Machine Learning Driven Advanced Défense Mechanisms Against Blackhole and Flooding Attacks in Wireless Sensor Networks

Dr. Ayesha Banu[1], S. Nikitha[2], K. Vinitha[2], E. Laxmi[2], Ayesha Tarannum[2]

[1]Professor and Head, [2]UG Student, [1,2]Department of CSE (Data Science)
[1,2]Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana, India

Corresponding Email: ayeshabanuvce@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) correspond of spatially distributed independent detectors that cover physical or environmental conditions, similar as temperature, sound, and pressure. These networks transmit their data to a central position for processing and analysis. The conception of WSNs surfaced in the early 2000s, driven by advancements in wireless communication and miniaturization of detector technologies. The original focus was on creating energy-effective protocols to extend the lifetime of these networks. Over time, as WSNs came more integral to critical operations, the need for robust security mechanisms grew, especially against pitfalls like blackhole and flooding attacks. Blackhole attacks involve a vicious knot falsely flashing optimal paths to block and discard data packets, leading to data loss. Flooding attacks overwhelm the network with inordinate business, causing network traffic and draining the battery life of detector bumps. These attacks can oppressively compromise the trustability, effectiveness, and life of WSNs, making it essential to develop advanced defense mechanisms. Traditional defense mechanisms in WSNs calculate on cryptographic ways and simple anomaly discovery styles. Cryptographic ways, while effective against unauthorized access, are computationally ferocious and consume significant energy, which is a scarce resource in WSNs. Anomaly discovery styles frequently fail to distinguish between licit high- business scripts and factual flooding attacks, leading to false cons and negatives. The need for advanced defense mechanisms in WSNs is consummate to ensure the integrity and vacuity of data in critical operations. Machine learning (ML) offers promising results by enabling the development of adaptive and intelligent defense systems that descry and respond to attacks in real- time. The significance of this design lies in its implicit to enhance the security and adaptability of WSNs.

Keywords: Blackhole Attack, Network Security, Wireless Sensor Networks (WSNs), Adversarial Attacks

1. INTRODUCTION

In the realm of Wireless Sensor Networks (WSNs), black holes and flooding attacks have been a critical area of concern since the early 2000s. These attacks pose significant pitfalls to the functionality and security of WSNs, which are employed in operations from environmental monitoring to military operations. Black hole attacks were first linked in 2004 when experimenters observed that vicious bumps could attract data packets by falsely claiming to be the most effective route, later discarding them. Flooding attacks, on the other hand, were noted in 2006 as an attack vector that involves overwhelming the network with a high volume of business, leading to business and prostration of knot coffers. According to studies conducted in 2010, WSNs facing black hole attacks endured up to a 40% reduction in data delivery rates, while submerging attacks could beget a 60% drop in network proliferation. The traditional defense mechanisms, primarily cryptographic ways and anomaly discovery styles, began to show limitations around 2015, particularly in their effectiveness and capability to handle sophisticated attack strategies. Advancing in machine knowledge (ML) has surfaced as an implicit result of addressing these limitations. As of 2020, ML-rested styles have been

explored to enhance the discovery and mitigation of similar attacks by using their adaptive knowledge capabilities. Research from 2022 highlights that ML ways, similar to supervised knowledge and neural networks, have shown a pledge in significantly reducing false positives and perfecting discovery delicacy in comparison to conventional styles. This elaboration on defense mechanisms underscores the growing significance of integrating ML into WSN security protocols to ensure robust and flexible network operations.

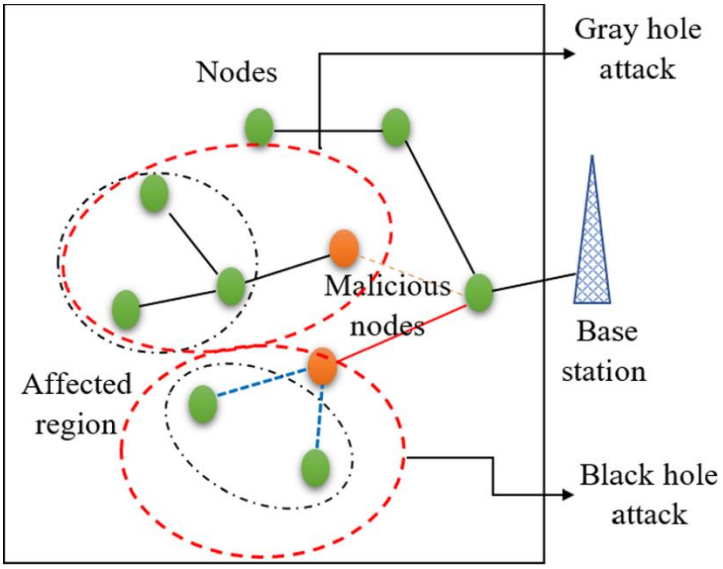

Fig. 1: Black hole attack

2. LITERATURE SURVEY

An overview of secure watermarking methods and how they relate to IoT technology was given by Wazirali et al. [1]. They also developed active watermarking techniques, which add watermarks to data to help verify its validity and integrity, to improve the security of IoT systems. The difficulties and outcomes of using watermarking techniques on IoT fabrics were the main topics of their review. Bouaziz and Rachedi [2] investigated mobility operating protocols in Wireless Sensor Networks (WSNs) based on 6LoWPAN. They analyzed dynamic protocols that control mobility to ensure efficient network functioning in low-power wireless scenarios. Their assessment's primary objectives were to evaluate procedure performance and identify areas that required improvement. With a focus on IoT integration, Al-Kashoash et al. [3] explored congestion control in wireless sensor and 6LoWPAN networks. In order to increase data transmission efficiency and reliability in Internet of Things networks, they examined several congestion control technologies and provided methods to improve network performance in congested situations. The effectiveness of ZigBee network topologies for communication and monitoring systems in subterranean spaces was examined by Moridi et al. [4]. The purpose of their study was to assess how well different ZigBee network configurations worked for communication and monitoring in subterranean environments. They emphasized each topology's advantages and disadvantages. The architecture, protocols, and technologies of LoRaWAN were studied by Ertürk et al. [5]. They went over the foundations of LoRaWAN, including its communication protocols. On low-power wireless particular area networks (6LoWPAN), Kumar and Tiwari [6] examined IPv6 routing styles. They looked at several routing protocols that were created to maximize data routing in 6LoWPAN settings. According to their check, these protocols are veritably good at handling routing jobs and enhancing network effectiveness. The BPA- CRP protocol is a balanced power- apprehensive clustering and routing system for wireless detector networks that was proposed by Darabkh et al. [7].

The thing of their work was to produce a protocol that balances routing effectiveness and power consumption in WSNs. They sought to use better clustering and routing ways to increase network performance and lifetime. Sah and Amgoth [8] offered a parametric check on wireless detector networkcross-layer infrastructures. Severalcross-layer design ways that combine several network protocol mound situations to maximize performance were examined. For safe and energy-efficient communication in wireless detector networks, Khashan et al. (2009) suggested an automated featherlight encryption technique. Their strategy sought to reduce energy usage and improve data security. They focused on creating an encryption system that would work in environments with limited resources. The influence of featherlight encryption and clustering techniques on the persistence of wireless detector networks was analyzed by Ahmad et al. (2010). They investigated the effects of various encryption techniques and clustering strategies on network continuity. Their goal was to identify the best outcomes for increasing WSNs' functional longevity. Dynamic critical operation techniques in wireless detector networks were examined by Yousefpoor and Barati [11]. They conducted a survey of robust encryption key management methods, confirming their efficacy in preserving security and managing funds in WSNs.

3. PROPOSED SYSTEM

The investigation starts with the upload of a dataset called "WSN-DS.csv," which includes details on various attack kinds and network conditions in Wireless Sensor Networks (WSNs). The dataset's structure, including the various attack kinds and the existence of any missing values, is first investigated. This first stage is essential for ensuring the integrity of the data before moving on to more intricate design stages.

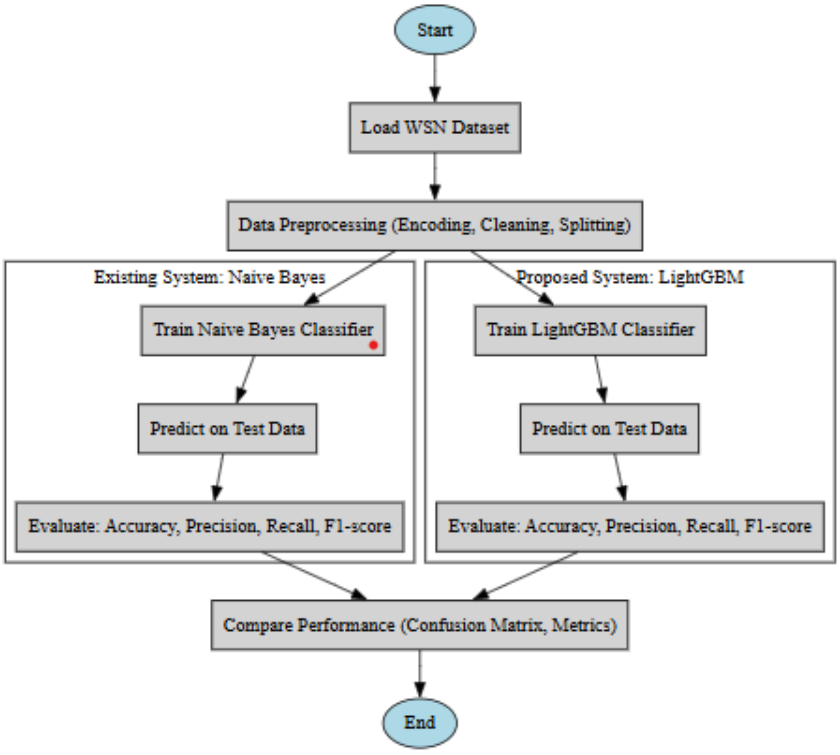

Fig. 2: Proposed Block Diagram.

3.1 ML Model Building

LightGBM, or Light Grade Boosting Machine, is an advanced machine learning method designed to be extremely effective and efficient. LightGBM is well-suited for challenging tasks like identifying attacks in WSNs and massive datasets because of its base in the grade boosting frame and performance and memory optimization. LightGBM builds an ensemble of decision trees, each of which corrects the violations of the preceding bones. This iterative procedure enables the model to learn intricate patterns and correlations between features. Two of LightGBM's primary features are its support for distributed training, which significantly speeds up the training process on large datasets, and its direct handling of categorical features. Furthermore, the LightGBM classifier is trained and estimated using the GNB classifier. The model is estimated on the testing data after being trained on the training data. LightGBM performs better because of its ability to capture intricate relationships in the data, as well as its robustness to point relations and data distributions.

Proposed algorithm LightGBM: Microsoft created the distributed, high-performance gradient boosting framework known as LightGBM (Light Gradient Boosting Machine). Because it maintains high accuracy while optimizing speed and memory efficiency, it is perfect for complicated classification jobs and big datasets.

How LightGBM Works

1. **Histogram: Realistically based literacy**
   For each data point, LightGBM replaces traditional split chancing with histogram-grounded binning, where nonstop point values are sorted into different lockers. This significantly reduces calculation time and memory operation.
2. **Depth-first growth, or tree growth by leaf**
   Other boosting algorithms (like XGBoost) use tree-level growth, but LightGBM uses leaf-wise growth. With the highest loss reduction, it expands the splint knot, resulting in deeper trees and enhanced delicacy while maintaining efficacy.
3. **Choosing Points and Their Importance**
   LightGBM uses feature donation to the decision trees to rank features in order to efficiently select the most pertinent features. It speeds up training and improves conception.
4. **Support for Categorical Features**
   LightGBM may significantly reduce dimensionality and enhance performance compared to traditional models that need one-hot encoding by handling categorical variables directly.
5. **GPU acceleration**
   LightGBM is fast on large datasets, especially when training deep trees, because it makes GPU training possible.in particular while training deep trees.

LightGBM Architecture

Although LightGBM is based on grade boosting decision trees (GBDT), it optimizes classic GBDT using a unique leaf-wise growth strategy and histogram-based binning to maximize training speed and delicacy. This is the architectural breakdown of LightGBM.

1. **Structured irregular data** (numerical and categorical) can be entered into the input subcaste (point processing and data binning). reduces computational and memory costs by using histogram-grounded binning rather than raw nonstop values. Categorical point running is efficient without requiring one-hot encoding.
2. **Histogram of Ground Point Splitting**

doi: 10.48047/ijiee.2025.15.4.22

LightGBM creates histograms and selects the optimal split from the histogram lockers rather than considering every possible split point like standard GBDT does. simplifies the computation by substituting O(#bins ×#features) for O(#data ×#features).

3. **Decision tree growth (leaf-wise splitting)**
   LightGBM grows treesleaf-wise as opposed to GNB's tree-level growth, which means it selects the splint knot with the highest loss reduction. Smaller duplications so result in trees that are more accurate and deeper. Regularization can be used to control overfitting, which can occur even though this method improves delicacy.
4. **Fourth-grade grounded leaf splitting**
   The slants of the loss function are computed to find the fashionable split. assigns advanced weights to samples that are more challenging to categorize for the next replication. It supports both L1 and L2 regularization to help with overfitting.
5. **A set of weak decision tree models is produced by the grade boosting decision trees (GBDT) boosting framework.**
   Each tree corrects the mistakes of the preceding trees via grade-grounded boosting. supports a wide variety of boosting types. GBDT, or boosting decision trees fury (many cumulative retrogression trees occur for dropouts) GOSS (grade-ground, one-side slice)
   Loss Function and Objective Optimization The loss function for this optimization is either Softmax (multi-class bracket) or Log Loss (double bracket) establishes the optimization grade and Hessian. makes use of effective resemblant computing to speed up training.

4. RESULTS AND DISCUSSION

In Figure 1, an example of the Wireless Sensor Network (WSN) dataset is displayed. This dataset consists of columns such as id, Time, Is_CH, person CH, Dist_To_CH, ADV_S, ADV_R, JOIN_S, JOIN_R, SCH_S, SCH_R, Rank, DATA_S, DATA_R, Data_Sent_To_BS, dist_CH_To_BS, send_code, Expanded Energy, and Attack type. These columns represent several attributes standards related to the detection of network attack types and detector bump functionality.

Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	dist_CH_To_BS	send_code	Expaned Energy	Attack type
0.00000	1	0	0	25	1	0	0	0	1200	48	130.08535	0	2.46940	Normal
75.32345	0	4	1	0	0	1	2	38	0	0	0.00000	4	0.06957	Normal
46.95453	0	4	1	0	0	1	19	41	0	0	0.00000	3	0.06898	Normal
64.85231	0	4	1	0	0	1	16	38	0	0	0.00000	4	0.06673	Normal
4.83341	0	4	1	0	0	1	25	41	0	0	0.00000	3	0.06534	Normal
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
0.00000	1	6	0	26	1	0	0	0	1196	0	0.00000	0	0.00720	Blackhole
0.00000	1	4	0	55	1	0	0	0	1320	0	0.00000	0	0.00722	Blackhole
0.00000	1	10	0	14	1	0	0	0	745	0	0.00000	0	0.00721	Blackhole
0.00000	1	10	0	11	1	0	0	0	921	0	0.00000	0	0.00726	Blackhole
0.00000	1	6	0	31	1	0	0	0	1240	0	0.00000	0	0.00722	Blackhole

Fig. 3: Sample Uploaded Dataset.

The dataset's distribution of various orders is seen using the count plot, which reveals a notable class imbalance. With 19,209 cases, the Normal order has the highest count, followed by the Grayhole with 14,596 and the Blackhole with 10,049 cases. Flooding has the lowest number of cases (3,312), while TDMA has 6,638. This disparity shows that while attack types like flooding and TDMA are relatively uncommon, regular network operations are the most common. The preponderance of Normal and Grayhole orders raises the possibility that machine learning models developed using this dataset are biased in favor of these classes, which could result in inadequate identification of attack types that are

doi: 10.48047/ijiee.2025.15.4.22

underrepresented. In order to ensure balanced model performance, strategies like oversampling, undersampling, or class-ladened literacy may be required to overcome this problem.

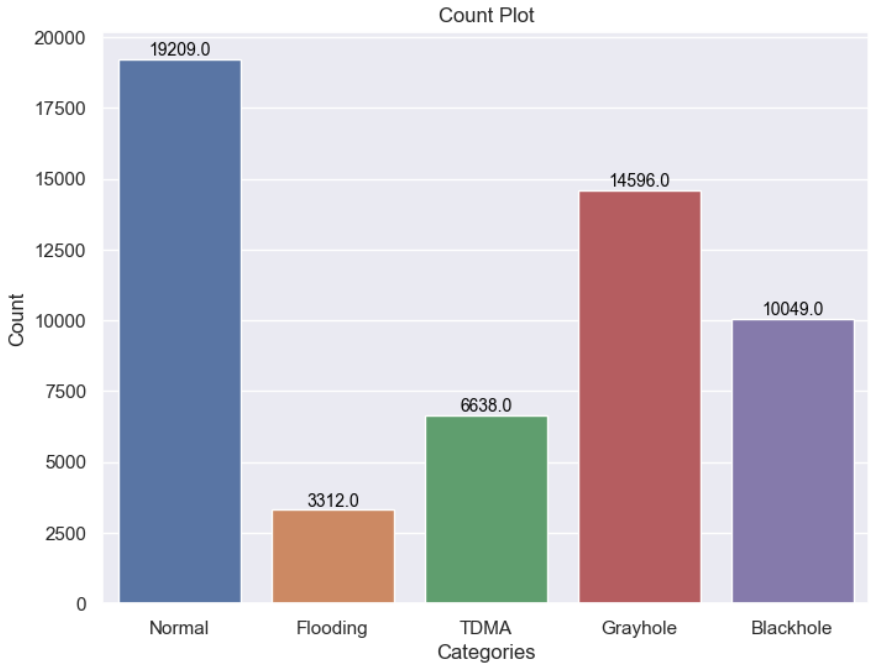

Fig. 4: Count plot.

Each bar in the bar plot indicates the number of occurrences in a specific category, visualizing the distribution of various attack types. The category labels are represented numerically on the x-axis (0, 1, 2, 3, 4), while the number of instances is displayed on the y-axis. The category with the highest number (19,209 instances) is the one with the highest frequency in the dataset. With 14,596 cases, category 2 is the second-highest category, and category 0 comes in at 10,049 instances. The numbers for Categories 1 and 4 are comparatively smaller, with 3,312 and 6,638 cases, respectively. This distribution draws attention to the disparity in class, with certain groups being overrepresented and others underrepresented. An imbalance like this could impact machine learning models' performance, necessitating methods like cost-sensitive learning, undersampling, or oversampling to increase classification accuracy.

doi: 10.48047/ijiee.2025.15.4.22

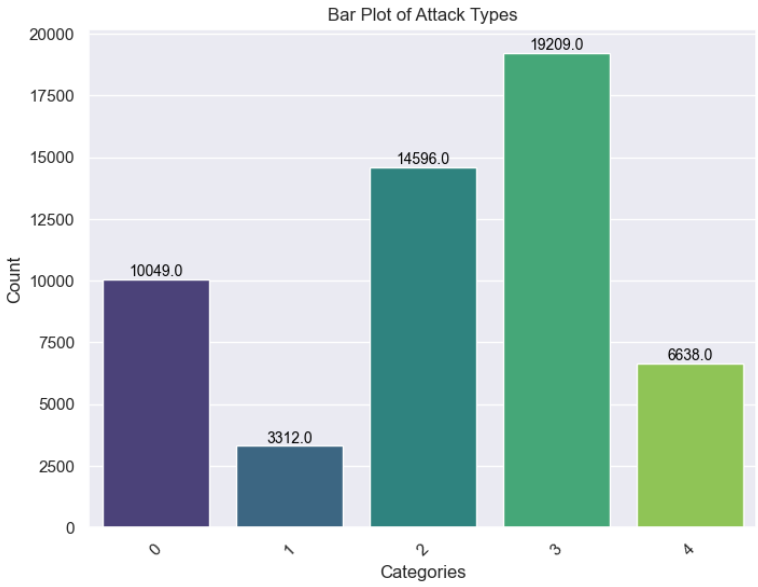

Fig. 5: Bar plot.

With the frequency of occurrences on the y-axis and the various attack categories (0, 1, 2, 3, 4) represented on the x-axis, the histogram illustrates the distribution of attack types in the dataset. While the superimposed density curve offers a smoother depiction of the distribution, the blue-shaded histogram bars show the number of each assault type. Attacks of type 3 are the most common, followed by attacks of type 2 and type 0. Due to their much lower frequency, attack types 1 and 4 show an imbalance in the sample. By displaying clear groupings of attack types, the density curve highlights the frequency distribution's peaks and troughs even more. The observed imbalance raises the possibility that class-weighted learning or data balancing strategies may be necessary to improve classification performance across all attack categories in machine learning models built on this dataset.

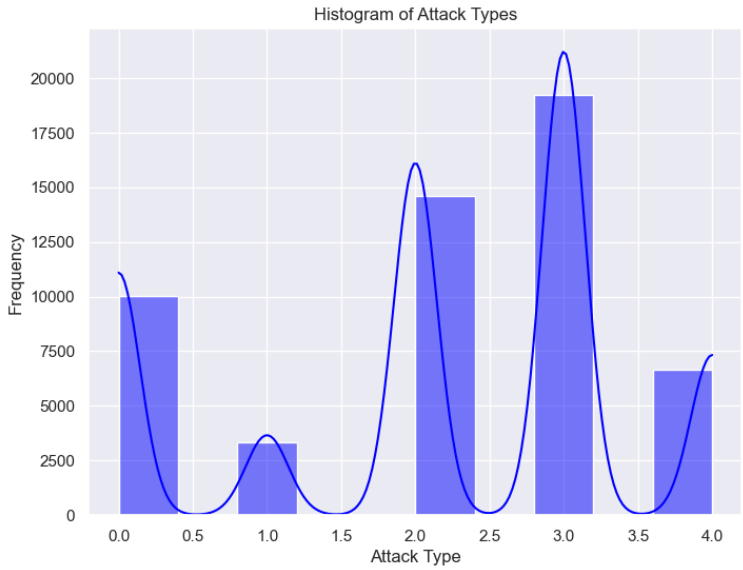

Fig. 6: Histogram plot

The confusion matrix shown in the image represents the performance of a Naïve Bayes classifier in classifying different attack types: Blackhole, Flooding, Grayhole, Normal, and TDMA. The x-axis denotes the predicted class, while the y-axis represents the true class. The diagonal values indicate

doi: 10.48047/ijiee.2025.15.4.22

correctly classified instances, while off-diagonal values represent misclassifications. From the matrix, the classifier performs well in identifying Normal traffic with 2,337 correctly classified instances but struggles with distinguishing Blackhole attacks, misclassifying 1,947 instances as Blackhole when they belong to other classes. The classifier also confuses Flooding and Grayhole attacks, as seen in the misclassification of 572 Flooding attacks as Blackhole and 1,097 Blackhole attacks as Grayhole. The TDMA class shows significant misclassification, with 526 instances misclassified as TDMA from other categories. These observations suggest that the model has difficulty differentiating between attack types, indicating potential improvements through feature engineering, data balancing, or using a more robust classifier.

The confusion matrix in the image represents the performance of the LGBMClassifier in classifying different attack types: Blackhole, Flooding, Grayhole, Normal, and TDMA. The x-axis represents the predicted class, while the y-axis denotes the true class. The diagonal elements indicate correctly classified instances, while off-diagonal values show misclassifications. From the matrix, the classifier performs well in identifying Normal traffic with 3,772 correctly classified instances and Grayhole attacks with 2,957 correctly classified instances. The Flooding attack class has 657 correctly classified instances, but some misclassifications exist, particularly into Normal and Grayhole. The TDMA class has a high number of misclassifications, with 1,317 instances incorrectly classified as TDMA, impacting the classifier's precision for this category. The Blackhole attack is predominantly classified correctly (1,985 instances), though some misclassifications occur. Overall, the LGBMClassifier performs significantly better than the Naïve Bayes classifier in terms of classification accuracy, reducing misclassification rates for most attack types. However, the misclassification of TDMA and some confusion between attack types still exist, suggesting potential improvements through hyperparameter tuning or feature selection.

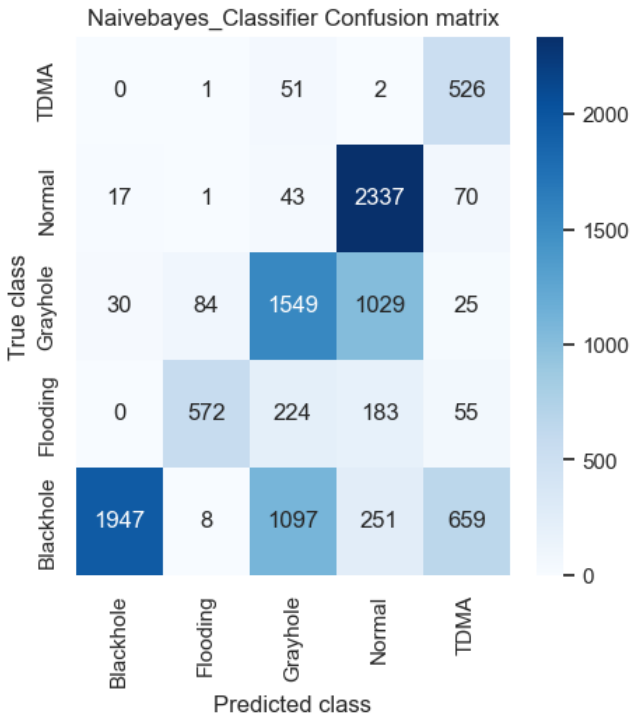

Fig. 7: Confusion matrix obtained using Naive Bayes Classifier

doi: 10.48047/ijiee.2025.15.4.22

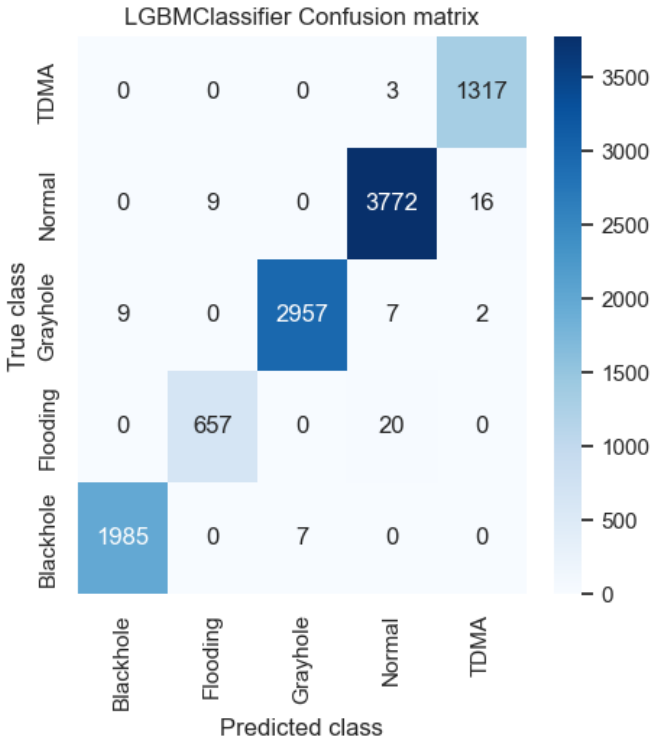

Fig. 8: Confusion matrix obtained using LightGBM Classifier.

5. CONCLUSION

This research implements the ML-driven approach for combatting against various attacks in WSN environment. A significant performance differences are seen when comparing the Naive Bayes and LightGBM classifiers for wireless sensor network attack type identification. The macro-average F1-score of the Naive Bayes classifier was 0.64, and its overall accuracy was 64.41%. Our classifier performed admirably in detecting Flooding and Blackhole attacks, but it had trouble recalling Grayhole and TDMA attacks. However, with a macro-average F1-score of 0.99 and an accuracy of 99.32%, the LightGBM classifier demonstrated remarkable performance. In every category, including Blackhole, Flooding, Grayhole, Normal, and TDMA attacks, our classifier produced almost flawless precision, recall, and F1-scores. LightGBM demonstrates its capacity to manage the complexity of attack classification in wireless sensor networks by outperforming Naive Bayes by a wide margin.

REFERENCES

[1] Wazirali, R.; Ahmad, R.; Al-Amayreh, A.; Al-Madi, M.; Khalifeh, A. Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview. Electronics 2021, 10, 1744.

[2] Bouaziz, M.; Rachedi, A. A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. Comput. Commun. 2016, 74, 3–15.

[3] Al-Kashoash, H.A.A.; Kharrufa, H.; Al-Nidawi, Y.; Kemp, A.H. Congestion control in wireless sensor and 6LoWPAN networks: Toward the Internet of Things. Wirel. Networks 2019, 25, 4493–4522.

[4] Moridi, M.A.; Kawamura, Y.; Sharifzadeh, M.; Chanda, E.K.; Wagner, M.; Okawa, H. Performance analysis of ZigBee network topologies for underground space monitoring and communication systems. Tunn. Undergr. Sp. Technol. 2018, 71, 201–209.

[5] Ertürk, M.A.; Aydın, M.A.; Büyükakkaşlar, M.T.; Evirgen, H. A Survey on LoRaWAN Architecture, Protocol and Technologies. Futur. Internet 2019, 11, 216.

[6] Kumar, V.; Tiwari, S. Routing in IPv6 over low-power wireless personal area networks (6LoWPAN): A survey. J. Comput. Netw. Commun. 2012, 2012, 316839.
[7] Darabkh, K.A.; El-Yabroudi, M.Z.; El-Mousa, A.H. BPA-CRP: A Balanced Power-Aware Clustering and Routing Protocol for Wireless Sensor Networks; Elsevier: Amsterdam, The Netherlands, 2019; Volume 82.
[8] Sah, D.K.; Amgoth, T. Parametric survey on cross-layer designs for wireless sensor networks. Comput. Sci. Rev. 2018, 27, 112–134.
[9] Khashan, O.A.; Ahmad, R.; Khafajah, N.M. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad. Hoc. Netw. 2021, 115, 102448.
[10] Ahmad, R.; Sundararajan, E.A.; Abu-Ain, T. Analysis the Effect of Clustering and Lightweight Encryption Approaches on WSNs Lifetime. In Proceedings of the 2021 International Conference on Electrical Engineering and Informatics (ICEEI), Kuala Terengganu, Malaysia, 12–13 October 2021; IEEE: Selangor, Malaysia, 2021; pp. 1–6.
[11] Yousefpoor, M.S.; Barati, H. Dynamic key management algorithms in wireless sensor networks: A survey. Comput. Commun. 2019, 134, 52–69.