IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 July 2023, accepted 4 August 2023, date of publication 7 August 2023, date of current version 11 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3303113

RESEARCH ARTICLE

Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach

MUAWIA A. ELSADIG
Deanship of Scientific Research, Imam Abdulrahman Bin Faisal University (IAU), Dammam 34212, Saudi Arabia
e-mail: muawiasadig66@gmail.com

ABSTRACT The characteristics and performance of wireless sensor networks (WSNs) are the main reasons for their rapid expansion in various fields. However, these networks are extremely susceptible to multiple security assaults, including denial-of-service (DoS) attacks, which are among the most prevalent in these networks. This study sheds light on WSN restrictions, weaknesses, and security threats with a focus on DoS attacks. Recent techniques for DoS attack detection have been investigated thoroughly, highlighting their achievements and limitations. This provides valuable insight into the current state of recent research in this field. Accordingly, this study proposes a lightweight machine learning detection approach based on a decision tree (DT) algorithm with the Gini feature selection method to detect DoS attacks in WSNs. An enhanced version of the WSN-DS dataset, developed by the author, was used to train and test the proposed approach. The proposed approach has shown good performance by achieving an accuracy rate of 99.5% with minimum overhead compared to random forest (RF), extreme gradient boosting (XGBoost), and k-nearest neighbor (KNN) classifiers. It only takes 9.7%, 13%, and 2% of the processing time required by FR, XGBoost, and KNN respectively, which indicates that our proposed approach significantly outperforms these classifiers in terms of processing time. It is noteworthy that RF achieved an accuracy that was somewhat superior; however, the proposed approach greatly surpassed RF by taking only 9.7% of the RF processing time, which is an important factor in meeting WSN constraints.

INDEX TERMS Deep learning, DoS attacks, cyber security, feature selection, IoT security, network security, machine learning, wireless sensor networks, WSN attacks, WSN constraints, WSN security.

I. INTRODUCTION

Wireless sensor networks (WSNs) have the potential to create a new generation of distributed systems and satisfy the requirements of many critical real-time applications. Moreover, most Internet of Things (IoT) devices are based on wireless sensor node technology because they provide an adequate communication platform. WSNs are the core and important fundamental components of the IoT [1], [2]. WSNs have a wide range of potential uses, and have recently attracted considerable attention. WSNs are one of the most significant technologies in the twenty-first century [3]. However, these networks face many challenges compared with traditional networks. Security and energy efficiency are significant challenges [4]. In terms of security, Denial of Service (DoS), node duplication, and node damage are the main threats to WSNs [5].

Using an unguided transmission medium renders WSNs more vulnerable to security attacks than other networks that use a guided transmission medium. In addition, the limits of computing power, batteries, and memory make the most common security measures inapplicable to WSNs (e.g., public key cryptography). Therefore, these types of networks require security solutions that cause a very low overhead, which is difficult to achieve.

WSNs are simple, easy, and inexpensive to implement in various critical fields, and meet the requirements of real-life applications. However, their constraints and limitations

The associate editor coordinating the review of this manuscript and approving it for publication was Qingchun Chen.

of computational capacity make WSNs highly susceptible to various types of security attacks [6], [7], particularly DoS attacks. DoS attacks are among the most frequently occurring attacks on these networks [8], [9], [10], and are very difficult to defend [11].

Although several research methods have been introduced to address the security issues in WSNs, finding an effective security solution remains challenging.

Given the drawbacks of the authentication procedures in these networks, there is a focus on the importance of utilizing blockchain technology in WSNs. Dener et al. [12] proposed an authentication protocol based on the blockchain technology for WSNs. However, there are several difficulties in using blockchain in WSN, including the processing time, storage, and power consumption. Blockchain requires significant processing power and energy, whereas WSNs have limited capacity nodes. In the other hand, significant attention has also been paid to device-free localization (DFL) technology, which has become feasible for WSNs owing to recent the advancements in wireless sensing technology. Interested readers can refer to [13] and [14].

This study provides comprehensive details on WSN constraints, vulnerabilities, and attack classification. It investigates recent methods to counter DoS attacks, aiming to develop a lightweight detection method for DoS attacks in WSNs, as the author is highly motivated to introduce a solution that meets the WSN constraints. The contributions of this study can be summarized as follows.

- It provides comprehensive details on WSN constraints, vulnerabilities, and attacks classification, with a focus on DoS attacks.
- It demonstrates the insufficient and drawbacks of cryptographic methods to resolve security issues of WSNs
- It investigates recent machine learning and deep learning methods to counter DoS attacks and evaluate their achievements and limitations.
- It develops an enhanced version of the WSN-DS dataset by applying an adequate feature selection method to improve the dataset. Evidence for this improvement has been provided through the results achieved.
- It Introduces a lightweight machine learning detection approach based on the decision tree (DT) classification algorithm and the Gini feature selection method. This approach achieved a high classification accuracy with an acceptable overhead.
- It compares the proposed detection approach with some detection approaches that have been recently presented to counter DoS attacks. The comparison results indicate that the proposed detection approach outperforms other classifiers.
- It provides a thorough discussion of the experimental results obtained.

This section defines the WSNs and briefly introduces their importance, constraints, and security issues. In addition, the contributions of this study are summarized.

The rest of this paper is organized as follows. Section II lists the security requirements for achieving the goal of obtaining secure WSN applications. Section III sheds light on WSN attack types and their classifications. Section IV briefly introduces and categorizes DoS attacks using a layer-based classification approach. Section V highlights the recent countermeasure approaches and their mechanisms for countering DoS attacks. The achievements and limitations of these approaches are also discussed. In addition, this section addresses the fact that traditional approaches are insufficient to work against these attacks; therefore, it provides a comprehensive investigation of detection methods based on machine learning approaches. A description of our proposed machine learning algorithm for detecting DoS attacks is presented in Section VI. Section VII presents the implementation results of the proposed detection method and provides a thorough discussion of these results. Finally, conclusions are summarized in Section VIII.

II. SECURITY REQUIREMENTS

Security in WSNs can be maintained by achieving security parameters that include integrity, availability, confidentiality, non-repudiation, accountability, authentication, freshness, backward secrecy and forward secrecy [15].

Although the security objectives of WSNs and traditional wired networks are similar, security in WSNs requires special solutions that incur low computational overhead to satisfy the WSN limitations and constraints.

III. WSN ATTACKS CLASSIFICATION

WSNs are extremely vulnerable to several security attacks [16] because of their broadcast nature, and their nodes are frequently situated in hostile or dangerous environments that are difficult to defend. WSN attacks have been categorized using a variety of methods, including active versus passive, insider versus external, and layer-based classification. Here, the author focuses on two types of classifications: internal/external and layer-based. Duru et al. [17] classified WSN attacks into three categories: (i) service integrity silence, (ii) secrecy and authentication, and (iii) network availability. The latter area of attack is concerned with attacks that threaten network availability and therefore affect the services provided by these networks. These types of attacks are known as DoS attacks, which prevent true users from accessing the network services. This is a major threat with an impactful effect [18].

A. INTERNAL\EXTERNAL CLASSIFICATION

Table 1 lists the categorization of WSN attacks into two approaches: internal attacks, which represent inside attacks, and external attacks, which represent attacks originating from outside [19]. Further details on this classification are provided in [20].

This categorization represents the higher proportion of internal attacks compared to external ones.

TABLE 1. WSN internal/eternal attacks classification.

External attacks	Internal attacks	External /Internal attacks
Node replication	Sybil attack	Man in the middle
Intelligent jamming	Worm hole	Denial of service
Basic jammers	Replay attack	Malicious code attack
Eavesdropping	Black hole	Attack on reliability
	Data integrity	Desynchrony attack
	Collision	Energy drain
	Sinkhole	Hello flood
	Selective forwarding	Spoofed/altered inf.
		Hardware hacking
		Node tampering

B. LAYER-BASED CLASSIFICATION

Based on the open system interconnection (OSI) approach, the security attacks that target the IoT and WSN Layers are classified as shown in Table 2 [21]. This table grouped these attacks based on WSN Layers.

TABLE 2. Layer-based classification.

Layer	Security attack
Application	Path-based DoS, Spoofing, false data ejection, alter routing.
Transport	Flooding and De-synchronization
Network	Sinkhole attack, grey hole attack, black hole attack, internet smurf attack, hello flood attack, wormhole attack, misdirection attack, spoofing attack, and selective forwarding attack.
Data link	Spoofing, replay attack, collision, Sybil Attack, altering routing attack, exhaustion, monitoring and traffic analysis
Physical layer	Sybil attack, tempering, jamming, radio interference, and Interception

The layer-based classification makes it evident that the network layer attacks outnumber those in the other layers.

IV. DoS ATTACK

DoS attacks are among the most widespread types of WSN attack and can be performed in different layers of WSNs [22], [23]. These attacks are considered as key security issues in these networks [24]. Owing to their resource constrained and distributed nature, WSNs are susceptible to these types of attack [25]. DoS assaults aim to block access to information and IT systems, and target their accessibility. The main objective of these attacks is to prevent the network from operating normally by preventing the services offered by sensor nodes. Attackers use several attack types to stop network nodes from using their resources. Some indicators of a DoS attack include a decline in network performance, slowness or loss of packets, unresponsiveness of some network components, and an increase in spam messages. There are numerous different types of DoS attacks according to each layer and protocol of the WSNs. Table 3 lists the different types of DoS attacks that exploit different WSN layers [26], [27], [28].

TABLE 3. DoS attacks.

Layer	Attack
Physical layer	Destruction, node tampering, and jamming
Data link layer	Collision, interrogation exhaustion, unfairness, and denial of sleep
Network and Routing layer	Homing, black holes, clustering messages, altering control traffic, replaying, spoofing, and hello floods
Transport layer	Synchronize flood and flooding, desynchronization.
Application layer	Deluge (reprogramming) attack, path-based DoS, and overwhelming sensors

V. RELATED WORK

This section provides a comprehensive review of WSN security issues and solutions for overcoming these issues. It provides the advantages and disadvantages of current solutions with a focus on DoS attacks, and recent machine learning and deep learning methods have been proposed to detect them. This section organized as follows. Section A provides a general overview of the importance of WSNs, security issues, and common strategies for mitigating these issues. Section B demonstrates the insufficiencies and drawbacks of cryptographic methods for resolving the security issues of WSNs. Section C provides a thorough review of the current machine learning and deep learning methods that have been presented to detect DoS attacks on WSNs. The advantages and disadvantages of these methods in mitigating or discovering these types of attacks are discussed. In addition, it highlights that deep learning approaches are not adequate solutions for WSNs because they cause more overhead than machine learning approaches.

A. OVERVIEW

Security of WSNs is an important and challenging task. These networks provide an adequate platform for the advancement of communication technology. The number of Internet of Things (IoT) devices is expected to exceed 70 billion by 2025 [29]. Low-cost power devices represent 70% of the total, indicating that WSNs are the core of IoT. In fact, low-power wireless networks provide an adequate communication platform for IoT; however, maintaining this connectivity remains a challenge. In addition, WSNs are vulnerable to a variety of attacks owing to their heterogeneous nature [30]. Roman and Lopez [31] analyzed security problems when

connecting WSNs to Internet. They acknowledged that some issues must be resolved when integrating sensor nodes into the Internet infrastructure; therefore, full integration remains an open issue.

The lack of node synchronization during data routing renders WSNs vulnerable to DoS attacks. In addition, the deployment of WSNs in hostile areas makes them susceptible to capture and manipulation, which leads to a denial of service [1], [26]. It is well known that the core functionality of WSNs depends on the routing protocols. However, a Low-rate Denial of Service (LDoS) attack can significantly compromise the routing systems. LDoS attacks pose a serious issue for WSNs because typical intrusion detection systems that are currently in use are unable to identify these attacks [32].

Some efforts have focused on addressing the limitations of WSNs without considering the security issues. For example, the discovery of wireless power transfer (WPT) in wireless technology has potentially enhanced the energy limitations of WSNs. Many researchers have focused on enhancing the performance of wireless rechargeable sensor networks (WRSN) by optimizing their charging schedules. Therefore, many efforts have been made to enhance charging schedule algorithms and system performance, without paying attention to security issues. For example, when a malicious node sends many charging requests, incorrect responses occur, leading to denial of charge (DoC) attacks, which in turn lead to DoS attacks. The collaborative denial-of-charge attack method (CoDoC) that developed by Lin et al. [33] presented a real scenario of such attacks, which was used to send fake charging requests. CoDoC exhausts the sensors and results in missed events. This demonstrates the importance of security experts, designers, and developers paying close attention to WRSN security vulnerability.

Belkhiri et al. [34] indicated that WSNs face several challenges in terms of network security, management, and energy consumption. A solution to overcome these issues was presented, which is based on the integration of software-defined networks (SDN) with WSN to form the SDWSN model. However, owing to the use of open interfaces and standard protocols, this model still faces many challenges in securing WSNs against different types of attacks, particularly DoS attacks.

B. CRYPTOGRAPHIC METHODS

Cryptographic procedures are typically used for security in WSNs. Nevertheless, this traditional approach addresses only a portion of the potential problems. For instance, nodes may be physically taken over by an adversary, which enables the adversary to use them to introduce or inject false data into a network. Consequently, this may cause various types of damage that may affect the entire network, such as interference with the communication between network nodes. According to Haiguang et al. [35], authentication and cryptographic systems such as TinySec, SERP, INSENS, key session scheme, and SPINS are insufficient for use alone. Allakany et al. [36] indicated that asymmetric cryptography techniques are resource intensive; therefore, they are inappropriate for WSNs.

Furthermore, symmetric key cryptography is used in most security strategies, which complicates the key management. Conversely, several new approaches demonstrate the availability of public key cryptography to be adopted in WSNs by choosing appropriate algorithms and parameters, although this is too expensive in terms of energy cost and computation [37], [38]. Further research on this is still necessary [39], and any encryption structure requires the transmission of additional bits, which requires additional processing and, therefore, more overhead [40]. Using an encryption technique in such networks causes an increase in delay, jitter, and packet loss [41].

Despite significant research efforts on key management, cryptography, secure data aggregation, secure routing and intrusion detection in WSNs, Sen [42] emphasized that there are still numerous security concerns to be solved, and that there are several challenges, such as the lack of a cryptographic method that fits all types of WSNs and selecting an appropriate cryptographic method depending on the computing power of the sensor nodes.

All of the aforementioned points prove that a lightweight method is required to present an effective solution that does not affect the performance of WSNs.

C. MACHINE LEARNING AND DEEP LEARNING

WSNs are severely threatened by DoS attacks. Owing to their open nature, WSNs are vulnerable to these types of attacks, which can have a significant impact on their behavior [43]. All types of DoS attacks are major threats to WSN reliability and security. DoS attacks can occur in any layer, including physical, network, transport, and application layers. However, WSN security remains an unresolved issue in this field. This section provides a thorough discussion that covers the current machine learning and deep learning approaches that have been recently presented to detect DoS attacks, with a focus on their achievements and limitations. A summary of this section is given in Table 4, which summarizes the advantages and disadvantages of the current detection methods compared to our proposed model.

Quincozes et al. [44] indicated that, despite the huge research efforts that have been presented recently, the detection of DoS attacks in IoT still poses a real challenge. The available option for spotting DoS attacks is the use of machine-learning approaches. In this context, Quincozes et al. presented a thorough assessment of both supervised and unsupervised machine learning approaches. They concluded that supervised approaches exhibit a better performance and are faster than unsupervised approaches. Machine learning is a branch of artificial intelligence (AI) that leverages past experiences to inform future actions without having to be explicitly programmed. Supervised, semi-supervised, and unsupervised learning are the main machine-learning categories. Machine learning technology

has ensured its capability in various fields, including network security [45]. According to Sagar et al. [46], machine learning plays an important role in many areas, such as real-time decision-making, and can process enormous amounts of data. However, hackers may exploit machine learning weaknesses to commit various adversarial attacks [47], such as when an illegitimate user intentionally raises false negative (FN) rates and reduces false positive (FP) rates in a manner that does not affect the overall error rate. Attackers can use this as a leverage to carry out highly sophisticated attacks. Sagar et al. pointed out that advanced attacks can exploit machine-learning-based malware detectors. Protecting machine-learning-based security solutions and addressing their flaws are essential.

Figure 1 displays the accuracy attained by various classifiers using the NSL-KDD dataset. A comparison of these classifiers was provided in [48]. The investigated classifiers included random forest (RF), deep belief network (DBN), support vector machine (SVM), naive Bayes (NB), artificial neural network (ANN), and decision tree (DT). The results show that all classifiers achieved an accuracy rate of over 95%, as shown in the figure. The DT classifier performed better than the other models, reaching an accuracy rating of 99.64%, whereas the RF had the lowest accuracy.

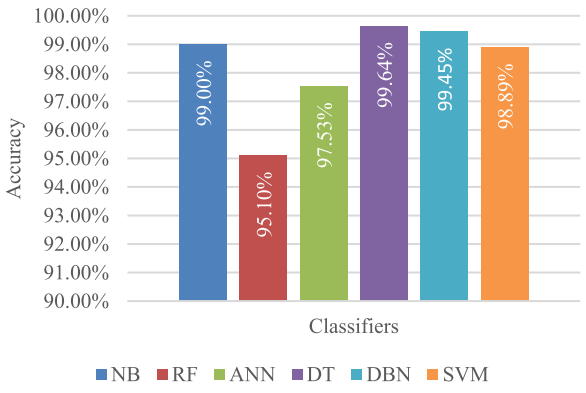

FIGURE 1. The accuracy of various classifiers that are trained and tested using NSL-KDD dataset.

Gebremariam et al. [49] proposed a scheme to detect multiple WSN attacks. Four datasets are used to train and test the proposed scheme. The scheme was built to detect ten classes of attacks, including DoS attacks. When the WNS-DS dataset was used, the accuracy rate of the proposed scheme was 99.65%. However, Neural networks are computationally expensive compared to traditional algorithms, which affects the QoS, especially when dealing with networks that have many constraints and limitations.

Osanaiye et al. [50] proposed a statistical method for detecting WSN DoS-jamming attacks. The normal operation of WSNs is disrupted by DoS-jamming attacks. It produces radio frequency waves to jam legitimate transmissions and obstruct services. The proposed method asserts that it can effectively detect jamming attacks and is suitable for real time applications. However, this approach must be tested on various datasets.

Le et al. [51] proposed an approach for detecting DoS attacks on WSNs. They used an RF classifier to recognize four types of attacks presented in the WSN-DS dataset. The proposed approach exhibited better classification accuracy than the ANN detection model presented in [52]. However, the results of this study were based on the use of a small number of instances, 94042 instances, during the test phase [53].

Almomani and Alenezi [54] indicated that RF outperformed ANN in detecting DoS attacks. They used different classification models, including SVM, NB, DT, RF, J48, ANN, and k-nearest neighbors (KNN). The employed dataset was WSN-DS, in which only some selected features were used and not all features were considered. However, RF is computationally expensive compared with other classification methods that are capable of achieving high detection accuracy.

Alsulaiman and Al-Ahmadi [55] evaluated several machine-learning algorithms to examine their potential for detecting DoS attacks. The WSN-DS dataset was used to train and test the models. The investigated algorithms included RF, j48, NB, SVM, and NN. They reported that RF achieved the highest accuracy of 99.72%, and the authors therefore recommended it. However, their results indicate that J48 achieved almost the same accuracy of 99.66%. and surpassed RF by taking less than 9% of the RF processing time. This indicates that J48 is better at meeting the WSN's limitations than RF.

Vinayakumar et al. [56] compared classical machine learning methods on different datasets, including KDDCup 99, NSL-KDD, WSN-DS, Kyoto, CICIDS 2017, and UNSW-NB15. They reported that, in the case of binary classification, DT, RF, and AB outperformed other classifiers, including NB, logistic regression (LR), SVM-rbf, and KNN. Moreover, DT, AB, and RF maintained the same performance over all datasets, indicating that these classifiers are generalizable and capable of discovering new attacks, whereas the other classifiers exhibited varied performance ranges. In terms of multi-class classification, DT and RF perform better, followed by AB and the rest of the classifiers.

A variety of methods have been developed for the detection and prevention of black-hole attacks in WSNs. However, these methods yield few false-positive results. The majority of non-WSN approaches are not appropriate for solving the black-hole problem in WSNs. This is because of the limitations of WSNs [57].

Wazirali and Ahmad [58] assessed the effectiveness of some machine learning techniques, including SVM, GBoost, KNN, DT, LR, multi layer perceptron (MLP), long short-term memory (LSTM), and NB. These classifiers were chosen to represent deep learning, statistical, logical, and instance-based classification categories. They evaluated the performance of the classifiers using the WSN-DS dataset, which was divided into six separate datasets. The authors claimed that, because the WSN-DS dataset contains

TABLE 4. DoS attack detection approaches.

Author	Approach descrption and achievments	Dataset	Limitations / obseravations	Year
Gebremariam et al. [49].	The authors introduced a method for identifying numerous WSN assaults. The proposed method is tested and trained on four datasets, including WNS-DS dataset. In case of using WNS-DS dataset, their method is successively achieved accuracy rate of 99.65% to detect DoS attacks.	WNS-DS, UNSW-NB, CICIDS2018, and NSL-KDD.	Neural network algorithms are computationally expensive compared to conventional machine learning algorithms, which has an impact on the quality of service, particularly when considering networks that have several restrictions and limitations such as WSNs.	2023
Salmi and Oughdir [6]	The authors developed and implemented some deep learning models to detect DoS attacks in WSNs. These models include Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), Dense Neural Network (DNN), and a model that combines the RNN and CNN architectures. All models were trained on WSN-DS dataset. Their results indicate that CNN outperformed the other models by achieving accuracy rate of 98.79%.	WSN-DS	In fact, deep learning models are causing more overhead compared to machine learning models. In case of WSNs, lightweight security solutions are required to meet these network constraints	2023
Wazirali et al [58]	The authors evaluated some classification models including SVM, GBoost, KNN, DT, LR, MLP, LSTM and NB. All models were tranied and tested using WSN-DS dataset, which was divided into six separate datasets. GBoost was the best based on the overall average of the performance metrics across all WSN-DS datasets. It achieved 99.6% accuracy rate.	WSN-DS	Due to the diversity of network threats, a single machine-learning method for DoS detection is no longer adequate, and other methods, such as feature learning and feature selection, are being integrated with machine-learning techniques to detect DoS attacks [60]. Moreover, ensemble approaches incur more overhead. They can enhance detection accuracy; however, they are not adequate for networks with limited computational power.	2022
Atitallah et al. [67]	The authors proposed a deep learning approach for identifying DoS attacks in WSNs. Several CNN models were combined using an ensemble approach using a voting method. They used WSN-DS dataset. Their approach showed good performance in terms of classification accuracy.	WSN-DS	The proposed approach uses deep learning method and an ensemble voting approach, both of which are computationally expensive and require more processing time.	2022
Ismail et al. [70]	The authors proposed a multi-layer machine learning detection model to mitigate cyberattacks in WSNs. They used a NB algorithm to form the first layer and a LightGBM algorithm to form the second layer. Using WSN-DS dataset, the proposed approach showed a detection accuracy rate of 99.3%	WSN-DS	The proposed approches consisted of two layers of classification methods which can increase the approach computational cost. In addition, some recent models outperformed this approach in terms of the accuracy rate, including our proposed approach.	2022
Tabbaa et al. [53]	The authors proposed two ensemble approaches, heterogeneous ensemble and homogeneous ensemble approaches. The heterogeneous ensemble consists of an adaptive RF and Hoeffding adaptive tree (HAT) algorithm, whereas the homogeneous ensemble HAT approach consists of ten models. The two approaches, homogeneous	WSN-DS	Both are ensemble approches that reqire more computitional power and also achieved less accuarcy rate compared to our proposed approach.	2022

TABLE 4. *(Continued.)* **DoS attack detection approaches.**

	and heterogeneous, were evaluated using WSN-DS dataset and showed detection accuracy rates of 97.2 % and 96.84% respectively.			
Alsulaiman et al. [55]	The authors invistigated several machine-learning modles to examine their potential for detecting DoS attacks. The WSN-DS dataset was used to train and test the models that included RF, j48, NB, SVM, and NN. The results indiacting that RF has outperformed others by achieving an accuracy of 99.72%.	WSN-DS	RF makes more overhead compared to our proposed model. Our proposed model is better in meeting WSN constraints.	2021
Alsahli et al. [71]	The authors evaluated three machine learning models including NB, RF, and instance base learner (IBK). These models were trained and tested on two datasets, KDDCup99 and WSN-DS. The reported results shoed that RF outperformed other classifiers by achieving high classification accuracy rate in both datasets whereas NB is lagged behind.	KDDCup99 and WSN-DS.	In terms of processing time, RF took considerable amount of time compared to the two other classifiers and also copmared to our proposed apparaoch.	2021
Ifzarne et al. [72]	A detection model built on incremental machine learning was provided by the authors. The online passive aggressive classifier and the information gain ratio feature selection method were used to build this model. It was trained to recognize DoS assaults using the WSN-DS dataset. The simulation results demonstrated a 96% accuracy rate.	WSN-DS	Many recent approaches outperformed this model in terms of accuracy rate, including our proposed approach.	2021
Ismail et al. [73]	The author conducted a comparative study of six machine learning classification approaches including Catboost, LightGBM, RF, KNN, NB, and GBM to examine their capability to detect cyberattacks in WSNs. The classifiers were trained on WSN-DS dataset. The results indicated that LightGBM outperformed other classifiers by achieving accuracy rate of 99.3% when considering the all attacks of the WSN-DS dataset.	WSN-DS	Many recent approaches outperformed this model in terms of accuracy rate, including our proposed approach.	2021
Premkumar et al. [26]	The authors proposed a deep learning detection approach to detect DoS attacks. Researchers have demonstrated the effectiveness of their approach in accurately separating adversaries and making the system more resistant to DoS attacks.	-	The proposed approach is appropriate for sensor nodes with no or low mobility, whereas nodes in WSNs are highly dynamic [66].	2020
Vinayakumar et al. [56]	The authors tranied and tested several classical machine learning methods on different datasets, including WSN-DS. They reported that DT, RF, and AB outperformed other over all datasets, which indicates that these classifiers are generalizable and capable of discovering new attacks, whereas the other classifiers showed varied performance ranges. In addition, the authors proposed a deep learinng approch to detect and classify unpredictable and unforeseen cyberattacks. They confirmed that the proposed model	WSN-DS, KDDCup 99, NSL-KDD, Kyoto, CICIDS 2017, and UNSW-NB15.	The computational cost of the proposed model is quetionable, specifically when cosidering WSNs that have many constrints and limitation.	2019

TABLE 4. *(Continued.)* **DoS attack detection approaches.**

	performed well compared to the classical machine learning classification approches.			
Otoum et al. [68]	The authors compared their proposed deep learning approach called RBC-IDS with their machine learning approach ASCH-IDS that was presented in [69]. The KDD'99 dataset was used to compare the two approches. The results indicated that the two approaches achieved the same detection accuracy.	KDD'99	The deep learing approach took twice as long as the machine learing approach which indicating that deep learning approaches generate more overhead and demand more computational power than machine learning approaches. Thefore, deep laering is not a recommended soluation for networks with limited resources susch as WSNs.	2019
Osanaiye et al. [50]	In this study, a detection method was proposed to detect WSN DoS jamming attacks. The proposed method was evaluated using CRAWDAD dataset. The author confirmed that their method can effectively detect jamming attacks and is suitable for real-time applications.	CRAWDAD	This approach needs to be tested on various datasets.	2018
Le et al. [51]	The authors proposed a detection approach using RF classification algorithm to discover DoS attacks in WSNs. They used WSN-DS dataset which include four types of DoS attacks. It attained high detection accuracy compared to the ANN detection model presented in [52].	WSN-DS	The approach was used small number of instances in testing phase [53]. Therefore, more evaluation is required for these findings to be considered.	2018
Almomani et al. [54]	The authors reported that RF outperformed ANN in detecting DoS attacks. They used different classification models, including SVM, NB, DT, RF, J48, ANN, and k-nearest neighbors (KNN). The employed dataset was WSN-DS, in which only some selected features were used and not all features were considered.	WSN-DS	RF is computationally expensive compared to other classification methods that are capable of achieving high detection accuracy. In addition, our proposed approach outperformed RF in terms of computational cost.	2018
The proposed approach by the author of this study	The proposed approach uses DT with Gini feature selection method for the detection of DoS attacks in WSNs. It was trained on an enhanced version of WSN-DS dataset that was developed by the author through applying Gini feature selection method to select only features that have significant influence in detection performance and reduce computational overhead. The proposed approach has shown good performance by achieving an accuracy rate of 99.5% with minimum overhead compared to RF, XGBoost, and KNN classifiers. It only takes 9.7%, 13%, 2% of the processing time that FR, XGBoost, and KNN take respectively, which indicates that our proposed approach has significantly outperformed the other classifiers in terms of the processing time. It is noteworthy to mention that FR achieved accuracy of 99.7%, however, the proposed approach has greatly surpassed RF by taking only 9.7% of RF processing time	WSN-DS	WSN-DS is unbalanced; therefore, our future work would focus in overcoming this issue by applying appropriate oversampling and under sampling techniques. Developing a balanced version of this dataset which is expected to significantly enhance perdition accuracy.	-

numerical statistical values, logical and statistical classifiers produced the best performance measures. Furthermore, they stated that GBoost was the best based on the overall average of the performance metrics across all WSN-DS datasets, and they also determined the best dataset sizes that led to the best performance. However, their analysis was limited to only one type of WSN packet traffic [59]. Moreover, owing to the diversity of network threats, a single machine-learning method for DoS detection is no longer adequate, and other methods, such as feature learning and feature selection, are being integrated with machine-learning techniques to detect DoS attacks [60].

Jaitly et al. [61] provided details regarding jamming technologies and their categories such as reactive and proactive technologies. In addition, their work includes listing many challenges that reflect the difficulty of developing anti-jamming and jamming mechanisms; however, Jaitly et al. discussed technologies that can help develop defense mechanisms against these attacks if exploited properly [61]. Further details on some common jamming attacks that have been proven effective are available in [62]. Ciuonzo et al. [63] proved that the proposed rules to mitigate the presence of a jammer are effective; however, forwarding decisions to the Decision Fusion center is difficult in the case of a wideband jammer [64]. Nguyen et al. [29] discussed different jamming attacks and concluded that no comprehensive and effective anti-jamming technique has been offered to counter them. The authors also noted that energy depletion attacks (EDAs) are still regarded as real dangers, particularly in sensor networks used for critical infrastructure. EDA is a resource-depletion attack that causes significant damage, particularly in applications in which network availability is crucial [65].

Premkumar and Sundararajan [26] proposed a deep-learning detection approach to detect DoS attacks. Researchers have demonstrated the effectiveness of their approach in accurately separating adversaries and rendering a system more resistant to DoS attacks. However, the proposed approach is appropriate for sensor nodes with no or low mobility, whereas nodes in WSNs are highly dynamic [66], and their proposed approach must be evaluated on different datasets.

Atitallah et al. [67] proposed a deep-learning approach for identifying DoS attacks in WSNs. Several convolutional neural network (CNN) models were combined using an ensemble approach based on the voting method. They used the WSN-DS dataset, which includes four types of DoS attack. Their approach was evaluated and showed good performance in terms of classification accuracy. However, this approach uses deep learning methods and an ensemble voting approach, both of which are computationally expensive and require additional processing time. Therefore, its efficiency in WSNs, characterized by limited resources, needs to be examined.

Vinayakumar et al. [56] employed a deep neural network (DNN) classifier to create an intrusion detection approach. Their approach demonstrated a good accuracy for various types of network traffic. It performed well on the KDD-Cup 99 dataset and was applied to other datasets, including NSL-KDD, WSN-DS, Kyoto, CICIDS 2017, and UNSW-NB15. However, no discussion has been presented on the cost of their approach in terms of the power and CPU [59]. Therefore, the computational costs of this approach must be evaluated.

Aiming to investigate the feasibility of deep learning-based intrusion detection approaches as an alternative to machine learning-based intrusion detection systems so as to be used in monitoring the critical infrastructure of WSNs, Otoum et al. compared their proposed deep learning approach called restricted Boltzmann based clustered IDS (RBC-IDS), which was presented in [68], with the machine learning approach called Adaptively Supervised and Clustered Hybrid (ASCH-IDS), which was presented in [69]. The KDD'99 dataset was used to compare the two methods. The authors stated that the two approaches achieved the same level of detection accuracy, but the RBC-IDS took twice as long as the ASCH-IDS, indicating that deep learning approaches generate more overhead and demand more computational power than machine learning approaches. Moreover, Ahmad et al. indicated that simple classification algorithms, such as (SVM, LR, and DT) are more ideal for real applications of intrusion detection than deep learning approaches [59].

VI. METHOD

A. INTRODUCTION

This section introduces our research method, which uses some common machine learning algorithms that are carefully selected based on their high impact and considerable contribution to achieving high performance in detecting many security attacks, particularly for their capability to identify DoS attacks. The WNS-DS dataset, which includes four types of DoS attacks, was used for the training and testing. In addition, a feature selection method was employed to enhance the dataset, thereby boosting classification accuracy and minimizing computational overhead.

The classifiers selected in this study included extreme gradient boosting (XGBoost), RF, KNN, and DT. All these classifiers were trained and tested using the WSN-DS of 18 features and the enhanced version, which included 16 features. The accuracy obtained using both datasets is reported, which ensures to the efficiency of the developed dataset.

All experiments in this study were conducted using Orange data mining software. It is a potent tool with great potential for effectively and professionally visualizing data. This open-source software is helpful for developing various machine-learning classification algorithms. With Python scripting and visual programming, Orange is a machine learning and data mining package for data analysis [74]. It offers a robust platform for data analysis as well as a wide range of tools. Orange version 3,34.0, was used to build all the models under investigation throughout this study.

TABLE 5. WSN-DS features.

Feature No.	Feature Name
1	ADV-S
2	Is-CH
3	Rank
4	SCH-S
5	Send-code
6	JOIN-S
7	Dist-To-CH
8	SCH-R
9	JOIN-R
10	DATA-S
11	Data-sent-To-BS
12	AVD-R
13	Who-CH
14	ID
15	Expaned Energy
16	Time
17	Dist_CH_To_BS
18	DATA-R

TABLE 6. Feature weight.

Feature	Weight (score)	Comment
ADV-S	0.093	selected
Is-CH	0.083	selected
Rank	0.043	selected
SCH-S	0.041	selected
Send-code	0.038	selected
JOIN-S	0.038	selected
Dist-To-CH	0.033	selected
SCH-R	0.030	selected
JOIN-R	0.028	selected
DATA-S	0.028	selected
Data-sent-To-BS	0.017	selected
AVD-R	0.014	selected
Who-CH	0.014	selected
ID	0.014	selected
Expaned Energy	0.013	selected
Time	0.010	selected
Dist_CH_To_BS	**0.005**	**ignored**
DATA-R	**0.003**	**ignored**

B. DATASET

The dataset employed in this study was WSN-DS created by Almomani et al. [52]. It includes four types of DoS attacks: blackhole, flooding, grayhole, and scheduling. The version used in this study was downloaded from the Kaggle website [75]. This version consists of 18 features, as listed in Table 5.

An enhanced version of this dataset was developed by applying an adequate feature-selection method. Both the original WSN-DS dataset and the enhanced version were used to train and test the machine learning models investigated in this study.

C. FEATURE SELECTION

Applying an adequate feature selection method is a crucial step in improving prediction accuracy and reducing computational overhead. Feature selection is a practical method for lightweight detection approches [76]. This process decreases the number of features by considering only the features with high influence and neglecting others; therefore, it significantly enhances the performance of classification models. When dealing with WSNs with limited resources and computational power, selecting an efficient feature selection method would be a great step towards enhancing classification accuracy and performance. Therefore, after applying different selection methods, the authors, based on the experimental results, decided to use the Gini feature selection method, which yielded good results.

By applying this feature selection method, 16 out of 18 features were selected; therefore, two features were excluded. Table 6 shows the calculated weight of all features; accordingly, all features that received a weight less than 0.01 were ignored.

D. VALIDATION

All models must be validated for acceptance. For each model used in our trials, a cross validation method with 10 folds was used to obtain realistic and reliable results. Equation 1 was used to compute the classification accuracy for each model:

$$Accuracy = \frac{TP + TN}{FN + TP + FP + TN} \tag{1}$$

True positive (TP) and true negative (TN) indicate the number of positive and negative cases that are correctly predicted, respectively.

False negatives (FN) reflect the number of positive cases incorrectly predicted as negative, whereas false positives (FP) refer to the number of negative cases incorrectly classified as positive.

Subsequently, the effectiveness and performance of the models are assessed using a confusion matrix. False negatives (FN) and false positives (FP) were used to measure the classification errors.

In addition, other metrics used to analyze the results, including recall, precision, and F1 score, were computed using Equations 2, 3, and 4, respectively. The receiver operating characteristic (ROC) curves of each classifier were

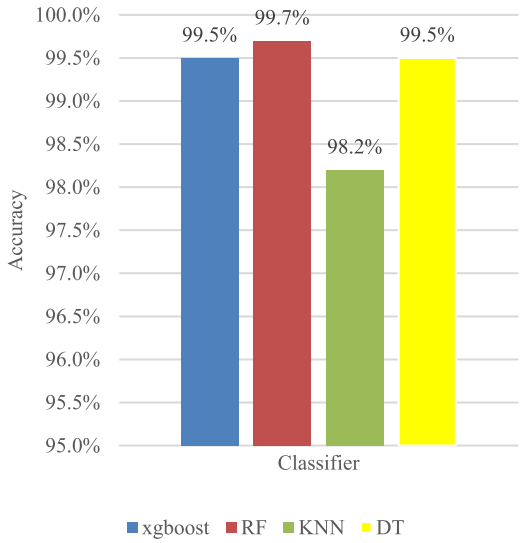

FIGURE 2. The accuracy of all classifiers when using the original dataset, WSN-DS.

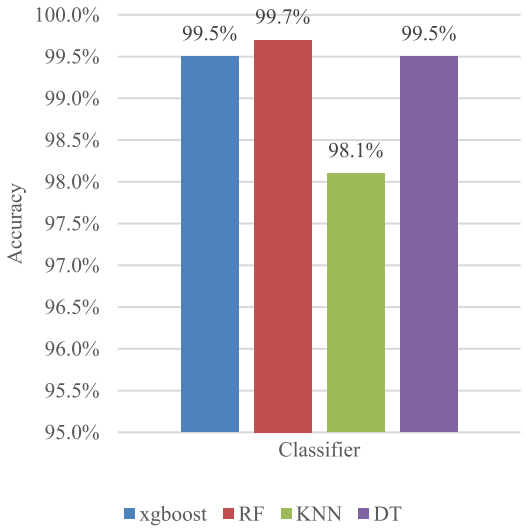

FIGURE 3. The accuracy of all classifiers when using the enhanced version of WSN-DS dataset.

computed to conduct further assessment.

$$Recall = \frac{TP}{FN + TP} \tag{2}$$

$$Precision = \frac{TP}{FP + TP} \tag{3}$$

$$F1Score = 2X\frac{PrecisionXRecall}{Precision + Recall} \tag{4}$$

VII. RESULTS AND DISSCUSSIONS

To evaluate the effectiveness of our developed dataset, all classifiers, including Xgboot, DT, KNN, and RF, were trained and tested using both datasets, the original dataset and the enhanced version of the dataset that was developed by applying the Gini feature selection method. The computed accuracies for all classifiers using the original dataset and the enhahnced version of the dataset are illustrated in Figure 2 and Figure 3, respectively. It is clear that the accuracy for all classifiers in both scenarios is almost the same, which indicates that the enhanced version of the dataset maintains the same accuracy level; however, it definitely reduces the computational time, which is required for networks that have limited computational resources. Any move towards reducing overhead is considered a significant enhancement for WSNs. Therefore, the authors recommend using the enhanced version of the WSN-DS dataset developed by applying the Gini feature selection method. In fact, the authors applied different feature selection methods, but all of them had a negative impact on classification accuracy, except for the Gini feature selection method.

Based on this finding, our proposed model (DT) was trained and tested using the developed version of the dataset and was validated using a cross validation method with 10 folds. In addition, Xgboot, KNN, and RF were trained, tested, and validated using the same dataset and validation method for comparison with the proposed model. After running these models, the performance metrics that included accuracy, recall, precision, and F1 Score were computed. Table 7 lists these metrics, and the ROC curves for KNN, XGBoost, RF, and the proposed approach (DT) are illustrated in Figure 4, Figure 5, Figure 6, and Figure 7 respectively. The performance metrics and ROC curves demonstrated the performance of all classifiers, including the proposed classifier.

TABLE 7. Performance metrics.

	Accuracy	Recall	Precision	F1 Score
XGBoost (No. of trees is 10)	99.5	99.5	99.5	99.5
RF (No. of trees is 10)	99.7	99.7	99.7	99.7
KNN (No. of neighbors is 5)	98.1	98.1	98.0	98.0
DT	99.5	99.5	99.5	99.5

It is clear that our proposed classifier (DT) outperformed KNN in terms of classification accuracy, as shown in Table 7 and processing time, as shown in Figure 8. DT requires only 2% of the processing time required by the KNN. In fact, KNN lags behind by achieving the lowest accuracy rate of 98.1 and the taking the highest processing time compared to other classifiers.

When comparing DT and RF, RF was slightly better in terms of accuracy, whereas DT significantly outperformed RF in terms of the processing time, as shown in Figure 8. DT takes only 9.7% of the RF processing time. Therefore, it is noteworthy that DT outperformed RF. On the other hand, when comparing DT with XGBoost, both achieve the

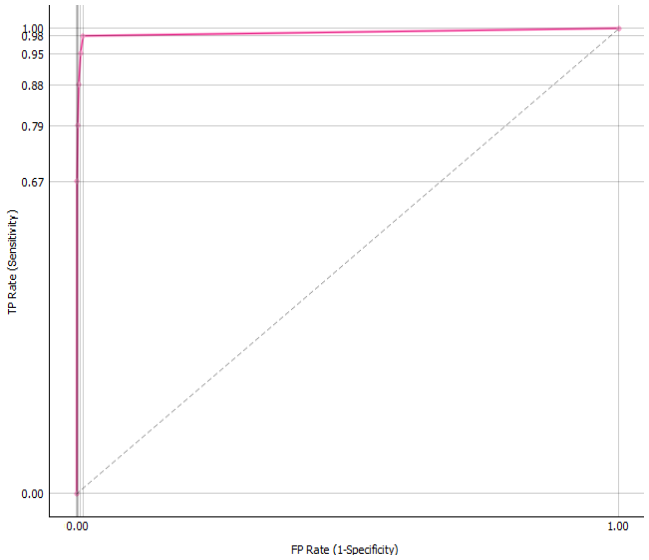

FIGURE 4. The ROC curve for the KNN classifier.

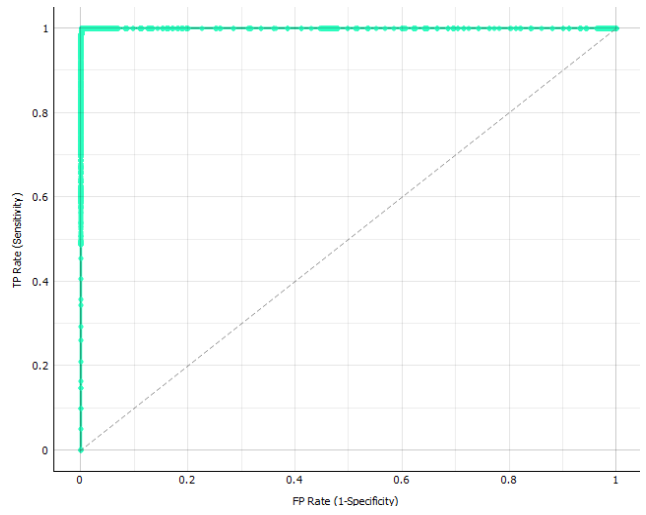

FIGURE 5. The ROC curve for the XGBoost classifier.

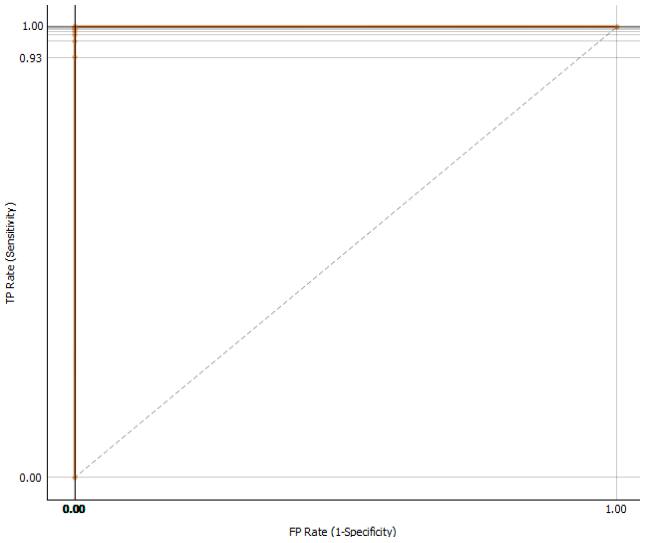

FIGURE 6. The ROC curve for the RF classifier.

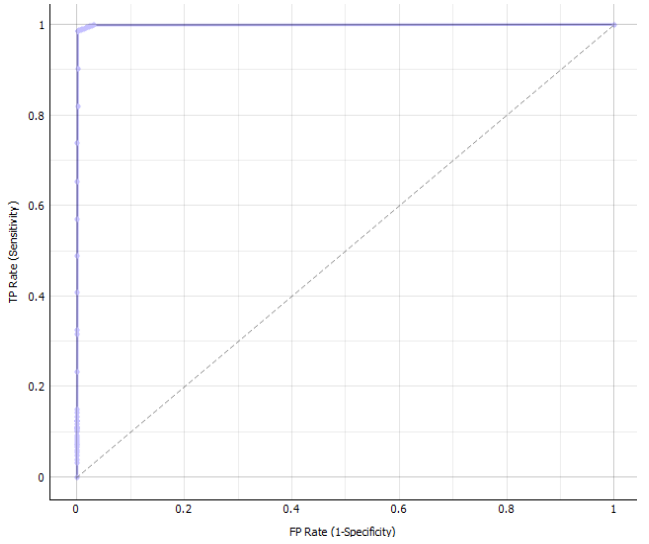

FIGURE 7. The ROC curve for the DT classifier, the proposed classier.

same accuracy. However, in terms of the processing time, DT surpassed XGBoost by taking only 13% of the XGBoost processing time, as shown in Figure 8. Therefore, this study recommends a DT classifier using the Gini feature selection method because it is more suitable for networks with many constraints, such as limited computational resources and memory.

Both RF and XGBoost are ensemble classifiers that are capable of improving prediction accuracy; however, this leads to more computational overhead that does not fit networks with limited resources. Therefore, both classifiers are not adequate for networks with limited computational resources.

We also noticed that by increasing the number of trees for both RF and XGBoost, the prediction accuracy can be enhanced; however, they require more processing time and, therefore, do not offer an adequate solution for WSNs. Such networks require a very light solution that can detect security attacks with an acceptable overhead. This balance requires a carefully designed solution, which poses a challenge.

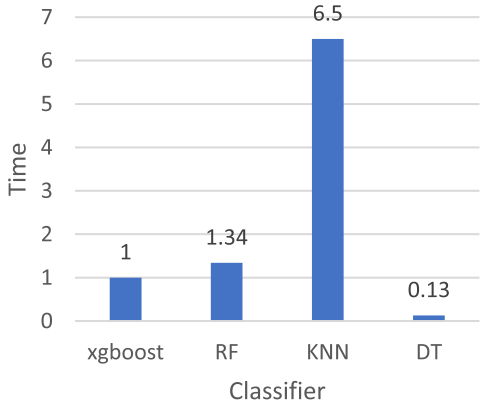

FIGURE 8. The processing time for all classifiers when using the enhanced version of WSN-DS dataset.

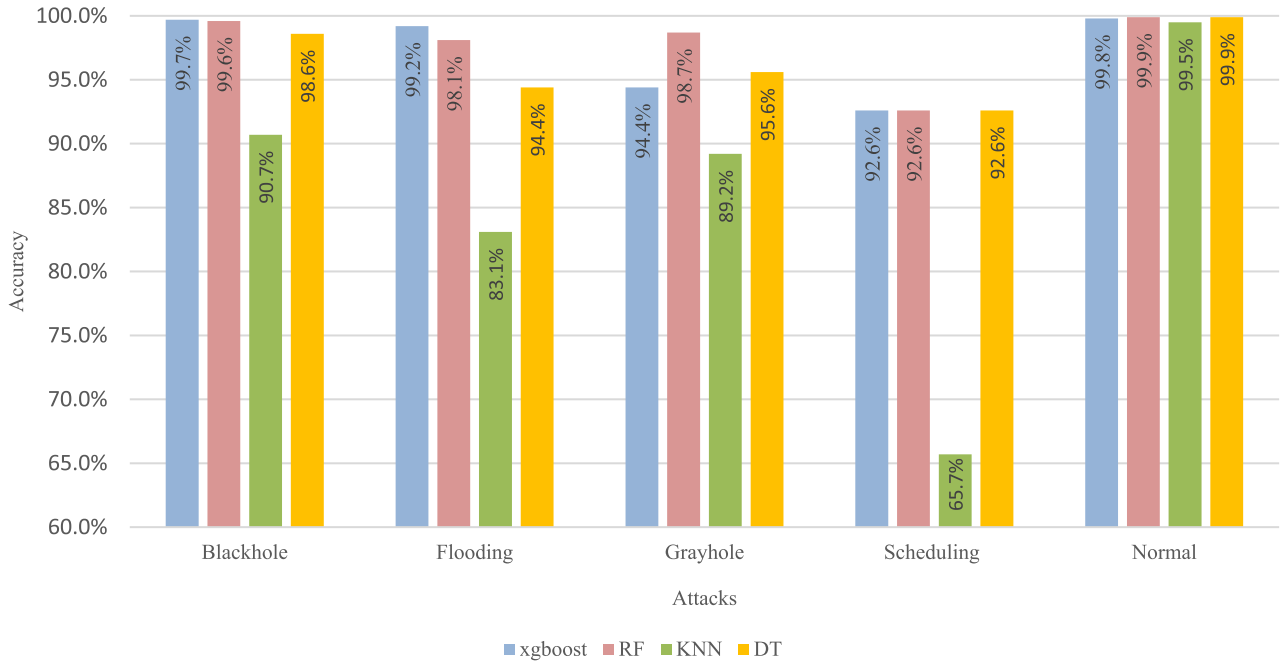

FIGURE 9. Attacks classification accuracy.

TABLE 8. Classifier errors.

Classifier	Error
XGBoost	0.0055
RF	0.0030
KNN	0.0192
DT	0.0051

TABLE 9. Attacks classification accuracy.

	Blackhole	Flooding	Grayhole	Scheduling	Normal
XGBoost	99.7	99.2	94.4	92.6	99.8
RF	99.6	98.1	98.7	92.6	99.9
KNN	90.7	83.1	89.2	65.7	99.5
DT	98.6	94.4	95.6	92.6	99.9

In terms of the classification error computed using the confusion matrix (error matrix), we noticed that RF had the least errors compared to the others, followed by DT and XGBoost, whereas KNN lagged behind by causing the highest number of errors. Table 8 lists the computed errors for all classifiers in the figures. This finding also supports our recommendation to use DT as the best classifier. Yes, DT comes at the second line but is still the best, as it causes a negligible amount of overhead compared to RF and other classifiers.

The classification accuracy achieved by all classifiers in detecting the four types of DoS attacks (blackhole, flooding, grayhole, and scheduling) is illustrated in Table 9 and Figure 9. It is clearly observed that DT achieves a high accuracy and is competitive with RF and XGBoost. However, it surpassed them in terms of classification processing time, which is a highly important factor in WSNs that reduces overhead. Therefore, DT with the Gini feature selection method provides a lightweight solution.

It is noteworthy that WSD-DS has imbalanced classes, which have a negative impact on detection accuracy [77]. Therefore, we expect that detection accuracy will be enhanced when using a balanced dataset.

Considering the aforementioned experiments and results, the authors conclude that the DT classifier with the Gini feature selection method is the most suitable classifier for WSN constraints. It achieves a high classification accuracy with the least processing overhead.

VIII. CONCLUSION

WSNs have emerged as one of the most promising solutions for a variety of applications, including healthcare, defense, environmental monitoring, and distributed control systems.

Smart sensor nodes in a WSN are inexpensive and simple to set up. However, because of their deployment in hostile environments and insecure routing protocols and architectures, they are susceptible to a wide range of attacks. Therefore, the WSN security remains an important research topic.

WSN security is essential for the operation of these networks. The challenge is not only how to secure WSNs but also how to create an acceptable security system that considers the constrained resources of such networks while maintaining the integrity of network performance.

The characteristics and performance of sensor networks are the main reasons for their explosive expansion in various fields. Therefore, any security measure that interferes with or hinders the operations is unnecessary and will not be considered. Determining an adequate security measure while maintaining balance is the primary challenge.

The rapid development of cutting-edge technologies for creating devices that can deliver high speed, lower energy consumption, lower cost, and enable appropriate storage spaces can improve the security of WSNs. This is because the core issue with the majority of the suggested security solutions is WSN resource limits, constraints, and particularities.

Developing a countermeasure that is capable of protecting WSNs from DoS attacks while maintaining the low cost and flexibility features of these networks is a challenge that requires further exploration. This motivated the author to contribute to this field by introducing a lightweight solution to counter DoS attacks in WSNs.

This study provides valuable insights into the current state of research on DoS attacks that target WSNs and presents a lightweight detection method to detect these attacks. The proposed detection scheme is based on a DT classifier using the Gini feature-selection method. An enhanced version of the WSN-DS dataset developed by the author was used to train and test the proposed model. This study confirmed the capability of the proposed classifier by comparing its results with those of the most common classifiers recently recommended to detect such types of attacks in WSNs. Compared to the RF, XGBoost, and KNN classifiers, the proposed classifier exhibited high accuracy with negligible overhead. It achieves an accuracy rate of 99.5% and only takes 9.7%, 13%, and 2% of the processing time required by FR, XGBoost, and KNN respectively. This indicates that our proposed approach significantly outperforms the other classifiers in terms of processing time, which is an important factor to consider when dealing with WSNs that face the challenge of limited resources. A limitation of this study is that the proposed approach was trained on one dataset. Therefore, our future work will focus on evaluating the proposed method on different datasets. In addition, WSN-DS is an unbalanced dataset; therefore, our future work will also focus on applying appropriate oversampling and undersampling techniques to develop a balanced version of this dataset, which is expected to significantly enhance the prediction accuracy.

REFERENCES

[1] G. G. Gebremariam, J. Panda, and S. Indu, "Blockchain-based secure localization against malicious nodes in IoT-based wireless sensor networks using federated learning," *Wireless Commun. Mobile Comput.*, vol. 2023, pp. 1–27, Jan. 2023, doi: 10.1155/2023/8068038.

[2] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless sensor network security: A recent review based on state-of-the-art works," *Int. J. Eng. Bus. Manage.*, vol. 15, Jan. 2023, Art. no. 184797902311572, doi: 10.1177/18479790231157220.

[3] S. Ashraf, O. Alfandi, A. Ahmad, A. M. Khattak, B. Hayat, K. H. Kim, and A. Ullah, "Bodacious-instance coverage mechanism for wireless sensor network," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–11, Nov. 2020, doi: 10.1155/2020/8833767.

[4] X. Feng, X. Ding, and S. Sun, "A security detection scheme based on evidence nodes in wireless sensor networks," in *Proc. 6th Int. Conf. Biomed. Eng. Informat.*, Dec. 2013, pp. 689–693, doi: 10.1109/BMEI.2013.6747027.

[5] H. Yang, L.-X. Wei, and X.-Y. Yang, "Sybil attack detection scheme in wireless sensor network," *Jisuanji Gongcheng/Comput. Eng.*, vol. 37, no. 12, pp. 122–124, 2011.

[6] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *J. Big Data*, vol. 10, no. 1, p. 17, Feb. 2023, doi: 10.1186/s40537-023-00692-w.

[7] S. Ismail, D. W. Dawoud, and H. Reza, "Securing wireless sensor networks using machine learning and blockchain: A review," *Future Internet*, vol. 15, no. 6, p. 200, May 2023, doi: 10.3390/fi15060200.

[8] M. N. U. Islam, A. Fahmin, M. S. Hossain, and M. Atiquzzaman, "Denial-of-service attacks on wireless sensor network and defense techniques," *Wireless Personal Commun.*, vol. 116, pp. 1993–2021, Feb. 2020, doi: 10.1007/s11277-020-07776-3.

[9] H. S. Sharma, M. M. Singh, and A. Sarkar, "Machine learning-based DoS attack detection techniques in wireless sensor network: A review," in *Proc. Int. Conf. Cogn. Intell. Comput.*, A. Kumar, G. Ghinea, S. Merugu, and T. Hashimoto, Eds. Singapore: Springer, 2023, pp. 583–591, doi: 10.1007/978-981-19-2358-6_53.

[10] V. Dani, "Detection of denial-of-service attack using weight based trust aware routing approach," *J. Inf. Assurance Secur.*, vol. 18, pp. 089–097, Jun. 2023.

[11] B. J. Santhosh Kumar and S. Sinha, "An intrusion detection and prevention system against DOS attacks for internet-integrated WSN," in *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2022, pp. 793–797, doi: 10.1109/ICCES54183.2022.9835838.

[12] M. Dener and A. Orman, "BBAP-WSN: A new blockchain-based authentication protocol for wireless sensor networks," *Appl. Sci.*, vol. 13, no. 3, p. 1526, Jan. 2023, doi: 10.3390/app13031526.

[13] J. Zhang, W. Xiao, and Y. Li, "Data and knowledge twin driven integration for large-scale device-free localization," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 320–331, Jan. 2021, doi: 10.1109/JIOT.2020.3005939.

[14] J. Zhang, Y. Li, W. Xiao, and Z. Zhang, "Online spatiotemporal modeling for robust and lightweight device-free localization in nonstationary environments," *IEEE Trans. Ind. Informat.*, vol. 19, no. 7, pp. 8528–8538, Jul. 2023, doi: 10.1109/TII.2022.3218666.

[15] M. A. Elsadig, "Security issues and challenges on wireless sensor networks," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, pp. 1551–1559, Aug. 2019, doi: 10.30534/ijatcse/2019/78842019.

[16] G. S. Rao, M. Harshitha, V. R. Joshitha, S. S. Sravya, and M. V. Priya, "DoS attack detection in wireless sensor networks (WSN) using hybrid machine learning model," in *Proc. 10th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Mar. 2023, pp. 384–388, doi: 10.1109/SPIN57001.2023.10117098.

[17] C. Duru, A. Aniedu, O. T. Innocent, and A. E. Eo, "Modeling of wireless sensor networks jamming attack strategies," *Amer. Sci. Res. J. Eng., Technol., Sci.*, vol. 67, no. 1, pp. 48–65, 2020.

[18] M. A. Elsadig and Y. A. Fadlalla, "VANETs security issues and challenges: A survey," *Indian J. Sci. Technol.*, vol. 9, no. 28, pp. 1–8, Jul. 2016, doi: 10.17485/ijst/2016/v9i28/97782.

[19] I. Tomic and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017, doi: 10.1109/JIOT.2017.2749883.

[20] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 38–43, Dec. 2004, doi: 10.1109/MWC.2004.1368895.

[21] M. Majid, S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu, and J. C.-W. Lin, "Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, p. 2087, Mar. 2022, doi: 10.3390/s22062087.

[22] D. Yu, J. Kang, and J. Dong, "Service attack improvement in wireless sensor network based on machine learning," *Microprocess. Microsyst.*, vol. 80, Feb. 2021, Art. no. 103637, doi: 10.1016/j.micpro.2020.103637.

[23] A. Aborujilah, R. M. Nassr, T. Al-Hadhrami, M. N. Husen, N. A. Ali, A. Al-Othmani, N. Syahela, and H. Ochiai, "Security assessment model to analysis DOS attacks in WSN," in *Emerging Trends in Intelligent Computing and Informatics*, F. Saeed, F. Mohammed, and N. Gazem, Eds. Cham, Switzerland: Springer, 2020, pp. 789–800, doi: 10.1007/978-3-030-33582-3_74.

[24] A. Puviarasu, P. Jeyabharathi, K. Lavanya, S. Vimalnath, V. Sureshkumar, and P. Naveen, "A deep Q network optimization algorithm for DoS attack in WSN," in *Proc. 3rd Int. Conf. Smart Electron. Commun. (ICOSEC)*, Oct. 2022, pp. 789–793, doi: 10.1109/ICOSEC54921.2022.9952125.

[25] O. H. Embarak and R. Abu Zitar, "Securing wireless sensor networks against DoS attacks in industrial 4.0," *J. Intell. Syst. Internet Things*, vol. 8, no. 1, pp. 66–74, 2023.

[26] M. Premkumar and T. V. P. Sundararajan, "DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks," *Microprocess. Microsyst.*, vol. 79, Nov. 2020, Art. no. 103278, doi: 10.1016/j.micpro.2020.103278.

[27] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan. 2008, doi: 10.1109/MPRV.2008.6.

[28] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018, doi: 10.1109/ACCESS.2018.2793841.

[29] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51915–51932, 2019, doi: 10.1109/ACCESS.2019.2911424.

[30] Z. A. Khan, S. Amjad, F. Ahmed, A. M. Almasoud, M. Imran, and N. Javaid, "A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks," *IEEE Access*, vol. 11, pp. 31036–31051, 2023, doi: 10.1109/ACCESS.2023.3259982.

[31] R. Roman and J. Lopez, "Integrating wireless sensor networks and the internet: A security analysis," *Internet Res.*, vol. 19, no. 2, pp. 246–259, Apr. 2009, doi: 10.1108/10662240910952373.

[32] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert–Huang transformation and trust evaluation," *IEEE Access*, vol. 7, pp. 32853–32866, 2019, doi: 10.1109/ACCESS.2019.2903816.

[33] C. Lin, Z. Shang, W. Du, J. Ren, L. Wang, and G. Wu, "CoDoC: A novel attack for wireless rechargeable sensor networks through denial of charge," in *Proc. IEEE INFOCOM*, Apr. 2019, pp. 856–864, doi: 10.1109/INFOCOM.2019.8737403.

[34] H. Belkhiri, A. Messai, A.-L. Beylot, and F. Haider, "Denial of service attack detection in wireless sensor networks and software defined wireless sensor networks: A brief review," in *Proc. Int. Conf. Big Data Internet Things*. Cham, Switzerland: Springer, 2022, pp. 100–115, doi: 10.1007/978-3-031-07969-6_8.

[35] C. Haiguang, W. Huafeng, Z. Xi, and G. Chuanshan, "Agent-based trust model in wireless sensor networks," in *Proc. 8th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distrib. Comput.*, 2007, pp. 119–124, doi: 10.1109/SNPD.2007.122.

[36] A. Allakany, A. Saber, S. M. Mostafa, M. Alsabaan, M. I. Ibrahem, and H. Elwahsh, "Enhancing security in ZigBee wireless sensor networks: A new approach and mutual authentication scheme for D2D communication," *Sensors*, vol. 23, no. 12, p. 5703, Jun. 2023, doi: 10.3390/s23125703.

[37] S. S. Desai and M. J. Nene, "Node-level trust evaluation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2139–2152, Aug. 2019, doi: 10.1109/TIFS.2019.2894027.

[38] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networks-revisited," in *Security in Ad-hoc and Sensor Networks* (Lecture Notes in Computer Science), vol. 3313, C. Castelluccia, H. Hartenstein, C. Paar, and D. Westhoff, Eds. Berlin, Germany: Springer, 2004, pp. 2–18, doi: 10.1007/978-3-540-30496-8_2.

[39] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2nd Quart., 2009, doi: 10.1109/SURV.2009.090205.

[40] A. S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: Issues and challenges," in *Proc. 8th Int. Conf. Adv. Commun. Technol.*, 2006, pp. 1–6, doi: 10.1109/ICACT.2006.206151.

[41] M. Saleh and I. Al Khatib, "Throughput analysis of WEP security in ad hoc sensor networks," in *Proc. 2nd Int. Conf. Innov. Inf. Technol.*, Sep. 2005, pp. 26–28.

[42] J. Sen, "A survey on wireless sensor network security," 2010, *arXiv:1011.1529*.

[43] M. Premkumar, S. R. Ashokkumar, V. Jeevanantham, G. Mohanbabu, and S. AnuPallavi, "Scalable and energy efficient cluster based anomaly detection against denial of service attacks in wireless sensor networks," *Wireless Pers. Commun.*, vol. 129, no. 4, pp. 2669–2691, Apr. 2023, doi: 10.1007/s11277-023-10252-3.

[44] S. E. Quincozes, J. F. Kazienko, and V. E. Quincozes, "An extended evaluation on machine learning techniques for denial-of-service detection in wireless sensor networks," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100684, doi: 10.1016/j.iot.2023.100684.

[45] M. A. Elsadig and Y. A. Fadlalla, "Packet length covert channel: A detection scheme," in *Proc. 1st Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Apr. 2018, pp. 1–7, doi: 10.1109/CAIS.2018.8442026.

[46] R. Sagar, R. Jhaveri, and C. Borrego, "Applications in security and evasions in machine learning: A survey," *Electronics*, vol. 9, no. 1, p. 97, Jan. 2020, doi: 10.3390/electronics9010097.

[47] M. A. Elsadig and A. Gafar, "Covert channel detection: Machine learning approaches," *IEEE Access*, vol. 10, pp. 38391–38405, 2022, doi: 10.1109/ACCESS.2022.3164392.

[48] K. Shaukat, S. Luo, V. Varadharajan, I. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 13, no. 10, p. 2509, May 2020, doi: 10.3390/en13102509.

[49] G. G. Gebremariam, J. Panda, and S. Indu, "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network," *Wireless Commun. Mobile Comput.*, vol. 2023, pp. 1–29, Jan. 2023, doi: 10.1155/2023/2744706.

[50] O. Osanaiye, A. Alfa, and G. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, p. 1691, May 2018, doi: 10.3390/s18061691.

[51] T.-T.-H. Le, T. Park, D. Cho, and H. Kim, "An effective classification for DoS attacks in wireless sensor networks," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 689–692, doi: 10.1109/ICUFN.2018.8436999.

[52] I. Almomani, B. A. Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sensors*, vol. 2016, Aug. 2016, Art. no. 4731953, doi: 10.1155/2016/4731953.

[53] H. Tabbaa, S. Ifzarne, and I. Hafidi, "An online ensemble learning model for detecting attacks in wireless sensor networks," 2022, *arXiv:2204.13814*.

[54] I. Almomani and M. Alenezi, "Efficient denial of service attacks detection in wireless sensor networks," *J. Inf. Sci. Eng.*, vol. 34, no. 4, pp. 977–1000, 2018.

[55] L. Alsulaiman and S. Al-Ahmadi, "Performance evaluation of machine learning techniques for DOS detection in wireless sensor network," *Int. J. Netw. Secur. Appl.*, vol. 13, no. 2, pp. 21–29, Mar. 2021, doi: 10.5121/ijnsa.2021.13202.

[56] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[57] B. K. Mishra, M. C. Nikam, and P. Lakkadwala, "Security against black hole attack in wireless sensor network—A review," in *Proc. 4th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2014, pp. 615–620, doi: 10.1109/CSNT.2014.129.

[58] R. Wazirali and R. Ahmad, "Machine learning approaches to detect DoS and their effect on WSNs lifetime," *Comput., Mater. Continua*, vol. 70, no. 3, pp. 4921–4946, 2022, doi: 10.32604/cmc.2022.020044.

[59] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," *Sensors*, vol. 22, no. 13, p. 4730, Jun. 2022, doi: 10.3390/s22134730.

[60] C. Yao, Y. Yang, K. Yin, and J. Yang, "Traffic anomaly detection in wireless sensor networks based on principal component analysis and deep convolution neural network," *IEEE Access*, vol. 10, pp. 103136–103149, 2022, doi: 10.1109/ACCESS.2022.3210189.

[61] S. Jaitly, H. Malhotra, and B. Bhushan, "Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey," in *Proc. Int. Conf. Comput., Commun. Electron.*, 2017, pp. 559–564, doi: 10.1109/COMPTELIX.2017.8004033.
[62] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May 2006, doi: 10.1109/MNET.2006.1637931.
[63] D. Ciuonzo, A. Aubry, and V. Carotenuto, "Rician MIMO channel- and jamming-aware decision fusion," *IEEE Trans. Signal Process.*, vol. 65, no. 15, pp. 3866–3880, Aug. 2017, doi: 10.1109/TSP.2017.2686375.
[64] S. Sciancalepore, G. Oligeri, and R. Di Pietro, "Strength of crowd (SOC)—Defeating a reactive jammer in IoT with decoy messages," *Sensors*, vol. 18, no. 10, p. 3492, Oct. 2018, doi: 10.3390/s18103492.
[65] N. Geethanjali and E. Gayathri, "A survey on energy depletion attacks in wireless sensor networks," *Int. J. Sci. Res.*, vol. 3, no. 9, pp. 2070–2074, 2014.
[66] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: A systematic review," *Soft Comput.*, vol. 27, no. 18, pp. 13039–13075, Sep. 2023, doi: 10.1007/s00500-021-06608-1.
[67] S. B. Atitallah, M. Driss, W. Boulila, and I. Almomani, "An effective detection and classification approach for DoS attacks in wireless sensor networks using deep transfer learning models and majority voting," in *Advances in Computational Collective Intelligence*, vol. 1653, C. Bădicva, J. Treur, D. Benslimane, B. Hnatkowska, and M. Krótkiewicz, Eds. Cham, Switzerland: Springer, 2022, pp. 180–192, doi: 10.1007/978-3-031-16210-7_14.
[68] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 68–71, Jun. 2019, doi: 10.1109/LNET.2019.2901792.
[69] S. Otoum, B. Kantarci, and H. Mouftah, "Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422401.
[70] S. Ismail, D. Dawoud, and H. Reza, "A lightweight multilayer machine learning detection system for cyber-attacks in WSN," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2022, pp. 0481–0486, doi: 10.1109/CCWC54503.2022.9720891.
[71] M. S. Alsahli, M. M. Almasri, M. Al-Akhras, A. I. Al-Issa, and M. Alawairdhi, "Evaluation of machine learning algorithms for intrusion detection system in WSN," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 5, pp. 617–626, 2021.
[72] S. Ifzarne, H. Tabbaa, I. Hafidi, and N. Lamghari, "Anomaly detection using machine learning techniques in wireless sensor networks," *J. Phys., Conf.*, vol. 1743, no. 1, Jan. 2021, Art. no. 012021, doi: 10.1088/1742-6596/1743/1/012021.
[73] S. Ismail, T. T. Khoei, R. Marsh, and N. Kaabouch, "A comparative study of machine learning models for cyber-attacks detection in wireless sensor networks," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Dec. 2021, pp. 0313–0318, doi: 10.1109/UEMCON53757.2021.9666581.
[74] J. Demsar, T. Curk, A. Erjavec, C. Gorup, T. Hočevar, M. Milutinovič, M. Možina, M. Polajnar, M. Toplak, A. Starič, M. Štajdohar, L. Umek, L. Žagar, J. Žbontar, M. Žitnik, and B. Župan, "Orange: Data mining toolbox in Python," *J. Mach. Learn. Res.*, vol. 14, no. 1, pp. 2349–2353, 2013.
[75] *WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks*. Accessed: Jan. 27, 2023. [Online]. Available: https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds?resource=download
[76] J.-S. Pan, F. Fan, S.-C. Chu, H.-Q. Zhao, and G.-Y. Liu, "A lightweight intelligent intrusion detection model for wireless sensor networks," *Secur. Commun. Netw.*, vol. 2021, May 2021, Art. no. 5540895, doi: 10.1155/2021/5540895.
[77] M. Dener, S. Al, and A. Orman, "STLGBM-DDS: An efficient data balanced DoS detection system for wireless sensor networks on big data environment," *IEEE Access*, vol. 10, pp. 92931–92945, 2022, doi: 10.1109/ACCESS.2022.3202807.

MUAWIA A. ELSADIG received the bachelor's degree in computer engineering, the M.Sc. degree in computer networks, and the Ph.D. degree in computer science (information security). He is currently an Assistant Professor in cybersecurity with the Deanship of Scientific Research, Imam Abdulrahman Bin Faisal University (IAU), Dammam, Saudi Arabia. He worked for different accredited international universities and had a rich record of publications in recognized international journals and conferences. He has many years of teaching experience and considerable industry contributions. His research interests include information security, network security, cybersecurity, wireless sensor networks, bioinformatics, and information extraction. Ranging from theory to design to implementation. He contributed as a reviewer to many reputable international journals and received many awards for his research activities.