest to declare in relation to the content of this article.

REFERENCES

[1] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of machine learning in wireless networks: Key techniques and open issues," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3072–3108, 2019.

[2] G. Bhatti, "Machine learning based localization in large-scale wireless sensor networks," Sensors, vol. 18, no. 12, p. 4179, 2018.

[3] V. Vijayakumar, "Application of machine learning in wireless sensor network," Journal of Information Fusion, Encyclopedia of Wireless Networks, Springer, pp. 1–7, 2019.

[4] H. Sharma, A. Haque, and F. Blaabjerg, "Machine learning in wireless sensor networks for smart cities: a survey," Electronics (Basel), vol. 10, no. 9, p. 1012, 2021.

[5] C. D. McDermott and A. Petrovski, "Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks.," International journal of computer networks and communications, vol. 9, no. 4, 2017.

[6] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An efficient dynamic trust evaluation model for wireless sensor networks," J Sens, vol. 2017, 2017.

[7] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, "Trust-based attack and defense in wireless sensor networks: a survey," Wirel Commun Mob Comput, vol. 2020, 2020.

[8] C. R. Morales, F. Rangel de Sousa, V. Brusamarello, and N. C. Fernandes, "Evaluation of Deep Learning Methods in a Dual Prediction Scheme to Reduce Transmission Data in a WSN," Sensors, vol. 21, no. 21, p. 7375, 2021.

[9] B. Hasan, S. Alani, and M. A. Saad, "Secured node detection technique based on artificial neural network for wireless sensor network.," International Journal of Electrical & Computer Engineering (2088-8708), vol. 11, no. 1, 2021.

[10] F. Sanhaji, H. Satori, and K. Satori, "Clustering Based on Neural Networks in Wireless Sensor Networks," in Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems, 2017, pp. 1–6.

[11] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," Wirel Pers Commun, vol. 69, no. 2, pp. 805–826, 2013.

[12] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, IEEE, 2007, pp. 335–340.

[13] A. Beheshtiasl and A. Ghaffari, "Secure and trust-aware routing scheme in wireless sensor networks," Wirel Pers Commun, vol. 107, no. 4, pp. 1799–1814, 2019.

[14] H. Rathore, "Case study: A review of security challenges, attacks and trust and reputation models in wireless sensor networks," Mapping Biological Systems to Network Systems, pp. 117–175, 2016.

[15] F. Ishmanov and Y. Bin Zikria, "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues," J Sens, vol. 2017, 2017.

[16] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A survey on trust evaluation based on machine learning," ACM Computing Surveys (CSUR), vol. 53, no. 5, pp. 1–36, 2020.

[17] H. Deng, X. Sun, B. Wang, and Y. Cao, "Selective forwarding attack detection using watermark in WSNs," in 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, IEEE, 2009, pp. 109–113.
[18] Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," Int J Distrib Sens Netw, vol. 9, no. 8, p. 205920, 2013.
[19] H. Alzaid, M. Alfaraj, S. Ries, A. Jøsang, M. Albabtain, and A. Abuhaimed, "Reputation-based trust systems for wireless sensor networks: A comprehensive review," in IFIP International Conference on Trust Management, Springer, 2013, pp. 66–82.
[20] M. M. AlQahatani and M. G. M. Mostafa, "Trust modeling in wireless sensor networks: state of the art," Journal of Information Security and Cybercrimes Research, vol. 1, no. 1, pp. 59–72, 2018.
[21] D. S. Ibrahim, A. F. Mahdi, and Q. M. Yas, "Challenges and issues for wireless sensor networks: a survey," Journal of global scientific research, vol. 6, no. 1, pp. 1079–1097, 2021.
[22] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," Sensors, vol. 22, no. 13, p. 4730, 2022.
[23] J. Zhang, "WSN Network Node Malicious Intrusion Detection Method Based on Reputation Score," Journal of Cyber Security and Mobility, pp. 55–76, 2023.
[24] R. V Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in 2009 international joint conference on neural networks, IEEE, 2009, pp. 1680–1687.
[25] D. P. Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," Information Fusion, vol. 49, pp. 1–25, 2019.
[26] M.A. Alwadi, "Energy efficient wireless sensor networks based on machine learning," PhD dissertation, University of Canberra, 2015.
[27] L.-Y. Sun, W. Cai, and X.-X. Huang, "Data aggregation scheme using neural networks in wireless sensor networks," in 2010 2nd international conference on future computer and communication, IEEE, 2010, pp. V1-725.
[28] A. Akbas, H. U. Yildiz, A. M. Ozbayoglu, and B. Tavli, "Neural network based instant parameter prediction for wireless sensor network optimization models," Wireless Networks, vol. 25, no. 6, pp. 3405–3418, 2019.
[29] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," International Journal of Computer Trends and Technology, vol. 1, no. 2, pp. 9–17, 2011.
[30] J. Zheng and A. Jamalipour, Wireless sensor networks: a networking perspective. John Wiley & Sons, 2009.
[31] S. Babar and P. Mahalle, "Trust management approach for detection of malicious devices in siot," Tehnički glasnik, vol. 15, no. 1, pp. 43–50, 2021.
[32] S. K. Singh, M. P. Singh, and D. K. Singh, "Routing Protocols in Wireless Sensor Networks - A Survey," International Journal of Computer Science & Engineering Survey, vol. 1, no. 2, pp. 63–83, Nov. 2010, doi: 10.5121/ijcses.2010.1206.
[33] A. V. Singh, V. Juyal, and R. Saggar, "Trust based intelligent routing algorithm for delay tolerant network using artificial neural network," Wireless Networks, vol. 23, no. 3, pp. 693–702, 2017.
[34] W. Song and V. V Phoha, "Neural network-based reputation model in a distributed system," in Proceedings. IEEE International Conference on e-Commerce Technology, 2004. CEC 2004., IEEE, 2004, pp. 321–324.
[35] V. Rathod and M. Mehta, "Security in wireless sensor network: a survey," Ganpat university journal of engineering & technology, vol. 1, no. 1, pp. 35–44, 2011.
[36] Z. Xia, Z. Wei, and H. Zhang, "Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks," Comput Intell Neurosci, vol. 2022, 2022.
[37] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," Wirel Pers Commun, vol. 117, pp. 177–213, 2021.
[38] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996–2018, 2014.
[39] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," Procedia Comput Sci, vol. 183, pp. 486–492, 2021.

[40] A. Yasin and K. Sabaneh, "Enhancing Wireless Sensor Network Security using Artificial Neural Network based Trust Model," Int. J. Adv. Comput. Sci. Appl, vol. 7, no. 9, pp. 222–228, 2016.
[41] B. Jaint, V. Singh, L. K. Tanwar, S. Indu, and N. Pandey, "An efficient weighted trust method for malicious node detection in clustered wireless sensor networks," in 2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), IEEE, 2018, pp. 1183–1187.
[42] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks and countermeasures," in The first IEEE international conference on system integration and reliability improvements, Citeseer, 2006, p. 94.
[43] J. Sen, "A survey on wireless sensor network security," arXiv preprint arXiv:1011.1529, 2010.
[44] A. Yaqini and F. Popalyar, "An artificial neural network based fault detection and diagnosis for wireless mesh networks," in 2018 Wireless Days (WD), IEEE, 2018, pp. 107–109.
[45] M. P. Nath, S. N. Mohanty, and S. B. B. Priyadarshini, "Application of machine learning in Wireless Sensor Network," in 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2021, pp. 7–12.
[46] F. Sanhaji, H. Satori, and K. Satori, "Cluster head selection based on neural networks in wireless sensor networks," in 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), IEEE, 2019, pp. 1–5.
[47] O. Khalid et al., "Comparative study of trust and reputation systems for wireless sensor networks," Security and Communication Networks, vol. 6, no. 6, pp. 669–688, 2013.
[48] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," (2006).CSE Journal Articles. 84.
[49] L. Chen, Wireless network Security Theories and Applications. Springer Science & Business Media, 2013.
[50] H. K. D. Sarma and A. Kar, "Security threats in wireless sensor networks," in Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, IEEE, 2006, pp. 243–251.
[51] X. Du and H. H. Chen, "Security in wireless sensor networks," IEEE Wirel Commun, vol. 15, no. 4, pp. 60–66, Aug. 2008, doi: 10.1109/MWC.2008.4599222.
[52] K. Venkatraman, J. V. Daniel, and G. Murugaboopathi, "Various attacks in wireless sensor network: Survey," International Journal of Soft Computing and Engineering (IJSCE), vol. 3, no. 1, pp. 208–212, 2013.
[53] G. M. Jinarajadasa and S. R. Liyange, "A survey on applying machine learning to enhance trust in mobile adhoc networks," in 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE), IEEE, 2020, pp. 195–201.
[54] H.-C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," Wirel Commun Mob Comput, vol. 12, no. 12, pp. 1091–1103, 2012.
[55] B. Rajasekaran and C. Arun, "Detection of malicious nodes in wireless sensor networks based on features using neural network computing approach," International Journal of Recent Technology and Engineering, vol. 7, no. 4, pp. 188–192, 2018.
[56] G. Mahalakshmi, E. Uma, M. Vinitha, and M. Aroosiya, "VANET: Trust Evaluation Using Artificial Neural Network," in Advances in Parallel Computing Technologies and Applications, IOS Press, 2021, pp. 9–17.
[57] Y. Trofimova, A. M. Moucha, and P. Tvrdik, "Application of neural networks for decision making and evaluation of trust in ad-hoc networks," in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2017, pp. 371–377.
[58] Y. Stelios, N. Papayanoulas, P. Trakadas, S. Maniatis, H. C. Leligou, and T. Zahariadis, "A distributed energy-aware trust management system for secure routing in wireless sensor networks," in International Conference on Mobile Lightweight Wireless Systems, Springer, 2009, pp. 85–92.
[59] M. Bhanderi and H. Shah, "Machine learning for wireless sensor network: a review, challenges and applications," Adv. Electron. Electr. Eng, vol. 4, pp. 475–486, 2014.
[60] P. Sarao, "Machine learning and deep learning techniques on wireless networks," International Journal of Engineering Research and Technology, vol. 12, no. 3, pp. 311–320, 2019.