Histogram Gradient Boosting Classifier-Based UWSN Cyber Attack Detection Incorporating Environmental Factors (HGBoostUCAD)

Hamid OUIDIR, Amine BERQIA, Siham AOUAD
ENSIAS, Mohammed V University in Rabat, Rabat, Morocco

***Abstract*—Underwater Wireless Sensor Networks (UWSNs) are commonly employed for exploring and exploiting aquatic areas, and its role is very important and more beneficial precisely in hostile and constrained marine environments. However, their security is more critical than terrestrial wireless sensor networks (TWSNs) due to the space in which they are deployed, the wireless communication medium, and the cost of damage repair, and their protection is a problematic issue that needs to be continuously resolved. Consequently, it is highly recommended see required to take procedure to protect UWSNs against attacks and intrusion and maintain service quality. In general, existing works on machine learning-based intrusion detection system (IDS) and cyber-attack detection approaches for (UWSNs) utilize dedicated datasets designed for (WSNs) without adapting them to the aquatic environment. Furthermore, these studies analyze the enhancement of UWSN performance based on network metrics separately from machine learning model metrics, and vice versa. In this way, this paper proposes a novel cybersecurity detection approach-based model learning Histogram Gradient Bosting (HGB) classifier called (HGBoostUCAD). It classifies four types of DoS attacks (Blackhole, Grayhole, Flooding, and Scheduling), employing an adjusted dataset for (IDS) in wireless sensor networks (WSN-DS) taking into account simulate realistic environmental factors: salinity, temperature, deep through Mackenzie's equation and node movement in training data. The insight of simulation results obtained, shows that our method reached 97% as accuracy and 96% as precision also outperformed both Deep Neural Network (DNN) as well as the recent study Hyper_RNN_SVM eventually referenced in this research, in terms of machine learning model metrics. In addition to machine learning model metrics, our approach provides network measurements by DoS attack type.**

Keywords*—UWSN; security; intrusion detection system; cyber-attack detection; cybersecurity; machine learning; histogram gradient boosting

TABLE I. ABBREVIATIONS

UWSN	**Underwater Wireless Sensor Network**
DoS Attack	**Denial of Service Attacks**
ASVs	**Autonomous Surface Vehicles**
AUVs	**Autonomous Underwater Vehicles**
NISTIR	**National Institute of Standards and Technology Internal Report**
FISMA	**Federal Information and Information Systems**
IDS	**Intrusion Detection Systems**
HGB	**Histogram Gradient Boosting**
DNN	**Deep Neural Network**
PDR	**Packet Delivered Ratio**
SNR	**Sound Noise Ratio**

I. INTRODUCTION

An underwater wireless sensor network (UWSN) is considered to serve as the main support network for the Internet of Things. The network architecture of a UWSN is shown in Fig. 1, with its key components—sensors—located in either shallow or deep water. The sensors' function is to collect data and send it via acoustic signals to objects like buoys, ships, Autonomous Surface Vehicles (ASVs), or Autonomous Underwater Vehicles (AUVs). These objects then use radio signals to send the data to a distant monitoring center. After obtaining the oceanic data, the monitoring center analyzes it [1]. These kinds of networks are usually unmonitored and placed in remote locations. Security methods must be implemented on them to protect them from threats and attacks [2], and compared to their analogs, such as wireless sensor networks (WSNs), UWSNs are more susceptible to security assaults. The entire network's functionality may be compromised by potential attacks in UWSNs [3]. The list of abbreviations is given in Table I.

In research [4] as application, the author classified UWSN deployment into five areas: 1) underwater research; 2) environmental monitoring; 3) disaster prevention; 4) military domain; and 5) other fields.

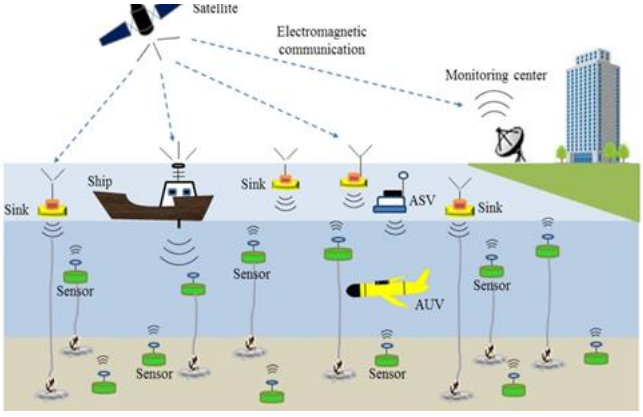

Fig. 1. UWSN architecture [1].

A. Basic Concepts and Challenges

1) Cybersecurity: The term "cyber security" refers to the set of rules, methods, tools, and procedures that cooperate to defend against attacks on the availability, confidentiality, and integrity of networks, software, and data. There are cyber protection methods at the network, application, data level and host. Many tools, including intrusion detection systems (IDSs), firewalls, antivirus programs, and intrusion protection systems (IPSs), operate in collaboration to prevent assaults and identify security failures [5]. In other words, cybersecurity concepts are measures taken to guarantee the confidentiality, integrity, and availability of systems, data (including software, hardware, and networks), and information that is processed, stored, and transmitted, as mentioned in the NISTIR (National Institute of Standards and Technology Internal Report) 7298 report (Glossary of Key Information Security Terms, July 2019). Moreover, the FISMA (Standards for Security, Categorization of Federal Information and Information Systems, February 2004) established the first three main security objectives for computer and information systems as follows:

a) Confidentiality: Taking into account appropriate limitations on information availability and sharing, as well as precautions to protect private and sensitive data.

b) Integrity: Preventing the rectification or destruction of erroneous data while guaranteeing the accuracy and non-repudiation of the relevant information.

c) Availability: Making certain that when resources are needed, authorized users can access them on time and continuously [6].

2) Intrusion detection: Define as "the act of detecting actions that attempt to compromise the confidentiality, integrity, or availability of a resource". An intrusion detection system (IDS) is a hardware or software program that keeps surveillance out for hostile activities or policy violations on a network or systems [7].

As well, we describe DoS attack types on the WSN-DS dataset, including Blackhole, Grayhole, Flooding, and Scheduling, as follows:

3) Blackhole attack: A blackhole attack is a kind of denial-of-service assault in which the attacker disrupts routing protocol by promoting itself at the start of the round. Playing the role of cluster head (CH), the Blackhole attacker will continue to drop packets transmitted by adjacent node rather than sending them to the BS.

4) Grayhole attack: The attacker disrupts the routing protocol by posing as a CH to other nodes. As a result, the pretending CH blocks some packets from reaching the BS by randomly or selectively dropping them when it receives data packets from other nodes.

5) Flooding attack: The attacker manipulates the routing protocol in multiple ways. By transmitting a lot of advertising CH messages with high transmission power. As a result, when sensors get a lot of messages notifications, they will use more energy and take longer to decide which CH to join. Additionally, the attacker tries to confuse victims into selecting it as a CH, particularly those nodes that are far away from it in order to drain their energy.

6) Scheduling attack: When CHs put up TDMA schedules for the data transmission time lots during the routing protocol configuration phase, scheduling attacks take place. All nodes will be given the identical time slot to send data by the attacker acting as a CH. This is accomplished by switching the TDMA schedule from broadcast to unicast. Such a modification will result in packet collisions and data loss [8].

Even though this type of networking is more beneficial in rich and expansive aquatic areas, they were limited by the basic open acoustic channel, excessive energy consumption, insufficient hardware capacity to execute computationally complex tasks, and dynamic network topology caused by node mobility. Moreover, a limited bandwidth and low attenuation [9].

B. Motivation

The problematic to ensure security through this specific network and addresses vulnerability in which they are exposed, have inspired some researchers to concentrate on UWSN attack and threat detection, which is crucial for safeguarding data and systems and may provide the high level of services that these underwater technologies are expected to offer. But, lacking completely appropriate UWSN data, we satisfied with the intrusion detection system (IDS) for Underwater Wireless Sensor Networks (UWSNs) based WSN-DS dataset customized to UWSN environmental factors (salinity, temperature, depth, and movement), with classification of four DoS attack types (Blackhole, Grayhole, Flooding, and Scheduling). Machine learning (ML) paradigm presents a new opportunity to accomplish the intended results in this aspect. In actuality, ML models successfully carry out detection, classification, and future event prediction [10]. Additionally, gradient boosting (GB) is an ensemble learning method for classification and regression problems, as suggested by Friedman [11]. An effective model can be produced by combining weak learners, commonly decision trees. The basic idea behind GB is to gradually build and generalize the ensemble model by optimizing an objective, arbitrary loss function [12].

Our study presents a novel technique based on the histogram gradient boosting (HGB) model evaluated precisely on the adjusted WSN-DS dataset commonly used on intrusion detection system in wireless sensor networks (WSNs) taking into account environmental factors as formulated by Mackenzie's equation. HGB is one of the most robust machine learning algorithms having high prediction speed and accuracy, particularly when working with large and complex datasets like WSN-DS [8]. The following is a summary of the study's most important findings and contributions:

- Implement a cyberattack detection on UWSN, using an adapted WSN-DS dataset and a histogram gradient boosting technique.
- Incorporate environmental adaptation: temperature, salinity, depth, mobility.

- Include per-attack network simulation adjustments (PDR, packet rate, delay, energy).
- Produce plots: ML comparison, per-attack network metrics.
- Provide technique with height performance both in terms of metrics model and performance network compared to DNN and to others recent works.

The remainder of this work is structured as follows: Section II provides a literature review. Section III describes research methodology adopted. Section IV introduces experimental results of research, analyze and discussion is given in Section V. Finally, the paper's conclusion is given in Section VI.

II. Related Works

We are satisfied with just a few of research that have mostly concentrated on the usage of artificial intelligence to enhance UWSN security process. In the same way, for the purpose of detecting cyberattacks, the study [13]. suggests an intelligent model-based approach that integrates machine learning and deep learning technology. Furthermore, a feature reduction strategy employing the machine learning techniques Principal Component Analysis (PCA) and Support Vector Machine (SVM) is employed to determine which properties are most closely associated with the selected attack categories. The accuracy of a proposed Recurrent Neural Network (RNN) method for deep learning-based intrusion classification and detection, following dimensional reduction and optimization, attains (97%) accuracy but using the NSL KDD dataset. The goal of this study is to provide a comprehensive overview of UWSN security by discussing security needs and the main UWSN security threats based on layered classification. This paper explores many security issues and looks at solutions, when in study [14], the current state-of-the-art for reactive jammer detection is built with terrestrial wireless sensor networks (TWSNs) in mind. Furthermore, cooperative jamming detection in UWSN is used in very little work. This research presents an Efficient Channel Access (ECA) model that uses cross-layer design to prevent reactive jammers in order to address research challenges. The ECA jointly optimizes the approved sensing device's cooperative hopping probability and channel accessibility probabilities. The detection accuracy achieved by the ECA model is 95.12%. Additionally, in [15], the authors suggest an intrusion detection model for underwater sensor networks that can identify many kinds of attacks in order to solve this issue. In order to reduce node computation, the reduced dimensional data is sent to sink nodes after cluster head nodes have extracted features using neighborhood sensitive sets. Furthermore, the data set is balanced, the quantity of minority class samples is increased, and the detection rate of minority class attacks is enhanced by the application of the synthetic minority oversampling method (SMOTE). After determining a node's confidence based on the cluster head node's trust evaluation, train the classifier to identify the type of attack using the random forest approach; it struggles to recognize intrusions from many attack types. According to simulation data, the model can detect imbalance classes with an accuracy of over 99% and enhance the effectiveness of intrusion detection of various types of attacks. Moreover, the methodology used in the work [16] makes use of real-time feature analysis of simulated WSN routing data. It creates a strong classification framework by combining Gaussian Mixture Models (GMM) and Hidden Markov Models (HMM). This scheme successfully detects anomalies, traces malicious network activity back to its source, and classifies it as either legitimate or suspicious network activity. According to authors, the algorithm outperformed the current classification methods by a large margin, with classification rates of approximately 83.65%, 84.94%, and 94.55%. Added to that, it provided a positive prediction value that was 11.84% greater than the current approaches. As well, to find the malicious attacks in a UWSN, the authors of this study [17] employed evidential evaluation using Dempster-Shafer theory (DST) of combined many evidences. Also, they provide a numerical process for combining multiple details from an unreliable and untrustworthy neighbor with a higher level of conflict security, but in paper [18], the purpose is to illustrate a wide range of algorithms used in the defense against different types of cyberattacks. In order to protect against a variety of cyberattacks, this study will look at different classification algorithms and defense strategies. Depending on how the attack is classified, these methods will differ in terms of implementation, accuracy, and testing time. The several types of these algorithms will be covered in this research. Other than, the survey [19] provides insights into the diverse intrusion detection system (IDS) methodologies utilized in various networking technologies and explains some of the techniques used in IDS design. Signature-based intrusion detection is the most widely used method for detecting threats and guaranteeing security. However, the emergence of Artificial Intelligence (AI), particularly Machine Learning, Deep Learning, and Ensemble Learning, has shown promise results in more effective attack detection. We can ensure that the cyber infrastructure is protected from intrusions and unwanted activity by using IDS and AI to defend a network according authors. Similarly, in [20] the paper introduces a novel method for detecting malicious network traffic using artificial neural networks suitable for use in deep packet inspection-based intrusion detection systems, achieving an average accuracy of 98% and a false positive rate of less than 2% in repeated 10-fold cross-validation, potentially improving the utility of intrusion detection systems in both conventional and cyber-physical systems. The research cited in [21] is based on the UNSW-NB15 dataset, which contains 49 features for 9 distinct attack samples. According to authors, the decision tree classifier provided the highest accuracy of 99.05% in comparison to other models. Also, the deep learning system for binary classification with an 80:20 train-test split ratio and two dense layers with ReLU activation and a third dense layer with Sigmoid activation function achieved an accuracy of 98.44% using the ADAM optimizer. The paper, also cited in [22] interested in attack detection methods founded on several architecture types, such as auto-encoders, generative adversarial networks, recurrent neural networks, and convolutional neural networks, based on classification on deep learning techniques. As well, authors illustrate the current state of attack detection techniques applying deep learning structures and evaluate the performance of representing approaches adopting a few benchmark datasets which are described.

III. METHODOLOGY OF RESEARCH

The following is the key components of the method adopted to implement a cyber-attack detection-based machine learning:

A. Criticism of Existing Studies

Despite their relevance in terms of findings, most of the studies reviewed in the literature use machine learning techniques that don't require datasets, such as reinforcement learning, while others use WSN datasets without taking environmental factors into account or use mathematical approaches for deploying a UWSN intrusion detection system. As well without integrating machine learning model measurements with network performance indicators in the same study.

B. Objectives and Hypotheses

- To implement a UWSN detection attack system supported by (Hist Gradient Boosting Classifier — HGB) using adapted WSN-DS dataset that includes four Denial-of-Service (DoS) attacks (Blackhole, Grayhole, Flooding, and Scheduling attacks) and incorporating environmental parameters: temperature, salinity, deep, mobility.
- To prove its performance by comparing it with DNN under the identical experimental conditions and with other current similar techniques in terms of metrics model.
- To analyze and interpret result of experimentation.

C. Experimental Design Overview

The experiment utilized the WSN-DS dataset augmented with UWSN environmental factors — namely salinity, temperature, depth, and node mobility — to reflect realistic underwater propagation and energy consumption patterns. The model employed a Histogram Gradient Boosting (HGB) classifier, an ensemble-based artificial intelligence algorithm recognized for its robustness and interpretability in intrusion detection tasks. Each record in the dataset represented a network state or node observation, labeled as either normal or one of the four Denial of Service (DoS) attack types: Blackhole, Grayhole, Flooding, and Scheduling.

The IDS was trained on 70% of the dataset and tested on the remaining 30%. Performance evaluation included both machine learning metrics (accuracy, precision, recall, and F1-score) and network-level performance metrics (packet delivery ratio, average delay, throughput, and energy consumption).

Step 1 — Load & Clean Dataset

Import D_(WSN-DS) dataset containing labeled samples of network activity

Step 2 — Synthesize UWSN Features

For each row i in data frame df:

Environmental features

- Generate Temperature Ti, Salinity Si, Depth Di, Node mobility Mi
- Append $E_{env} = \{S_i, T_i, D_i, M_i\}$ to feature vector.

Distance & propagation

- Randomized distance
- Compute sound speed via Mackenzie 's equation cited in [23]:

C = mackenzie_sound_speed (T, S, D)

$$C(T,S,D) = 1448.96 + 4.591T - 0.05304T^2 + 0.0002374T^3 + 1.34(S-35) + 0.0163D$$

- Propagation delay = distance / c

Link success probability algorithm

Inputs:

- d: link distance (meters)
- SNR: signal-to-noise ratio (dB)
- α: attenuation coefficient
- β, γ: SNR logistic parameters

Output: $\boldsymbol{p_0}$: baseline link success probability

The term $\mathbf{P_0}$ represents the baseline probability of successful packet transmission between two underwater sensor nodes, given the distance separating them and the signal-to-noise ratio (SNR) at the receiver. Mathematically, "base_link_success_prob"(·) illustrates how the transmission success rises with increased SNR, indicating a stronger received signal relative to background noise, and declines as the propagation distance grows (due to geometric spreading and absorption losses).

P0 = base_link_success_prob (distance, snr_db)

$$\mathbf{P0} = [1 \div (1 + e^{-\beta(\mathrm{SNR}-\gamma)})] \times e^{-\alpha d}$$

where: $\mathbf{P0} \in [0,1]$ and SNR proxy (dB) as function of distance and mobility (noisy),

d is the distance between nodes,

"SNR" (in dB) measures channel quality,

α, β, and γ are environment-dependent parameters modeling attenuation and detection sensitivity.

(α = 0.002;β = 0.15; γ = 10.0)

Attack-Adjusted Packet Delivery Ratio (PDR) Algorithm

This modifies $\mathbf{p_0}$ according to UWSN attack types

- pdr = apply_attack_pdr (p0, attack_type)

Inputs :

- p_0: baseline success probabilities (vector)
- AttackType[i] ∈ {normal, blackhole, grayhole, flooding, scheduling}

Output:

- p: attack-modified link success probabilities

This equation represents how the Packet Delivery Ratio (PDR) — the ratio of successfully delivered packets to total transmitted packets — is affected by the presence of cyberattacks or network disruptions in the underwater environment.

The function "apply_attack_pdr"(·) modifies this baseline probability according to the type and severity of attack acting on the network.

- pdr = apply_attack_pdr (p0, attack_type)

In this study we employ WSN-DS adapted dataset, which classifies network behavior as either normal or one of four Denial-of-Service (DoS) attacks (Blackhole, Grayhole, Flooding, and Scheduling attacks) [8].

Step 3 — Train & Evaluate Models (per seed)

HGBoostUCAD algorithm

- Train on X_train, y_train
- Predict y_pred_hgb on X_test

Deep Neural Network (DNN)

- Build sequential model: Dense → BatchNorm → Dropout → Dense → Softmax.

Compile with

adam, loss sparse_categorical_crossentropy

- Train with early stopping
- Predict y_pred_dnn on X_test

Compute ML metrics (accuracy, precision, recall, F1) for both models

Compute network metrics

Store results.

D. Results Evaluation

Step 4 — Statistical testing

- Determine model with highest mean metric (accuracy, precision, F1)
- Retrain best model on entire dataset (train/test split)
- Compute confusion matrix
- Save confusion matrix plot

Step 5 — Plotting

- ML metrics bar plot → HGBoostUCAD vs DNN
- Per-attack network metrics
- Loss curves
- DNN training & validation loss
- Gradient boosting log-loss.

IV. Experimental Results

A. Machine Learning Metrics

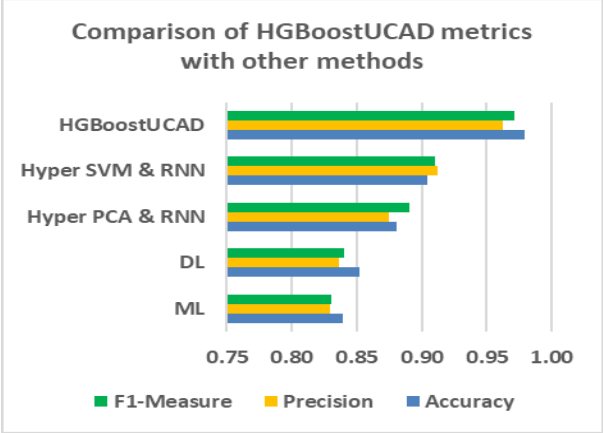

Fig. 2. Comparison proposal method with other similar methods.

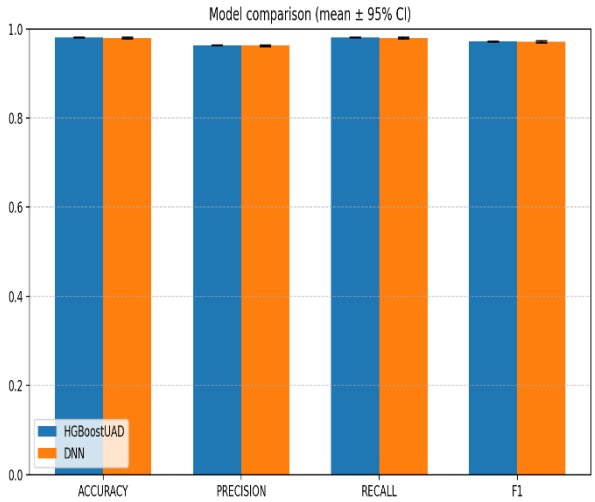

Fig. 3. Comparison between HGBoostUCAD and DNN method.

B. Network Performance Metrics

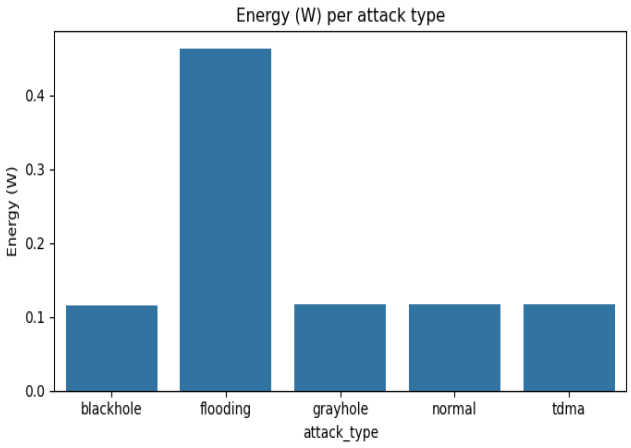

Fig. 4. Consumption energy per attack type.

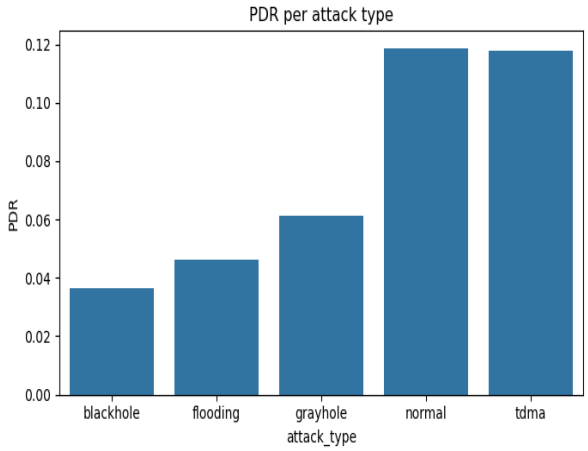

Fig. 5. Delivered packer ratio per attack type.

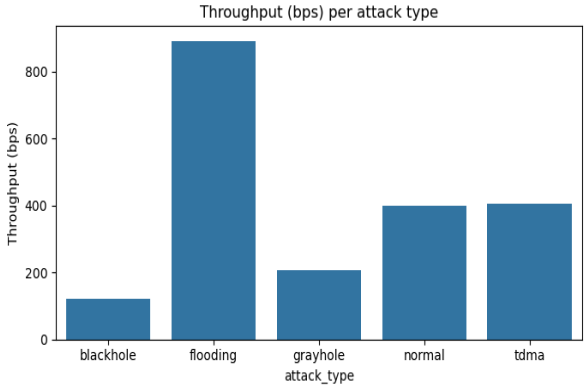

Fig. 6. Throughput variation for each type of attack.

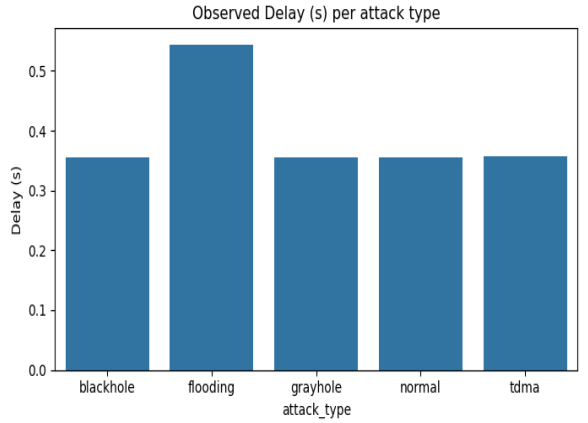

Fig. 7. Delay variation per attack type.

V. Analysis and Discussion

The experiment's outcomes are evaluated and explained from two perspectives: machine learning metrics and network metrics.

A. Machine Learning Metrics

In terms of machine learning model metrics, our approach surpassed both Deep Neural Network (DNN) and the previous study Hyper_RNN_SVM, cited in paper [13], as demonstrated by the simulation results (Fig. 2), which attained 97% accuracy and 96% precision. Also, high accuracy indicates that the IDS's detections are trustworthy.

- Accuracy for Classification Performance (see Fig. 3)

Both models demonstrate high and nearly identical accuracy, with mean values around 97%.

HGBoostUCAD: 0.97969; DNN: 0.97855

- Precision and False Alarm Behavior

Precision reflects the model's ability to avoid false positives (normal traffic misclassified as attacks).

HGBoostUCAD: 0.96236; DNN: 0.96121

The gradient-boosting ensemble performs slightly better than the DNN in preventing false alarms, according to the HGB's marginally higher precision. Because HGB builds additive trees that effectively divide local areas of feature space, it may be naturally resistant to noisy or non-linear feature interactions.

- Recall and detection sensitivity

Recall measures the ability to detect actual attacks (true positives). Both models again perform at a similar level:

HGBoostUCAD: 0.97969; DNN: 0.97855

The nearly equal recall results show that both approaches successfully identify malicious activity, indicating that neither one has significant insufficient detection.

- F1 score and balance of metrics

The compromise between missed detections and false alarms is taken up by the F1-score, which is the balance of precision and recall. The nearly identical F1-scores confirm that both models maintain an excellent balance between sensitivity and specificity, with our model HGBoostUCAD having a slight advantage.

HGBoostUCAD: 0.97090; DNN: 0.96973

B. Network Performance Metrics

We have selected four network performance parameters—energy consumed, packet delivered ratio, packet delivered delay and throughput of network communications,—that can function as essential evaluation metrics according attack type since the aim of DoS attacks is to render a target unreachable and isolated from the rest of the network. Also, to enhance comprehension of the results analysis and discussion, we describe the following network metric indicators below:

1) Energy: It is the total quantity used for data/control packet exchange by all nodes. The network will be less effective and have a shorter lifespan with high energy consumption, and vice versa [24].

2) Packet Delivery Ratio (PDR): It is calculated by dividing the total number of successfully delivered packets to the destination node or nodes by the total number of packets that were originally sent. A higher PDR means that there is less packet loss in the network [24]. When malicious traffic attacks the network, packet loss that affect PDR grows. To determine

how much legal traffic is impacted by the attack and how many data packets fail to reach their destination, the simulation assesses packet loss [25].

3) Packet Delivery Delay (Delay): The entire amount of time required for a packet to be transmitted from the sender to its successful delivery at the final destination node [24]. When servers are overloaded with fraudulent traffic, delay increases significantly, making it impossible for the server to react quickly to legitimate requests [25].

4) Average throughput: Throughput is a direct indicator of the network's capacity to manage traffic both normally and under attack. High-intensity volumetric attacks typically overload the network bandwidth, significantly decreasing it [25]. It is defined as average number of packets that the base station successfully receives in a given amount of time. Bits per second are used to measure it [26].

a) Flooding attacks: A smaller PDR (Fig. 5) usually leads to many retransmissions and congestion, which increase delays as seen in (Fig.7) and energy consumption (Fig. 4).

b) Blackhole attacks: significantly reduce throughput by greatly (Fig. 6) often impacted by congestion near the sink. Also, this attack type reduces PDR (automatically lost packets) (Fig. 5) and increase delay (Fig. 7).

c) Scheduling and Grayhole attack: IDS finds it challenging to identify attacks like Scheduling and Grayhole, which causes a slight reduction in performance (Fig. 5, Fig. 6) while maintaining efficiency on PDR concerning TDMA schedules.

In summary, the flooding attack caused more energy dissipation and increased delay than the three other DOS attacks, while the black hole attack provoked a significant diminution of both the packet delivery ratio and the throughput compared to TDMA schedules. Although our approach is effective in detecting malicious activity, as evidenced by accuracy and precision values, it has weaknesses, which are first evident in the actual scenario's implementation, which is constrained by various real-world constraints, and then in the UWSN dataset's unavailability in contrast to the WSN.

VI. Conclusion

In conclusion, this work enables it possible to implement a cyberattack detection on UWSN using an adjusted WSN-DS dataset and a histogram gradient boosting technique with a type of ensemble machine learning suitable for classification category; to incorporate environmental adaptation: temperature, salinity, depth, and mobility; to prove the efficacy of the suggested method in comparison to similar approaches; in fact, our approach outperformed both the Deep Neural Network (DNN) and the previous study Hyper_RNN_SVM, as illustrated by the simulation results; to provide metrics model (Accuracy, Precision, Recall, and F1 score); to show how network performance varies depending on the type of attack., and to offer an adaptive helpful model for future research to enhance performance and successfully address potential UWSN security issues. Extended research on various attack types and machine learning classifiers aims to enhance resource efficiency and accuracy in underwater wireless sensor networks (UWSN) security. Intrusion detection systems (IDS) play a vital role as a secondary defense, monitoring and detecting threats that bypass primary security measures like firewalls or encryption. A critical challenge is managing the resource constraints of sensor nodes—such as battery, memory, and CPU—while maintaining high detection accuracy in WSN-specific IDS.

Conflict of interest: No declaration required. Financing: No reporting required.

Acknowledgment

I want to express my gratitude to Mohammed V University in Rabat's Hight School of Computer Sciences and Systems Analysis for promoting academic researchers. I also want to thank the supervisor, Pr. Amine Berqia and, the co-supervisor Pr. Souad Aouad for their guidance and support.

References

[1] Mohsan, Syed Agha Hassnain, Yanlong Li, Muhammad Sadiq, Junwei Liang, et Muhammad Asghar Khan. « Recent Advances, Future Trends, Applications and Challenges of Internet of Underwater Things (IoUT): A Comprehensive Review ». Journal of Marine Science and Engineering 11, no 1 (January 2023): 124. https://doi.org/10.3390/jmse11010124.

[2] Yang, G.; Dai, L.; 3390/s18113907Wei, Z. Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks. Sensors 2018, 18, 3907,

[3] Saeed, Khalid, Wajeeha Khalil, Ahmad Sami Al-Shamayleh, Sheeraz Ahmed, Adnan Akhunzada, Salman Z. Alharthi, et Abdullah Gani. « A Comprehensive Analysis of Security-Based Schemes in Underwater Wireless Sensor Networks ». Sustainability 15, no 9 (April 2023): 7198. https://doi.org/10.3390/su15097198.

[4] Kao, C.C.; Lin, Y.S.; Wu, G.D.; Huang, C.J. "A comprehensive study on the internet of underwater things: Applications, challenges, and channel models ". Sensors 2017, 17, 1477.

[5] D. Berman, A. Buczak, J. Chavis, and C. Corbett, "A survey of deep learning methods for cyber security," Information, vol. 10, no. 4, p. 122, 2019.

[6] Neda Azizi, Omid Haass, "Cybersecurity Issues and Challenges," DOI: 10.4018/978-1-6684-5284-4.ch002, Torrens University, Australia RMIT University, Australia, 2022.

[7] P, W. (2020). A Survey of Intrusion Detection System. International Journal of Informatics and Computation, 1(1), 1. https://doi.org/10.35842/ijicom.v1i1.7. New reference list.

[8] Almomani,1,2 Bassam Al-Kasasbeh,2 and Mousa AL-Akhras and titled WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks, 2016, Journal of Sensors.

[9] Ouidir, Hamid, Amine Berqia, et Siham Aouad. « Improving UWSN Performance Using Reinforcement Learning Algorithm QENDIP ». 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, 23 Jully 2024, 1 6. https://doi.org/10.1109/WINCOM62286.2024.10656891.

[10] Alpaydın, Ethem, "Introduction to Machine Learning. Third edition ", MIT Press, 2014.

[11] Alqahtani, Mnahi, Abdu Gumaei, Hassan Mathkour, et Mohamed Maher Ben Ismail. "A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks". Sensors 19, no 20 (October 2019): 4383. https://doi.org/10.3390/s19204383.

[12] Xia, Y.; Liu, C.; Li, Y.; Liu, N. "A boosted decision tree approach using Bayesian hyper-parameter optimization for credit scoring". Expert Syst. Appl. 2017, 78, 225–241.

[13] Altameemi, Atyaf Ismaeel, Sahar Jasim Mohammed, Zainab Qahtan Mohammed, Qusay Kanaan Kadhim, and Shaymaa Taha Ahmed. "Enhanced SVM and RNN Classifier for Cyberattacks Detection in Underwater Wireless Sensor Networks." International Journal of Safety and Security Engineering 14, no. 5 (October 2024): 1409–17. https://doi.org/10.18280/ijsse.140508.

[14] Bagali S, Sundaraguru R.” Efficient Channel Access Model for Detecting Reactive Jamming for Underwater Wireless Sensor Network.”, In: 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET). 2019.

[15] Haijie Huang, Na Liu, Dandan Chen, Qiuling Yang, Xiangdang Huang, "Research on the Intrusion Detection Model of Underwater Sensor Networks", Journal of Sensors, vol. 2022, Article ID 2323747, 17 pages, 2022.

[16] Affane M., Anselme R., et Hassan Satori. « Machine Learning Attack Detection Based-on Stochastic Classifier Methods for Enhancing of Routing Security in Wireless Sensor Networks ». Ad Hoc Networks 163 (octobre 2024): 103581. https://doi.org/10.1016/j.adhoc.2024.103581.

[17] Zenia, and Z. I.Chowdhury, "A novel algorithm for malicious attack detection in UWSN,” in Proceedings of the 2015 IEEE International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), pp. 1–6, Dhaka, Bangladesh, May 2015.

[18] Note, Johan, Erind Mullalli, et Betim Cico. « Machine Learning Algorithms for Cyber Attack Detection And Classification ». Proceedings of the International Conference on Computer Systems and Technologies 2024, ACM, 14 June 2024,29-36. https://doi.org/10.1145/3674912.3674937.

[19] Z. Junqing, Z. Gangqiang and L. Junkai, "Wormhole Attack Detecting in Underwater Acoustic Communication Networks," 2021 OES China Ocean Acoustics (COA), Harbin, China, 2021, pp. 647-650.

[20] Shenfield, Alex, David Day, and Aladdin Ayesh. "Intelligent intrusion detection systems using artificial neural networks." Ict Express 4.2 (2018): 95-99.

[21] Dhanya, K.A., Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T. Senthil Kumar, et T. Gireesh Kumar. “Detection of Network Attacks Using Machine Learning and Deep Learning Models “. Procedia Computer Science 218 (2023): 57 66.

[22] Y.Wu, D.Wei, and J.Feng, “Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey,” 2020.

[23] Mackenzie, K. V. (1981). Nine-term equation for sound speed in the oceans. J. Acoust. Soc. Am., 70(3), 807–812.

[24] Altaweel, A., Aslam, S., & Kamel, I. (2024). Security attacks in Opportunistic Mobile Networks: A systematic literature review. Journal of Network and Computer Applications, 221, 103782. https://doi.org/10.1016/j.jnca.2023.103782.

[25] Kumavat, K., Sardhara, A., Shinde, T., Salunkhe, V. \& Satpute, M. Analyzing the Impact of Distributed Denial Of Service Attacks Using NS2: A Scenario-Based Study. (2025).

[26] A. Salih, M., & R. Sulaiman, D. (2023). Throughput and energy efficiency evaluation of wsn using efficient routing protocols. University of Thi-Qar Journal for Engineering Sciences, 13(1), 25-33. https://doi.org/10.31663/tqujes13.1.438(2023).