Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 27 No. 4 (2024)

Selective Features Based Machine Learned Intrusion Detection Framework for Wireless Sensor Networks: A Need for Cryptographic Approach

Minal Ghute[1], Yogesh Suryawanshi[2]

[1]Research Scholar, Yeshwantrao Chavan College of Engineering, Nagpur, India
mrsminalghute@gmail.com

[2]Electronics Department, Yeshwantrao Chavan College of Engineering, Nagpur, India
yogesh_surya8@rediffmail.com

Article History:

Received: *13-03-2024*

Revised: *22-05-2024*

Accepted: *04-06-2024*

Abstract

Intruder attacks are a curse to wireless sensor network (WSN) nodes that affect their regular performance differently. The attacker cheats the cooperative characteristics of sensing elements pretending as a trustworthy node. Such intruders drastically degrade the WSN performance by affecting the sensing, collecting, processing, and transmitting capabilities of ideal nodes in the network. Due to their pretending behaviour, detecting such harmful nodes in the network is difficult since they are sometimes foes and other times friends. This paper introduces a selective feature-based machine-learning (SF-BML) framework that can detect an intruder node with a higher accuracy. The WSN-DS dataset constructed for four different attacks (Flooding, Blackhole, Grayhole, and Scheduling) is experimented with different feature attributes. The optimum features are found and tested for detection accuracy relating to all five categories. The experimental results using six significant features (SF) and a combination of eight other semi-significant features (SSF) showed that the normal-attacker node's detection accuracy increases with increasing features up to fourteen. The maximum training and test accuracy using fourteen features for the support vector machine (SVM) was 99.17% and 99.00% respectively.

Keywords: Intruder attacks, WSN, ideal nodes, selective feature, machine-learning, detection accuracy, and SVM.

1. Introduction

Networks are connected today with the advent of the Internet of Things which covers WSNs also. These integrated networks function cooperatively and influence people's lifestyles to a great extent [1]. Networks are overcrowded with distinct information that also includes secured personal data, medical records, business secrets, etc. Therefore, security is a crucial aspect of data over an unsecured medium. Data encryption, authentication, and authorization are commonly used and ensured methodologies in traditional security-providing technologies. However, recent thieves are more advanced and possess the ability to fool the best security system. Thus, for large-scale WSNs, there is an urge to provide urgent comprehensive solutions against unseen intruder attacks [2].

Proactive defence mechanisms are better solutions rather than passive defence in WSN since the latter does not guarantee robust protection [3]. Moreover, an intrusion detection system (IDS) actively identifies the attack in the network. But there seems to be a great difference between the actual real-world scenario inside the network and the aggregated data made available to IDS. This is due to the rapidly changing environment relating to increasing uncertain traffic. Also, the effectiveness of an IDS depends on its data processing power. That is how efficiently and rapidly the WSN information can be processed at any instant. The WSN environment fields on the other hand are not constant and carry unknown parameters under abnormal traffic conditions. Certain attacks have the ability to change the network traffic from its normal conditions [5]. Variable fields or attributes in the real-time network make it difficult for the classifier to discriminate between normal and abnormal systems [6]. Dominating attributes and unwanted noises create havoc in the network causing problems in detecting suspicious activities. This results in a reduced detection rate while consuming a large amount of available resources [7].

The performance of a classifier is determined by the input features, model parameters, and data used for training and testing. Therefore, selecting appropriate features plays a crucial role in machine learning. Advanced data relating to various fields or areas, in reality, has numerous dimensions of the feature space. However, only limited features present in the available dataset can represent the data as a whole. These significant features are cursed by some redundant and unrelated features that drastically affect the performance of machine learning protocols. Literature shows that many researchers have integrated feature selection strategies with machine learning in various fields such as network security and controlling congestions in heavy traffic scenarios.

As far as intrusion detection is concerned, higher accuracy is required for detecting the attacker node in a short time. Although several traditional network IDS are available, WSN possesses distinct characteristics regarding topology, routing, and other aspects. Therefore, the IDS frameworks specially meant for traditional networks do not apply to WSNs, and more sophisticated IDS is required. IDS for WSN must provide maximum detection accuracy in detecting an attacker and it must respond in less or minimum time, also ensuring minimum overhead on the network [8].

The article proposes an IDS called SF-BML framework that conforms to the WSN requirement and contributes in the following aspects:

1. A systematic approach to the feature selection mechanism is carried out to find the optimum number of features required in detecting the Denial of Service (DoS) attacks in the WSN-DS dataset.

2. The features based on standard feature selection approaches (Information Gain (IG), Chi-Square test (CST), Correlation Feature Selection (CFS), and Sequence Backward Selection (SBS)) are categorized into significant (SF) and semi-significant features (SSF) for eliminating redundant and unrelated features.

3. SVM-based classification is performed by concatenating the SF and randomized combination of SSF to show that the multi-class detection accuracy increases gradually with increasing features up to a certain number of features and thereafter saturates.

The rest of the article is organized as: Section 2 summarizes the work suggested by different researchers relating to IDS. The proposed SF-BML framework for IDS is described in Section 3.

Section 4 includes experimental results and analysis, and the last section concludes the work with future extensions.

2. Related Work

The intense need for an IDS, especially for wireless networks, has excited several researchers in the last decade. The idea behind detecting abnormal activities in many research studies was to find any deviation in the network from the normal characteristic. Accordingly, a few anomaly detection schemes were proposed, including distinctive learning algorithms, clustering–based algorithms, and artificial immune methods.

An immune theory called danger theory to protect WSN was introduced in [9]. The authors monitored various network parameters and computed weight-based outputs. The cooperative nature of the network nodes ensures the detection of intrusions, enhances robustness, reduces energy consumption, and increases the detection rate. The model worked better for networks when the interfering nodes were lower. However, increasing interfering nodes significantly reduced the detection rate and increased the energy loss.

The authors in [10] concentrated on reducing the attack detection time by reducing the features to a considerable extent while achieving greater detection accuracy. They proposed the SLGBM IDS method that covered the redundancy issue and high correlation between network details. The priory focussed on reducing the feature dimension of the traffic data to minimize the computational overheads using the SBS scheme. They found that their SLGBM IDS performed better with 10 features on all four attacks in the WSN-DS dataset using a LightGBM algorithm reducing the detection time by 65% and feature dimension by 44%. However, their model lacks in use of a distributed technique to further enhance the consumption time for real applications.

The work proposed in [11] concentrated on growing networks and unseen attacks developed by malicious users or attackers. The author suggested a CNN-LSTM-based framework to classify the samples into two classes and for all classes using three different datasets. The composite neural network was used for extracting features which were normalized and the labels were converted to numeric form (One-Hot-Encoder). The best features were selected considering all three datasets and partitioned in an 80:20 ratio for processing. They evaluated the network for binary and multi-class configuration (5, 6, and 10 classes) for samples from CIC-IDS 2017, UNSW-NBi5, and the WSN-DS datasets. Experimental results with LSTM and CNN showed that detection accuracy for the binary class was higher as compared to multi-class, the highest detection accuracy being 99% in the case of CIC-IDS 2017, and the WSN-DS datasets. Their model failed to perform with certain attacks and quoted the reason as data imbalance.

The authors in [12] showed that solving data imbalance problems and dimension reduction improves the detection rate in IDS. They balanced the dataset from three different datasets using the synthetic minority excessive method. Further, the feature dimension was reduced using singular value decomposition, principal component analysis, and k-means clustering. They encoded labels, normalized the data, separated training, validation, and test samples, and classified the samples using deep learning. They experimented on full features and reduced features and found that the detection rate using the reduced features was better and above 99% for all three datasets.

A federated learning-based LSTM network was employed for better security and privacy in [13]. The SCNN-Bi-LSTM model was introduced to discriminate different DoS attacks from two different datasets: CIC-IDS 2017 and the WSN-DS. The objective of their work is to handle carefully complex and unseen attacks in the network and place the effectiveness of deep-learned networks in preserving data privacy. Their approach succeeded in performing intrusion detection tasks, however, it showed limited performance in terms of data scalability, adaptability, quality, processing, and training and performed poorly for variable network conditions and unseen attacks.

The work in [14] used only four attributes namely packets received/sent by the nodes, energy dissipation, and the trust score of the nodes to detect three different attacks from the CICIDS2017 dataset. An artificial neural network (ANN) was incorporated to model the dynamic behavior of the WSN and detect regular and real-world attack patterns. Although the detection rate (average accuracy) obtained using the ANN was about 99%, their work lacked focus on the computational time that was required to respond against the attacker node.

Geo Francis E. and Sheeja S worked with three datasets for classifying attackers [15]. They pre-processed the datasets and reduced the feature dimension using the Pelican Optimization Algorithm. Their fine-tuned Multilayer Perceptron and CatBoost classifiers over CSE-CIC-IDS2018, UNSW-NB15, and the AWID datasets showed better performance on the binary class (normal and attacker) problem. Similar work was introduced in [20] with three different datasets that included the NSL-KDD, UNSW-NB15, and the CICIDS2017 datasets. The network model included the RF and RF-Extreme Gradient Boost classifiers obtained 99.8% accuracy on the first dataset and 100% on the latter two datasets. They concluded that higher detection accuracy can be achieved with hybrid ML techniques, quality features through novelty in feature extraction techniques, and advanced intrusion detection. However, their framework does not show immunity against network dynamic changes.

Internal intrusions are caused by a member node in the network itself which had changed its behavior due to being destroyed. Such types of intrusions are caused due to two types of nodes: Independent nodes are non-cooperative but utilize network resources and do not harm other members [16]. On the other hand, a malicious node disguised as a normal node actively participates in the communication process thereby resulting in eavesdropping, interfering, and also controlling the complete network activities. Therefore, due to the limited resources of WSN, there is a need to change the architecture of IDS according to the requirements and environment.

3. Material and Method

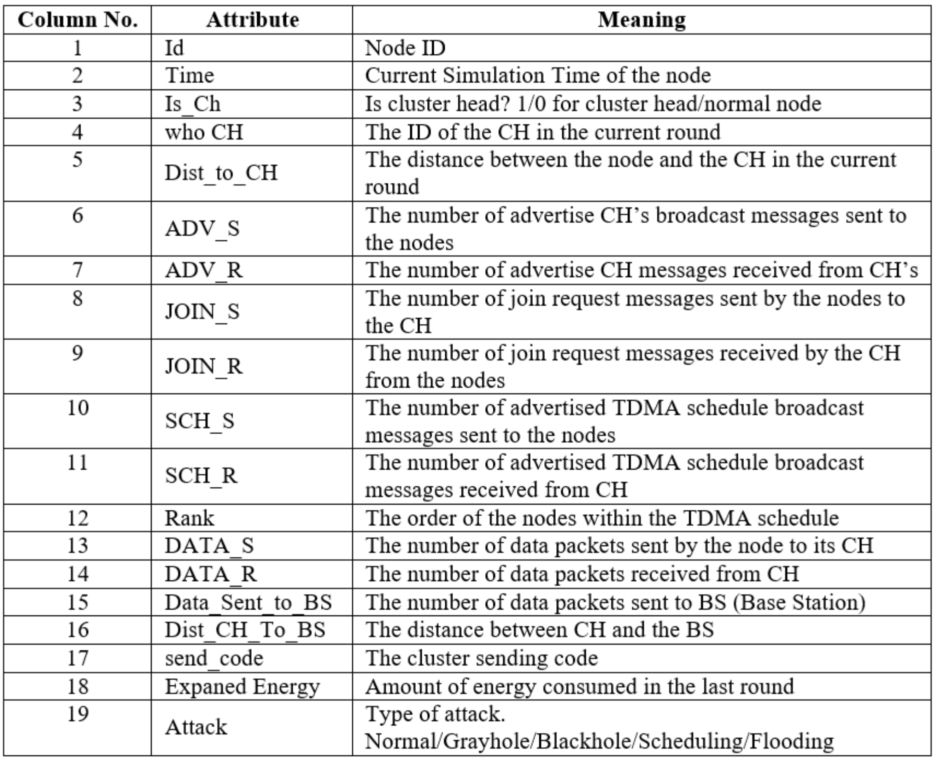
The proposed optimum feature selection and classification approach using machine learning (SF-BML) uses WSN-DS, the publicly available dataset [17]. It was developed for WSN and used the LEACH protocol in the NS-2 environment. Table 1 shows the complete description of the types of DoS attacks (GH attacks, BH attacks, FD attacks, and SH (TDMA)). The dataset contains 22 attributes and a label. However, Almomani et al. [18] ignored some of the attributes and were not used.

Table 1 – Particulars of attacks from the WSN-DS dataset.

Attacks	Number of Records	Description of DoS attack
Blackhole (BH)	14596	Publish themselves as cluster head during the initial time
Grayhole (GH)	10049	Publish themselves as cluster heads for other nodes at the initial time
Flooding (FD)	6638	Affects the mechanism of Routing protocol in a different way
Scheduling (SH)	3312	Affects during the setup phase of the Routing
Normal (N)	340066	No attack
Total	**374661**	

The current attributes and their meaning are listed in Table 2 while the omitted attributes are not listed.

Table 2 – Fields and their meaning for the latest WSN-DS dataset



Column No.	Attribute	Meaning
1	Id	Node ID
2	Time	Current Simulation Time of the node
3	Is_Ch	Is cluster head? 1/0 for cluster head/normal node
4	who CH	The ID of the CH in the current round
5	Dist_to_CH	The distance between the node and the CH in the current round
6	ADV_S	The number of advertise CH's broadcast messages sent to the nodes
7	ADV_R	The number of advertise CH messages received from CH's
8	JOIN_S	The number of join request messages sent by the nodes to the CH
9	JOIN_R	The number of join request messages received by the CH from the nodes
10	SCH_S	The number of advertised TDMA schedule broadcast messages sent to the nodes
11	SCH_R	The number of advertised TDMA schedule broadcast messages received from CH
12	Rank	The order of the nodes within the TDMA schedule
13	DATA_S	The number of data packets sent by the node to its CH
14	DATA_R	The number of data packets received from CH
15	Data_Sent_to_BS	The number of data packets sent to BS (Base Station)
16	Dist_CH_To_BS	The distance between CH and the BS
17	send_code	The cluster sending code
18	Expaned Energy	Amount of energy consumed in the last round
19	Attack	Type of attack. Normal/Grayhole/Blackhole/Scheduling/Flooding

IIIA. Feature Selection Strategy

We extended the work carried out in [10] to find quality features from the remaining 19 features shown in Table 2. Therefore, all four feature selection methods (IG, CST, CFS, and SBS) were applied to the

18 available features and the best data representative features respective to each of the methods were found. Table 3 below shows the methods and respective selected attribute numbers. The table also provides the sequence of the features for better performance. Similar results were obtained by Shuai Jiang et al. [10] who concluded that increasing just one feature from 9 [19] to 10 stabilizes the classification accuracy. The experimentation conducted in [19] analyzed that there exists some redundancy in the dataset.

Table 3 – Ten selected features using feature selection algorithms.

Feature Selection Method	**Optimum features (Columns)**
IG	3, 6, 11, 7, 8, 15, 16, 18, 13, 2
CST	4, 1, 2, 14, 13, 9, 16, 10, 5, 6
CFS	3, 8, 11, 7, 6, 9, 13, 17, 5, 2
SBS	18, 6, 10, 15, 14, 4, 7, 2, 9, 16

Analyzing Table 3, we found that attributes [2, 6, 7, 9, 13, and 16] are significant (SF) as they exist in all four methods. Features in columns [3, 4, 5, 8, 10, 11, 14, 15, and 18] are semi-significant (SSF) as they are part of three methods. Features in columns 1 and 17 have a low impact as they correspond to not more than two methods. Lastly, no selection strategy shows the involvement of column 12.

Priory, we eliminated column 1 and column 17 since they were of no significance. The first column represented the node ID whereas the 17th column contained 16 unique values for all observations (374661) representing the cluster code. Column 12 showed no participation in any of the selection strategies and was neglected. The last column (attribute 19) represented the type of attack (GH, BH, FD, SH, and Normal) and was isolated for categorical labels.

Therefore, the final feature selection process included the SF and combination from SSF while neglecting other features from 1 and 17. The combination involves finding the optimum columns concerning the best classification accuracy for normal and all four attacks. We selected a minimum of two columns and a maximum of eight columns from the SSF and concatenated with the SF to obtain the feature set. Therefore, experiments were conducted for seven configurations to find the effect of increasing features on the classification accuracy. Table 4 shows the seven configurations used for experimentation using the machine learning approach.

Table 4 – Seven configurations to find the effect of increasing attributes.

Configuration	**SF Attributes**	**Columns from SSF Attributes [3, 4, 5, 8, 10, 11, 14, 15, and 18]**
1	[2, 6, 7, 9, 13, and 16]	Two from SSF
2		Three from SSF
3		Four from SSF
4		Five from SSF
5		Six from SSF
6		Seven from SSF
7		Eight from SSF

The proposed SF-BML framework is worked out in Figure 1. The samples in the dataset are loaded and unrelated columns or attributes are eliminated concerning suggestions in [10] by Shuai Jiang et al. Further, all four feature selection methods are applied to find the feature order and then the minimum optimum features. The feature order is not part of our work and has been omitted from Table 3.

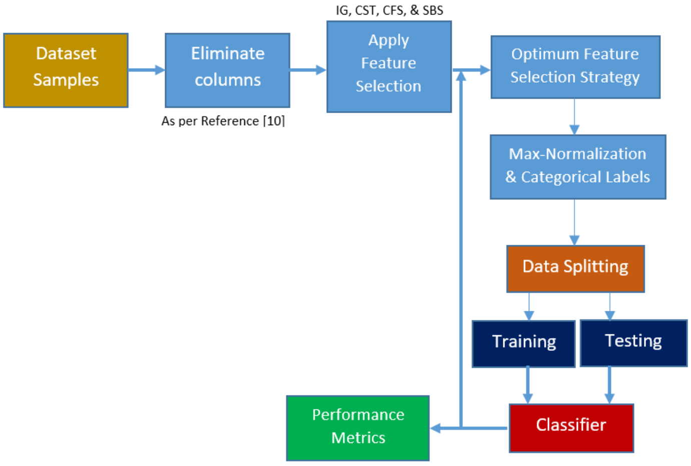


Figure 1 – The SF-BLM Framework for Intrusion Detection.

The Optimum feature selection strategy concatenates the Sf and combinations from the SSF to form a feature set which is then used to classify the test samples. The best combination from SSF is found from the maximum classification accuracy. The algorithm is iterated for all seven configurations and the performance metrics are evaluated. Once the Sf and SSF combination is concatenated, the corresponding columns of the dataset are normalized using the Max-Normalization algorithm.

The data is partitioned in training and test sets with a 70:30 ratio respectively. The training samples are used to train an SVM using the radial basis function and SMO optimizer. The trained SVM is used to predict the test sample classes which are then compared to compute the confusion matrix and the classification accuracy for each class.

IV. Results and Discussion

We carried out an experimental analysis on the WSN-DS dataset samples using Machine Learning. The experiments were carried out on a Windows 11 PC with Intel Core i5 Processor @ 2.80 GHz, 16 GB memory, and 512 GB SSD on the MATLAB 2019b platform. Table 5 shows the SF and SSF along with the classification accuracies of training and test samples.

Table 5 – Training and test accuracy concerning seven configurations of SF and SSF.

Configuration	SF	SSF	Accuracy-Training	Accuracy-Test
1	[2, 6, 7, 9, 13, and 16]	[5, 8]	98.05	98.01
2		[3, 4, 15]	98.38	98.36
3		[3, 4, 5, 18]	98.91	98.72
4		[4, 5, 11, 14, 18]	98.93	98.78
5		[4, 5, 8, 10, 11, 15]	99.14	98.99

6		[4, 5, 8, 10, 11, 15, 18]	99.14	99.00
7		[3, 4, 8, 10, 11, 14, 15, 18]	99.17	99.00

Table 5 shows that with increasing SSF the training and test accuracies gradually increase up to 13 features while the test accuracy stabilizes afterwards. We have experimented further with increasing the SSF but the test accuracy showed no improvement. A clear picture showing train and test accuracies is shown in Figure 2.

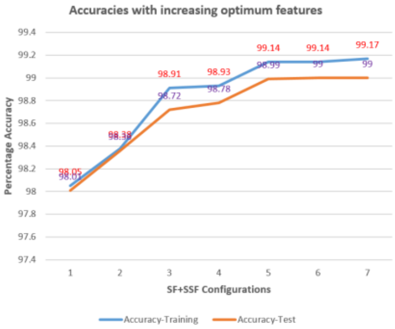


Figure 2 – Percentage accuracies for SF+ Optimum SSF.

The respective confusion matrices are shown in Figures 3 to 9 for each configuration below.

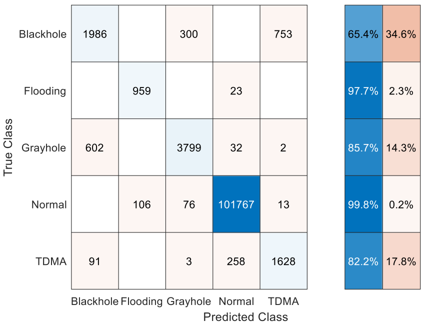


Figure 3 – Confusion matrix for SF=6+SSF=2

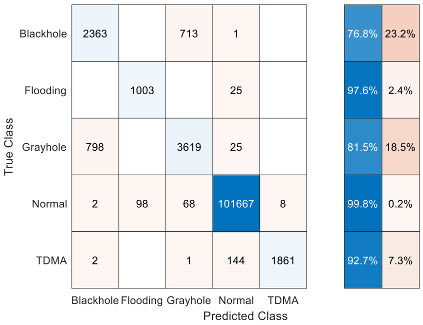


Figure 4 - Confusion matrix for SF=6+SSF=3

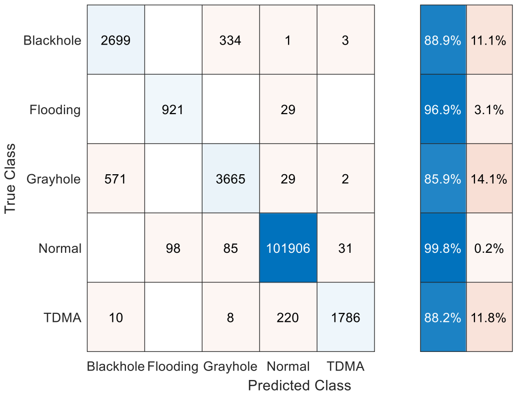


Figure 5 – Confusion matrix for SF=6+SSF=4

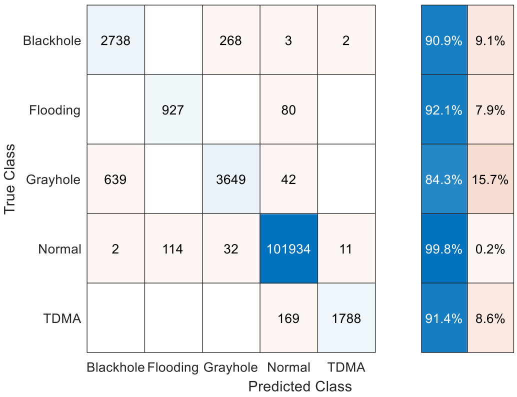
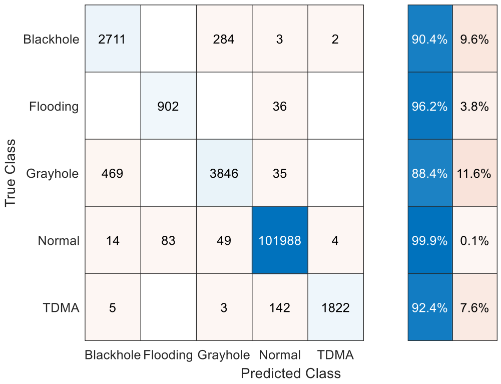


Figure 6 - Confusion matrix for SF=6+SSF=5



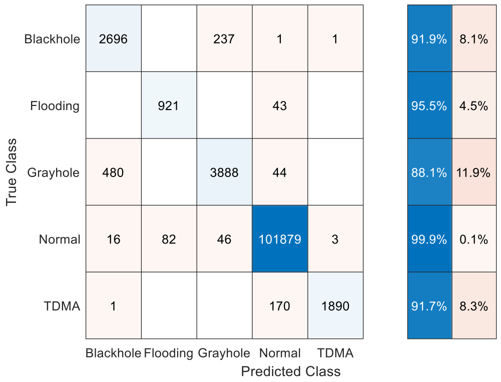


Figure 7 – Confusion matrix for SF=6+SSF=6

Figure 8 - Confusion matrix for SF=6+SSF=7

The detection rate of normal samples in all configurations is above 99% due to an unbalanced dataset. The number of normal samples is the highest (340066). There is a slight improvement seen in the overall detection rate of normal samples from 99.8% to 99.9%. However, there is a conflict between the attacker samples. The attacker samples do not show gradual improvement. Instead, their detection rate depends on other attacker samples. We have used different train and test samples for each configuration. That is the train-test split was randomized in the iterated loop. The overall test accuracy from Figure 2 and Figure 9 is 99% for fourteen features (SF=6+SSf=8).

This shows that some features in the dataset are not useful to distinguish the categories. Therefore, adding such unrelated features not only burdens the classifier but also increases the false detection rate unnecessarily. The essence of the experiments is to show that only a few features truly represent the whole thing. On the other hand, these few relevant features are distorted with redundant and unrelated elements which significantly affects the classifier performance. Using a feature selection strategy, irrelevant features are washed out, which reduces the feature dimension, computational complexity, and processing time and increases the framework generalization capability. It helps to simplify the model. Therefore, the selective feature strategy improves classification accuracy and reduces the overhead burden.

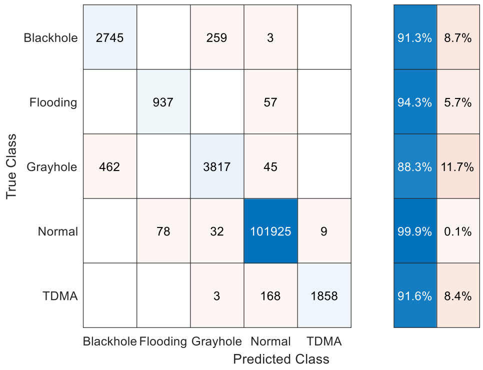


Figure 9 – Confusion matrix for SF=6+SSF=8

We compared the performance of our DoS attack detection framework with the other four competing models from [18][19][20] found in the literature. The proposed threat attack detection framework is competitive with others as shown in Table 6.

Table 6 – Comparison based on metrics for DoS attack detection with other methods

Model	N	GH	BH	SH	FD
ANN [18]	0.998	0.756	0.928	0.922	0.994
DNN [20]	0.98	0.919	0.939	0.992	0.994
J48 [19]	0.999	0.982	0.993	0.927	0.975
SMO [19]	0.994	0.501	0.955	0.862	0.941
SF-BML Scheme	0.999	0.883	0.913	0.916	0.942

V. Conclusion

Feature Selection strategies in combination with machine learning techniques are currently being embedded for malware detection. To improve the generalization ability of the framework and mitigate overfitting, feature selection algorithms are efficient and effective. It gives a better picture of uncorrelated and correlated features. Selective features reduce the burden on the classifier thus improving the response time in detecting the actual sample class. The proposed SF-BML framework is effective in dimension reduction and redundancy elimination thus reducing the high computational cost of the IDS.

Thus, if the significant attributes are priory known using the selective feature strategy, a suitable mechanism can be incorporated to discriminate correlated features and improve the classifier performance. The WSN-DS dataset is small, but for high dimensional data, such strategies can be used to eliminate irrelevant features and reduce the time consumption in the real-world scenario. The dataset samples can be augmented and the weight of all the classes can be made equal. The normal class has the highest number of samples in the dataset and the highest classification rate. This adversely affects the poor classes.

The best alternative to identify intruder interference is to use cryptographic approach for secured transmission. The intruder's characteristic to respond quicker can be used as a weapon against the intruder through authentication and encoded messages. Wherein the intruder receives the request, it will fail to authenticate itself.

References

[1] M. Zhou, Y. Wang, Z. Tian, Y. Lian, Y. Wang, and B. Wang, “Calibrated data simplification for energy-efficient location sensing in the Internet of things,” IEEE Int. Things, vol. 6, no. 4, pp. 6125–6133, 2018.

[2] C. Wang, H. Lin, R. Zhang, and H. Jiang, “Send: A situation-aware emergency navigation algorithm with sensor networks,” IEEE Trans. Mobile Comput., vol. 16, no. 4, pp. 1149–1162, 2016.

[3] J. Su, A. Liu, and Y. Chen, “A partitioning approach to RFID identification,” IEEE/ACM Trans. Netw., pp. 1-14, 2020.

[4] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, “Denial of service defense for resource availability in wireless sensor networks,” IEEE Access, vol. 6, pp. 6975–7004, 2018.

[5] T. Park, D. Cho, H. Kim et al., “An effective classification for dos attacks in wireless sensor networks,” in 10th Int. Conf. Ubiq. Fut. Net. (ICUFN), 2018, pp. 689–692.

[6] R. Kaur, G. Kumar, and K. Kumar, “A comparative study of feature selection techniques for intrusion detection,” in 2nd Int. Conf. Comp. Sust. Glob. Dev. (INDIACom), 2015, pp. 2120–2124.

[7] P. Li, W. Zhao, Q. Liu, X. Liu, and L. Yu, “Poisoning machine learning based wireless idss via stealing learning model,” in Int. Conf. Wire. Algort., System., and App., 2018, pp. 261–273.

[8] A. Mitrokotsa and A. Karygiannis, “Intrusion detection techniques in sensor networks,” Wire. Sens. Net. Secu., pp. 251–272, 2008.

[9] X. Liu, C. Sun, M. Zhou, C. Wu, B. Peng, and P. Li, “Reinforcement learning-based multi-slot double-threshold spectrum sensing with Bayesian fusion for industrial big spectrum data,” IEEE Trans. Ind. Inform., 2020.

[10] S. Jiang, J. Zhao, and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in IEEE Access, vol. 8, pp. 169548-169558, 2020.

[11] Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022.

[12] Mohamed H. Behiry and Mohammed Aly, “Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods”, Journal of Big Data, 2024, 11:16.

[13] Syed Muhammad Salman Bukhari, Muhammad Hamza Zafar, Mohamad Abou Houran, Syed Kumayl Raza Moosavi, Majad Mansoor, Muhammad Muaaz, and Filippo Sanfilippo, “Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability,” Adhoc Networks, 155, 2024, 103407.

[14] Khan, S.; Khan, M.A.; Alnazzawi, N. Artificial Neural Network Based Mechanism to Detect Security Threats in Wireless Sensor Networks. Sensors 2024, 24, 1641.

[15] Geo Francis E. and Sheeja S., “An optimized intrusion detection model for wireless sensor networks based on MLP-CatBoost algorithm,” Multimedia Tools Applications, 2024. https://doi.org/10.1007/s11042-023-18034-6.

[16] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” In Adva. Commu. Multi. Secu., 2002, pp. 107–121.

[17] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

[18] Imam Almomani, Bassam Al-Kasasbeh, and Mousa AL-Akhras, “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks,” Journal of Sensors, Volume 2016, Article ID 4731953.

[19] 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.

[20] R. Vinayakumar, M. Alazab, K. 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.