A Multi-layer Machine Learning-based Intrusion Detection System for Wireless Sensor Networks

Nada M. Alruhaily[1], Dina M. Ibrahim[2]
Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia[1,2]
Department of Computers and Control Engineering, Faculty of Engineering, Tanta University, Egypt[1]

***Abstract*—With the increase relay on the internet, and the shift of most business to provide remote services, the burdens of protecting the network and detecting any attack quickly become more significant, as the attack surface and Cyberattack increases in return. Most current Wireless Sensor Networks (WSNs) intrusion detection models that use machine learning methods to identify non-previously seen attacks utilize one layer of detection, meaning that a costly algorithm should be run before detecting any suspicious activity. In this paper, we propose a multi-layer intrusion detection framework for WSN; in which we adopt a defense-in-depth security strategy, where two layers of detection are deployed. The first layer is located on the network edge sensors are distributed; it uses a Naive Bayes classifier for real-time decision making of the inspected packets. The second layer is located on the cloud and utilizes a Random Forest multi-class classifier for an in-depth analysis of the inspected packets. The results demonstrate that our proposed multi-layer detection model gives a relatively high performance of the TPR, TNR, FPR, and FNR, additionally achieving a high Precision rate with values of, 100%, 90.4%, 99.5%, 97%, 99.9% for the Normal, Flooding, Scheduling, Grayhole, and Blackhole attacks, respectively.**

Keywords*—*Intrusion detection; wireless sensor networks; machine learning; defence in depth strategy

I. Introduction

With the emergence of wireless devices, especially in the Wireless Sensor Networks (WSN), and due to the rapid spread of the Internet of Things technology, this has led to a dramatic increase of the attack surface resulting in the network being exposed to various types of attacks [1]. For this reason, intrusion detection methods with highly stability, efficiency, and adaptability are in urgent need to protect such networks. At present, the traditional wireless network intrusion detection methods suffer from some limitations like: low detection accuracy, low precision rate, and high false positive rate [2]. Therefore, there is a growing need to propose a more accurate and efficient intrusion detection framework to enhance the intrusion detection qualification in the wireless sensor network environment.

Nowadays, the application of artificial intelligence methods to intrusion detection systems has become one of the most important research fields carried out by researchers, especially using machine learning algorithms. Additionally, some researches are applying other methods including neural networks [3], [4], [5], genetic algorithms [6], [7], and deep learning techniques [8], [9], [10].

Most of the current frameworks proposed for detecting intrusions in Wireless sensor Networks deal with the network as a whole; thus, they tend to propose one layer of detection, while WSNs consist of a considerable number of sensors distributed in a large area, as the works done by [1], [2], [3]. Therefore, our target in this paper is to divide the task of detecting the network intrusions between two detection layers. Where in the first layer, a simple classifier that has a very low computational cost (i.e. Naive bayes) is used to filter the malicious traffic and pass it to the second layer in which more extensive processing is carried out by utilizing a multi-class Random Forest classifier [11]. In the last few years, many approaches have been proposed to design intrusion detection systems for wireless sensor networks. authors in [12] introduced an evolutionary mechanism to extract intrusion detection rules. In order to extract diverse rules and control the number of rule sets, rules are checked and extracted according to the distance between rules in the same type of rule set and rules in different types of rule sets.

Likewise, Sun et al. [13] proposed a WSN-NSA intrusion detection model based on the improved V-detector algorithm for wireless sensor networks (WSN). The V-detector algorithm is modified by modifying detector generation rules and optimizing detectors, and principal component analysis is used to reduce detection features. Similarly, Tajbakhsh et al. [14] proposed an intrusion detection model based on fuzzy association rules, which uses fuzzy association rules to construct classifiers, and uses some matching metrics to evaluate the compatibility of any new samples with different rule sets.

Singh et al. [15] proposed an advanced hybrid intrusion detection system (AHIDS) that automatically detects wireless sensor network attacks. Moreover, authors in [16] proposed a method of using the synthetic minority oversampling technique (SMOTE) to balance the dataset and then uses the random forest algorithm to train the classifier for intrusion detection. The simulations are conducted on a benchmark intrusion dataset, and the accuracy of the random forest algorithm has reached 92.39%, which is higher than other comparison algorithms.

The rest of this paper is organized as follows. Section 2 illustrates reviews on related works with some background. In Section 3, our proposed Multi-Layer detection model is demonstrated. Then, Section 4 presents the implementation and the experimental results obtained from our proposed model. the results' analysis and discussions were clarified in Section 5. Finally, conclusions and future work are presented in Section 6.

II. Related Works and Background

WSN faces threats and security issues during the transmission process of data packets between its elements. This is mainly due to the vulnerable nature of WSNs, as these types of network has a considerable number of sensor nodes which are prone to being attacked and receive severe kinds of threats. From the previous studies, we found that such issues have been tackled by abnormal detection methods [17], [18], [19] and misuse detection methods [20], [21]. Authors in [22] proposed an anomaly detection framework in heterogeneous WSNs using real-data. They combined two different approaches: the first approach is the short-term approach, which locally analyzed the data that sense the individual nodes; the second approach is the long-term approach that compares data coming from several heterogeneous sensors over the network. The proposed framework demonstrated a combination of short-long term approaches which can reduce the drawbacks of using each of them separately and gives better performance.

According to [1], the authors presented an intrusion detection method for wireless networks based on improved Conventional Neural Network (ICNN) by first pre-processing the network traffic data, and then used the ICNN to model that data. Their results give an improved accuracy and a higher true positive rate of intrusion detection; it also gives a lower false positive rates compared with the other models. In the work presented by [23], an approach for jamming detection in WSN is proposed based on cooperation with the feedback received from the other connected neighbor's nodes. The model used two techniques, a connected mechanism and an extended mechanism. the results display that this model is more effective when applied on a hierarchical protocol like the Multi-Parent hierarchical.

Another intrusion detection model based on deep learning was proposed by [2]. They built a Deep Belief Network (DBN) combined with multi-restricted Boltzmann machine (RBM), in addition to using the support vector machine (SVM) in training the model. Their experimental results showed that the proposed detection model improved the detection accuracy. An intelligent WSN intrusion detection approach was introduced by [24], which shows that it could decrease the attacks efficiently. They proposed an Artificial Neural Network classifier with Multilayer Perceptron (ANN-MLP) by using holdout and 10-Fold cross-validation methods. In addition to building their own dataset that specialized for the WSN attacks. Their results concluded that with one hidden layer they got the most high accuracy values; however, their approach was mainly based on one detection layer that applies a very computationally expensive learning method.

III. The Proposed Multi-Layer Detection Model

In this paper, we propose a framework for intrusion detection in WSN, that is shield with a defence in depth strategy; leading to an increased security of the working system as a whole. Fig. 1 shows an overview of the system, where the two protection layers represented as the Edge-based Method, and the Cloud-based Method; both layers deploy a machine learning algorithms to facilitate the process of identifying non-previously seen network attacks. This is an extension work of our recent research paper [25]. The following subsections described the deployed methods in details:

A. First Detection Layer: Naive bayes-based Method

In order to avoid complexity and overwhelming the first detection layer, we chose to implement a binary classifier where the traffic is classified to either, normal or malicious traffic only [26], [27]. We have used Naive bayes algorithm as a base of the classifier, due to its simplicity and computational efficiency, that makes it a promising choice for real-time decision making of the inspected packets.

Naive Bayes classifier is based on the well-known Bayesian theorem; and it is particularly suited to high-dimensional datasets [28]. Despite its relative simplicity, in many complex real-world conditions this classifier works very well and it might outperform more sophisticated classification methods. Naive Bayes model allows each attribute to contribute equally and independently to the final decision, in which it results in being more computationally efficient compared to other classifiers.

B. Second Detection Layer: Random Forest-based Method

As discussed in the previous subsection, the first layer will classify the monitored traffic into either: normal or malicious traffic, with no further details in terms of the attack type; this is mainly due to the fact that on that layer we are mainly seeking for simplicity and time efficiency of the decision making process. However, as the second detection layer is located on the cloud and mainly handle the suspicious traffic, there will be less complications in terms of the provided resources, meaning that more complex algorithms and more thorough analysis could be carried out. Therefore, the Random Forest (RF) with multi-class classifier has been used to confirm the traffic with the malicious intent; the classifier has been used also to identify the type of the launched attack, thus, providing guidelines for choosing the appropriate defence mechanism.

Random Forest classifier composed of a set of Decision trees, where every tree provides an insight about each sample's class. At the end of the classification, the class with the most votes is selected as the likely class. The aggregation approach follows in this classifier is based on Breiman 's concept of bagging with randomly selected features on each generated bag, thus creating a set of variation decision trees [29]. Decision trees, which are constructed during the classification task on Random forest classifier, are supervised learning algorithms that are used to address both classification and regression tasks. They originates rules from training several samples represented by a set of attributes; where they derives specific rules that can be easily interpreted as they are visualized as a tree-like graph.

IV. Implementation and Experimental Results

Python 3.7 has been used to implement the proposed framework, in addition to using the latest version of Sciket-learn, which is an open source machine learning library [24]. For the testing purposes, we have used WSN-DS, which is a dataset generated mainly for intrusion detection systems in wireless sensor networks.

A number of metrics have been utilized to assist and evaluate the performance of the implemented system, those metrics could be described briefly as follows:

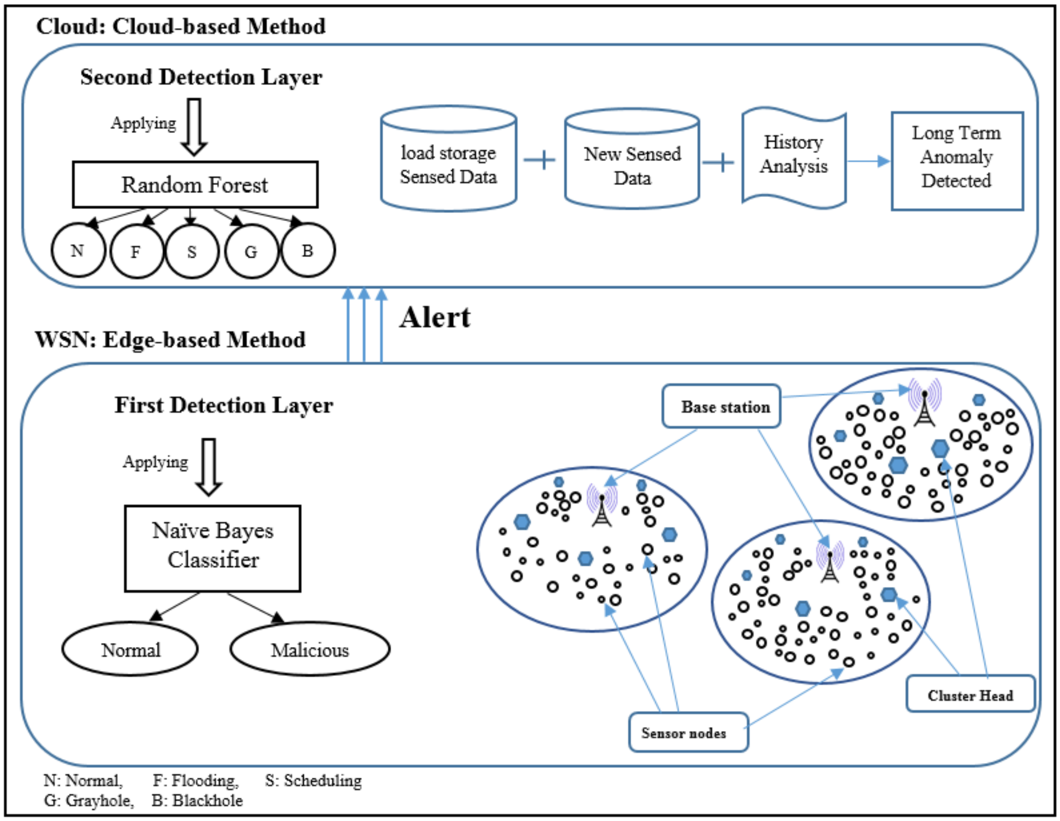


Fig. 1. The Proposed Multi-Layer Detection Model, with Two Protection Layers.

- True positive (TP): the number of network connections correctly identified as attacks.
- True negative (TN): the number of network connections correctly identified as normal connections.
- False positive (FP): the number of network connections incorrectly identified as attacks.
- False negative (FN): the number of network connections incorrectly identified as normal connections.

Those terms have been used to derive different evaluation metrics, i.e. the True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), and False Negative Rate (FNR); in addition, they have been used also to calculate the $Precision$ (P), as follows:

$$TPR = TP/(TP + FN) \tag{1}$$

$$TNR = TN/(TN + FP) \tag{2}$$

$$FPR = FP/(FP + TN) \tag{3}$$

$$FNR = FN/(FN + TP) \tag{4}$$

$$Precision = TP/(TP + FP) \tag{5}$$

To establish the feasibility of the proposed approach, and to determine its accuracy we have used a dataset generated mainly for evaluating Intrusion Detection Systems in Wireless Sensor Networks (referred to as he WSN-DS) [24]. The dataset consists of a number of 19 features monitored during normal and abnormal scenarios, where in the latter various number and types of Denial of Service (DOS) attacks were simulated (i.e. Blackhole, Grayhole, Flooding, and Scheduling attacks (TDMA)). Table I gives an overall view of the WSN-DS dataset features including their description.

V. Results Analysis and Discussions

A. *First-Layer Results and Discussions*

As the main purpose of the first layer is identifying the abnormal traffic with the least resources possible, we used Mutual information (MI) algorithm to quantify the importance of each feature (as seen in Fig. 2), therefore, selecting the most relevant ones; MI is widely known as a good indicator to determine the relevance between variables, and it is usually used in the area of AI as a feature selection algorithm [30], [31]. Fig. 2 emphasises the computed MI score for each feature, where the higher the score, the more important the feature.

Based on some preliminary tests, we have found that choosing the best three features, as ranked by MI, will give the highest classification performance. Fig. 3 (a & b) shows the classification accuracy when including the best three features, and all of the 19 features provided by WSN-DS, respectively. Thus, the first three features, ADV_S, Is_CH, and Join_S, have been used as an input to the Naive bayes classifier in order to filter the malicious traffic and pass it to the second protection layer for further examination. It can be seen from Fig. 3 (a) that a 99% detection accuracy of the abnormal activities has

TABLE I. THE WSN-DS DATASET FEATURES DESCRIPTION

No.	Feature	Description
1	id	unique ID to distinguish the sensor node
2	Time	current node simulation time
3	Is_CH	distinguish whether the node is Cluster Head
4	who CH	ID of the CH in the current round
5	Dist_To_CH	distance between the node and its CH
6	ADV_S	number of advertised CH sent messages
7	ADV_R	number of advertised CH received messages
8	JOIN_S	number of joined request CH sent
9	JOIN_R	number of joined request CH received
10	SCH_S	number of scheduled CH sent messages
11	SCH_R	number of scheduled CH received messages
12	Rank	order of this node in the schedule
13	DATA_S	number of data packets sent to CH
14	DATA_R	number of data packets received from CH
15	Data_Sent_To_BS	number of data packets sent to BaseStation
16	dist_CH_To_BS	distance between CH and BS
17	send_code	the cluster sending code
18	Consumed Energy	the amount of energy consumed in the round
19	Attack type	the type of the attack

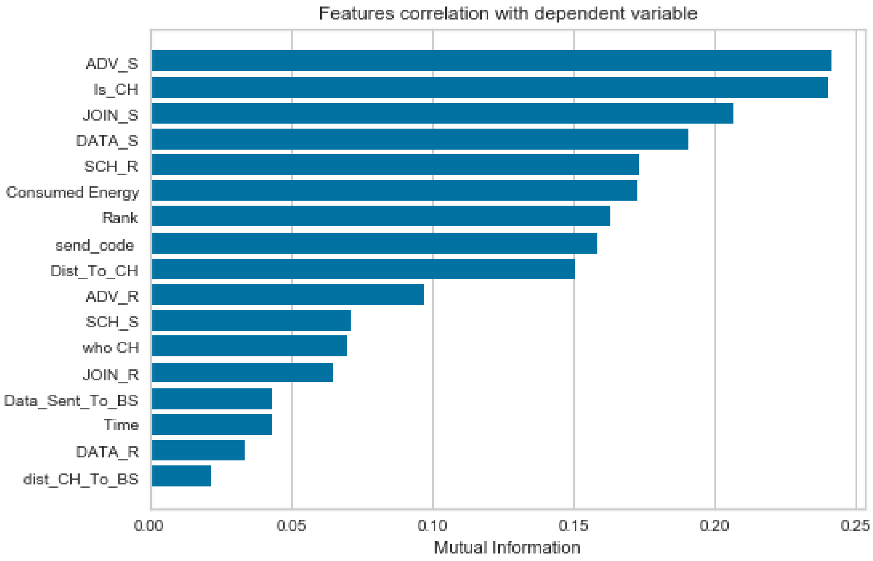


Fig. 2. MI Score for Each Monitored Feature.

be achieved with the use of 3 features only, while maintaining a low usage of computational resources; the Area Under the Curve (AUC), which is a commonly used stat to show the overall performance of a classification method, is also shown on Fig. 4.

B. Second-Layer Results and Discussions

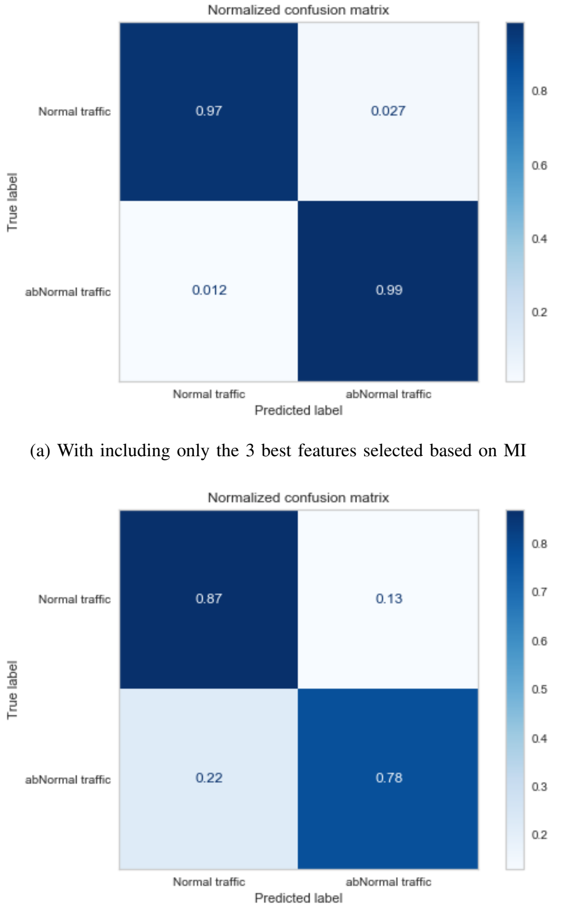
On the second detection layer, more examination of the malicious traffic will be carried out; thus, a multi-class classification using RF classifier is performed to identify the specific type of the attack, thereby choosing the appropriate defence mechanism. Classification results obtained by RF classifier is shown on Fig. 5; it could be seen that a relatively high performance was achieved as illustrated in Table II. Therefore, such a high detection performance allows more concrete countermeasures to be adopted automatically by the system.

Generally, the aim of an IDS is to obtain a high precision [32], as this measure shows how many cases, predicted as an intrusive, are actually correct. Based on that, when we compare the performance obtained with the RF classifier in this paper with a previous work that used the same dataset, e.g. [24], it could be clearly seen that a higher precision has been achieved, where the precision of the attacks detection were 73%, 90%, 99.5%, 91.1%, and 99% in Blackhole, Flooding, Scheduling, and Grayhole attacks, in addition to the normal case (without attacks), respectively. A comparison of the performance metrics between the previous work done by [24] and our proposed model is illustrated in Fig. 6 & 7, which show an improvement in the performance values of TPR, TNR, FPR, FNR and Precision, compared to the previous work.

However, Fig. 6 shows one case where our proposed work has achieved a slightly lower value; this is the case of the TNR

TABLE II. RF Performance of 10-fold Cross-Validation Compared with the Previous Work

Attack Type	The previous work results					The proposed results					P % Change
	TPR	FPR	FNR	TNR	P	TPR	FPR	FNR	TNR	P	
Normal	0.998	0.018	0.002	0.982	0.998	0.998	0.023	0.002	0.977	1.0	+0.2%
Flooding	0.994	0.001	0.006	0.999	0.904	0.991	0.001	0.009	0.999	0.904	0
Scheduling	0.922	0	0.078	1.0	0.995	0.927	0.0	0.073	1.0	0.995	0
Grayhole	0.756	0.003	0.244	0.997	0.911	0.955	0.001	0.045	0.999	0.970	+6.5%
Blackhole	0.928	0.009	0.072	0.991	0.730	0.991	0.001	0.009	0.999	0.999	+37%



(a) With including only the 3 best features selected based on MI

(b) With including all the features

Fig. 3. Classifying Network Attacks using Naive bayes Classifier.

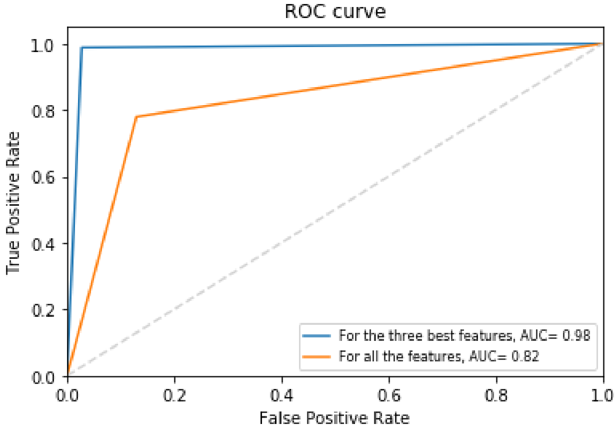


Fig. 4. ROC Curve Showed Comparison between the Classification Results for All the Features and the Three best Only.

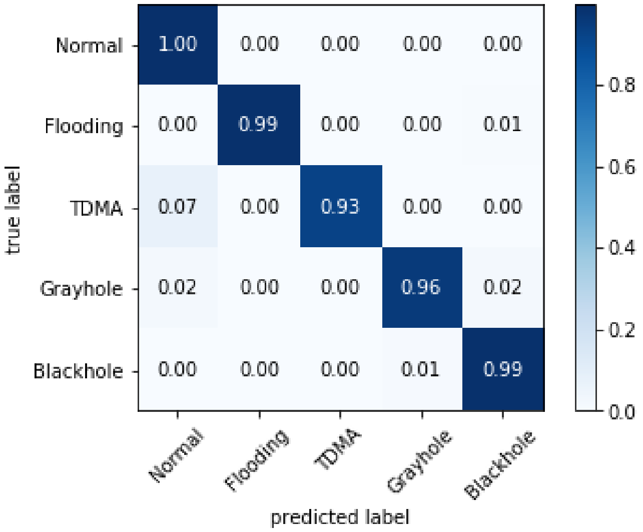
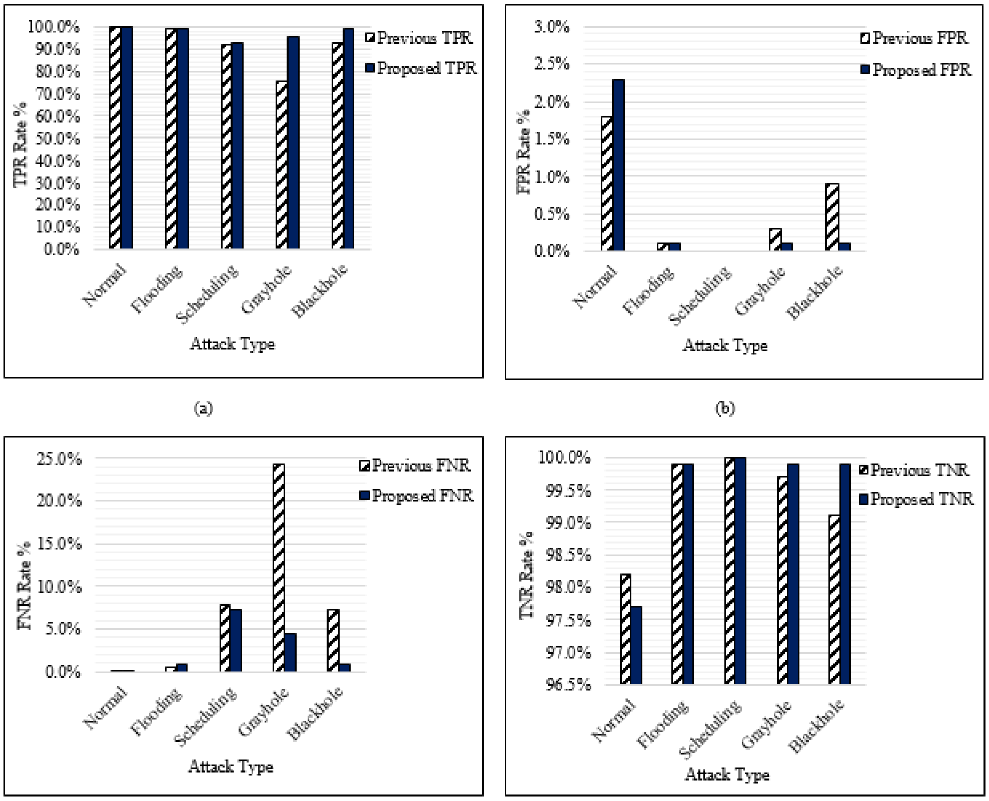


Fig. 5. Classifying Network Attacks using Random Forest Classifier (Performance Rounded to Two Decimal Points).

of the Normal packets. Consequently, the FPR derived from the Normal packets becomes higher. In such a case, this means that more packets will be inspected further, and flagged as malicious, although they do not carry any harmful intentions. This case could be costly (in terms of the time spent during the investigation); however, it would not be as expensive as if a malicious packet has been missed to be identified, and instead recognised as a Normal one.

Moreover, our work provides other advantages inherited by the use of RF classifier (rather than artificial neural network on [24]), such as the fact that it is considered less computationally expensive compared with ANN classifier. The usage of RF classifier also increases the performance of the security of the system as a whole in that it provides the interpretability and transparency of the results, as shown in Fig. 8 where the result of a tree generated by RF classifier could be easily interpreted; the resulting rules could also be investigated further using tools such as [33]. Such properties are very important in the analysis of the attacks, optimisation and handling of the system errors [34]. Most importantly, the proposed work employs a layered defence mechanism that enhances the security by providing



(a)

(b)

(c)

(d)

Fig. 6. Performance Metrics Results for the Previous the Proposed Multi-layer Model; (a) TPR, (b) FPR, (c) FNR, and (d) TNR.

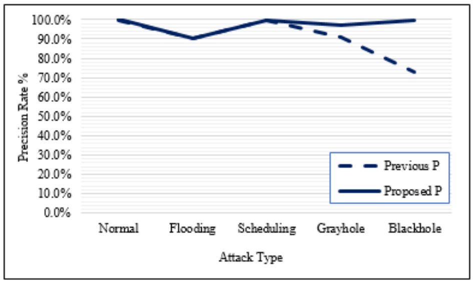


Fig. 7. Precision Improvement for the Proposed Multi-layer Model.

an extra protection layer to defend the whole system in cases where the first layer has been bypassed or fail as a result to the ever-changing attack techniques, and the present increasing threat landscape.

VI. Conclusions

Intrusion detection in wireless sensor networks is a very challenging task. The majority of the current WSN intrusion detection models were using machine learning methods, but they apply only one method for the whole network. In this paper, we propose a multi-layer framework for intrusion detection system in WSN, leading to increase the network security. Our proposed model consists of two consequent protection layers; the first layer is located on the edge of the network where the sensors are located. It used the Naive bayes classifier where the traffic is classified into normal or malicious traffic which achieving simplicity and time efficiency of the decision-making process. While the second layer is located on the cloud, and mainly handle the suspicious traffic by using a multi-class Random Forest classifier.

The implementation results demonstrate that our proposed multi-layer protection model improved the values of TPR, TNR, FPR, and FNR in addition to achieving a high Precision rate with values 100%, 90.4%, 99.5%, 97%, 99.9% for the Normal, Flooding, Scheduling, Grayhole, and Blackhole attacks, respectively. While the previous work has the values 99.8%, 90.4%, 99.5%, 91.1%, 73% for the Normal, Flooding, Scheduling, Grayhole, and Blackhole attacks, respectively. Nevertheless, the results in Fig. 6 show only one case where our proposed work has achieved a slightly lower value; this is the case of the TNR of the Normal packets. Consequently, the FPR derived from the Normal packets becomes higher. In such an instance, this means that more packets will be inspected further, and flagged as malicious, although they do not carry any harmful intentions. This case could be costly (in terms of the investigation time); however, it would not be as expensive as if a malicious packet has been missed to be identified, and instead recognised as a Normal one.

As future work, we plan to improve the performance of our multi-layer detection model in WSN by using one of the deep learning techniques in the second layer, where the higher number of attacks types appear.

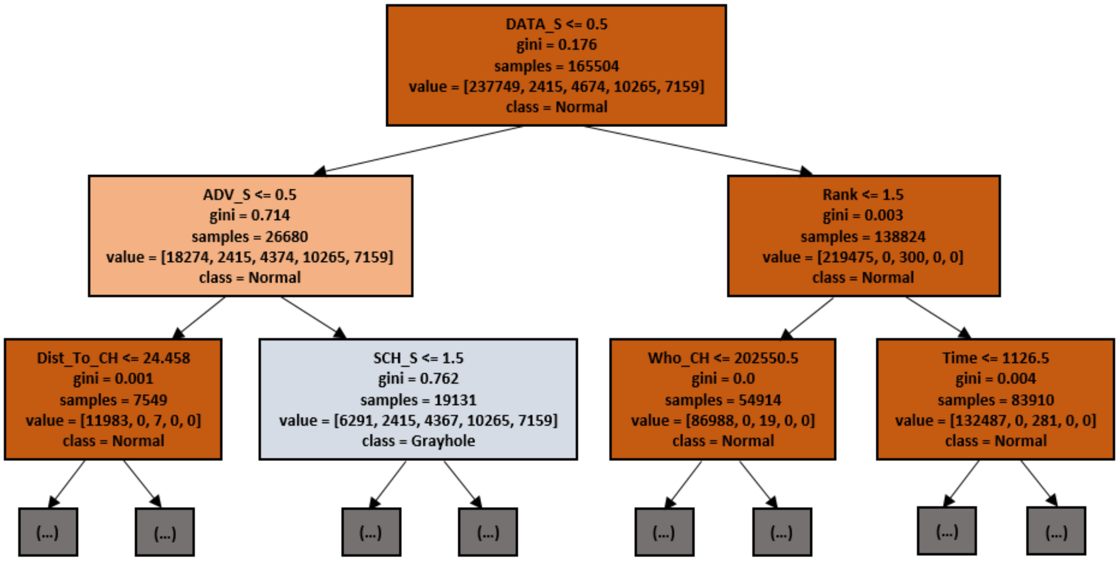


Fig. 8. A sample of the Tress Generated by the Random Forest Classifier, where Interpretable and Transparent Rules are Obtained During the Classification Task.

References

[1] H. Yang and F. Wang, ”Wireless network intrusion detection based on improved convolutional neural network,” IEEE Access, vol. 7, pp. 64366–64374, 2019.

[2] H. Yang, G. Qin, and L. Ye, ”Combined Wireless Network Intrusion Detection Model Based on Deep Learning,” IEEE Access, vol. 7, pp. 82624–82632, 2019.

[3] S.S. Roy, A. Mallik, R. Gulati, M.S. Obaidat, P.V. Krishna, ”A deep learning based artificial neural network approach for intrusion detection,” In International Conference on Mathematics and Computing, Springer, Singapore, pp. 44–53, 2017.

[4] Y. Liu, S. Liu, and X. Zhao, ”Intrusion detection algorithm based on convolutional neural network. Transactions on Engineering and Technology Research, vol. 37, pp. 1271–1275, 2019.

[5] M. Wang, and J. Liu, ”Network intrusion detection based on convolutional neural network,” Net information Security, vol. 3, pp. 990–994, 2019.

[6] M.A. Yong, ”A network intrusion detection schemer based on fuzzy inference and Michigan genetic algorithm,” Electron. Des. Eng., vol. 24, pp. 107–110, 2016.

[7] Q. Yaun, and L.T. Lv, ”Network intrusion detection method based on combination of improved ant colony optimization and genetic algorithm,” J. Chongqing Univ. Posts Telecommun, vol. 29, pp. 85–89, 2019.

[8] H. Chen, G.X. Wan, Z.J. Xiao, ”Intrusion detection method of deep belief network model based on optimization of data processing,” Journal of Computer Applications, vol. 37, pp. 1636–1643, 2017.

[9] C. Yin, Y. Zhu, J. Fei, X. He, ”A deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, vol. 5, pp. 21594–21961, 2017.

[10] N. Shone, T.N. Ngoc, V.D. Phai, and Q. Shi, ”A deep learning approach to network intrusion detection,” IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, pp. 41–50, 2018.

[11] C. Giuseppe, C. Calafiore, and F. Giulia , ”Sparse ℓ_1 and ℓ_2 Center Classifiers,” arXiv preprint arXiv:1911.07320, 2019.

[12] N. Lu, Y. Sun, H. Liu, and S. Li, ”Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks,” J. Sens., vol. 2018, pp. 1-–8, 2018.

[13] Z. Sun, Y. Xu, G. Liang, and Z. Zhou, ”An Intrusion Detection Model for Wireless Sensor Networks with an Improved V-Detector Algorithm,” IEEE Sens. J., vol. 18, pp. 1971-–1984, 2018.

[14] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, ”Intrusion detection using fuzzy association rules,” Appl. Soft. Comput., vol. 9, pp. 462-–469, 2009.

[15] R. Singh, J. Singh, and R. Singh, ”Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks,” Wirel. Commun. Mob. Comput., vol. 2017, pp. 1-–14, 2017.

[16] X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo, X. Sun, and L. Li, ”Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm,” Sensors, vol. 19, no. 1, pp.203–218, 2019.

[17] P. Li, W.H. Zhou, ”Hybrid intrusion detection algorithm based on k-means and decision tree,” Computer Modernization, vol. 37, pp. 12–16, 2019.

[18] Y.M. Qi, L. Ming, F. Yanming, ”Research on SVM network intrusion detection based on PCA,” Information Network Security, vol. 2, pp. 15–18, 2015.

[19] X. Wang, ”Design of temporal sequence association rule based intrusion detection behavior detection system for distributed network,” Modern Electron. Techn., vol. 41, pp. 108–114, 2018.

[20] K. Zheng, Z. Cai, X. Zhang, Z. Wang, and B. Yang, ”Algorithms to speedup pattern matching for network intrusion detection systems,” Computer communications, vol. 62, pp. 47–58, 2015.

[21] S. Kim, Pattern matching acceleration for network intrusion detection systems. In International Workshop on Embedded Computer Systems. Springer, Berlin, Heidelberg, 2005; pp. 289–298, 2005.

[22] F. Cauteruccio, G. Fortino, A. Guerrieri, A. Liotta, D.C. Mocanu, C. Perra, G. Terracina, and M.T. Vega, ”Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance,” Information Fusion, vol. 52, pp. 13–30, 2019.

[23] C.; Del-Valle-Soto, L.J.; Valdivia, and J.C. Rosas-Caro, ”Novel detection methods for securing wireless sensor network performance under intrusion jamming,” In the International Conference on Electronics, Communications and Computers (CONIELECOMP), IEEE, pp. 1–8, 2019.

[24] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, ”WSN-DS: A dataset for intrusion detection systems in wireless sensor networks,” Journal of Sensors; Hindawi, vol. 2016, pp. 1–16, 2016.

[25] D.M.; Ibrahim, and N.M. Alruhaily, ”Anomaly detection in Wireless Sensor Networks: A Proposed Framework,” International Journal of Interactive Mobile Technologies (iJIM), vol. 14, pp. 150–158, 2020.

[26] S.L. Ting, W.H. Ip, Tsang, and H.C. Albert, ”Is Naive Bayes a good classifier for document classification,” International Journal of Software Engineering and Its Applications, vol. 5, pp. 37–46, 2011.

[27] E. Frank, Bouckaert, and R. Remco, ”Naive bayes for text classification with unbalanced classes,” In European Conference on Principles of Data Mining and Knowledge Discovery, Springer, pp. 503–510, 2006.

[28] A. El Abdouli, L. Hassouni, and H. Anoun, ”Sentiment Analysis of Moroccan Tweets using Naive Bayes Algorithm,” International Journal of Computer Science and Information Security (IJCSIS), vol. 15, 2007.

[29] L. Breiman, ”Bagging predictors Machine learning,” Springer, vol. 24, pp. 123–140, 1996.

[30] N. Kwak, and C.H. Choi, ”Feature selection by mutual information based on Parzen window,” IEEE transactions on pattern analysis and machine intelligence, vol. 24, pp. 1667–1671, 2002.

[31] N. Barraza, S. Moro, M. Ferreyra, and A. de la Peña, ”Mutual information and sensitivity analysis for feature selection in customer targeting: A comparative study,” Journal of Information Science, vol. 45, pp. 53–67, 2019.

[32] Ghorbani, A.A.; Lu, W. Tavallaee, M. Network intrusion detection and prevention: concepts and techniques. In Springer Science & Business Media, 2009.

[33] Ribeiro, M.T., Singh, S. and Guestrin, C. Why should i trust you?” Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, pp. 1135–1144, 2016.

[34] V. Rodriguez-Galiano, M. Sanchez-Castillo, M. Chica-Olmo, and M. Chica-Rivas, ”Machine learning predictive models for mineral prospectively: An evaluation of neural networks, random forest, regression trees and support vector machines,” Ore Geology Reviews, Elsevier, vol. 71, pp. 804–818, 2015.