electronics

MDPI

Article

Recent Advances and Future Prospects of Using AI Solutions for Security, Fault Tolerance, and QoS Challenges in WSNs

Walid Osamy [1,2,*,†], Ahmed M. Khedr [3,4,†], Ahmed Salim [4,5,*,†], Ahmed A. El-Sawy [2,6,†], Mohammed Alreshoodi [1,†] and Ibrahim Alsukayti [7,†]

1 Unit of Scientific Research, Applied College, Qassim University, Buraydah 52571, Saudi Arabia
2 Computer Science Department, Faculty of Computers and Artificial Intelligence, Benha University, Benha 13511, Egypt
3 Computer Science Department, University of Sharjah, Sharjah 27272, United Arab Emirates
4 Mathematics Department, Zagazig University, Zagazig 44519, Egypt
5 Department of Computer Science, College of Sciences and Arts, Al-Methnab, Qassim University, Buridah 52571, Saudi Arabia
6 Information Technology Department, Faculty of Technological Industry and Energy, Delta Technological University, Quesna 32631, Egypt
7 Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
* Correspondence: w.elsherif@qu.edu.sa or walid.osamy@fci.bu.edu.eg (W.O.); a.salem@qu.edu.sa (A.S.)
† These authors contributed equally to this work.

Abstract: The increasing relevance and significant acceptance of Wireless Sensor Network (WSN) solutions have aided the creation of smart environments in a multitude of sectors, including the Internet of Things, and offer ubiquitous practical applications. We examine current research trends in WSN using Artificial Intelligence (AI) technologies and the potential application of these methods for WSN improvement in this study. We emphasize the security, fault detection and tolerance, and quality of service (QoS) concerns in WSN, and provide a detailed review of current research that used different AI technologies to satisfy particular WSN objectives from 2010 to 2022. Specifically, this study's purpose is to give a current review that compares various AI methodologies in order to provide insights for tackling existing WSN difficulties. Furthermore, there has been minimal existing related work concentrating employing AI approaches to solve security, fault detection and tolerance, and quality of service (QoS) concerns associated to WSN, and our goal is to fill the gap in existing studies. The application of AI solutions for WSN is the goal of this work, and we explore all parts of it in order to meet different WSN challenges such as security, fault detection and tolerance, and QoS. This will lead to an increased understanding of current AI applications in the areas of security, fault detection and tolerance, and QoS. Secondly, we present a comprehensive study and analysis of various AI schemes utilized in WSNs, which will aid the researchers in recognizing the most widely used techniques and the merits of employing various AI solutions to tackle WSN-related challenges. Finally, a list of open research issues has been provided, together with considerable bibliographic information, which provides useful recent research trends on the topics and encourages new research directions and possibilities.

Keywords: internet of things; fault detection and tolerance; artificial intelligence; security; quality of service; wireless sensor networks

Citation: Osamy, W.; Khedr, A.M.; Salim, A.; El-Sawy, A.A.; Alreshoodi, M.; Alsukayti, I. Recent Advances and Future Prospects of Using AI Solutions for Security, Fault Tolerance, and QoS Challenges in WSNs . *Electronics* **2022**, *11*, 4122. https://doi.org/10.3390/electronics11244122

Academic Editor: Djuradj Budimir

Received: 4 November 2022
Accepted: 7 December 2022
Published: 10 December 2022

1. Introduction

Over the years, the domain of ad hoc network technology has attracted a lot of academic interest [1]. Mobile Ad hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) are the two types of ad hoc networks. When compared to MANETs, WSNs consume less power and contain lower-cost components [2–5]. Many IoT applications require precise discovery of node positions in order to communicate data effectively across nodes [6]. WSN

is recognized as the foundation of IoT and allows for numerous applications [7]. The IoT integration with WSN enables the dynamic interconnection of sensor devices to the internet and execution of tasks more efficiently. WSN offers essential capabilities to applications in research, defense, industry, surveillance, home applications, medical services, catastrophe prediction, and other areas, but it also confronts various challenges due to its resource constraints [8].

The primary goal of this study is to give insight into current Artificial Intelligence (AI) applications in handling different Security, Fault Detection and Tolerance, and Quality of Service (QoS) challenges in WSN. We emphasize major problems in WSN and provide a full discussion on current research that used various AI technologies to accomplish certain WSN objectives in a period of 2010 to 2022. We then provide a systematic assessment and analysis of various AI schemes used in WSNs, which will help the researchers in recognizing the most widely adopted AI strategies to address the Security, Fault Detection and Tolerance, and Quality of Service challenges, as well as the advantages of using different AI methods to address these WSN challenges.

While there are survey articles on studying various issues that WSNs confront, the majority of them concentrated on utilizing AI approaches to tackle a specific challenge, such as data gathering or energy utilization, while others concentrated on overcoming a few of the challenges facing WSN. A related paper addressed or partially examined the literature on AI protocols for overcoming various WSN issues. This study differs from others in that it aims to give a latest review of current literature. We examine several AI approaches that allow us to uncover promising strategies for handling existing WSN challenges and improving the efficiency of WSN, along with multiple optimization techniques that handle various WSN concerns. This survey's main focus is on AI schemes for WSN, where we cover multiple elements in handling diverse WSN concerns such as security, fault detection and tolerance, and quality of service. Furthermore, we conducted a thorough examination and comparison of publications in a period between 2010 and 2022. The article includes a detailed review of 95 relevant publications from credible database sources spanning several academic areas such as AI and computer science. Different AI techniques for WSN enhancement have been explored and classified among the selected papers. The first step is to provide an overview of various strategies. This taxonomy of AI approaches is then used to demonstrate how AI strategies handled each task in WSN. Some articles will be assessed for each category because they may address multiple factors. The research trends that portray the usage of AI in WSN are examined in this study. The study also discusses challenges and possible research opportunities in adopting AI solutions to different WSN problems, with the goal of encouraging future studies.

The study's significant contributions are as follows:

1. We present the most adopted AI techniques to overcome the Security, Fault Detection and Tolerance, and Quality of Service challenges of WSNs. A taxonomy of these AI techniques is also provided.
2. An overview and detailed discussion of current research that used various AI methodologies to accomplish certain WSN objectives between 2010 and 2022 is provided. We include a thorough discussion of the main WSN Security, Fault Detection and Tolerance, and QoS problems that were addressed using AI-based solutions.
3. Fill the gap in existing studies by studying the benefits of employing AI tools to solve the WSN challenges such as security, fault tolerance, and QoS.
4. We provide a detailed comparison of the AI strategies utilized to solve each problem in contrast to existing related work that covered only a portion of the literature by concentrating on single or a few AI approaches. The comparison was performed on multiple aspects such as the proposed approach, AI algorithm, objectives, and performance.
5. With the goal of promoting and facilitating additional studies, we highlight interesting research possibilities in adapting AI schemes to specific WSN issues.

We primarily present an overview and a review of different AI techniques. The applications of AI approaches for tackling the aforementioned difficulties and improving WSN

performance are then shown. The reader will gain adequate knowledge of the challenging concerns in WSNs, as well as the strength of AI approaches in resolving them. The rest of the article is structured as follows: Security challenges and their AI solutions are given in Section 5. Fault detection and tolerance challenges along with their AI solutions are given in Section 6. In Section 7, quality of service and its AI solutions are discussed. We also state the open research challenges while discussing each of the challenges. Section 8 provides the discussion, and finally we conclude the paper in Section 9.

2. Research Methodology

In this section, we follow the same research methodology presented by [9,10]. As indicated in Figure 1, the research methodology used here is separated into four phases. The first phase (Phase 1) involves the selection of articles. The papers are then classified in Phase 2. Phase 3 entails the analysis of articles, which is discussed further in Sections 5–7. Phase 4 entails discussions and future scope, which will be detailed in Section 8.

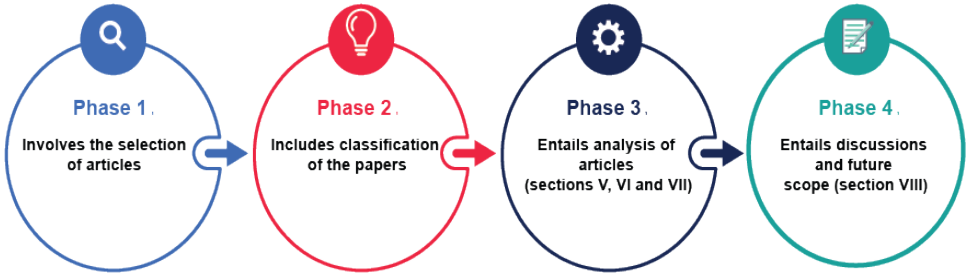

Figure 1. Research methodology.

2.1. Selection of Articles

- **Step 1: Select database sources** The quality of research may be influenced by database sources and key searching tactics. The articles in this study were selected from reputable sources such as IEEE Explorer, Web of Science, and Scopus. Furthermore, only indexed journals are taken into account. To perform a decent search that covers the most relevant matter, the search query and keywords related to the study topic are carefully considered.
- **Step 2: Selection and screening of articles** Research-related terminology, simple phrases, and Boolean operators make up the search queries. The figure in Figure 2 depicts the entire task of forming query strings. To uncover the important relevant publications from 2010 to 2022, search queries are executed on abstracts, keywords, and titles from the selected sources. Journal papers are considered, whereas other categories are omitted. The subsequent search results are gathered and sorted to realize the most important works, rejecting irrelevant, duplicated, or poor quality papers. Furthermore, in order to establish if the filtered papers are eligible for our aims, the abstract is reviewed first, and if it does not provide a sign of eligibility, the article's content is examined. The 95 most significant papers are designated as primary papers using this method.

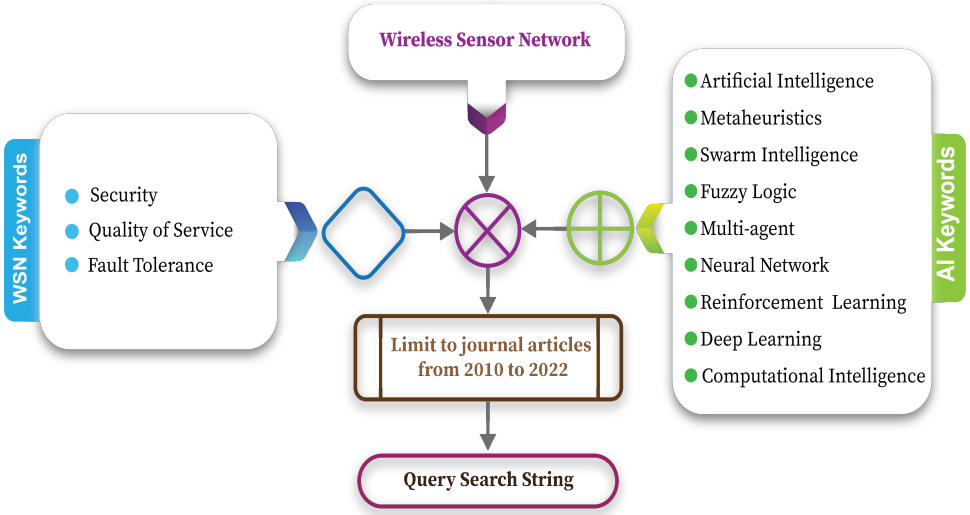

Figure 2. Diagram: search query construction.

2.2. Classification of Articles

Different AI approaches in WSNs have been detected and categorized from primary database sources among the 95 publications examined. Fuzzy Logic, Artificial Neural Networks, Evolutionary Computation, Nature-inspired, Multi-Agent Systems, Trajectory-based, Physical computation, Reinforcement Learning, and Hybrid are some of the approaches employed. In addition, this classification of AI methods is being used throughout the discussion of each problem in WSN to highlight how AI approaches tackled each challenge. Section 3.4 gives an overview of these techniques.

3. Background

In this section, we initially present the security, fault detection and tolerance, and QoS problems in WSNs. Then, various AI approaches for WSNs are discussed.

3.1. Security

Security is an important feature like performance and energy efficiency as the WSN nodes are deployed for use in various applications such as battlefield applications, hospitals, surveillance, monitoring and targeting. So, maintaining security of a WSN is very challenging. Security encompasses different characteristics like authentication, integrity, privacy, and anti-playback [11]. Different threats such as spoofing, changing the routing information, attacking the sink node, information gathering, jamming and denial of service (DoS) attack may affect the performance of WSNs. As the dependency on the information from a WSN has increased, the higher is the risk of secure transmission over the network [12,13]. Various security issues, including node discovery and verification, key establishment [14], node authentication [15,16], secure group management, secure localization, and secure data aggregation [17,18], must be handled in WSNs.

3.2. Fault Detection and Tolerance

Many application domains need WSNs to be deployed in harsh conditions, making them more vulnerable to failures. This exacerbates the design challenge of meeting application requirements that include the challenges such as scheduling, quality of service, fault identification and tolerance. WSNs are vulnerable to faults as they often work autonomously in hostile environments. Besides its characteristics (e.g., storage size, battery capacity), there are several other faults. Fault tolerance represents the capability of nodes to cope with the failure of nodes. For example, in the event of node failure because of power drain, impairment or some other cause, the nodes must be able to decide an alternative

best transmission path. This means that fault identification and fault tolerance strategies for successful fault control are critical and essential to the operation of WSNs [19].

3.3. Quality of Service

We can define QoS as a collection of services that must be fulfilled during source to destination data communication. This corresponds to a networking QoS characteristic that demands the network to have a range of service attributes to track the QoS, such as jitter, delay, bandwidth and packet loss. The main difficulties in establishing QoS are (i) improving end-to-end reliability, (ii) lowering end-to-end latency, (iii) shortening package delivery miss ratio, (iv) lowering bandwidth use, (v) enhancing energy consumption and sensor load balance, (vi) reducing channel access delay, (vii) reducing collisions, (viii) reducing interference, and (ix) optimizing concurrent transmissions [20–22].

3.4. Overview: Artificial Intelligence (AI) Methods

The term AI refers to the study and design of intelligent entities (agents) that observe their environments and act towards achieving goals. An agent could be defined as anything that perceives its environment through sensors and acts upon that environment through actuators. Hence, AI-enabled agents can range from machines truly capable of reasoning to search algorithms used to play board games. Since the birth of AI in the 1950s, various approaches have been applied to create thinking machines. These approaches include symbolic reasoning, logic-based, fuzzy logic, knowledge-based systems, soft computing, and statistical learning. In nature, there exist groups of thousands, millions, or trillions of individual elementary entities that can self-organize into multifarious forms to fit a functional objective purely through local and ordinary interactions. Throughout nature, different organisms often profit from acting in swarms. By shared information, the group could make better decisions than a single individual; this phenomenon is called "collective intelligence". By studying the characteristics of individuals and their relationships with groups, algorithms for the corresponding mechanism, known as "swarm intelligence" have been formalized. These are essentially biologically inspired calculations that have been identified as an emerging topic and a key component of AI [23]. Due to the distributed nature of some systems there is the need for approaches that can learn, plan and make decisions in an environment that involves multiple interacting intelligent agents. The tools to study these problems are provided by a sub-area of distributed AI called multi-agent systems (MAS) [24].

Machine learning (ML) includes a set of supervised/unsupervised methods that try to learn from data, and it is a core subset of AI. This group of AI techniques envelopes methods that can identify patterns in the data in an automatic way, and then use these patterns to predict, and techniques to perform other ways of decision making in an uncertain environment. Learning from interaction is a fundamental idea in almost every learning paradigm such as Reinforcement Learning (RL) [24], Artificial Neural Networks (ANNs) [24], and Deep learning [24] Genetic algorithms (GAs) are stochastic search algorithms which act on a population of possible solutions [25]. GAs are used in AI like other search algorithms to search a space of potential solutions to find the best one that solves the problem [26]. Also in ML, GA is used to search over a class of candidate solutions to find the most effective one [26]. The AI tools such as the optimization tools, forecasting tools (such as time series) and the classification tools (such as the Naive Bayes classifiers) can perform better with the aid of GA [25].

AI is beneficial in addressing a range of challenging issues in several domains owing to its ability to handle deficient and noisy data, non-linear problems, and prediction and generalization at fast speed when trained [27]. The survey's major focus is on AI approaches for WSN. Various AI approaches used in WSN have been explored and categorized. WSNs and AI methods are used in a variety of applications that include:

Agriculture: AI-based WSNs can be combined to improve agricultural productivity and efficiency [28]. Forest fire detection: Feedforward Neural Network (FNN) in con-

junction with WSN can identify firestorms in the forest and by predicting the firestorm in the forest [29]. Intelligent Transportation System: AI-based WSNs can be integrated with Intelligent Transportation System for solving challenges in Intelligent Transportation Systems [30,31]. Health care and smart environments: AI-based WSNs can improve the quality of life for people and provide a smart environment [32–35]. Structural Health Monitoring: Automated Monitoring systems are available as a result of the glue of sensors along with AI methods such as ANN, ML, DL, CNN, Hybrid Intelligence and Cloud Computing [36]. Monitoring: intelligent monitoring devices based on ANN and IoT-based WSNs for observing the amount of charges on different appliances in each household [37].

The following is an overview of various adopted approaches.

1. **Metaheuristics**

   Metaheuristics are used in several optimization problems by employing a degree of randomness to reach near-optimal solutions [38]. Metaheuristic algorithms are classified in a variety of ways. One such scheme is: trajectory-based and population-based [39]. Piecewise style movement in the search space is commonly used in trajectory-based methods to find a single best solution (e.g., simulated annealing). Population-based methods, on the other hand, explore space for numerous solutions and work together to arrive at a final answer (e.g., physical inspired, evolutionary and nature inspired computation). Genetic Algorithm, Differential Evolution and Memetic Algorithm are examples of Evolutionary computation. Central Force Optimization, Gravitational Search Algorithm and Intelligent Water Drops are examples of Physical inspired computation. Nature inspired computations imitate how naturally occurring events interact in diverse environmental circumstances, for example, bat algorithm, cuckoo search and so on [40]. Swarm Intelligence (SI) is the collective behavior that emerges from a collection of social insects, information sharing for learning, self-organization and co-evolution throughout iterations [41]. In order to learn new things and make choices, agents search for neighboring agents and interact with them or the environment. Agents use their expertise to make conclusions and execute appropriate actions in order to fulfill their given goal [42,43].

2. **Learning Methods**

   Without being specifically designed, learning is the capacity to spontaneously acquire new knowledge and enhance it through experience [44]. Examples of such AI methods include Reinforcement Learning (RL), Artificial Neural Networks (ANN), and Deep Learning (DL).

   ANNs have proven effective in handling complicated problems due to their capacity to replicate biological brain networks and human qualities. New data samples can be supplied after an ANN has been trained using training data sets, allowing the trained ANN to be utilized for forecasting and classifying purposes. The capacity to describe non-linear and complicated functions without much disruption between input/output variables is a fundamental benefit of employing ANNs over other approaches. Many problems involving optimization, function approximation, time series analysis, etc., are solved using it. Radial Basis Function network, Multi-Layer Perception (MLP), Back-Propagation, and Recurrent Neural Network (RNN) are examples of ANN designs found in the literature [27].

   RL is a field of AI that deals with how intelligent creatures should behave in a particular situation in order to maximize the idea of cumulative reward. In the RL process, learning is performed by the interaction between the learning entities and their surrounding environment. The three elements of RL are the value function, reinforcement function, and environment. The RL context is frequently dynamic, with a variety of states where each state has a set of feasible options at any given moment [45].

   DL is an interesting AI method using representation learning since it can learn without supervision and from unstructured and unlabeled data. DL design contains several levels and is regarded as a universal learning method that is utilized to solve a wide

range of problems [46]. DL is also utilized to handle big data challenges and produce effective data abstractions and representations [47]. DL differs from other machine learning algorithms in that feature extraction is expressed on numerous hierarchical levels. DL is currently being utilized in a variety of scenarios where intelligent machines is beneficial:

- Humans cannot describe their knowledge (sound, speech, language recognition, and vision).
- The answer must be tailored to a specific situation (e.g., biometrics).
- If the answer to an issue evolves through time, e.g., weather forecasting, predicting stock price.
- Unavailability of human experts (e.g., navigating in Mars).
- High complexity problems for restricted reasoning abilities (e.g., ranking web page, determining advertisement matches in Facebook, sentiment analysis).

3. **Fuzzy Logic (FL)**
   FL is an AI method that mimics how humans make decisions. It is used for uncertain reasoning and partial information management [27]. FL operates on the basis of a "truth-value" range of 0 to 1 [48]. Membership value in a fuzzy set can be any number from 0 to 1. Centroid defuzzification, maximum, and mean-of-maxima citer3 are some examples [45].
4. **Multi-Agent System (MAS)**
   MAS stands for self-organized intelligent system, which models a complex and unpredictable real-world domain with many diverse interacting components, and where system-level qualities are difficult to extract from component properties. MAS is made up of several autonomous intelligent agents, all of which can cooperate to address issues that are above the capacity of an individual agent. Distributed AI incorporates MAS and have been shown to have several applications [43]. Agents address issues and give more flexibility because of their intrinsic ability to analyze and make inferences. Agents learn new contexts and behaviors through their interactions with other agents and the surroundings. Agents then utilize their knowledge to determine and carry out an action in order to complete their assigned objective.

These are some of the most common AI strategies for dealing with WSN problems in recent years. In the following sections, we will provide the current research trends in AI approaches used in WSN. We then discuss the security, fault detection and tolerance, and quality of service challenges in WSN, and highlight alternative strategies to handle these challenges using various AI techniques, as well as open research issues. Furthermore, we compare them to identify appropriate technique(s) for addressing these WSN challenges, as well as open research topics and future scope.

4. Related Surveys

In this section, we present and discuss existing studies and surveys in the security, fault tolerance, and quality of service research categories that are relevant to WSNs. Tables 1 and 2 show a comparison of the existing related surveys.

4.1. Security

The work in [49] provides an overview of WSN attacks as well as mitigating measures against threats in WSNs. A comprehensive review is undertaken in [50] to highlight recent sinkhole attacks in WSNs and associated preventive measures. State-of-the-art systems for managing trust for WSN are studied in [51], their merits and weaknesses, as well as their protection against internal threats, are equally assessed. In [52], WSN threats as well as reactive and non-reactive jammers are studied and explored. Various algorithmic ways to identify jammer threats were also examined and compared. Ref. [53] discussed a review of the literature for trustworthy research on WSNs and security considerations, where a study of important WSN security features is undertaken based on reputable literature,

and various security elements are assessed using security-related characteristics to generate various security criteria. The work in [54] addresses the possibility of reducing the security costs of WSNs using machine learning (ML) algorithms. This paper conducted an analytical study of the recent studies that worked to improve security in WSNs using ML algorithms. Additionally, the authors showed the pros and cons of each study and the promising future trends in this field. Ref. [55] examines the role of ML in solving the challenge of intrusion detection in WSNs.

In [56], several sorts of threats in WSN are addressed and categorized as active/passive. Furthermore, many Intrusion Detection Systems (IDS) were thoroughly studied, with defects in tolerance, service denial, IDS-focused outcomes, trust, DL and functional selection approaches all being investigated. Ref. [57] presents an in-depth examination of the features of different authentication, trust, and key management techniques, as well as the benefits, methodologies, and drawbacks of the existing key exchange, trust and authentication mechanisms in WSN.

In [58], the authors explore several security challenges in WSN and briefly discuss each type of difficulty in order to introduce open research issues. They also addressed how ML may benefit WSNs, and they looked through articles based on ML from 2011 to 2019 to have a better idea of the recent developments in the area of WSN. The study in [59] provides a brief review of 12 articles to handle security and privacy problems in WSN. Ref. [60] discusses the security standards for WSNs and the current security challenges along with the importance of security in WSNs, as well as analyzes the current situation of security problems facing WSNs which includes active and passive attacks that come from internal and external sources. In addition, it discusses reputation and trust in WSNs, its history, significance, concept, and characteristics. The aim of the work in [61] is to analyze cybersecurity and identify the threats generated by WSNs, as well as the encryption algorithms incorporated into WSNs for data security.

4.2. Quality of Service

Due to the changing network environments, varied traffic patterns, and constrained resources, providing QoS to various areas of WSN applications remains a problem [62]. In this context, ref. [62] presents a study of QoS techniques in WSN for computational intelligence driven routing strategies. The work in [63] has a brief discussion on QoS in relation to MAC protocols in WSNs. Ref. [64] studied QoS-guaranteed routing methods for WSN-MANETs. The authors presented a systematic review of QoS parameters in light of ML approaches in [65]. They propose a methodological framework for assessing performance as well as a statistical analysis of ML utilized for QoS indicators during the previous 10 years, from 2011 to 2021. Ref. [66] provides a comprehensive review and analysis of QoS usage in IoT networks and protocols, including QoS-aware IoT architectures, layers-dependent QoS metrics, and resource-optimization methods for IoT networks.

4.3. Fault Detection and Tolerance

A fault detection system examines network status data, narrows the problem range, and locates and detects defective nodes. The fault diagnosis refines the fault type and diagnoses the reason for the network issue based on the fault detection [67]. In this regard, the work in [67] examines techniques and algorithms that can be used to monitor and diagnose defects, and then summarizes the shortcomings and advantages after examining their relevant technology and algorithm. Six ML methods for fault detection in WSNs are summarized and compared in [68]. The most accurate methods were determined to be SVM and DL. In [69], a comparative study of existing fault-tolerant methods is proposed. A new categorization of fault management frameworks has been presented in [19] based on how well they control faults and how many nodes are involved. The frameworks were then examined in terms of their primary issues. A comprehensive classification and analysis of fault tolerance structures and their essential components is presented in [70], as well as a categorization of errors from multiple angles. Several existing automated fault

detection and diagnosis approaches in WSNs are discussed in [71], along with their benefits and drawbacks.

It should be emphasized that earlier work only covered a portion of the literature on using AI approaches to handle security, fault detection and tolerance, and QoS concerns in WSN. This study's purpose is to give a current review that compares various AI methodologies in order to propose new ideas for tackling existing WSN difficulties. Furthermore, there has been minimal existing related work concentrating on employing AI approaches to solve security, fault detection and tolerance, and quality of service concerns associated with WSNs, and our goal is to fill the gap in existing studies. The application of AI solutions for WSNs is the goal of this work, and we explore all parts of it in order to meet several WSN difficulties such as security, fault detection and tolerance, and QoS. A list of open research issues has been provided, together with considerable bibliographic information, which provides useful recent research trends on the topic and encourages new study possibilities.

Table 1. Existing surveys and reviews related to security, fault detection and tolerance, and quality of service in WSNs.

Reference	Year	Title	Limitations
[49]	2020	A Review On Security in WSN	Only consider overview on WSN attacks along with limited discussion about defend techniques against threats in WSNs. AI methods utilization in WSNs not considered.
[50]	2020	Addressing Sinkhole Attacks in WSNs-A Review	Only focus on highlight sinkhole attacks in WSNs and their prevention methods. AI methods utilization in WSNs not considered.
[51]	2020	Trust-based attack and defense in WSNs: a survey	Only focus managing trust for WSN and discussion about their advantages and disadvantages. AI methods utilization in WSNs not considered.
[52]	2020	WSN jammer attack: A detailed review	Only focus reactive jammers along with non-reactive jammers in WSNs. AI methods utilization in WSNs not considered.
[53]	2020	A survey on security requirements for WSNs: focusing on the characteristics related to security	AI methods utilization in WSNs not considered.
[59]	2020	Security and Privacy in WSNs: Advances and Challenges	Limited discussion focus on security and privacy problem in WSN. AI methods utilization in WSNs not considered.
[55]	2021	Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey	Focus on identifying intrusion in WSNs. ML method is only considered.
[56]	2021	Survey On Various Attacks And Intrusion Detection Mechanisms In WSNs	Focus on Attacks and Intrusion Detection problem in WSNs. Limited discussion on Deep learning to handle Attacks And Intrusion Detection was proposed.
[57]	2021	A comprehensive study on key management, authentication and trust management techniques in WSNs	AI methods utilization in WSNs not considered.
[58]	2021	Security issues in wireless sensor network—A survey	Focus on Intrusion Detection problem in WSNs. ML method only considered.
[60]	2022	Review on Security Issues and Applications of Trust Mechanism in WSNs	Focus generally on security challenges and trust mechanisms in WSNs. AI methods utilization in WSNs not considered.
[54]	2022	Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues	ML method is only considered.
[62]	2020	A survey on QoS mechanisms in WSN for computational intelligence based routing protocols	Focus only QoS-aware routing approaches based on CI.
[63]	2020	Review on QoS aware MAC protocols for multichannel wireless sensor network	Limited discussion focus on QoS aware MAC protocols in WSN. AI methods utilization in WSNs not considered.
[65]	2021	A Systematic Review of Quality of Service in Wireless Sensor Networks using Machine Learning: Recent Trend and Future Vision	ML method only considered.
[64]	2021	A Survey of QoS-aware Routing Protocols for the MANET-WSN Convergence Scenarios in IoT Networks	Focus on QoS-aware Routing Protocols. AI methods utilization in WSNs not considered.
[66]	2022	QoS-aware IoT networks and protocols: A comprehensive survey	AI methods utilization in WSNs not considered.
[19]	2020	Fault Management Frameworks in WSNs: A Survey	Not focused on the role of AI methods to fault management problem in WSNs.
[67]	2021	A Review on Fault Diagnosis in WSN	Focus on fault diagnosis in WSN. Limited number of AI methods are considered.
[69]	2021	Survey on fault tolerance-based clustering evolution in WSN	Focus mainly on clustering in WSNs. Fault detection and diagnosis and the role of AI methods are not considered.
[68]	2021	A Review of ML Based Fault Detection Algorithms in WSNs	ML methods are only considered.
[70]	2022	Fault Tolerance Structures in WSNs: Survey, Classification, and Future Directions	ML methods are only handled.
[71]	2022	Automated Fault Diagnosis in WSNs: A Comprehensive Survey	The role of AI methods are not considered.

Table 2. Comparison: Proposed work with existing related reviews of security, fault detection and tolerance, and quality of service in WSNs with respect to different AI methods.

Ref. (Year)	SI	EC	NI	FL	DL	MAS	PC	RL	ANN	Hybrid	ML
[49] (2020)	×	×	×	×	×	×	×	×	×	×	×
[50] (2020)	×	×	×	×	×	×	×	×	×	×	×
[51] (2020)	×	×	×	×	×	×	×	×	×	×	×
[52] (2020)	×	×	×	×	×	×	×	×	×	×	×
[53] (2020)	×	×	×	×	×	×	×	×	×	×	×
[59] (2020)	×	×	×	×	×	×	×	×	×	×	×
[62] (2020)	✓	✓	×	✓	×	×	×	✓	×	×	×
[63] (2020)	×	×	×	×	×	×	×	×	×	×	×
[19] (2020)	×	×	×	×	×	×	×	×	×	×	×
[55] (2021)	×	×	×	×	×	×	×	×	×	×	✓
[56] (2021)	×	×	×	×	✓	×	×	×	×	×	×
[57] (2021)	×	×	×	×	×	×	×	×	×	×	×
[58] (2021)	×	×	×	×	×	×	×	×	×	×	✓
[65] (2021)	×	×	×	×	×	×	×	×	×	×	✓
[64] (2021)	×	×	×	×	×	×	×	×	×	×	×
[67] (2021)	×	×	×	✓	×	×	×	×	✓	✓	✓
[69] (2021)	×	×	×	×	×	×	×	×	×	×	×
[68] (2021)	×	×	×	×	×	×	×	×	×	×	✓
[60] (2022)	×	×	×	×	×	×	×	×	×	×	×
[54] (2022)	×	×	×	×	×	×	×	×	×	×	✓
[66] (2022)	×	×	×	×	×	×	×	×	×	×	×
[70] (2022)	×	×	×	×	×	×	×	×	×	×	✓
[71] (2022)	×	×	×	×	×	×	×	×	×	×	×
Proposed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

5. Security Challenges in WSNs

Numerous security issues in WSNs must be handled, such as node detection and verification, key establishment [12,14], node authentication [15,16], secure group management, secure localization and secure aggregation of data [17,18]. Tables 3 and 4 gives a summary of AI solutions to WSN security issues.

5.1. AI Based Solutions to Security Challenges in WSNs

Rapid advancement and large scale implementations of WSN have both made sensor localization security a critical challenge as well as a serious step. The efficiency of node localization cannot be guaranteed in hostile conditions without appropriate protection measures. In [17], a trust-based scheme for secure WSN localization is proposed using neural network. It performs localization of nodes with the proper evaluation and use of beacon nodes and ensures that the unknown nodes are localized with valid location information. The evaluation model examines the activity of beacon nodes and uses a screening strategy to identify malicious beacons.

WSN gathers sensitive data that must be secured from intruders. The authors of [12] presented a method for ensuring privacy of node locations by applying Ant Colony Optimization (ACO). They introduced an energy efficient and flexible approach for modifying the routing strategy of nodes that makes it hard for an attacker to identify the actual location of nodes. A random strategy for forwarding the packet is achieved through the use of ACO, and this helps in ensuring privacy. Any neighbor node can be the receiver, and it is unlikely to recognize the next-hop node. By tracking the movement of the packets, the intruder therefore cannot infer the position of the source node since the packets are delivered after a random delay. The scheme is efficient in preserving the location privacy of sensors and also enhances the network lifetime. Another intrusion detection system

proposed by [72] is based on point-to-point communication by imitating the web spider hunting procedure, in which the fake WSN nodes acted as spiders and the attacker as prey. To analyze the performance, the authors conducted two tests, one by evaluating the impact of communicating directly between the intruder and the node, whilst the other measuring the response time of nodes with various latencies.

A light weight and dynamic TRUST model is presented in [73]. Honey Bee Mating Algorithm is utilized to restrain a malicious node from becoming a CH and selects the most suitable node as CH. The new scheme is more energy efficient and secure. In [74], a hybrid system that combines spectral clustering (SC) and a sparse auto encoder-based deep neural network (DNN) called SCDNN is proposed. The data set is initially converted into k-subsets according to sample similarity as done in SC. In the next step, the distance between data points in the training and testing set is computed and provided to DNN as input for detecting intrusion. An SI technique to defend from cheating and tampering attacks using a trusted node, called SBTN-TC, is introduced in [75]. The trusted node (TN) is responsible for recognizing the cheating or tampered node by adopting SI. To ensure security in communication between TN and a node, a cryptographic method based on puzzle hiding is utilized.

The authors of [76] developed a secure WSN middleware (SWSNM) using an unsupervised learning algorithm known as generative adversarial network. SWSNM involves two networks, a discriminator (D) and a generator (G). The G generates and merges fake data that resemble the original sample with the original sensor data, which creates confusion for the attacker. The D involves multiple layers and is responsible for differentiating fake data from the original one. The desired output is the actual data interpretation communicated safely in the WSN. The results of implementation depicts that the framework improves data accuracy and security. In [77], a DL-based architecture is proposed to detect the WSN localization attacks. A feature representation scheme based on complex network theory is introduced which integrates location features with topological indexes for enhancing classification performance. Stacked Denoising Autoencoder is adopted to learn and interpret the characteristics of input data. The weights are updated through back propagation. The method is found to be successful in efficiently identifying the Normal Beacons, Replay attacks, Sybil attacks and Interference attacks.

A trust value evaluation model to analyze the trust degree of nodes is proposed by [78]. The scheme, named SRPMA, aims to achieve the goal of maximizing the WSN security with minimal consumption of energy by introducing a secure scheme for WSN routing using multi-objective ACO. SRPMA modified ACO to include the trust value of the routing path and the nodes residual energy as the two objectives for optimization. The final route optimization result is achieved using the Pareto optimal solution method.

A WSN security technique by using attack graph and enhanced binary particle swarm optimization (BPSO) is proposed by [79]. Upon detection of intrusion with the help of an attack graph, a series of weighted security strategies are utilized to analyze the cost for defending the attack. Then, improved BPSO is applied for optimization and selects the minimal cost defense scheme. The optimal security scheme is then determined using M-IDS along with game theory, and Markov Decision Process (MDP) is utilized to further predict and prevent future intrusion by devising suitable defense schemes.

An important security challenge in WSN is the safe transmission of data packets between nodes. As a solution to this challenge, [80] proposed an efficient clustering scheme in which the CH is determined using adaptive Cuckoo Search Optimization (CSO). The method is successful in improving scalability and lifetime of the WSN with reduced delay. A fuzzy based jamming attack detection scheme by incorporating Fuzzy Inference System (FIS) (based on Takagi–Sugeno FL) and adaptive neuro-fuzzy inference system (ANFIS) is proposed in [81]. The two proposed methods make use of RSSI and packet delivery ratio (PDR) for jamming attack detection. The schemes are implemented in CH and BS to determine attacks at CMs and CH. The use of FL helps to optimize the used metrics for

better identification of jammer attacks. The results indicate that the ANFIS-based scheme achieves better performance than the FIS-based scheme.

Another approach for protecting WSNs from jamming attacks is provided in [82], which introduced two schemes to identify the maliciousness level of nodes in clustered WSNs. The first scheme contains two modules named monitoring and certification modules. The monitoring module is responsible for discovering the victim nodes of jamming attacks, and the other module secures the WSN from such attacks. The second scheme uses FL to optimize the metrics for accurate detection of jamming attacks.

A detailed analysis on the application of ML and DL techniques in providing better intrusion detection systems (IDS) for WSN is presented in [83]. The performance is studied and compared with existing adaptive ML-based IDS (ASCH-IDS). Ref. [84] modeled the cooperative communication process using selected relay in WSN as MDP and is based on Deep RL. The proposed DQ-RSS (DQN-based relay selection scheme) involves training of the deep-Q-network(DQN) based on mutual information and outage probability, and the optimal relay selection is achieved without using any prior data or a WSN model. This helps to accelerate the learning process by processing high-dimensional state spaces. DQ-RSS is compared with Q-learning based relay selection technique, and the effectiveness is studied in terms of system capacity, outage probability and energy expenditure. The results prove that DQ-RSS offers better performance with faster convergence than the other schemes.

A secure DL scheme for dynamic WSN-IoT networks based on dynamic clustering is proposed in [85]. The network is developed with Bi-Concentric Hexagons and MS technology to boost energy efficiency. Within the Bi-Hex network, dynamic clusters form, and the best CHs are chosen using the Quality Prediction Phenomenon to ensure energy efficiency and QoS.

Because IoT users can access sensory data, this research also focuses on IoT user security. To authenticate IoT users, they employ a data mining approach. The a priori-based validation algorithm authenticates all IoT users by mapping the best authentication feature set for each user. Ref. [86] proposed a method for obtaining IoT data that is both secure and efficient. Setup, secure data gathering, and reconstruction are the three phases of the proposed approach. The features of primes are used in the setup phase for effective clustering and routing tree method lowers the power expended during data communication. Secure intra- and inter-communication methods are elements of the secure data collection step. The compressive sensing-based data encryption and compression is employed during safe intra-communication procedures. Incorporating Private and Public key schemes while taking into consideration the energy of IoT devices in the secure inter-communication method improves the security performance. Finally, a viable recovery method that is a hybrid of Bees and Genetic Algorithms effectively retrieves actual data from compressed data, thereby improving the data recovery performance.

In [87], a feature selection method that picks the ideal amount of features for detecting identified and unidentified categories of attacks based on an intelligent DT approach is introduced. Furthermore, an intelligent modification to the DT based on fuzzy temporal constraints is proposed for more precisely identifying network traffic and network users. Convolutional neural networks are also used to classify enormous amounts of data. Ref. [88] develops a dynamic smart key management system with the aim to improve the network's security by eliminating cryptanalyzed nodes, increase the network's resistance against cryptanalysis attacks, and minimize memory and energy usage and communication overload. For path key creation and additional nodes insertion, the fuzzy systems of FSDS1 and FSDS2 were used in the design of this system. Malicious nodes that disrupt mobile WSNs are a threat.

A Reinforcement Learning-based malicious node detection model is introduced in [89]. They also devised a reinforcement learning approach for detecting smart harmful nodes and built a strong classifier for detecting these smart malicious nodes that is updated on a regular basis. Ref. [90] examined cyber-physical systems, which are made up of a network of sensor and robotic nodes. The authors have looked into the challenge of connectivity

restoration once multiple nodes die at the same time. The suggested strategy involves a distributed repositioning of the highly eligible nodes in each partition to the center of deployment (CoD). FL is used to choose recovery participants according to residual energy, node rank, and distance from CoD. They tested the proposed methods (connectivity restoration with FL, CoRFL2, CoRFLN) using rigorous simulations and a testbed with a few robots. Ref. [91] presented a privacy preserving data fusion method to enhance secure and reliable fusion of data in WSNs. To reduce energy utilization, the ideal number of CHs is chosen, and adaptive clusters are formed based on node energy and node location relationships. The cluster members then gather and encrypt data, which the CH then cleans and aggregates. Furthermore, CHs and the sink may fuse data within as well as between clusters by assessing data correlation and forming a back propagation neural network for improved data fusion performance.

In the paper [92], a fuzzy rule-based system (called FzMAI) was presented to prevent intrusions in WSN. The suggested technique works by categorizing nodes into three groups: "red," "orange," and "green." The color "red" indicates malicious nodes and should not be allowed into the network. The color "orange" indicates that the node "may be malicious" and should be treated with caution. The color "green" indicates non-malicious nodes. Packet transmit to base station, power usage, packets obtained and packet delivery rate are the parameters used in the method.

In [93], a hybrid solution using MS is introduced to secure the WSN data gathering. The scheme includes a LEACH-based Firefly algorithm, and a Hopfield NN (WSN-FAHN). MS is used to enhance energy efficiency and to maximize WSN life. Firefly algorithm conduct clustering and authentication in two levels is used to overcome DoS attack. Moreover, the Hopfield NN identifies the route of the MS for successful transfer of data from CH.

In [94], clustering is performed by integrating distributed autonomous fashion with fuzzy if–then rules. For routing, an adaptive method that preserves the privacy of source location is suggested. A Principle Component Analysis (PCA) based secure scheme for data collection is utilized to provide end-to-end authenticity and privacy. The work in [95] proposed a complete trust estimation technique to improve power usage, trust, and safety. The dynamic trust is assessed after clustering by integrating direct and indirect trust. Finally, the unified trust mechanism may adjust the parameter and updates the trust level to provide adaptability. A physical danger is posed by a clone attack, in which an attacker may quickly seize a node and steal data from it, then reprogram it to make a copy of the node. As a replicated node cannot be discovered, copies will be dispersed throughout all network regions and dubbed real networkers. The WSN can be either static or dynamic when centralized clone attack detection mechanisms are applied. A promising approach for the identification and categorization of clone nodes is provided in the paper [96]. The preprocessed input data is further normalized to eliminate any undesired content. The best characteristics are chosen for the classification procedure. Modified PSO is utilized in order to achieve the best results. After that, the data is grouped using the K-means cluster scheme. MPSO and the Modified ANN (MANN) are used for training, and MANN helps to identify and categorize the clone attack as normal or harmful. Monitoring illegal movement within WSNs is the most difficult task. The attacker favors mobile malicious nodes because the variety of paths allows him to strengthen his intention. An approach using three-step negotiation is used in [97] to detect the mobile intruder node by employing the mobile agent. Multi-mobile agents are employed in several techniques for WSN data gathering following authentication. However, due to mobility, power expenditure, and latency, authenticating entire nodes in WSN is inefficient. As a solution, clustering is performed, and the corresponding cluster heads are then validated by a mobile agent. In [98], a DL-based intrusion detection process is demonstrated. By leveraging cross-correlation to choose appropriate features, the computational cost of the proposed DNN is lowered. The model efficiently classifies various types of threats in the NSL-KDD dataset. It is compared to traditional ML techniques like SVM, DT and random forests. In [99], different secure routing strategies are proposed to improve packet transmission efficiency;

however, finding the ideal path without compromising reliability is difficult in WSNs. Particle-Water Wave Optimization (P-WWO), an efficient and optimum security routing method, is introduced for data routing along a safe path. The cluster head is chosen using PSO-based cellular automata with fitness value to estimate the secure path required to broadcast the data packets. The suggested optimization utilizes the path maintenance procedure to determine if the packets travel along the designated path or are to be re-routed. Due to its strong capacity to mix and efficiently blend input characteristics to create suitable conclusions about CHs, FISs are the ideal alternative for constructing successful clustering methods for energy-efficient routing protocols in WSN. In [100], fuzzy type-2 based on CS is used for electing CH. In inter-cluster transmission, a threshold-based communication technique as well as a multi-hop routing strategy are utilized for data communication. Intrusion detection models are defined to analyze occurrences that exceed security controls and expose regular data flow to risk. Ref. [101] proposed an approach to analyze the traffic flow processing time in the existence of an attacker, but it has no influence on the unfairness of the traversing flow. The use of Graph Neural Networks to conserve network flow from source to sink is being implemented. This successfully identifies the presence of traffic flow fairness in multi-hop transmission with resilience to variable connections. Because localization procedures completely rely on nearby relations to infer the position of nodes, WSNs are extremely sensitive to localization threats. Ref. [102] proposed methods for localization threats, independent and collusion threats. The Improved Randomized Consistency Position Technique is the first method they offer for determining the position of unknown nodes and the PSO to identify the unknown nodes' coordinates. The other is Enhanced Attack-Resistant Secure Localization Technique, which is a mix of voting technique, position optimization, and PSO for identifying the position of unknown nodes. The work in [103] introduced a security model for WSNs. It can withstand the majority of known network intrusions without dramatically affecting the power usage of nodes. It also ensures security by calculating trustworthiness and forming mutual trust between trustworthy nodes, as well as operating the trust evaluation system using a centralized strategy. Finally, based on the LEACH contract, it suggests a novel safety structure suitable for securing the WSN.

In [104], a hybrid method of PSO and GWO is employed for secure data communication and power efficiency. To realize the environment, a Learning Dynamic Deterministic Finite Automata (LD2FA) is proposed and implemented. The main purpose of LD2FA is to send the learned and approved string to a hybrid model in order to optimize the paths. Ref. [105] suggested a simple system known as the cuddling death model, which is based on the Artificial Bee Colony algorithm (ABC). The goal of the strategy is to locate any unfit or fraudulent cluster heads in the WSN and replace them before they pose a danger to any of the other nodes within the WSN. Due to suspicious occurrences such as replication nodes, some nodes in the WSN have to expend high energy. To eliminate data loss and save power usage, the node replication must be anticipated. The authors of [106] developed a unique method for node identity verification based on Whale optimization to recognize replicating nodes in a Mobile WSN. The objective function is employed to determine each node's power consumption and to discover precise replicating nodes. After establishing the needed number of nodes, the specifications of each node are recorded, and the replicating node is discovered during the screening and predicting phase by examining the node's characteristics and conduct. The work in [107] aimed to enhance different QoS metrics such as latency, hops and energy by proposing a power effective and secure routing scheme based in fuzzy logic and trustworthiness values of nodes. The node's instant as well as overall trust is examined for efficient and safe routing. Ref. [108] proposes an intrusion detection scheme to satisfy the QoS metrics such as energy, security and lifetime. In this, a neuro-fuzzy model is used for clustering. Then, optimal heads are decided based on Deer Hunting Optimization method (DHO). A cross layer protection method based on fuzzy logic and trust values is proposed in [109]. It employs several parameters retrieved from cross-layer data to mitigate the impacts of safety threats in WSN. The fault tracking

mechanism uses an enhanced CNN model based on trustworthiness to discover malicious nodes in WSN.

In [110], a secure method using fuzzy and dragonfly algorithm (DA) is utilized for data aggregation. Using fuzzy scheduling, the data transmission rates are adapted and an aggregation tree between CHs is built for inter cluster aggregation. A fuzzy scheduling system is used to adapt the appropriate data transmission rates of cluster member nodes during the intra-cluster data aggregation phase. An aggregation tree is built between the cluster head nodes during the intercluster data aggregation phase. To discover the best aggregation tree between CHs, DA is applied. A modified Residue Number System (RNS+) based encryption scheme is used for securing the data transmission. An enhanced model based on PSO and SVM is introduced for intrusion detection in [111]. The results suggest that this model boosts the detection rate of new threats while improving the accuracy of unknown threats. Moreover, adequate SVM parameters are chosen to avoid excessive or low fitting problems. Ref. [112] developed a Multi-Ant Colonies based Routing Mechanism scheme based on enhanced ant meta-heuristic and an enhanced trust evaluation strategy. Ref. [113] presented an attack recognition model using fuzzy and feed-forward NN where five types of attack on routing is examined and successfully identified to enhance QoS and overall network performance. The feed-forward NN is trained using fuzzy rules, and the accuracy level is assessed using experiment. The findings show that the suggested model outperforms others in terms of prediction accuracy.

5.2. Open Research Issues and Challenges

In the future, safe trust-based routing and trust management solutions will be necessary since WSNs face multiple security risks and system failures. Future work in this approach will include the employment of intelligent agents for distributed communication, as well as system testing on a real network test bed to improve and evaluate performance. In addition, using several MSs to minimize energy usage in WSNs is advised. Performance experiments using different attackers to examine the reply times can be conducted to enhance the existing works. This can help in developing a better model, extending the work to larger networks with more sensors, considering the sensor nodes' mobility and challenging communication models to investigate their influence on real WSNs.

Additional aspects of a real-time localization threat recognition system for realistic WSNs may be researched and implemented to secure localization schemes by employing AI techniques. To increase the applicability, creditability, and reliability of the assessment findings, more criteria must be addressed in trust evaluation and under various network circumstances. Other aspects of node localization efficiency, such as processing expenses and communication cost, must be looked into and evaluated. Study into effective data fusion strategies for WSNs, extraction of features, data communication privacy and location privacy preservation will all require more attention in the future.

Data protection and resilience in WSNs is a relatively recent subject of study. Since network resources are limited, energy efficiency, computational efficiency, and overall quality of performance must be taken into account. To build an ideal protection mechanism, further study is required. In future research, security and protection for the task of data aggregation must be ensured using methods like digital signature and watermarking. This assures data integrity.

Table 3. Summary of AI-based solutions to WSN security problems discussed in Section 5.

AI Techniques	Algorithm	Ref.	Objectives	Implementation	Approach	Mobility	Performance Metrics
SI	ACO	[75]	Tampering and Cheating Attack	Not specified	Distributed	Static	Residual Energy, Packet Delivery Ratio, Packet Drop and Overhead.
SI	Ant Colony Algorithm with Multi-objective (SRPMA)	[78]	Increase residual energy of nodes and the trust value of a route path	NS2 simulation	Distributed	Static	Packet loss rates, Routing loads, and Average energy consumption.
SI	Binary PSO	[79]	Minimizing key strategy set	Simulation	Centralized	Static	Average number of iterations, and Average calculation time of a single iteration.
SI	ACSO	[80]	Optimal CH selection	PYTHON simulation	Distributed	Static	Performance value of Bandwidth and Bit Error Rate, Rate of Packet Delivery, Sensitivity, QoS, Decryption Time, Encryption time, and Accuracy.
SI	Honey Bee mating	[73]	CH selection	Test bed	Distributed	Static	Network effectiveness, Scalability, and Average residual energy.
SI	Web Spider	[72]	Intruder detection in the WSN	Real test bench	Centralized	Static	Response time.
SI	EELP	[12]	Preserve sensor's location	Simulation	Centralized	Static	Scalability, Fault Tolerance, Latency and Energy difference.
SI	PSO	[102]	Solve the sensor localization estimation problem under the localization attacks in WSNs	C# simulation	Centralized	Static	Positioning success rate, average positioning error of positioning methods, success rate of changing the number of malicious nodes.
SI	Artificial Bee Colony	[105]	Secure scheme for the organization of WSNs	MATLAB simulation	Distributed	Static	Energy consumption, packet delivery ratio, energy efficiency, authentication delay, and throughput.
SI	Multi-Ant Colonies (MACRAT)	[112]	Enhance security in WSN using trust, Increase network life, Choose the path with the least number of hop to destination and High throughput	MATLAB simulation	Distributed	Static	Packet loss rate, exchange latency, malicious nodes detection rate, error rate, transmitted data receiving rate, and throughput rate.
SI	Particle Swarm Optimization	[111]	Improve the detection accuracy and convergence speed of intrusion detection	MATLAB simulation	Distributed	Static	Detection rate, accuracy, and false alarm rate.
SI	Whale-based Node Identity Verification (WbNIV)	[106]	Detecting replication nodes in the Mobile WSN	MATLAB simulation	Distributed	Mobile	Accuracy, packet drop and delay rate and power consumption.
FL	FIS and ANFIS	[81]	Jamming detection metrics	MATLAB simulation	Distributed	Static	RMSE, ANOVA test, and true detection ratio.
FL	FIS	[82]	True detection ratio, false detection ratio	MATLAB simulation and NS2 simulations	Centralized	Static	True detection ratio, undetection ratio and false detection ratio.
FL	FzMAI	[92]	Avert intrusions	NS2 simulation	Distributed	Static	Sensitivity, Positive Predicted Value, and Negative predicted Value.
FL	DSKMS	[88]	Key management	NS-Alinone-2.35 simulation	Distributed	Static	Memory space requirements, communication overload, and energy usage.
FL	CoRFL, CoRFL2, and CoRFLN	[90]	Select best recovery candidate	MATLAB simulation and Prototype-based Experiments	Distributed	Mobile	Traveled Distance Per Partition, Recovery Team Energy, Total Traveled Distance, Total Replacement Travel Distance, Average Movement Per Node, Messaging Overhead, and Running Time Complexity.
FL	IDAF-FIT	[94]	Secure Data Aggregation in WSN	Tiny OS	Distributed	Mobile	Network lifetime, packet delivery ratio, packet dropping ratio, residual energy and energy consumption.
FL	CLS-FLTCM	[109]	Identify malicious nodes on the network	NS-2 simulation	Centralized	Static	Detection accuracy, false-positive rate (FPR), and fake-negative rate (FNR).
FL	SUCID	[108]	Secure unequal clustering protocol with with intrusion detection	MATLAB simulation	Distributed	Mobile	Energy Efficiency, Network Lifetime, and Average Delay.
FL	SEORMP	[107]	Secured and energy-efficient routing	NS2 simulation	Distributed	mobile	Packet Transmission Ratio, Energy level, and Network Lifetime.

Table 4. Summary of AI-based solutions to WSN security problems discussed in Section 5.

AI Techniques	Algorithm	Ref.	Objectives	Implementation	Approach	Mobility	Performance Metrics
Hybrid	PSO and GWO	[104]	Optimal route	MATLAB simulation	Distributed	Static	Consumption of energy, network lifetime, throughput
Hybrid	fuzzy type-2 and CSO	[100]	Overcome the limitations in clustering algorithms by optimizing routing protocol, and trust management	Matlab simulation	Centralized	Static	total energy consumption, energy balancing, and network lifetime.
Hybrid	PSO and WWO	[99]	Optimal secure routing algorithm	PYTHON simulation	Distributed	Static	Energy balancing index, coverage, number of alive-nodes, and average energy.
Hybrid	FL and dragonfly	[110]	Secure data aggregation	NS-Allinone-2.35 simulation	Centralized	Static	consumed energy, Processing time of the sensor nodes , end to end delay, Network delay, Network lifetime, and Packet delivery rate.
Hybrid	GA and BEEs	[86]	Minimize reconstruction error	Simulation	Centralized	Static	MAPE, Average consumed energy, standard deviation, ANMSE, and Network lifetime.
Hybrid	FL and CNN	[87]	Intrusion detection	NS2 simulation	Distributed	Static	Comparative analysis, Packet delivery analysis, and Delay analysis.
Hybrid	of FL and FFA	[93]	Prolong network lifetime	NS2 simulation	Distributed	Static	Misbehaving sensor ratio, Residual Energy, and Throughput.
Hybrid	MPSO and MANN	[96]	The detection and classification of clone node	Not specified	Distributed	Mobile	Packet delivery ratio and detection ratio.
Hybrid	FL and FFNN	[113]	Intrusion detection	NS2 simulation	Distributed	Static	Accuracy, precision, recall, F-score, and specificity.
DL	SCDNN	[74]	Attack detection	Simulation	Centralized	Static	Accuracy, recall, Error rate, and Specificity.
DL	SWSNM	[76]	Reduce energy consumption	Python simulation	Centralized	Static	Energy usage, End-to-End Delay and Throughput.
DL	RBC-IDS	[83]	Increase accuracy rate	NS3 simulation	Centralized	Static	Accuracy Rate, Detection Rate, False Negative Rate, F1 Score curve, and Receiver Operating Characteristic curve.
DL	DQ-RSS	[84]	Cooperative communications with relay selection	Simulation	Centralized	Mobile	Performance convergence and Energy consumption.
DL	SDALAIA	[77]	Increase average classification accuracy	Simulation	Centralized	Static	The number of hidden layers, back-propagation, the ratio of suspicious beacons, and beacon density.
DL	Secure DL	[85]	Improve energy efficiency	NS3 simulation	Centralized	Static	Analysis on Encryption time, Analysis on delay, and Analysis on throughput.
DL	Deep neural network	[98]	Detect unauthorized access to improve the security features of WSNs	MATLAB simulation	Distributed	Static	Accuracy, precision, recall, and f1-score.
DL	GNNSFR	[101]	Intrusion detection	NS-2 simulation	Centralized	Static	Energy consumption, Packet size, Attack interval, Execution time, and end to end delay.
RL	Neural Network	[89]	Detect malicious nodes	Simulation	Centralized	Mobile	Detection accuracy and False detection rate.
ANN	Neural Network	[17]	Increase accuracy of sensor localization	Simulation	Centralized	Mobile and Static	Average localization error.
ANN	Back propagation Neural Network	[91]	Minimize the network energy consumption	OPNET simulation	Distributed	Static	Network lifetime, Average residual energy, Death of nodes, Data fusion efficiency, and Privacy leakage probability.
MAS	MWC-DTE	[95]	Enhance the energy consumption, trustworthiness and security	MATLAB simulation	Centralized	Static	Analysis of the trust value for malicious node, normal node, and dead node.
MAS	Mobile agent	[97]	Identifying the mobile malicious	Not specified	Distributed	Mobile	Traffic overhead, mobility, delay, energy consumption, and drop ratio.
NI	Biological immune system	[103]	Developed a trust management system based on clustered WSN	Not specified	Distributed	Static	Collusion and Oscillation Attack Experiment, Energy Difference between Nodes, Number of alive nodes.

6. Fault Detection and Tolerance Challenges in WSNs

This section discusses various fault detection and tolerance challenges in WSNs and their solutions through diverse AI methodologies. The continually changing topology of the network requires mechanisms to achieve self-organization and tolerance to faults. It is critical in the case of WSN applications owing to changes that may occur in the network as well as the underlying applications. As a result, the researchers are concentrating their efforts on the creation of AI-based intelligent models for creating self-organizing and fault-tolerant WSNs.

Table 5 gives the summary of the AI-based solutions to fault detection and tolerance challenges discussed in Section 6.

6.1. AI Based Solutions to Fault Detection and Tolerance Challenges in WSNs

In [114], a technique for fault detection of nodes in WSN based on PSO is presented to address the high energy consumption issue and difficult computations in previous methods. The threshold value range is determined by optimizing the measured data of nodes using the PSO's rapid convergence rate and simple principles.

In [115], a primary/backup strategy is employed to create a soft fault-tolerant task allocation system in real-time. The discrete PSO building approach is achieved by using a binary matrix encoding procedure to reduce job execution time, minimize node energy costs, load handling, and establish a objective function to improve scheduling efficiency and network stability. Additionally, it uses simultaneous passive backup copies and may adaptively assess backup copy mode by arranging main copies as soon as feasible and backup copies as slowly as possible. In [116], a PSO-based fault-tolerant and unequal cluster model termed PSO-UFC is discussed. The PSO-UFC protocol uses an uneven clustering technique in order to solve the unbalanced clustering problem. The network connection is also recovered by picking an additional CH called Surrogate CH, which overcomes the unexpected Master CH loss.

A distributed filtering strategy is designed to cope with the fault tolerance challenge in nonlinear stochastic systems with WSNs [117]. Interval type-2 Takagi-Sugeno (IT2 T-S) fuzzy scheme describes the nonlinear stochastic models of discrete-time form. Each WSN sensor may obtain measurements subject to deterministic interconnection from itself and its neighboring nodes in the topology. A fault reference scheme also improves the efficiency of the model. A novel defect detection framework is designed in this model. They used the Lyapunov functional approach to assess the reliability and performance of the developed defect detection system. In the design process, new approaches are used to solve the decoupling problem. The desired parametric matrices of fuzzy filters are built in compliance with the parameters laid down, which is an essential prerequisite of reliable medium-square asymptotic stability for the overall disruption attenuation performance in the fault detection method.

A fault tolerant routing mechanism, using ABC and PSO algorithms, for mobile WSNs (MWSN) is introduced in [118]. Their work focused on creating a reliable and robust data transmission environment with the help of an efficient route recovery strategy, which could offer enhanced lifetime and energy efficiency for MWSNs. A feed-forward NN trained using a hybrid meta-heuristic algorithm that blends the ideas of exploitation and exploration of the search space is used in [119]. For both nodes and connections in the WSN, the implemented approach is successful in identifying composite faults such as soft permanent, hard permanent, transient, and intermittent faults. Moreover, the technique can categorize various types of faulty behavior of nodes as well as links in the WSN,

A modified PSO (MPSO) based fault detection in WSN suitable for use in monitoring 3D structures is proposed in [120]. After formation of WSN by placing the nodes on 3D structure, the nodes send a signal to the destination. This is done to ensure if there is any obstacle or problem in the path. MPSO is applied to determine the optimal solution. After that, the shortest path between any two sensors is determined using Dijkstra's algorithm. The bandwidth is then analyzed using link fitness, and the round trip time is

calculated to see if the path is good or not. The defects are identified using the accumulated data received at the sink. This is a reliable and resilient method for 3D constructions' health monitoring with a small number of sensors.

The constrained resources and diverse deployment environments make fault detection a challenging task in WSNs. In [121], six classifiers are applied and analyzed, which include: Multilayer Perceptron, Support Vector Machine, Stochastic Gradient Descent, Convolutional Neural Network, Probabilistic Neural Network, and Random Forest (RF) on the prepared data-set. The evaluation is done according to the performance measured using the metrics: True Positive Rate, Matthews Correlation Coefficients, F1-score and Detection Accuracy. The analysis shows that the RF classifier outperformed the remaining classifiers in terms of the mentioned metrics.

A distributed FL-based defective node detection technique for heterogeneous WSNs is described in the paper [122]. In the case of events such as fire and transient failures, each sensor node can accurately identify its condition using this technique. The approach allows for recognizing and isolating problematic nodes in heterogeneous WSNs, as well as the recognition of network events (such as fire) and a reduction in false positives. To do so, each node employs a FL Controller (FLC), which multiplies the weight of the values detected by neighboring nodes by different parameters. When the majority of nearby nodes have detected different values from the tester node, the tester node might determine that it is malfunctioning and enter the sleep mode.

The authors of [123] established a fault tolerance scheme to overcome errors that arise due to link/node failure during data transfer from nodes to sink. It includes an improved-handoff (Imp-Handoff) mechanism to offer fault tolerance during node failure, as well as an enhanced quadratic minimum spanning tree (Imp-QMST) approach to discover the alternative connection if it fails due to different situations. In addition, four SI methods (ACO, PSO, Imperialistic Competitive Algorithm, and Firefly algorithm) and also the PRIMS algorithm have been used to construct MST to improve the data collection performance.

The work in [124] provides a method for fault detection and classification using continuous density hidden Markov model (CDHMM) and multiple neural networks (NNs) hybridization, including probabilistic neural network, learning vector quantization, radial basis function and adaptive probabilistic NN. Hybrid models of each NN are used to classify sensor defects, such as bias, drift, and random faults. The suggested methods are analyzed using multiple performance measures, including precision in detection, Matthews correlation coefficient, false positive rate, and F1-score.

A pre-fault detection mechanism for multilevel communication, which is based on fuzzy rules in distributed WSNs, is discussed in [125]. To determine forwarding decisions, it employs a fuzzy rule set. A fuzzy decision rule set is used to execute routing based on a node's fuzzy fault score state. To conserve energy and increase performance, the method performs advance diagnosing of fault and determines the best path. The data communication rate is set based on the node failure state to avoid unnecessary energy usage.

A neuro-fuzzy optimization scheme for WSNs is proposed in [126]. To identify problematic nodes, the fuzzy estimator is utilized. When the primary fails, traditional techniques use a centralized method to eliminate problematic nodes. In contrast to this, the fuzzy estimator technique is used to identify and classify the problematic nodes.

The goal of the research in [127] is to investigate the energy efficiency and fault handling challenges faced by the traditional LEACH-based approach. It uses a random CH voting approach to accomplish dynamic use of resources with little regard for the nodes' residual energy levels. In sophisticated obstacle conditions, the Q-Learning algorithm calculates the best path for data communication. CH node uses the auxiliary data to proactively determine the next hop, resolving the blind search problem. This approach considerably improves the algorithm's quality of learning and speed of convergence.

A smart fault tolerance technique is developed in [128] to improve the resilience of IoT-WSNs. Regular and special are the two categories of nodes considered in this work. The Maximum Coverage Location Problem approach is utilized to discover the best loca-

tions for special nodes after regular nodes are deployed at random in the region. Clusters are established depending on special node's communication range once the best locations have been found. Then, a Multi-objective Deep RL scheme finds the malfunctioning nodes with the least amount of energy usage. Moreover, for optimization of Q-values, Double DNN is employed. Ultimately, in each iteration, data is collected from special nodes using a mobile sink.

The cluster-based fault tolerant routing scheme presented in [129] is a hybrid model of FA and GWO. The proposed method increases the network's QoS. Metrics including the node's energy, gateway load, distance between node to CH/BS, hop-count, and QoS are among the fitness functions. The proposed fault-tolerant mechanism permits data routing to nearby nodes if one node failure occurs. For validation purposes, the fault model adopted is Weibull distribution.

6.2. Open Research Issues and Challenges

The future work in this area can focus more to expand the scope of the application. Recommendations for further research in fault-tolerance should be encouraged to decrease unneeded redundancy by incorporating technologies such as active backup overlapping technology or others. The fault tolerance model that was used for statically installed sensor nodes may be modified and validated for dynamic deployment settings; additional security protocols and regulations can be added for further investigation.

For non-linear systems with sophisticated constrained communication, such as the network-induced latency restriction and the event-triggered process in WSNs, extended works can be devised. Researchers should focus more on assessing the correctness of sensed data in future research and studies by using meta-heuristic algorithms to discover more trustworthy nodes with fewer defective attributes.

Hidden Markov Model (HMM) based approaches like Weibull distribution and Bath-tub distribution might be used to diagnose and forecast the remaining usable life and aging profile of the sensors. In a real-time context, a hybridized algorithm may be used to identify errors online. Alternative algorithms can be used to overcome issues relating to training speed.

In terms of training and implementation, maintaining small training sets will help you save time throughout the training phase, especially when it comes to online defect detection. The efficacy of different classifiers in detecting an incoming data failure may be investigated further so that a better system for fault prevention can be established.

Additionally, fault detection in WSNs necessitates a higher degree of attention in order to effectively identify and detect abnormalities at the sensor node level. The algorithm's resilience may also be tested by altering the number of nodes. This will allow researchers to determine how robust a WSN is to threats in various network circumstances and react accordingly. In the future, studies on guaranteeing the security using cryptography techniques to help WSNs for real time, resilient and energy efficient tolerance against faults can be explored.

Table 5. Summary of AI-based solutions to fault detection and tolerance surveyed in Section 6.

AI Techniques	Algorithm	Ref.	Objectives	Implementation	Approach	Mobility	Performance Metrics
SI	MPSO-SHM	[120]	Path optimization	Simulation	Centralized	Static	Routing overhead, Throughput, Packet delivery ratio, End to end delay and Average message overhead.
SI	PSO	[114]	Diagnose the fault nodes	MATLAB simulation	Centralized	Static	Diagnosis accuracy and Convergence rate.
SI	FTAOA	[115]	Fault-tolerant task allocation	Simulation	Distributed	Static	Rate of convergence, Energy consumption, Deadline missing ratio, Execution time consumption, Reliability cost, and Network lifetime.
SI	PSO	[116]	Construct a multi-hop routing tree between the CHs with the optimum number of clusters	MATLAB simulation	Centralized	Static	Total energy consumption, Residual energy, and Network lifetime.
Hybrid	Firefly Optimization (FA) and Grey Wolf Optimization (GWO)	[129]	Enhance lifespan	Matlab simulation	Distributed	Static	network lifetime, average rate of success, nodes survival ratio, and end-to-end latency.
Hybrid	Imp-QMST, Imp-Handoff	[123]	Fault-tolerant and improve quadratic minimum spanning tree	MATLAB simulation	Centralized	Static	End-to-End Delay, Energy consumption, and Throughput.
Hybrid	ABC and PSO (IABC)	[118]	Reduce energy consumption	MATLAB simulation	Centralized	Static with MS	Network reliability, Network connectivity, Packets loss rate, and Energy utilization rate.
Hybrid	ANN and combination of gravitational search algorithm (GS) and particle swarm optimization (PSO)	[119]	Fault diagnosis	Testbed and Matlab simulation	Centralized	Static	Mean squared error, False positive rate (FPR), False alarm rate (FAR), and False classification rate (FCR).
FL	IT2 T-S Fuzzy	[117]	Fault detection	MATLAB simulation	Distributed	Static	Plant reactions to disturbances and faults, residual signal, weighting fault signals and their mistakes, and state responses.
FL	EAPFM	[125]	Detect faulty nodes and find best suitable path for routing	Matlab simulation	Distributed	Static	Fuzzy fault count, Data delivery rate, and power usage.
FL	ANFIS estimator	[126]	Detect faulty nodes	Matlab simulation	Distributed	Static	Fault detection accuracy.
FL	FIS	[122]	Fault detection	Omnet++ and MATLAB simulations	Distributed	Static	Detection accuracy and Number of false positives.
ANN	CDHMM	[124]	Sensor Fault Detection and Classification	Matlab simulation	Centralized	Static	F1-Score, Average detection accuracy, False Positive Rate, and Detection accuracy.
RL	Q-Learning algorithm	[127]	Analyze the energy conservation and fault-handling problems inherent in the classic LEACH-based technique	Matlab simulation	Distributed	Static	Energy efficiency, Life Cycle, Delay Time, Perception accuracy, Scalability, and Fault tolerance
DL	Multi-Objective Deep RL (MO-DRL)	[128]	High precision and low complexity detection of defective nodes	NS-3.33	Distributed	Static with mobile sink	Fault Detection Accuracy (FDA), Network Lifetime, False Alarm Rate (FAR), False Positive Rate (FPR), and Throughput.
DL	SVM, CNN, MLP, SGD, RF, and PNN	[121]	Fault detection in WSNs	PYTHON simulation	Centralized	Static	Detection Accuracy and True positive Rate.

7. Quality of Service Challenges in WSNs

This section discusses various QoS challenges in WSNs and their solutions using different AI techniques. The inclusion of AI techniques in WSNs has been proved to be helpful in enhancing the network performance. QoS-driven algorithms based on AI are gaining increased attention from researchers.

Table 6 gives the summary of the AI-based solutions to Quality of service challenges discussed in Section 7.

7.1. AI Based Solutions to QoS Challenges in WSNs

WSNs' degree of assistance for their users is determined by the QoS they give. The energy usage rate of sensor nodes and bandwidth are network-specific factors for QoS. Node measures, distribution, and node count are all application-specific factors. Significant resource constraints, unexpected traffic, duplicated data, sophisticated networks, energy management, scalability, variable sinks, and traffic classification are all issues in maintaining QoS for WSNs [130].

In [131], an agent-based QoS-aware routing method for WSNs is discussed. Network topology changes, network traffic flow, and the routing status of each node are all monitored using intelligent software agents. These agents will then aid with network routing and administration. An agent model is applied to perceive the changes in network topology, the network communication flow, and each node's energy state. Multi-agents can also participate in network routing and network maintenance. Compared with the traditional algorithm, the proposed algorithm can effectively improve the QoS metrics of WSN. The paper considers the synthetic effect of QoS parameters, including delay, bandwidth, and packet loss. Using PSO and agent-based routing (referred to as QoS-PSO algorithm), an optimal path for nodes is determined based on the synthetic QoS metrics. AODV (Adhoc On-Demand Distance Vector Routing) [132] and EEABR (Energy-Efficient Ant-Based Routing Algorithm) [133] have been chosen as the two benchmark algorithms for PSO-QoS performance testing. AODV can be applied to all kinds of network environments and support QoS requirements while EEABR is a SI-ACO-based WSN routing algorithm. QoS-PSO algorithm reduces end-to-end delay by 10–50% more than AODV algorithm and by 10% more than EEABR algorithm. When there are few nodes in the network, QoS-PSO algorithm exhibits the same packet loss as AODV and EEABR, whereas QoS-PSO requires a large number of nodes to achieve good performance. AODV's packet loss is about 0.52, EEABR's is 0.47, and QoS-PSO's is only 0.38 with 100 nodes, which is about 30% less than AODV, and about 20% less than EEABR. QoS-PSO algorithm payed more attention to synthetic QoS metrics, and it observed that delay and packet loss are reduced by only 10–50%, but the synthetic QoS ratio rises up to 25–100% through considering the synthetic QoS metrics.

With unpredictable sink mobility, a swarm intelligence-based sensor selection technique (referred to as SISSA) is proposed to fulfill established QoS constraints [134]. It does a mathematical analysis of the algorithm in order to reach theoretical constraints on energy usage, count of sent packets, and rate of convergence. For the set of network parameters considered, SISSA achieves an average lifetime approximation ratio level of 56.9%. SISSA is compared with the 802.15.4 and TDMA schemes. SISSA and TDMA are energy-efficient irrespective of the number of nodes, while 802.15.4 becomes inefficient as the network size assumes significant values. This is because SISSA and TDMA provide a contention-free channel access to the sensor nodes, allowing them to transmit their data efficiently regardless of the number of nodes considered. Both 802.15.4 and TDMA fail to provide any of the minimum throughput constraints required by the application. Conversely, SISSA guarantees all throughput constraints using a (much) lower duty cycle than both TDMA and 802.15.4. This is because SISSA allows just a subset of nodes to communicate during each tour, the time slot allocated to each node becomes larger as compared to TDMA.

In [135], ant-based mobility assisted routing for QoS-efficient data collecting (AR-QEDE) in WSN was proposed. The ACO approach is first utilized to analyze a trustworthy

path. The ant colony considers the consistency of the link and the time it takes to complete it while choosing a path. After deciding on a route, the source sends data packets to the destination. The robotic nodes are positioned between the two successive intermediate nodes in a weak connection if the link quality is deemed to be inadequate. This boosts the consistency of the link and improves link efficiency. Then, the data is transmitted to the destination by adding robotic nodes if the efficiency of the communication is estimated to be low. For QoS efficient data collection of WSN, every mobile robot is fitted with multiple antennas that allow the use of Space Division Multiple Access(SDMA) technology to gather data efficiently. The performance of ARQEDE is compared with RoCoMAR [136] and MoXMAC [137] protocols. The associated delay of ARQEDE is 73% less when compared to RoCoMAR and 64% less when compared to MoX-MAC; this is because ARQEDE includes the link delay metric in path establishment. Moreover, the results show that at higher data rates, the packet drop linearly increases for RoCoMAR, whereas ARQEDE shows a steady packet drop and delivery ratio. Accurate estimation of link quality in ARQEDE yields a 63% higher delivery ratio and 90% less packet drops when compared to RoCoMAR, and ARQEDE yields a 70% higher delivery ratio and 88% less packet drops than MoXMAC. The use of ACO technique in ARQEDE reduces the huge packet exchange involved in route discovery. Hence, the overhead of ARQEDE is 84% less when compared to RoCoMAR and 85% less when compared to MoXMAC. ARQEDE has 21% higher residual energy than RoCoMAR since the number of route disconnections is minimized in ARQEDE, thereby reducing the energy involved in retransmission and 18% higher residual energy than MoXMAC. The use of ACO technique in ARQEDE reduces the huge packet exchange involved in route discovery. Hence, the overhead of ARQEDE is 46% less when compared to RoCoMAR, and 68% less when compared to MoXMAC.

Industrial WSNs (IWSNs) allow battery-powered nodes to be used to provide fast deployment and low maintenance, even in harsh environments. The optimum configuration of the network can be a challenging concern because, many restrictions and criteria must be addressed, especially the energy consumption. In [138], a FL-based technique for enhancing energy efficiency of IWSN is proposed. This technique determines the sleep time of nodes using the node's available energy and the throughput to workload ratio. A PSO-based method is adopted to determine the suitable values of parameters for FL controller through optimization of membership functions and by adjusting their range, for enhancing energy efficiency of IWSN. In general, the ratio of Throughput to Workload fluctuates between 27% and 81% using the fuzzy-based approach proposed in [138]. The values achieved without Fuzzy Logic Controller (FLC) shift from 67% to 82%, which represents the best results regarding the ratio of Throughput to Workload but at the expense of battery consumption. However, in the case of PSO with 40 particles, the ratio of Throughput to Workload fluctuate from 60% to 81%, and at the same time prolongs the battery life.

LECR-GA (Low Energy-efficient hierarchical Clustering and Routing protocol based on Genetic Agorithm) were presented in [139] contain two algorithms, one for energy-efficient clustering and the other for WSN routing, were presented in the report. They have demonstrated that the clustering algorithm balances the CHs' lifespan as well as decreases the sensor nodes' energy usage. The routing method was created by evaluating a trade-off between communication distance and hops. Both algorithms have been defined with the correct representation of the chromosome and fitness function derivation, followed by the necessary GA operations. It can be found that the periodic application of a clustering and route generation using GA can help to preserve the system's total resources with optimum operability. Simulation results revealed that a network employing the LECR-GA protocol has 100% alive nodes even after round 600 in contrast to a network that uses LEACH and LEACH-C protocols [140], where there are no alive nodes (LND) after rounds 500 and 600, respectively. LECR-GA protocol is better than LEACH and LEACH-C in terms of the number of packets received by the BS. The number of messages received by the BS using the LECR-GA protocol is five times more than that of the other protocols. Moreover, LECR-GA protocol has significant abatement in terms of energy consumption. This is

because the LECR-GA protocol tries to find out the nodes with higher values of weight as well as residual energy making the energy consumption more balanced, and by using the genetic algorithm, LECR-GA explore the entire search space to arrive at the desired optimization (best number and location of the CH), therefore, saving of energy.

Ticket-based routing is a viable routing strategy since it may determine routes based on several essential characteristics, such as path cost and latency. However, it suffers from the requirement to send a significant count of tickets in order to validate the WSN and determine the route's latency and cost. GA can be utilized to reduce the tickets count and the overhead of the discovery message. Ref. [141] implemented a scheme incorporating genetic algorithm and TBR (called GA-TBR) to obtain state details within the Smart Grid WSN framework and thereby improve the process of route selection to guarantee the desired QoS. In GA-TBR, genetic algorithm operations are used to explore new feasible routes without sending any extra number of tickets. Mutated routes are evaluated using the information stored in sensor nodes caches. Therefore, there is no extra routing message overhead required for validating new routes (off springs) due to unicast traffic, which is a huge advantage of this approach compared to existing works. On the other hand, the results of genetic algorithm running time demonstrated that GA-TBR has minimum execution overhead. In addition, in terms of the number of hop counts and total delay, in some cases, GA-TBR shows 68% improvement, and compared to AODV [132], it gives 28% average improvement.

In [142], a highly efficient and robust Evolutionary computing-based routing scheme for WSN is proposed for ensuring QoS and enhancing energy-efficiency. Evolutionary Computing assisted Dual-Disjoint Forwarding Path (EC-DDFP) [142] employs a dual objective function where the first intends to achieve the optimal forwarding nodes for path planning, while the other functions to achieve best dual disjoint forwarding path estimation for reliable transmission. GA is applied to obtain fault-resilient dual-disjoint best forwarding paths for QoS-centric transmission and to maintain low-hop counts, high connectivity (low-connectivity loss) and high availability with minimum shared components for QoS centric communication. EC-DDFP model achieves a (dual) set of best forwarding paths to perform data transmission between the source and the destination. Besides, EC-DDFP model preserves the energy because of the low or reduced computational complexity and retransmission probability.

A hybrid model with an improved optimization method is addressed in [143] with the intention of enhancing the QoS qualities of WSNs. On the Destination Sequence Distance Vector (DSDV) routing approach [144], a set of two soft computational algorithms, including genetic algorithm (GA) and Bacteria Foraging Optimization (BFO) algorithm, are applied independently, and then hybrid GA and BFO are utilized for further performance optimization. The results show that when GA is applied on DSDV routing protocol, the throughput score lies between 76 and 94.5. It means that the throughput increases with the increase in the number of nodes. The value of packet delivery ratio goes up to 95.5 from 81, indicating a gradual rise in packet delivery ratio with the increase in the number of nodes. The end to end delay is quite less when the number of nodes is more than 50. When the soft computing technique, BFO, is implemented on DSDV routing protocol, the value of throughput is more better, showing a rise from 77 to 95.6. As observed, data packet delivery ratio increases with respect to GA as the collision is less which lowers the number of packet drops caused by collisions. Its value is ranging up to 95 from 78. When the hybridization of GA and BFO is implemented with DSDV, there is a marginal increase in the score of throughput. In regard to the data packet delivery ratio, it came out to be 97.8. The end-to-end delay in this case is decreased and it is in between 0.15 and 0.16. From the simulation results, it is evident that the combination of two optimization approaches along with DSDV routing protocol performs better than using DSDV alone in a WSN scenario, and the proposed approach can be best utilized in a small-sized WSN.

In [145], a Grey wolf-based metaheuristic is utilized for node placement to ensure a number of QoS measures, such as improving coverage, connectivity, and lowering

the network's total cost. The goal is to determine the optimal distribution of nodes for various p-coverage and q-connectivity settings. The results show that the efficiency of the proposed method in selecting appropriate positions with desired coverage and connectivity is improved by 11%, 14%, and 20%, respectively, when compared to PSO, GA, and Greedy approach.

An ideal WSN clustering technique, which comprises cluster creation and CH selection, may considerably enhance QoS and extend the service life of a WSN. GWO-based clustering and routing is proposed in [146] to enhance the network lifespan while giving exact QoS guarantees. Energy usage, network life span, latency, data rate, cost, stability, efficiency, and other QoS characteristics are all taken into account while studying network QoS. The proposed technique is simulated and evaluated based on the Quality of Service (QoS) parameters viz. residual energy, stability period, throughput, network lifetime, and delay. The proposed technique improves the overall network performance by 10.00%, 23.75%, and 54.54% when compared to ESO [147], GECR [148], and LEACH [140]. The reasons behind these results include: (1) consistent transmission of sensed data to BS through CH, (2) use of normal, advanced, and supernodes to elect them as CHs, which in turn increase the overall throughput of the network by increasing the number of packets received at the BS, (3) giving less chances to the nodes with low residual energy to become CH, which overcomes the rapid death of nodes and consequently increases network lifetime, (4) considering the intra-cluster distance and average sink distance while electing CH and (5) minimizes the end-to-end delay and energy consumption by selecting the optimal path between the BS and CH.

The hybrid PSO-CS optimization technique for multi-path routing is proposed in [149]. It presents a QoS aware method to identify reliable routes multi-hop data communication. It uses routes that do not compromise QoS for quick data transport. In contrast to conventional QoS methods, it also increases the network lifespan by regularly updating CHs depending on remaining energy and by using the appropriate routes for data transfer. PSO-CS uses several paths for delivering data packets and has excellent control over data traffic in the network. Simulation results show that PSO-CS outperforms the existing QoS centric protocols like EE-LEACH [150], EPSO-CEO [151] and OQoSCMRP [152] in terms of throughput, end-to-end delay, packet delivery ratio, network lifetime and energy conservation. Hence, PSO-CS can be used in various delay sensitive applications. The energy consumption of PSO-CS is decreased by 40.06%, 32.4%, and 18.21% compared with EE-LEACH, EPSO-CEO and OQoS-CMRP protocols.

Ref. [153] proposes an enhanced QoS aware algorithm based on GA (called ENSGRA). It updates points of reference to get better solutions by using a dynamically balanced clustering vector. In addition, an advanced crossover approach is used to acquire the best Pareto Fronts (PF). ENSGRA relies on Non-Dominated Sorting Genetic Algorithm 3 (NSGA-III), but adjusts reference points through the use of a dynamic weighted clustered scheduled vector to obtain new solutions. Moreover, ENSGRA can be used to find an integration between two parents through crossover with multi-parent crossover (MPX) to produce multiple children and improve new offspring to obtain the optimal Pareto Fronts (PF). This algorithm excelled the lagged multi-objective jumping particle swarm optimization [154], Non-dominated Sorting Genetic Algorithm–II [155] and NSGA-III [156] In terms of the QoS aspects, this approach outperforms the existing schemes (31% better optimization performance). Results show that this proposed ENSGRA is superior over other algorithms in the evaluation measures for multi-objective algorithms.

In order to enhance routing and maximize QoS in WSNs, the study in [157] proposes a multi-objective GWO (called QAMO-GWO). Nodes gather environment data periodically and deliver it to the respective CHs. The method attempts to pick the best CHs by optimizing QoS factors.

In [157], multiobjective grey wolf optimization algorithm (MO-GWO) balances the QoS parameters and focuses on selecting the optimal CHs. Simulation results show that MO-GWO has been able to improve QoS criteria by balancing the goals in the network. MO-

GWO method is compared with other methods [158–160] according to network lifetime and the energy usage in the network. Compared to the other methods, MO-GWO gives a lower average energy usage per 100 nodes. MO-GWO has improved the energy consumption in WSN by about 11% and improved the data delivery rate by about 1%. Additionally, the first node in MO-GWO dies much later than the other methods, which reflects the balance of energy and the network lifetime in WSN improved by about 16%. Besides, MO-GWO has a higher delivery rate in comparison to [158–160] due to the optimal selection of the route, avoidance of bottlenecks and the loss of the least amount of packets.

7.2. Open Research Issues and Challenges

As a future work, the network with variable traffic load scenario needs further research to study the QoS aspects. This necessitates improving fault tolerance, network dependability, and energy usage rates, as well as expanding the network's message capacity and extending its lifetime. These new research paths will be crucial for studies on mobile WSN fault tolerance and QoS.

In the future, new solutions will be necessary to be successful for networks with high mobility nodes, as well as routing networks with numerous sink nodes, by establishing certain correct WSN settings. In order to meet QoS requirements and extend the lifespan of WSN, a mix of additional bio-inspired optimization approaches can be used for other energy sensitive routing protocols. In order to analyze and compare the hybrid algorithms in terms of processing and memory needs of the participating node, more testing of the hybrid algorithms is required. In the future, spatio-temporal characteristics based on network dynamics may be produced, and different classifiers or AI approaches can be used to leverage the interrelationship between spatial and temporal behavior of nodes to detect malicious nodes that can impair the QoS of the connected application. Malicious patterns may be transformed into knowledge, allowing for faster judgments in subsequent phases without having to repeat the detection process. Safety period (time between successful data transmissions), packet latency, and energy usage are all essential QoS criteria. The researchers should consider all the important parameters while designing a new QoS-aware algorithm as this can affect the network performance. To achieve good QoS performance with fewer calculations, a balanced trade-off between location privacy and energy usage is preferable. Modeling a safe and robust strategy that addresses all necessary parameters, on the other hand, is a complex task, thus researchers should concentrate on all of these factors while developing new solutions. In addition, the present work must be updated for usage in IoT-based real-time applications like catastrophe monitoring and control. The solution should be able to survive all main security threats while also protecting the privacy of the sink location from both local and global adversaries. In the future, alternative evolutionary strategies for node deployment issues in three-dimensional (3D) settings and target mobility can be investigated, and also to ensure different QoS measures in terms of optimizing coverage, connection, and lowering the network's total cost.

Table 6. Summary of AI-based solutions to QoS problem surveyed in Section 7.

AI Techniques	Algorithm	Ref.	Objectives	Implementation	Approach	Mobility	Performance Metrics
SI	Ant Colony	[135]	QoS-effective data collection	NS2 simulator	Distributed	Mobile	Throughput, End to end delay, PDR and Routing overhead.
SI	Grey wolf optimization	[145]	Satisfy QoS metrics like coverage optimization, connectivity and lowering total network's cost	Matlab simulations	Centralized	Static	Change in location and number of targets without changing the network size setting.
SI	Grey wolf optimization	[146]	Enhance QoS and network lifetime	Matlab simulation	Distributed	Static	QoS metrics like residual energy, stability period, lifetime, throughput, and delay.
SI	Grey wolf optimization	[157]	Optimize routing and improve QoS in WSNs	Matlab simulation	Centralized	Static	transmission rate, latency, number of dropped packets, and delivery rate.
Hybrid	PSO and CS algorithm	[149]	Enhance QoS metrics like throughput, packet drop, delay and lifespan of network.	NS-2 Simulator	Centralized	Static	QoS parameters such as throughput, packet delivery ratio, end-to-end delay, and network lifetime.
Hybrid	FLC-PSO	[138]	Decrease the energy consumption	MATLAB simulation	Centralized	Static	Energy usage and Throughput-Workload ratio.
Hybrid	GA-BFO	[143]	Optimizing the quality of service	MATLAB simulation	Centralized	Static	Throughput, End to end delay, PDR and Routing overhead.
MAS	Multi-agent and PSO	[131]	Improve QoS	Real network deployment	Distributed	Mobile	Synthetic QoS, Average residual energy, Packet loss, and Mean delay.
MAS	SISSA	[134]	Optimizes network lifetime and meets predefined QoS constraints	Experimental	Distributed	Static with mobile sink	Network Lifetime, Throughput and Energy per byte.
EC	Genetic Algorithm	[139]	Prolong lifetime and increase the QoS	NS2 simulation	Distributed	Static	Amount of data, Alive nodes, Energy consumption, Packets received by the BS and First node death.
EC	Genetic Algorithm	[141]	Improve the QoS	NS2 and Matlab simulations	Centralized	Static	Delay Cost.
EC	Genetic Algorithm	[142]	Improve QoS and energy-efficiency	NS2 and Matlab simulations	Centralized	Static	Energy exhaustion, End-to-End delay, and Packet Drop.
EC	NSGA-III	[153]	Improve the QoS in WSNs	Matlab simulation	Centralized	Static	Hyper Volume and Number of Non-Dominated Solution. indicators.

8. Discussion

In the area of WSNs, we have seen an increase in the application of AI-based solutions that help with service optimization. The coupling of AI methodologies with WSNs has become a reality, bringing benefits to the IoT by allowing the frameworks to learn and track activities while also assisting in decision-making.

We have presented a survey of different issues and concerns in WSNs in this study. Various AI approaches used in WSNs are briefly discussed, as well as their categories. For the year 2010 to 2022, AI strategies utilized by researchers to handle the Security, QoS, and fault detection and tolerance concerns in WSNs are briefly outlined. The use of AI to solve these problems has been studied and summarized. The use of these methods in Security have been reviewed and summarized in Tables 3 and 4. For QoS, and fault detection and tolerance, the methods are reviewed and summarized in Tables 5 and 6.

The following findings can be summarized from Figures 3 and 4:

- Security: Figure 3 shows that for security, the most appropriate AI methods are Swarm Intelligence, FL, DL, RL, Hybrid and ANN. Overall, 28% of papers applied SI followed by Hybrid by 21%, 21% for FL, then 19% for deep learning, while the other methods (Nature inspired, Reinforcement learning, Evolutionary Computation, Multi-Agent Systems, Trajectory based, Physical computation) are considered not appropriate by the research community.
- QoS: As evident from Figure 3, for QoS problems in WSNs, the most adopted method is Evolutionary Computation (31%), followed by Hybrid (23%), 23% for SI then by 15% for Multi-Agent Systems, and 8% for Nature inspired.
- Fault detection and tolerance: from Figure 3, the most appropriate AI methods are Swarm Intelligence, and FL. Overall, 25% of papers applied SI and FL, followed by Hybrid 19%, then ANN and 13% by 13% and 6% for Reinforcement learning.

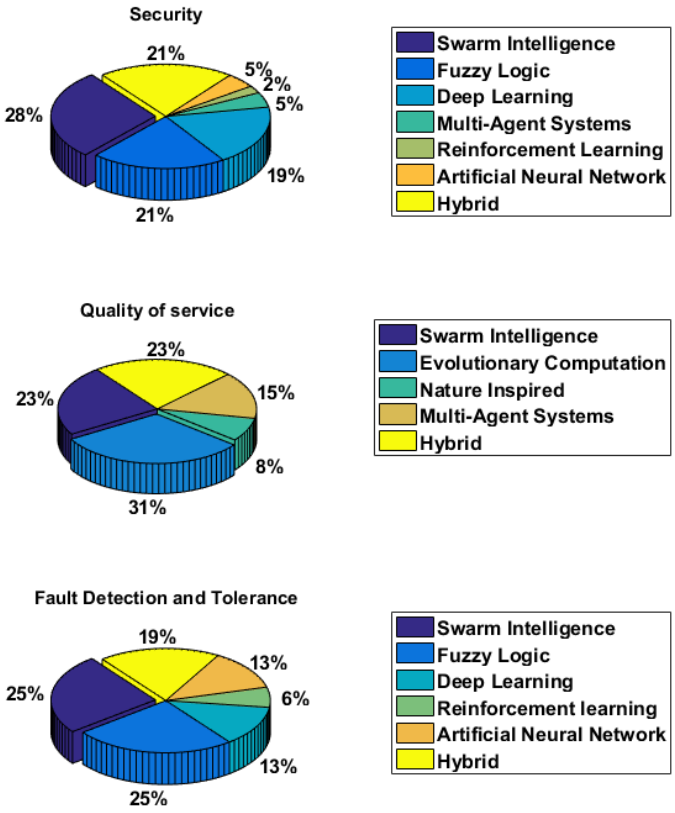

Figure 3. AI approaches in relation to different WSN challenges.

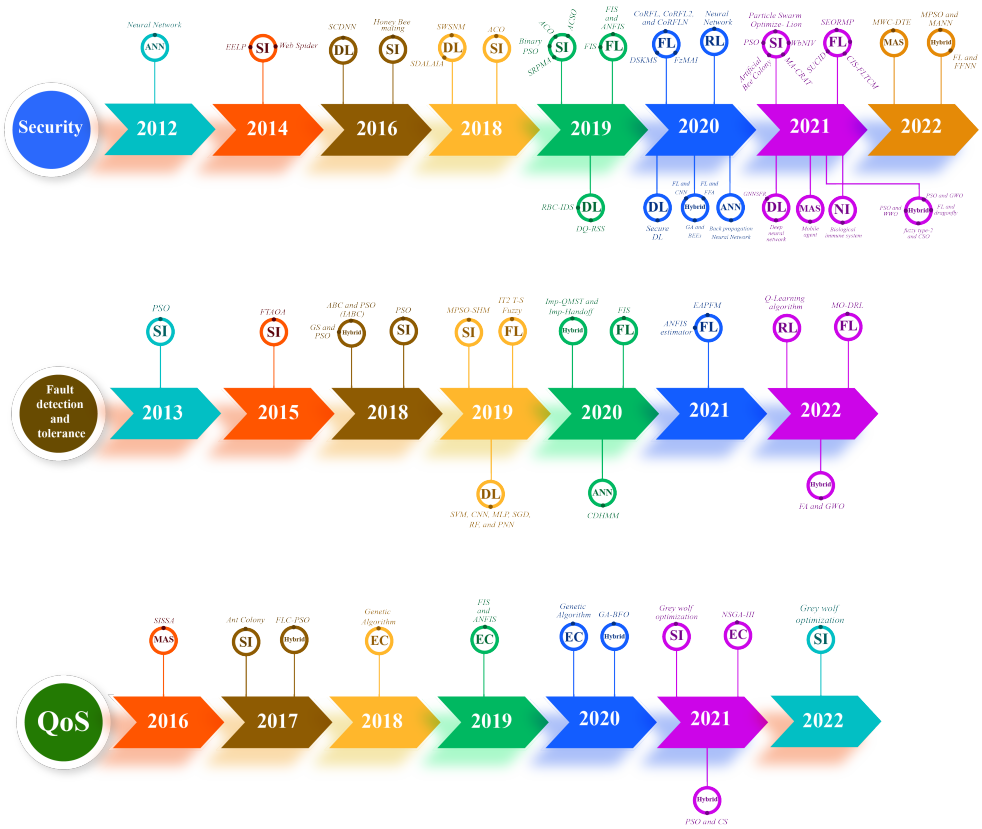

Figure 4. Diagram of route of technology development for each application.

It can be argued that one of the most common AI techniques widely adopted for solving the critical challenges of WSN is SI. This can be attributed to its efficiency and applicability for different WSN architectures. SI algorithms can effectively meet WSN objectives and ensure high WSN performance. It can also be noticed that implementing hybrid AI solutions is another commonly adopted approach to address WSN challenges. This is mostly due to the ability of these solutions to improve the efficiency of the algorithm by developing more effective combinations of AI algorithms. However, there is always a need to maintain the complexity of any AI solution to meet WSN limitations in terms of energy, bandwidth, storage and computational resources. The balance between efficiency and complexity should be emphasized as a key design issue that needs to be resolved before implementing hybrid AI solutions at scale.

Furthermore, Figure 5 provides a summary of the main WSN problems addressed using AI-based solutions considering the major WSN topics. It is evident that the research community gave careful considerations to a multitude of diverse WSN aspects. The common WSN problems among the different challenging topics of interest is data traffic routing and nodes clustering. Accordingly, addressing such problems was approached using different AI techniques with SI being the mostly adopted one. Another critical problem that received considerable attention is node deployment and localization, which are deemed critical for effective support of security, failure handling, and QoS in WSNs. Among the multiple AI methods utilized for addressing this problem, SI and DL were the preferred choices due to their usability and efficiency. For effective AI-based security support, there has been a noticeable trend to develop intrusion detection systems considering diverse AI approaches. Less attention has been paid to other important considerations such as real-time threat recognition, data protection, node identity verification, and trust management. In regards to fault detection and tolerance, several challenges were adequately investigated, whereas other important issues such as node mobility and data fault detection still require further AI-based research. Node mobility also gained limited interest in the context of AI-based QoS support in WSNs, but remains an open WSN research problem. Moreover,

it is apparent how difficult it is to have one-solution-fits-all, but a feasible consideration would be jointly addressing multiple aspects using a fusion of several AI methodologies in an effective design with well-maintained complexity. Overall, this review made it clear that WSN challenges have exposed adequate room for further AI-based improvements towards effective support of security, failure handling, and QoS in WSNs.

Figure 5. A summary of the main WSNs problems addressed using AI-based solutions.

In exploring the search space for global optimum solutions, GA is particularly efficient and stable, and it excels in large-scale optimization. It is possible to employ both continuous and discrete factors [161–163]. In order to tackle a wide range of WSN difficulties, researchers employ GA for these qualities.

Tables 3–6 emphasize that PSO is applied abundantly in all WSN problems. This is because PSO poses a great deal of benefits compared to alternative optimization methods. The PSO does not require any derivatives. It can be used in tandem with other optimization techniques. It is less sensitive to the objective function's nature and can deal with stochastic objectives. PSO has few parameters, able to run parallel computation, can converge fast and is easy to implement [163].

ACO algorithm is based on ants where their task is to search for food. Each ant takes a path in searching. That makes ACO suitable to work in parallel problems and is applicable to solve some WSN challenges. ACO has many characteristics that encourage researchers for usage. It can adapt to changes, have guaranteed convergence and can provide good solutions rapidly [163].

New AI solutions, as well as various methodologies for embedding these schemes in WSNs, must be promoted in the future for WSN advancement. The majority of the solutions described thus far have leveraged AI to address particular difficulties in specific industries. Learning platforms and models are needed instead of specialist solutions. The majority of issues arise from layer incompatibility and significant human contact. Setting and adjusting solutions necessitates self-adaptivity. Hybrid techniques to resource usage optimization in

WSN must be developed [164]. Further research into developing an effective distributed data mining solution for WSN, as well as advancements in the noisy data filtering process, should be encouraged in the future. DNN's layered structure and other common traits make it an attractive alternative for use in such circumstances. The primary problems are distributed multi-layered DNN training and a better balance between processing and transmission power usage. Parameter learning and optimization is another fascinating area of research for AI approaches in WSNs.

Many attempts have been sought to address the WSN interference categorization problem. With the growing use of license-free frequency bands, appropriate wireless interference detection and control has become a major concern. Future research opportunities include interference mitigation strategies, deployment planning, and other possible uses. A choice is the DL classification model.

WSN traffic flow management might be a future path. Another interesting study area that may be aided by head nodes, normal nodes, and BS is mobility. The most crucial hurdles to overcome are modifications in WSN structure and control message complexity generated by dynamic topology. Few studies have been conducted to increase mobile agent intelligence for improved route planning and data collection. An combination of DL and RL utilizing numerous mobile agents is a suitable technique to handle node distribution in dynamic setting. The application of RL can help mobile agents make more intelligent conclusions about what action to take in a given environment. Furthermore, identifying the appropriate count of mobile agents and their path by considering many criteria that might deliver efficient outcomes would necessitate future research. Furthermore, most existing algorithms failed to take into account the data security and/or privacy in numerous mobile agent settings. Future studies are likely to pay more attention to these concerns. To address real-world difficulties, more robust and efficient mobile agent learning approaches must be developed in the future.

A potential future approach is the use of AI schemes to tackle the problems of MWSNs. Transmission delay, energy usage, dependability, and security of MWSNs are all research concerns that have yet to be answered. In the future, combining SI with other optimization approaches should be promoted. During the optimization of MWSNs, cross-layer optimization model issues must be adequately addressed. The findings of the research of human-related biological characteristics can be used to develop future solutions to similar situations. Distributed and real-time deployment of light-weight algorithms may be a potential path for addressing the issues of dynamic MWSNs.

According to the study, the majority of AI-based solutions are just simulation-based. In a real-time setting, AI approaches should be applied and examined [165,166]. In the future, this should be promoted. More research is needed to demonstrate how AI approaches may be applied. Cross-layer techniques based on AI methodologies are infrequently used to solve problems and remain an important field of study. Hybrid AI approaches are also underutilized and must be thoroughly studied. Future research is anticipated to take heterogeneity, dynamic contexts, and different transmission restrictions into account while developing algorithms. The WSN becomes cognitive when AI approaches are used to manage and overcome issues that develop during operation. We hope that the concepts discussed in this paper will encourage researchers to use AI to address complex WSN challenges by making nodes intelligent.

In order to determine whether WSNs are appropriate before deployment, simulation is an effective method. By simulating algorithms, one can assess scalability without being limited by the hardware. Furthermore, it simplifies the development of WSN application, making them a powerful and popular research tool. According to Tables 3–6, over 90% of implementations are simulations based. MATLAB is widely used for implementation with 37%, 26% uses NS-2/NS-3, 6% uses PYTHON, 1% uses OPNET, 1% uses OMNet++, and 20% uses other packages.

In terms of memory requirements, flexibility, and computational requirements, a general comparison of AI methods [167–177] is presented in Figure 6. The centralized approach

at BS is more suitable for AI methods that have a high or medium level of computational and memory requirements, respectively. On the other hand, methods with low class requirements could be fitted for execution in distributed manner. Flexibility is the capability of AI methods to be adapted to the changes in the environment [167]. Additionally, AI methods are capable of finding the best solution for certain problems. It is important that the designer selects the right method or set of methods according to the application's specification in order to provide the best performance. We have summarized the performance metrics adopted in each article in the last column of Tables 3–6. According to these tables, the performance metrics vary with regard to the objectives of the problem presented in each article. It is noted that most of the articles do not evaluate the AI method itself in terms of computational and memory complexities during its utilization for solving the given problem. In the future, it is recommended to employ performance metrics for the AI methods along with performance metrics for the problem itself.

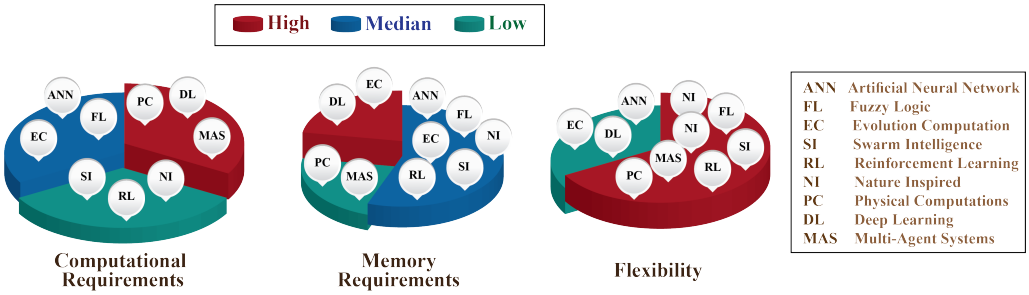

Figure 6. General comparison of computational, memory, and flexibility requirements of utilized AI methods.

Open Challenges and Issues

Some insights into open challenges and issues can be summarized as follows:

- WSNs are considered as additional components of a heterogeneous system that contribute to a wide range of applications (for example, in Intelligent Transportation Systems, where WSNs collaborate with other technologies such as VANET). In future study, security, QoS, and fault detection and tolerance for such a heterogeneous system-based WSN should be extensively explored by utilizing different AI solutions.
- Security vulnerabilities, link and node failures, and degradation of QoS performance are still evident and open challenges in WSN architectures. WSNs lack standardized solutions addressing such issues. As a result, wide deployment of effective WSN networks would be highly hindered in demanding IoT applications.
- WSN architectures have exposed adequate room for effective incorporation of AI techniques. A wide variety of AI solutions have also been proposed by combining multiple AI algorithms. However, no effort has been made yet to effectively develop a comprehensive solution addressing multiple WSN challenges.
- When it comes to integrating AI algorithms into WSNs, there is no one-solution-fits-all choice. Future studies might look towards integrating diverse AI solutions into a single WSN implementation.
- The trade-off between efficiency and complexity is insufficiently emphasized in the context of developing AI solutions for WSNs. This is more evident in the case of implementing hybrid AI solutions.
- Experimental simulation testing is a predominant implementation methodology among the current studies. Little consideration has been given to realistic experimentation using physical testbeds. A shift towards such a viable methodology is important to increase evaluation practicality and credibility.
- Frameworks and mechanisms could be designed to mitigate high computations of AI methods. Moreover, it is recommended to employ performance metrics for the AI methods along with performance metrics for the problem itself.

- Intelligent fault detection and tolerance techniques, as well as QoS for collaborative routing with link scheduling needs to be examined in dynamic IoT networks to enable real-time adaptation to network changes.
- There is a limited number of works considering fault tolerance and data storage issues in IoT/WSN. Further investigation is required to enhance storage of IoT/WSN, which can result in an improvement of recoverable data and energy.
- Employing learning -based AI methods could open the way to develop a rapid fix and self-healing techniques to tolerate node faults according to applications requirements [178]. However, several studies utilizing learning-based AI algorithms have raised ambiguity on how they can be implemented in WSN environments. As a result, it was advised that more research and discussion should be conducted in terms of training and complexity of learning-based AI approaches in WSNs.
- Frameworks for fault tolerance and back up node placement-based optimizations methods could be further discussed by considering the flexibility and the strength of the application requirements (e.g., surveillance application). Moreover, these frameworks could employ a mechanism that intelligently performs backup node switching to maintain continuous acquisition of data [179].
- It is desirable to test and explore the applicability of ML methods to networks with a large number of event parameters and data with complex properties.
- For population-based metaheuristic methods, future research could be done on the population size of these methods and their applicability for a given problem.
- Considering QoS while also satisfying privacy and security constraints as an extension to existing work by developing effective techniques that address both of these challenges could be handled in future research.
- Designing node deployment techniques that are aware of QoS parameters in three-dimensional environments based on various AI methods could be further explored.
- Based on the application requirements for reliability and energy, predicting QoS parameters needs further investigation and recommendations for future solutions based on AI methods or hybrid combination of them is required for improving the overall performance.
- Optimization approaches as well as the creation of fitness functions have been used to address issues with QoS, fault tolerance, and security. However, most of the current work ignores multiple fitness function evaluations using the same AI approach; hence, it is desirable to test different fitness functions for the same problem while evaluating optimization techniques.
- It is common in trust management that trust reports may generate message overhead; also, trust calculation is a resource intensive process for large and dense networks [180]. As a result, optimizing the reporting mechanism is essential to reduce message overhead, and additional research is required to optimize trust management in WSNs.
- It would be beneficial to study deep reinforcement learning algorithms with more sophisticated exploration methods. Moreover, multi-agent and partially distributed learning techniques can be introduced to overcome the scalability issues in existing learning solutions [180].

9. Conclusions

There has been a growing interest in advancing WSNs with AI-based solutions in a wide-range of smart applications. Incorporating AI systems in WSN would enrich its applicability and revive its potentiality for real-life IoT deployments. In this study, thorough review and thoughtful analysis of the recent research activities on enhancing WSN efficiency with different AI technologies is presented. It provides insight towards establishing a firm understanding of the standing state and future prospects of AI-based solutions addressing security, fault detection and tolerance, and quality of service challenges in WSN. The review in this paper demonstrates the potential of AI-based approaches to improve these major WSN aspects considering different AI algorithms. It is found out that Swarm

Intelligence and Evolutionary Computation were the mostly employed AI techniques in addition to other techniques such as FL, DL, RL, and ANN. Hybrid AI algorithms were also of interest as well as Multi-Agent Systems, particularly for QoS support in WSNs. Moreover, the study provides a comprehensive exploration and discussion of possible future AI-based enhancements to WSN efficiency. It emphasizes different potential research directions for future studies to address critical relevant topics such as cross-layer AI solutions, mobility-aware QoS support, and secure trust management. These also include the need for intensively researching hybrid AI approaches and advanced techniques combining multiple optimization algorithms. Another important consideration is promoting real-life experimental evaluation using a physical testbed to increase testing credibility and reliability. It is accordingly envisaged that this research study facilitates broad comprehension of recent AI-supported WSN enhancements and paves the way for addressing further WSN challenges in follow-up AI-oriented studies.

Author Contributions: W.O., A.M.K., A.S., A.A.E.-S., M.A. and I.A. contributed equally to this paper, where all authors participated in sorting the experiments, discussed and analyzed the results, performed the experiments and analyzed the results, wrote the paper, discussed the result, and review/edited the manuscript. All authors have read and agreed to this version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education, Saudi Arabia for funding this research work through the project number (QU-IF-2-4-1-27127). The authors also thank to Qassim University for technical support.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education, Saudi Arabia for funding this research work through the project number (QU-IF-2-4-1-27127). The authors also thank to Qassim University for technical support

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence.
ACO	Ant Colony Optimization.
ANN	Artificial Neural Network.
ABC	Artificial Bee Colony.
BA	Bat Algorithm.
CSO	Cuckoo Search Optimization.
CI	Computational Intelligence.
DNN	Deep Neural Network.
DC	Data Collection.
DL	Deep Learning.
EC	Evolutionary Computation.
IoT	Internet of Things.
GA	Genetic Algorithm.
PSO	Particle Swarm Optimization.
QoS	Quality of Service.
RL	Reinforcement Learning.
ML	Machine Learning.
MAS	Multi-Agent Systems.
NI	Nature Inspired.
PC	Physical computation.

SI	Swarm Intelligence.
WSN	Wireless Sensor Network.
WOA	Whale Optimization Algorithm.

References

1. Bellavista, P.; Cardone, G.; Corradi, A.; Foschini, L. Convergence of MANET and WSN in IoT urban scenarios. *IEEE Sens. J.* **2013**, *13*, 3558–3567. [CrossRef]
2. Jabbar, W.A.; Saad, W.K.; Ismail, M. MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT. *IEEE Access* **2018**, *6*, 76546–76572. [CrossRef]
3. Osamy, W.; Khedr, A.M.; Aziz, A.; El-Sawy, A.A. Cluster-tree routing based entropy scheme for data gathering in wireless sensor networks. *IEEE Access* **2018**, *6*, 77372–77387. [CrossRef]
4. Osamy, W.; El-sawy, A.A.; Khedr, A.M. SATC: A simulated annealing based tree construction and scheduling algorithm for minimizing aggregation time in wireless sensor networks. *Wirel. Pers. Commun.* **2019**, *108*, 921–938. [CrossRef]
5. Khedr, A.M. Effective data acquisition protocol for multi-hop heterogeneous wireless sensor networks using compressive sensing. *Algorithms* **2015**, *8*, 910–928. [CrossRef]
6. Bradai, A.; Benslimane, A.; Singh, K.D. Dynamic anchor points selection for mobility management in Software Defined Networks. *J. Netw. Comput. Appl.* **2015**, *57*, 1–11. [CrossRef]
7. Amri, S.; Khelifi, F.; Bradai, A.; Rachedi, A.; Kaddachi, M.L.; Atri, M. A new fuzzy logic based node localization mechanism for wireless sensor networks. *Future Gener. Comput. Syst.* **2019**, *93*, 799–813. [CrossRef]
8. Wang, F.; Liu, J. Networked wireless sensor data collection: Issues, challenges, and approaches. *IEEE Commun. Surv. Tutor.* **2010**, *13*, 673–687. [CrossRef]
9. Osamy, W.; Khedr, A.M.; Salim, A.; AlAli, A.I.; El-Sawy, A.A. Recent Studies Utilizing Artificial Intelligence Techniques for Solving Data Collection, Aggregation and Dissemination Challenges in Wireless Sensor Networks: A Review. *Electronics* **2022**, *11*, 313. [CrossRef]
10. Osamy, W.; Khedr, A.M.; Salim, A.; Ali, A.I.A.; El-Sawy, A.A. Coverage, Deployment and Localization Challenges in Wireless Sensor Networks Based on Artificial Intelligence Techniques: A Review. *IEEE Access* **2022**, *10*, 30232–30257. [CrossRef]
11. Pathan, A.S.K.; Lee, H.W.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 2006 8th International Conference Advanced Communication Technology, Phoenix Park, Republic of Korea, 20–22 February 2006; Volume 2, p. 6.
12. Zhou, L.; Wen, Q. Energy efficient source location privacy protecting scheme in wireless sensor networks using ant colony optimization. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 920510. [CrossRef]
13. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-based Secure Energy Efficient Beamforming in Multibeam Satellite Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *in press*. [CrossRef]
14. Qin, Z.; Zhang, X.; Feng, K.; Zhang, Q.; Huang, J. An efficient identity-based key management scheme for wireless sensor networks using the bloom filter. *Sensors* **2014**, *14*, 17937–17951. [CrossRef] [PubMed]
15. Mármol, F.G.; Pérez, G.M. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommun. Syst.* **2011**, *46*, 163–180. [CrossRef]
16. Jiang, S.; Zhang, J.; Miao, J.; Zhou, C. A privacy-preserving reauthentication scheme for mobile wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 913782. [CrossRef]
17. Zhang, T.; He, J.; Zhang, Y. Secure sensor localization in wireless sensor networks based on neural network. *Int. J. Comput. Intell. Syst.* **2012**, *5*, 914–923. [CrossRef]
18. Kifayat, K.; Merabti, M.; Shi, Q.; Llewellyn-Jones, D. Security in wireless sensor networks. In *Handbook of Information and Communication Security*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 513–552.
19. Moridi, E.; Haghparast, M.; Hosseinzadeh, M.; Jassbi, S.J. Fault management frameworks in wireless sensor networks: A survey. *Comput. Commun.* **2020**, *155*, 205–226. [CrossRef]
20. Venugopal, K.; Kumaraswamy, M. An Introduction to QoS in Wireless Sensor Networks. In *QoS Routing Algorithms for Wireless Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–21.
21. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS-Aided Hybrid Satellite-Terrestrial Relay Networks: Joint Beamforming Design and Optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [CrossRef]
22. Lin, Z.; Lin, M.; Wang, J.B.; de Cola, T.; Wang, J. Joint Beamforming and Power Allocation for Satellite-Terrestrial Integrated Networks With Non-Orthogonal Multiple Access. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 657–670. [CrossRef]
23. Tang, J.; Liu, G.; Pan, Q. A review on representative swarm intelligence algorithms for solving optimization problems: Applications and trends. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1627–1643. [CrossRef]
24. Antonopoulos, I.; Robu, V.; Couraud, B.; Kirli, D.; Norbu, S.; Kiprakis, A.; Flynn, D.; Elizondo-Gonzalez, S.; Wattam, S. Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review. *Renew. Sustain. Energy Rev.* **2020**, *130*, 109899. [CrossRef]
25. Sohail, A. Genetic algorithms in the fields of artificial intelligence and data sciences. *Ann. Data Sci.* **2021**, 1–12. [CrossRef]
26. Grefenstette, J.J. Genetic algorithms and machine learning. In Proceedings of the Sixth Annual Conference on Computational Learning Theory, Santa Cruz, CA, USA, 26–28 July 1993; pp. 3–4.

27. Bello, O.; Holzmann, J.; Yaqoob, T.; Teodoriu, C. Application of artificial intelligence methods in drilling system design and operations: A review of the state of the art. *J. Artif. Intell. Soft Comput. Res.* **2015**, *5*, 121–139. [CrossRef]
28. Mekonnen, Y.; Namuduri, S.; Burton, L.; Sarwat, A.; Bhansali, S. Machine learning techniques in wireless sensor network based precision agriculture. *J. Electrochem. Soc.* **2019**, *167*, 037522. [CrossRef]
29. Anand, S.; Manjari, R.K.K. FPGA implementation of artificial Neural Network for forest fire detection in wireless Sensor Network. In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 23–24 February 2017; pp. 265–270. [CrossRef]
30. Goswami, P.; Mukherjee, A.; Hazra, R.; Yang, L.; Ghosh, U.; Qi, Y.; Wang, H. AI Based Energy Efficient Routing Protocol for Intelligent Transportation System. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 1670–1679. [CrossRef]
31. Machin, M.; Sanguesa, J.A.; Garrido, P.; Martinez, F.J. On the use of artificial intelligence techniques in intelligent transportation systems. In Proceedings of the 2018 IEEE wireless communications and networking conference workshops (WCNCW), Barcelona, Spain, 15–18 April 2018; pp. 332–337.
32. Li, L.; Jiang, L.; Liu, Z. Optimization Research of Artificial Intelligence and Wireless Sensor Networks in Smart Pension. *Sci. Program.* **2021**, *2021*, 5421668. [CrossRef]
33. Borelli, E.; Paolini, G.; Antoniazzi, F.; Barbiroli, M.; Benassi, F.; Chesani, F.; Chiari, L.; Fantini, M.; Fuschini, F.; Galassi, A.; et al. HABITAT: An IoT Solution for Independent Elderly. *Sensors* **2019**, *19*, 1258. [CrossRef]
34. Zhao, Y. Combination of Wireless Sensor Network and Artificial Neuronal Network: A New Approach of Modeling. Ph.D. Thesis. Sea and Sciences Doctoral School, La Garde, France, 2013.
35. Jacoby, M.; Tan, S.Y.; Katanbaf, M.; Saffari, A.; Saha, H.; Kapetanovic, Z.; Garland, J.; Florita, A.; Henze, G.; Sarkar, S.; et al. WHISPER: Wireless Home Identification and Sensing Platform for Energy Reduction. *J. Sens. Actuator Netw.* **2021**, *10*, 71. [CrossRef]
36. Sofi, A.; Jane Regita, J.; Rane, B.; Lau, H.H. Structural health monitoring using wireless smart sensor network—An overview. *Mech. Syst. Signal Process.* **2022**, *163*, 108113. [CrossRef]
37. Manoharan, H.; Teekaraman, Y.; Kuppusamy, R.; Radhakrishnan, A. An Intellectual Energy Device for Household Appliances Using Artificial Neural Network. *Math. Probl. Eng.* **2021**, *2021*, 7929672. [CrossRef]
38. Luke, S. *Essentials of Metaheuristics*, 2nd ed.; Lulu: Morrisville, NC, USA, 2013. Available online: http://cs.gmu.edu/$\sim$sean/book/metaheuristics/ (accessed on 1 September 2022).
39. Yang, X.S. *Nature-Inspired Metaheuristic Algorithms*; Luniver Press: London, UK, 2010.
40. Xing, B.; Gao, W.J. Fruit fly optimization algorithm. In *Innovative Computational Intelligence: A Rough Guide to 134 Clever Algorithms*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 167–170.
41. Brownlee, J. *Clever Algorithms: Nature-Inspired Programming Recipes*; Lulu: Morrisville, NC, USA, 2011.
42. Jagtap, V. Survey of different swarm intelligence algorithms. *Int. J. Adv. Eng. Res. Dev.* **2014**, *1*, 12.
43. Dorri, A.; Kanhere, S.S.; Jurdak, R. Multi-agent systems: A survey. *IEEE Access* **2018**, *6*, 28573–28593. [CrossRef]
44. Zhang, J.; Su, Q.; Tang, B.; Wang, C.; Li, Y. DPSNet: Multitask Learning Using Geometry Reasoning for Scene Depth and Semantics. *IEEE Trans. Neural Networks Learn. Syst.* **2021**, *in press*. [CrossRef] [PubMed]
45. Chen, S.H.; Jakeman, A.J.; Norton, J.P. Artificial intelligence techniques: An introduction to their use for modelling environmental systems. *Math. Comput. Simul.* **2008**, *78*, 379–400. [CrossRef]
46. Alom, M.Z.; Taha, T.M.; Yakopcic, C.; Westberg, S.; Sidike, P.; Nasrin, M.S.; Hasan, M.; Van Essen, B.C.; Awwal, A.A.; Asari, V.K. A state-of-the-art survey on deep learning theory and architectures. *Electronics* **2019**, *8*, 292. [CrossRef]
47. Chang, C.W.; Lee, H.W.; Liu, C.H. A review of artificial intelligence algorithms used for smart machine tools. *Inventions* **2018**, *3*, 41. [CrossRef]
48. Boucher, P. *How Artificial Intelligence Works*; Scientific Foresight Unit: Luxembourg, 2019.
49. Kumar, R.; Tripathi, S.; Agrawal, R. A Review On Security in Wireless Sensor Network. In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 12–14 March 2020; pp. 304–308.
50. Ali, M.; Nadeem, M.; Siddique, A.; Ahmad, S.; Ijaz, A. Addressing Sinkhole Attacks in Wireless Sensor Networks-A Review. *Int. J. Sci. Technol. Res. (IJSTR)* **2020**, *9*, 406–411.
51. Fang, W.; Zhang, W.; Chen, W.; Pan, T.; Ni, Y.; Yang, Y. Trust-based attack and defense in wireless sensor networks: A survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 2643546. [CrossRef]
52. Dhivyasri, K.; Suphalakshmi, A.; Revathi, M. Wireless sensor network jammer attack: A detailed review. *Int. J. Res. Appl. Sci. Eng* **2020**, *8*, 201–221. [CrossRef]
53. Yu, J.Y.; Lee, E.; Oh, S.R.; Seo, Y.D.; Kim, Y.G. A survey on security requirements for WSNs: Focusing on the characteristics related to security. *IEEE Access* **2020**, *8*, 45304–45324. [CrossRef]
54. Ahmad, R.; Wazirali, R.; Abu-Ain, T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors* **2022**, *22*, 4730. [CrossRef] [PubMed]
55. Baraneetharan, E. Role of machine learning algorithms intrusion detection in WSNs: A survey. *J. Inf. Technol.* **2020**, *2*, 161–173.
56. Jinisha, J.J. Survey On Various Attacks And Intrusion Detection Mechanisms In Wireless Sensor Networks. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 3694–3704.
57. Gautam, A.K.; Kumar, R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Appl. Sci.* **2021**, *3*, 1–27. [CrossRef]

58. Vikas; Sagar, B.; Munjul, M. Security issues in wireless sensor network—A survey. *J. Discret. Math. Sci. Cryptogr.* **2021**, *24*, 1415–1427. [CrossRef]
59. Lee, C.C. Security and Privacy in Wireless Sensor Networks: Advances and Challenges. *Sensors* **2020**, *20*, 744. [CrossRef]
60. Xia, Z.; Wei, Z.; Zhang, H. Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks. *Comput. Intell. Neurosci.* **2022**, *2022*, 3449428. [CrossRef]
61. Parreño, I.F.; Avila, D.F. Analysis of the Cybersecurity in Wireless Sensor Networks (WSN): A Review Literature. In *Proceedings of the Developments and Advances in Defense and Security, Cartagena, Colombia, 11–13 July 2022*; Rocha, Á., Fajardo-Toro, C.H., Rodríguez, J.M.R., Eds.; Springer: Singapore, 2022; pp. 83–102.
62. Kaur, T.; Kumar, D. A survey on QoS mechanisms in WSN for computational intelligence based routing protocols. *Wirel. Netw.* **2020**, *26*, 2465–2486. [CrossRef]
63. Adhyapok, S.; Sarma, H.K.D. Review on QoS aware MAC protocols for multi-channel wireless sensor network. In Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 13–14 March 2020; pp. 1–5.
64. Quy, V.K.; Nam, V.H.; Linh, D.M.; Ban, N.T.; Han, N.D. A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. *Wirel. Pers. Commun.* **2021**, *120*, 49–62. [CrossRef]
65. Pundir, M.; Sandhu, J.K. A systematic review of quality of service in wireless sensor networks using machine learning: Recent trend and future vision. *J. Netw. Comput. Appl.* **2021**, *188*, 103084. [CrossRef]
66. Dilek, S.; Irgan, K.; Guzel, M.; Ozdemir, S.; Baydere, S.; Charnsripinyo, C. QoS-aware IoT networks and protocols: A comprehensive survey. *Int. J. Commun. Syst.* **2022**, *35*, e5156. [CrossRef]
67. Xiao, J.; Zhu, Y.; Zhong, Y.; Lin, Z. A Review on fault diagnosis in wireless sensor networks. In Proceedings of the IOP Conference Series: Earth and Environmental Science, Guangzhou, China, 20–21 December 2020; Volume 428, p. 012070.
68. Yadav, S.A.; Poongodi, T. A Review of ML Based Fault Detection Algorithms in WSNs. In Proceedings of the 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 28–30 April 2021; pp. 615–618.
69. Mohapatra, H.; Rath, A.K. Survey on fault tolerance-based clustering evolution in WSN. *IET Netw.* **2020**, *9*, 145–155. [CrossRef]
70. Adday, G.H.; Subramaniam, S.K.; Zukarnain, Z.A.; Samian, N. Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions. *Sensors* **2022**, *22*, 6041. [CrossRef] [PubMed]
71. Swain, R.R.; Dash, T.; Khilar, P.M. Automated Fault Diagnosis in Wireless Sensor Networks: A Comprehensive Survey. *Wirel. Pers. Commun.* **2022**, *127*, 3211–3243. [CrossRef]
72. Canovas, A.; Lloret, J.; Macias, E.; Suarez, A. Web spider defense technique in wireless sensor networks. *Int. J. Distrib. Sens. Networks* **2014**, *10*, 348606. [CrossRef]
73. Sahoo, R.R.; Sardar, A.R.; Singh, M.; Ray, S.; Sarkar, S.K. A bio inspired and trust based approach for clustering in WSN. *Nat. Comput.* **2016**, *15*, 423–434. [CrossRef]
74. Ma, T.; Wang, F.; Cheng, J.; Yu, Y.; Chen, X. A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. *Sensors* **2016**, *16*, 1701. [CrossRef] [PubMed]
75. Periyanayagi, S.; Sumathy, V. Swarm-based defense technique for tampering and cheating attack in WSN using CPHS. *Pers. Ubiquitous Comput.* **2018**, *22*, 1165–1179. [CrossRef]
76. Alshinina, R.A.; Elleithy, K.M. A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware. *IEEE Access* **2018**, *6*, 29885–29898. [CrossRef]
77. Wang, H.; Wen, Y.; Zhao, D. Identifying localization attacks in wireless sensor networks using deep learning. *J. Intell. Fuzzy Syst.* **2018**, *35*, 1339–1351. [CrossRef]
78. Sun, Z.; Wei, M.; Zhang, Z.; Qu, G. Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks. *Appl. Soft Comput.* **2019**, *77*, 366–375. [CrossRef]
79. Dong, C.; Zhao, L. Sensor network security defense strategy based on attack graph and improved binary PSO. *Saf. Sci.* **2019**, *117*, 81–87. [CrossRef]
80. Borkar, G.M.; Patil, L.H.; Dalgade, D.; Hutke, A. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. *Sustain. Comput. Informatics Syst.* **2019**, *23*, 120–135. [CrossRef]
81. Vijayakumar, K.; Kumar, K.P.M.; Kottilingam, K.; Karthick, T.; Vijayakumar, P.; Ganeshkumar, P. An adaptive neuro-fuzzy logic based jamming detection system in WSN. *Soft Comput.* **2019**, *23*, 2655–2667. [CrossRef]
82. Kanagasabapathy, P.M.K.; Kedalu Poornachary, V.; Murugan, S.; Natesan, A.; Ponnusamy, V. Rapid jamming detection approach based on fuzzy in WSN. *Int. J. Commun. Syst.* **2019**, *35*, e4205. [CrossRef]
83. Otoum, S.; Kantarci, B.; Mouftah, H.T. On the feasibility of deep learning in sensor network intrusion detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71. [CrossRef]
84. Su, Y.; Lu, X.; Zhao, Y.; Huang, L.; Du, X. Cooperative Communications With Relay Selection Based on Deep Reinforcement Learning in Wireless Sensor Networks. *IEEE Sens. J.* **2019**, *19*, 9561–9569. [CrossRef]
85. Sujanthi, S.; Nithya Kalyani, S. SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT. *Wirel. Pers. Commun.* **2020**, *114*, 2135–2169. [CrossRef]
86. Salim, A.; Osamy, W.; Khedr, A.M.; Aziz, A.; Abdel-Mageed, M. A Secure Data Gathering Scheme based on Properties of Primes and Compressive Sensing for IoT based WSNs. *IEEE Sens. J.* **2020**, *21*, 555–5571. [CrossRef]

87. Nancy, P.; Muthurajkumar, S.; Ganapathy, S.; Santhosh Kumar, S.V.N.; Selvi, M.; Arputharaj, K. Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks. *IET Commun.* **2020**, *14*, 888–895. [CrossRef]
88. Yousefpoor, M.S.; Barati, H. DSKMS: A dynamic smart key management system based on fuzzy logic in wireless sensor networks. *Wirel. Netw.* **2020**, *26*, 2515–2535. [CrossRef]
89. Gao, B.; Maekawa, T.; Amagata, D.; Hara, T. Detecting Reinforcement Learning-Based Grey Hole Attack in MobileWireless Sensor Networks. *IEICE Trans. Commun.* **2020**, *E103B*, 504–516. [CrossRef]
90. Baroudi, U.; Aldarwbi, M.; Younis, M. Energy-Aware Connectivity Restoration Mechanism for Cyber-Physical Systems of Networked Sensors and Robots. *IEEE Syst. J.* **2020**, *14*, 3093–3104. [CrossRef]
91. Wang, Z.; Li, L.; Ao, C.; Wu, D.; Zhou, W.; Yu, X. Multi-level data fusion algorithm towards privacy protection in wireless sensor networks. *Int. J. Commun. Netw. Distrib. Syst.* **2020**, *25*, 265–283. [CrossRef]
92. Singh, N.; Virmani, D.; Gao, X.Z. A Fuzzy Logic-Based Method to Avert Intrusions in Wireless Sensor Networks Using WSN-DS Dataset. *Int. J. Comput. Intell. Appl.* **2020**, *19*, 2050018. [CrossRef]
93. Fotohi, R.; Firoozi Bari, S. A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. *J. Supercomput.* **2020**, *76*, 6860–6886. [CrossRef]
94. Babu, M.V.; Alzubi, J.A.; Sekaran, R.; Patan, R.; Ramachandran, M.; Gupta, D. An Improved IDAF-FIT Clustering Based ASLPP-RR Routing with Secure Data Aggregation in Wireless Sensor Network. *Mob. Netw. Appl.* **2021**, *26*, 1059–1067. [CrossRef]
95. Das, R.; Dwivedi, M. Multi agent dynamic weight based cluster trust estimation for hierarchical wireless sensor networks. *Peer-to-Peer Netw. Appl.* **2022**, *15*, 1505–1520. [CrossRef]
96. Devi, P.P.; Jaison, B. Optimal Scheme for the Detection and Classification of Clone Node Attack in WSN Using TAIGBRFCNIA. *Wirel. Pers. Commun.* **2022**, *125*, 1615–1629. [CrossRef]
97. Gandhimathi, L.; Murugaboopathi, G. Mobile Malicious Node Detection Using Mobile Agent in Cluster-Based Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *117*, 1209–1222. [CrossRef]
98. Gowdhaman, V.; Dhanapal, R. An intrusion detection system for wireless sensor networks using deep neural network. *Soft Comput.* **2021**, *26*, 13059–13067. [CrossRef]
99. Khot, P.S.; Naik, U. Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection. *Wirel. Pers. Commun.* **2021**, *119*, 2405–2429. [CrossRef]
100. Mittal, N.; Singh, S.; Singh, U.; Salgotra, R. Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks. *Wirel. Netw.* **2021**, *27*, 151–174. [CrossRef]
101. Prasad, S.N.; Selvan, K.S.; Dhevi, B.L. Intrusion Detection System in Wireless Sensor Networks and Fair Resource Allocation Using Geometric Deep Learning Techniques. *Wirel. Pers. Commun.* **2021**, *123*, 3401–3412. [CrossRef]
102. Nguyen, T.N.; Le, V.V.; Chu, S.I.; Liu, B.H.; Hsu, Y.C. Secure Localization Algorithms Against Localization Attacks in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *in press*. [CrossRef]
103. Wang, S.; Chen, Y. Optimization of Wireless Sensor Network Architecture with Security System. *J. Sens.* **2021**, *2021*, 7886639. [CrossRef]
104. Prithi, S.; Sumathi, S. Automata Based Hybrid PSO–GWO Algorithm for Secured Energy Efficient Optimal Routing in Wireless Sensor Network. *Wirel. Pers. Commun.* **2021**, *117*, 545–559. [CrossRef]
105. Raghav, R.S.; Prabu, U.; Rajeswari, M.; Saravanan, D.; Thirugnanasambandam, K. Cuddle death algorithm using ABC for detecting unhealthy nodes in wireless sensor networks. *Evol. Intell.* **2021**, *15*, 1605–1617. [CrossRef]
106. Sajitha, M.; Kavitha, D.; Reddy, P.C. An optimized whale based replication node prediction in wireless sensor network. *Wirel. Netw.* **2022**, *28*, 1587–1603. [CrossRef]
107. Dhanalakshmi, B.; SaiRamesh, L.; Selvakumar, K. Intelligent energy-aware and secured QoS routing protocol with dynamic mobility estimation for wireless sensor networks. *Wirel. Netw.* **2021**, *27*, 1503–1514. [CrossRef]
108. Maheswari, M.; Karthika, R.A. A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *118*, 1535–1557. [CrossRef]
109. Sumalatha, M.S.; Nandalal, V. An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN). *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 4559–4573. [CrossRef]
110. Yousefpoor, E.; Barati, H.; Barati, A. A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 1917–1942. [CrossRef]
111. Zhang, T.; Han, D.; Marino, M.D.; Wang, L.; Li, K.C. An Evolutionary-Based Approach for Low-Complexity Intrusion Detection in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *126*, 2019–2042. [CrossRef]
112. Hajiee, M.; Fartash, M.; Eraghi, N.O. Trust-based routing optimization using multi-ant colonies in wireless sensor network. *China Commun.* **2021**, *18*, 155–167. [CrossRef]
113. Ezhilarasi, M.; Gnanaprasanambikai, L.; Kousalya, A.; Shanmugapriya, M. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. *Soft Computing* **2022**, *in press*. [CrossRef]
114. Chengbo, Y.; Rui, L.; Qiang, H.; Lei, Y.; Jun, T. Fault Diagnosis of Nodes in WSN Based on Particle Swarm Optimization and Gaussian Distribution. *J. Vib. Meas. Diagn.* **2013**, *8*, 9908–9912.
115. Guo, W.; Li, J.; Chen, G.; Niu, Y.; Chen, C. A PSO-Optimized Real-Time Fault-Tolerant Task Allocation Algorithm in Wireless Sensor Networks. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 3236–3249. [CrossRef]

116. Kaur, T.; Kumar, D. Particle Swarm Optimization-Based Unequal and Fault Tolerant Clustering Protocol for Wireless Sensor Networks. *IEEE Sens. J.* **2018**, *18*, 4614–4622. [CrossRef]
117. Gao, Y.; Xiao, F.; Liu, J.; Wang, R. Distributed Soft Fault Detection for Interval Type-2 Fuzzy-Model-Based Stochastic Systems With Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 334–347. [CrossRef]
118. Yue, Y.; Cao, L.; Hang, B.; Luo, Z. A swarm intelligence algorithm for routing recovery strategy in wireless sensor networks with mobile sink. *IEEE Access* **2018**, *6*, 67434–67445. [CrossRef]
119. Swain, R.R.; Khilar, P.M.; Dash, T. Multifault diagnosis in WSN using a hybrid metaheuristic trained neural network. *Digit. Commun. Netw.* **2018**, *6*, 86–100. [CrossRef]
120. Surya, S.; Ravi, R. MPSO-SHM: Modified PSO Based Structural Health Monitoring System for Detecting the Faulty Sensors in WSN. *Wirel. Pers. Commun.* **2019**, *108*, 141–157. [CrossRef]
121. Noshad, Z.; Javaid, N.; Saba, T.; Wadud, Z.; Saleem, M.Q.; Alzahrani, M.E.; Sheta, O.E. Fault Detection in Wireless Sensor Networks through the Random Forest Classifier. *Sensors* **2019**, *19*, 1568. [CrossRef] [PubMed]
122. Masdari, M.; Ozdemir, S. Towards Coverage-Aware Fuzzy Logic-Based Faulty Node Detection in Heterogeneous Wireless Sensor Networks. *Wirel. Pers. Commun.* **2020**, *111*, 581–610. [CrossRef]
123. Menaria, V.K.; Jain, S.; Raju, N.; Kumari, R.; Nayyar, A.; Hosain, E. NLFFT: A novel fault tolerance model using artificial intelligence to improve performance in wireless sensor networks. *IEEE Access* **2020**, *8*, 149231–149254. [CrossRef]
124. Emperuman, M.; Chandrasekaran, S. Hybrid Continuous Density Hmm-Based Ensemble Neural Networks for Sensor Fault Detection and Classification in Wireless Sensor Network. *Sensors* **2020**, *20*, 745. [CrossRef]
125. Talmale, R.; Bhat, M.N. Energy Attentive and Pre-fault Recognize Mechanism for Distributed Wireless Sensor Network Using Fuzzy Logic Approach. *Wirel. Pers. Commun.* **2021**, *124*, 1263–1280. [CrossRef]
126. Rajan, M.S.; Dilip, G.; Kannan, N.; Namratha, M.; Majji, S.; Mohapatra, S.K.; Patnala, T.R.; Karanam, S.R. Diagnosis of fault node in wireless sensor networks using adaptive neuro-fuzzy inference system. *Appl. Nanosci.* **2021**, *in press*. [CrossRef]
127. Mahmood, T.; Li, J.; Pei, Y.; Akhtar, F.; Butt, S.A.; Ditta, A.; Qureshi, S. An intelligent fault detection approach based on reinforcement learning system in wireless sensor network. *J. Supercomput.* **2022**, *78*, 3646–3675. [CrossRef]
128. Agarwal, V.; Tapaswi, S.; Chanak, P. Intelligent Fault-Tolerance Data Routing Scheme for IoT-enabled WSNs. *IEEE Internet Things J.* **2022**, *9*, 16332–16342. [CrossRef]
129. Jaiswal, K.; Anand, V. FAGWO-H: A hybrid method towards fault-tolerant cluster-based routing in wireless sensor network for IoT applications. *J. Supercomput.* **2022**, *78*, 11195–11227. [CrossRef]
130. Asif, M.; Khan, S.; Ahmad, R.; Sohail, M.; Singh, D. Quality of service of routing protocols in wireless sensor networks: A review. *IEEE Access* **2017**, *5*, 1846–1871. [CrossRef]
131. Liu, M.; Xu, S.; Sun, S. An agent-assisted QoS-based routing algorithm for wireless sensor networks. *J. Netw. Comput. Appl.* **2012**, *35*, 29–36. [CrossRef]
132. Perkins, C.; Royer, E.M.; Das, S. Ad-Hoc on Demand Distance Vector Routing (AODV). In Proceedings of the Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, 25–26 February 1999.
133. Camilo, T.; Carreto, C.; Silva, J.S.; Boavida, F. An Energy-Efficient Ant-Based Routing Algorithm for Wireless Sensor Networks. In *Proceedings of the Ant Colony Optimization and Swarm Intelligence, Brussels, Belgium, 4–7 September 2006*; Dorigo, M., Gambardella, L.M., Birattari, M., Martinoli, A., Poli, R.; Stützle, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 49–59.
134. Restuccia, F.; Das, S.K. Optimizing the lifetime of sensor networks with uncontrollable mobile sinks and QoS constraints. *ACM Trans. Sens. Netw. (TOSN)* **2016**, *12*, 1–31. [CrossRef]
135. Farzana, A.H.F.; Neduncheliyan, S. Ant-based routing and QoS-effective data collection for mobile wireless sensor network. *Wirel. Netw.* **2017**, *23*, 1697–1707. [CrossRef]
136. Le, D.V.; Oh, H.; Yoon, S. RoCoMAR: Robots' Controllable Mobility Aided Routing and Relay Architecture for Mobile Sensor Networks. *Sensors* **2013**, *13*, 8695–8721. [CrossRef] [PubMed]
137. Ba, P.D.; Gueye, B.; Niang, I.; Noel, T. MoX-MAC: A low power and efficient access delay for mobile wireless sensor networks. In Proceedings of the 2011 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2011), Toulouse, France, 26–128 October 2011; pp. 1–6. [CrossRef]
138. Collotta, M.; Pau, G.; Maniscalco, V. A fuzzy logic approach by using particle swarm optimization for effective energy management in IWSNs. *IEEE Trans. Ind. Electron.* **2017**, *64*, 9496–9506. [CrossRef]
139. Hamidouche, R.; Aliouat, Z.; Gueroui, A.M. Genetic Algorithm for Improving the Lifetime and QoS of Wireless Sensor Networks. *Wirel. Pers. Commun.* **2018**, *101*, 2313–2348. [CrossRef]
140. Xinhua, W.; Sheng, W. Performance comparison of LEACH and LEACH-C protocols by NS2. In Proceedings of the 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science, Hong Kong, China, 10–12 August 2010; pp. 254–258.
141. Baroudi, U.; Bin-Yahya, M.; Alshammari, M.; Yaqoub, U. Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 1325–1338. [CrossRef]
142. Sunitha, R.; Chandrika, J. Evolutionary Computing Assisted Wireless Sensor Network Mining for QoS-Centric and Energy-efficient Routing Protocol. *Int. J. Eng.* **2020**, *33*, 791–797. [CrossRef]

143. Rani, S.; Balasaraswathi, M.; Reddy, P.C.S.; Brar, G.S.; Sivaram, M.; Dhasarathan, V. A hybrid approach for the optimization of quality of service metrics of WSN. *Wirel. Netw.* **2020**, *26*, 621–638. [CrossRef]
144. Tripathi, K.; Agarwal, T.; Dixit, S. Performance of DSDV protocol over sensor networks. *Int. J. Next Gener. Netw.* **2010**, *2*, 53–59. [CrossRef]
145. Jaiswal, K.; Anand, V. A QoS aware optimal node deployment in wireless sensor network using Grey wolf optimization approach for IoT applications. *Telecommun. Syst.* **2021**, *78*, 559–576. [CrossRef]
146. Jaiswal, K.; Anand, V. A Grey-Wolf based Optimized Clustering approach to improve QoS in wireless sensor networks for IoT applications. *Peer Netw. Appl.* **2021**, *14*, 1943–1962. [CrossRef]
147. Nigam, G.K.; Dabas, C. ESO-LEACH: PSO based energy efficient clustering in LEACH. *J. King Saud Univ.—Comput. Inf. Sci.* **2021**, *33*, 947–954. [CrossRef]
148. Wang, T.; Zhang, G.; Yang, X.; Vajdi, A. Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks. *J. Syst. Softw.* **2018**, *146*, 196–214. [CrossRef]
149. Mohanadevi, C.; Selvakumar, S. A qos-aware, hybrid particle swarm optimization-cuckoo search clustering based multipath routing in wireless sensor networks. *Wirel. Pers. Commun.* **2021**, *127*, 1985–2001. [CrossRef]
150. Arumugam, G.S.; Ponnuchamy, T. EE-LEACH: Development of energy-efficient LEACH Protocol for data gathering in WSN. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 76. [CrossRef]
151. Vimalarani, C.; Subramanian, R.; Sivanandam, S. An enhanced PSO-based clustering energy optimization algorithm for wireless sensor network. *Sci. World J.* **2016**, *2016*, 8658760. [CrossRef]
152. Saha, S.; Chaki, R. QoS-based congestion evasion clustering framework of wireless sensor networks. *Kuwait J. Sci.* **2021**. [CrossRef]
153. Moshref, M.; Al-Sayyed, R.; Al-Sharaeh, S. An Enhanced Multi-Objective Non-Dominated Sorting Genetic Routing Algorithm for Improving the QoS in Wireless Sensor Networks. *IEEE Access* **2021**, *9*, 149176–149195. [CrossRef]
154. Shujaa, M. Lagged multi-objective jumping particle swarm optimization for wireless sensor network deployment. *J. Theor. Appl. Inf. Technol.* **2019**, *97*, 423–433.
155. Deb, K.; Pratap, A.; Agarwal, S.; Meyarivan, T. A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Trans. Evol. Comput.* **2002**, *6*, 182–197. [CrossRef]
156. Deb, K.; Jain, H. An evolutionary many-objective optimization algorithm using reference-point-based nondominated sorting approach, part I: Solving problems with box constraints. *IEEE Trans. Evol. Comput.* **2014**, *18*, 577–601. [CrossRef]
157. Nabavi, S.R.; Osati Eraghi, N.; Akbari Torkestani, J. Intelligent Optimization of QoS in Wireless Sensor Networks Using Multiobjective Grey Wolf Optimization Algorithm. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5385502. [CrossRef]
158. Singh, S. Improved artificial bee colony metaheuristic for energy-efficient clustering in wireless sensor networks. *Artif. Intell. Rev.* **2019**, *51*, 329–354.
159. Singh, S. Improved multiobjective weighted clustering algorithm in Wireless Sensor Network. *Artif. Intell. Rev.* **2017**, *18*, 45–54.
160. Ma, Z.F.; Li, G.M. Improvement on LEACH-C protocol for wireless sensor network (LEACH-CC). In Proceedings of the Artificial Intelligence Science and Technology: Proceedings of the 2016 International Conference (AIST2016), Shanghai, China, 15–17 July 2017; pp. 362–368.
161. Bajpai, P.; Kumar, M. Genetic algorithm–an approach to solve global optimization problems. *Indian J. Comput. Sci. Eng.* **2010**, *1*, 199–206.
162. El-Sawy, A.A.; Hussein, M.A.; Zaki, E.; Mousa, A. An introduction to genetic algorithms: A survey a practical issues. *Int. J. Sci. Eng. Res.* **2014**, *5*, 252–262.
163. Abdmouleh, Z.; Gastli, A.; Ben-Brahim, L.; Haouari, M.; Al-Emadi, N.A. Review of optimization techniques applied for the integration of distributed generation from renewable energy sources. *Renew. Energy* **2017**, *113*, 266–280. [CrossRef]
164. Jabbar, S.; Iram, R.; Minhas, A.A.; Shafi, I.; Khalid, S.; Ahmad, M. Intelligent optimization of wireless sensor networks through bio-inspired computing: Survey and future directions. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 421084. [CrossRef]
165. Sarobin, M.V.R.; Ganesan, R. Swarm Intelligence in Wireless Sensor Networks: A Survey. *Int. J. Pure Appl. Math.* **2015**, *101*, 773–807.
166. Montoya, A.; Restrepo, D.C.; Ovalle, D.A. Artificial intelligence for wireless sensor networks enhancement. In *Smart Wireless Sensor Networks*; BoD: Norderstedt, Germany, 2010; pp. 73–81.
167. Kulkarni, R.V.; Forster, A.; Venayagamoorthy, G.K. Computational intelligence in wireless sensor networks: A survey. *IEEE Commun. Surv. Tutor.* **2010**, *13*, 68–96. [CrossRef]
168. Yang, X.S. Nature-inspired mateheuristic algorithms: Success and new challenges. *arXiv* **2012**, arxiv:1211.6658.
169. Kar, A.K. Bio inspired computing–a review of algorithms and scope of applications. *Expert Syst. Appl.* **2016**, *59*, 20–32. [CrossRef]
170. Darwish, A. Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications. *Future Comput. Inform. J.* **2018**, *3*, 231–246. [CrossRef]
171. Renman, C.; Fristedt, H. *A Comparative Analysis of a Tabu Search and a Genetic Algorithm for Solving a University Course Timetabling Problem*; KTH Royal Institute of Technology: Stockholm, Sweden, 2015.
172. Henderson, D.; Jacobson, S.H.; Johnson, A.W. The theory and practice of simulated annealing. In *Handbook of Metaheuristics*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 287–319.

173. Sabri, N.M.; Puteh, M.; Mahmood, M.R. A review of gravitational search algorithm. *Int. J. Advance. Soft Comput. Appl* **2013**, *5*, 1–39.
174. Thompson, N.C.; Greenewald, K.; Lee, K.; Manso, G.F. The computational limits of deep learning. *arXiv* **2020**, arxiv:2007.05558.
175. Chen, C.; Zhang, P.; Zhang, H.; Dai, J.; Yi, Y.; Zhang, H.; Zhang, Y. Deep Learning on Computational-Resource-Limited Platforms: A Survey. *Mob. Inf. Syst.* **2020**, *2020*, 8454327. [CrossRef]
176. Siebers, P.O.; Aickelin, U. Introduction to multi-agent simulation. In *Encyclopedia of Decision Making and Decision Support Technologies*; IGI Global: Hershey, PA, USA, 2008; pp. 554–564.
177. Salazar, L.A.C.; Mayer, F.; Schütz, D.; Vogel-Heuser, B. Platform independent multi-agent system for robust networks of production systems. *IFAC-PapersOnLine* **2018**, *51*, 1261–1268. [CrossRef]
178. Wu, H.; Han, X.; Yang, B.; Miao, Y.; Zhu, H. Fault-Tolerant Topology of Agricultural Wireless Sensor Networks Based on a Double Price Function. *Agronomy* **2022**, *12*, 837. [CrossRef]
179. Wang, K.; Yang, J. Fault-Tolerant Relay Node Placement in Wireless Sensor Networks for Surveillance of Overhead Transmission Lines. *Math. Probl. Eng.* **2022**, *2022*, 247588363. [CrossRef]
180. Ben Yahya, M. Security of Software-Defined Wireless Sensor Networks. Ph.D. Thesis, Waterloo, Ontario, Canada, 2022, UWSpace. Available online: http://hdl.handle.net/10012/18302 (accessed on 1 September 2022).