Using Machine Learning for Intrusion Detection System in Wireless Body Area Network

Fheed Alsubaie

College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, KSA
S170002401@seu.edu.sa

Cyber Security Division, Communication and IT department, Royal Saudi Naval Forces (RSNF), Riyadh, 1495-22463, KSA

Mousa Al-Akhras

College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, KSA
m.akhras@seu.edu.sa

King Abdullah II School of 3King Abdullah II School of Information Technology, The University of Jordan, Amman 11942, Jordan
mousa.akhras@ju.edu.jo

Hamdan A. Alzahrani

College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, KSA
h.alzahrani@seu.edu.sa

***Abstract*—This paper introduces a technique that enhances the capabilities of an intrusion detection system (IDS) in a wireless body area network (WBAN). This technique involves adopting two known machine-learning algorithms: artificial neural network (ANN) and the J48 form of decision trees. The enhanced technique reduces the security threats to a WBAN, such as denial-of-service (DoS) attacks. It is essential to manage noise, which might affect the data gathered by the sensors. In this paper, noise in data is measured because it can affect the accuracy of the machine learning algorithms and demonstrate the level of noise at which the machine-learning model can be trusted. The results show that J48 is the best model when there is no noise, with an accuracy reaching 99.66%, as compared to the ANN algorithm. However, with noisy datasets, ANN shows more tolerance to noise.**

Keywords—wireless body area network, intrusion detection systems, machine learning, security threats, denial of service.

I. INTRODUCTION

Wireless body area networks (WBANs) are a key innovation that make continuous wellbeing checks of a patient and analyze numerous hazardous maladies. A WBAN works close to, on, or inside of a human body and supports an assortment of therapeutic and non-restorative applications [1].

Protecting wireless sensor networks (WSNs) from various security threats is important yet challenging because of WSNs' limited resources. WSNs are vulnerable to attacks due to their open and distributed nature. An attacker can compromise a sensor node, eavesdrop on messages, inject fake messages, alter data, and waste network resources. Denial-of-service (DoS) attacks are one of the most dangerous forms of attacks that can threaten WSNs' security.

Because one cannot always completely avoid or prevent security threats, an intrusion-detection system (IDS) is needed to detect known attacks using signature-based methods and unknown attacks using anomaly-based methods, and to alert sensor nodes about such attacks. The implementation of IDSs for WSNs is more difficult than implementing other systems because sensor nodes are usually designed to be tiny and cheap. In addition, the IDS must have high accuracy in detecting an intruder, including unknown attacks, and it also must be lightweight to ensure minimum overhead on the WSN's infrastructure.

In this paper, a machine-learning algorithm is combined with an IDS. The WSN-DS dataset was used, which is a specialized WSN dataset that is constructed with four types of DoS attacks.

The rest of this paper is organized as follows: Section II provides an overview of the literature about machine learning and WBAN networks as well as a review of the related work. Section III discusses the methodology and the materials used to conduct this study. Section IV discusses and analyzes the results. Section V is the conclusion and lists future work that may be conducted to add further aspects to analyze as well as recommendations.

II. LITERATURE REVIEW

A WBAN is an autonomous system of small processing gadgets. These sensor gadgets can be installed inside the human body or under the skin, mounted on the body (wearable), or conveyed by people as convenient gadgets [2]. WBANs play a successful and indispensable role in human lives by cooperating with people's wellbeing details. It is important to ensure that the framework realizes the correct security components and offers safe information transmutation from the source (understanding sensors) to the goal (medicinal services framework) and vice versa.

Different security dangers obstruct the improvement of WBANs because of because of the powerlessness of the remote channel. Security issues that might face WBANs

978-1-7281-7407-5/20/$31.00 ©2020 IEEE
DOI 10.1109/SMART-TECH49988.2020.00036

range from data modification to eavesdropping and DoS attacks. One of the requirements to ensure a WABN's security is to detect and block suspicious activities. Bengag et al. [3] proposed an IDS that allowed them to detect three jamming attacks by utilizing four network parameters: the packet delivery ratio (PDR), bad packet ratio (BPR), energy consumption amount (ECA), and received signal strength indication (RSSI).

Sundararajan and Shanmugam enhanced the ability to detect misbehaved nodes in WBANs by incorporating the negative selection algorithm (NSA) [4]. Anguraj et al. [5] presented a trust-based intrusion-detection and clustering technique. They were able to detect malicious nodes and isolate them from the network.

Artificial intelligence and machine learning have become vital components of computer security. Machine learning algorithms are mainly used in areas such as malware prevention, risk analysis, and anomaly detection, as well as in areas with deficiencies in automation, speed, decision-making accuracy, or fraud. They are used to analyze and classify malware, which is a very important aspect of preventing online security threats. Machine learning is mainly used in to reduce the complexity of the analyses performed by humans; as such, it is a very effective security tool [6].

Ensuring that a system can provide security within the digital world is of great importance, and machine learning increasingly has been used within this particular field. Machine learning is a data-analysis method used to automate analytical model building [7]. The general context of machine learning is to allow systems that can use data to learn and improve without being explicitly programmed to do so. An important factor within machine learning is that the models must have minimal to no human intervention, which is where supervised and unsupervised learning within machine learning come into play [8].

A good machine-learning dataset repository is judged mainly based on the number of datasets it contains [9]. Several studies have indicated that machine learning has been increasingly used within information security. According to Abadi et al. [10], it is a very effective tool that can be used to analyze threats within a given business and to respond to attacks and security incidents. As such, it is utilized to automate menial tasks.

As indicated by Feurer et al. [6], machine learning and artificial intelligence are considered very effective tools. Most researchers highlight the fact that they continue to improve, which is another strength. The more data they experience or receive, the more they will continue to improve in terms of knowledge. Algorithms continue to improve based upon what they learn and the accuracy they obtain. They have become faster at predicting and identifying system threats. Other strengths include handling huge amounts of data and having a wide range of applications in various security fields. Finding the right dataset for a project can be difficult, and several factors must be considered, such as the reliability of the data, their validity, and the legally binding aspects behind behind use of the data [11].

III. METHODOLOGY

In this paper, we used the WSN-DS dataset, which consists of 23 attributes and five possible outputs: four types of attacks—blackhole, grayhole, flooding, and scheduling—in addition to the normal state (no attack). The dataset is fully described in [12].

In a blackhole attack, a malicious node publicizes itself as a legitimate route to the destination node and continuously drops data packets. In a grayhole attack, a malicious node presents itself as a legitimate node and drops the received packets randomly or selectively. In a flooding attack, a large number of messages are sent to the nodes to consume the network's resources and disrupt the whole network. A scheduling attack changes the nodes' behavior to unicast, instead of multicast, to cause packet collision [12, 13].

The WSN-DS [12] implements the LEACH protocol to collect WSN characteristics. The WSN-DS contains 374,661 records, with 340,066 normal records and the remaining records distributed between the four types of attacks.

In addition, we generated different datasets from the original dataset, as described in Table I.

TABLE I. DATASETS USED IN THIS EXPERIMENT

Datasets	**Structure**
WSN-DS	WSN-DS without noise
WSN-DS-5%-noise	WSN-DS + noise (5%)
WSN-DS-10%-noise	WSN-DS + noise (10%)
WSN-DS-20%-noise	WSN-DS + noise (20%)
WSN-DS-30%-noise	WSN-DS + noise (30%)
WSN-DS-40%-noise	WSN-DS + noise (40%)

The Anaconda and Pandas platforms were used to create these datasets, which involved generating Gaussian distributions with different levels of noise to be added to the original datasets. Therefore, the methodology used in this paper was to test the original datasets with both J48 and artificial neural networks (ANNs), with one hidden layer, two hidden layers, and three hidden layers, and analyze them with the help of the Waikato Environment for Knowledge Analysis (WEKA) platform.

WEKA is an open-source data-mining tool based on the Java programming language. It was designed and developed at the University of Waikato, New Zealand. WEKA is mainly used for data-mining tasks and for modeling machine-learning algorithms. WEKA supports several data-mining tasks such as data pre-processing, data clustering, feature selection, and regression [14]. We utilized WEKA to build decision trees (J48) and ANNs [15].

Seven performance metrics were used in this research. True positive (TP) is the number of cases that are indeed positive and that the machine learning technique predicts as being positive. False negative (FN) is the number of cases that are indeed positive but the machine-learning technique predicts as being negative. Hence, the true positive rate (TPR) is illustrated in the following equation:

$$\text{TPR} = \frac{TP}{TP+FN} \quad (1)$$

True negative (TN) is the number of cases that are actually negative and that the machine-learning technique predicts as being negative, and false positive (FP) is the number of cases that are indeed negative but the machine-learning technique predicts as being positive. Hence, the true negative rate (TNR) is illustrated in the following equation:

$$\text{TNR} = \frac{TN}{TN+FP} \quad (2)$$

The false positive rate (FPR) is the ratio of cases that were incorrectly predicted as positive to the total number of negative cases:

$$\text{FPR} = \frac{FP}{TN+FP} \quad (3)$$

$$\text{FNR} = \frac{FN}{FN+TP} \quad (4)$$

Accuracy is the ratio of the correctly predicted cases, either positive or negative, to all cases. Accuracy is illustrated as follows:

$$\text{A} = \frac{TPR+TNR}{TPR+FPR+TNR+FNR} \quad (5)$$

Precision (P) is described as the TPR over the sum of TPR and FPR.

$$\text{P} = \frac{TPR}{TPR+FPR} \quad (6)$$

Root mean square error (RMSE) is the residual or the measure of the difference between the real and predicted values.

IV. Implementation and Results

Two sets of results are introduced in this section, J48 and ANN.

A. J48 Algorithm Results

WEKA showed the following results after we loaded the original dataset with no injected noise and used the J48 model. Table II shows the TPR, the FPR, and the precision for the five output classes. The true accuracy and overall accuracy with this model were 99.664%. The time taken for the machine learning to build a model for J48 was 22 seconds

In the experiments, 66% of the data were used to train the selected model, and the remaining instances were used for testing the model. J48 was very sensitive to noise, as its accuracy fell to 98.37%, 95.565, 93.56%, and 90.134% at 5%, 10%, 20%, 30%, and 40% noise levels, respectively, as shown in Figure 1.

Tables III and IV show the confusion matrix for J48 when it was tested with 5% and 40% noise levels, respectively. Notably, the true positive instances for the normal class dropped from 334,666 to 293,456, and the number of false positives for the normal class increased from 530 instances when tested with a dataset with 5% noise to 1,078 instances when tested with 40% noise level. This indicates that this algorithm is sensitive to noise because its performance greatly deteriorated as the noise level increased.

TABLE II. Summary Results of the J48 Model

Class	TP Rate	FP Rate	Precision	Recall
Normal	0.999	0.019	0.998	0.999
Flooding	0.974	0	0.949	0.974
TDMA	0.934	0	0.999	0.934
Grayhole	0.983	0.001	0.979	0.983
Blackhole	0.986	0	0.988	0.986
Average	0.997	0.017	0.997	0.997

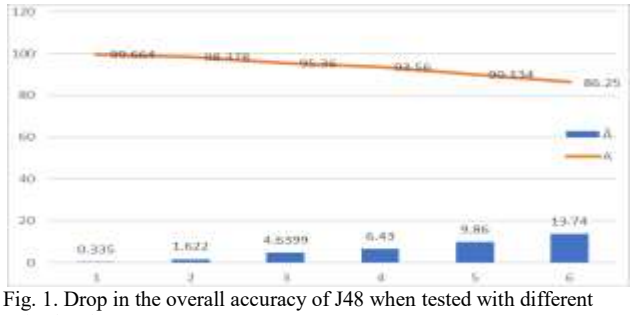

Fig. 1. Drop in the overall accuracy of J48 when tested with different noise levels.

TABLE III. J48 Confusion Matrix for J48 with 5% Noise

A	B	C	D	E	<-- Classified as
334,666	322	1,652	3,054	372	A = Normal
33	3,230	49	0	0	B = Flooding
462	0	6,169	4	3	C = TDMA
35	0	0	14,479	82	D = Grayhole
0	0	0	9	10,040	E = Blackhole

TABLE IV. JCONFUSION MATRIX FOR J48 WITH 40% NOISE

A	B	C	D	E	<-- Classified as
293,456	1,334	4,745	33,002	7,529	A = Normal
35	3,132	144	1	0	B = Flooding
365	56	6,127	76	14	C = TDMA
678	2,597	631	10,414	276	D = Grayhole
0	0	0	9	10,040	E = Blackhole

B. ANN ALGORITHM RESULTS

When testing the datasets with the ANN, the number of hidden layers needed to be decided [16]. If the default variable value *a* is selected, it gives one hidden layer with 11 neurons. However, this is insufficient to decide the best performance for the ANN. Hence, we decided to conduct the experiments on datasets with three forms of ANN, as shown in Table V. Their accuracy is shown in Table VI. It took 716 seconds to train ANN-1, 957.97 seconds to train ANN-2, and 853.9 seconds to train ANN-3.

TABLE V. Three Types of ANN Algorithms

ANN Architecture	Number of Hidden Layers	Number of Neurons in the Layers
ANN-1	1	11
ANN-2	2	11, 5
ANN-3	3	11, 5, 2

TABLE VI. ACCURACY FOR THE DIFFERENT LAYERS OF THE ANNS

ANN Models	A	Â
ANN-1	98.711%	1.288%
ANN-2	98.37%	1.6%
ANN-3	98.298%	1.7%

Table VI shows that the model with only one layer and 11 neurons had the best accuracy, at 98.711%. The least accurate model was ANN-3, which had three hidden layers with 11, five, and two neurons, at 98.298%.

Tables VII and VIII show that ANN-1's sensitivity to noise was very low. This is clear by looking at the TP rate of 0.998 for the normal class, which did not change as the noise increased.

TABLE VII. SUMMARY OF ANN-1

Class	TP Rate	FP Rate	Precision	Recall
Normal	0.998	0.016	0.998	0.998
Flooding	0.997	0.001	0.893	0.997
TDMA	0.92	0	0.995	0.92
Grayhole	0.789	0.002	0.931	0.789
Blackhole	0.958	0.008	0.765	0.958
Aaverage	0.987	0.015	0.988	0.987

TABLE VIII. TP RATES OF ANN-1 WITH DIFFERENT LEVELS OF NOISE

TP Rates for ANN-1						
	0%	*5%*	*10%*	*20%*	*30%*	*40%*
Normal	0.998	0.998	0.998	0.998	0.997	0.997
Flooding	0.997	0.982	0.967	0.966	0.969	0.965
TDMA	0.92	0.894	0.892	0.885	0.865	0.867
Grayhole	0.789	0.866	0.866	0.866	0.866	0.75
Blackhole	0.958	0.638	0.638	0.638	0.638	0.638

Table IX compares the three ANN architectures in terms of different tested noise ratios. Table IX shows that ANN-2 was a very robust model with good performance despite the increase in noise.

TABLE IX. ACCURACY FOR DIFFERENT ANN LAYERS TESTED WITH DIFFERENT NOISE RATIOS

Algorithm	Accuracy percentage with a different noise level					
	0%	*5%*	*10%*	*20%*	*30%*	*40%*
ANN-1	98.71	98.14	98.07	98.04	97.97	97.48
ANN-2	98.38	98.77	98.75	98.74	98.72	98.68
ANN-3	98.30	98.28	98.23	98.22	98.10	98.05

V. CONCLUSIONS AND FUTURE WORK

This study investigates the processes and endeavors leading to the design of an intelligent-intrusion detection and prevention mechanism that works efficiently to limit DoS attacks at reasonable processing and energy costs. A specialized dataset for wireless sensor networks was used to train four machine-learning algorithms: J48, ANN-1, ANN-2, and ANN-3. In this paper, the WSN-DS dataset was used to train WEKA through machine learning. The dataset contains normal and malicious network traffic, and was used to obtain the experimental results. The attacks considered in this dataset were blackhole, grayhole, flooding, and scheduling attacks. ANN and J48 models were built using the WEKA toolbox. Attacks were classified by a model built using 66% of the original dataset, and the remaining instances were used to test the model. The results show that J48 is the best model to use when there is no noise. It generated an accuracy rate of 99.66%, which is better than that of the ANN model. After introducing noise to the datasets, the ANN with two layers and 11 and five neurons in the first and second layers, respectively, was the most robust model and was not greatly affected by the noise. However, the time taken for the machine learning to build a model for J48 was 22 seconds which is faster than all ANN models. It took 716 seconds, 957.97 seconds, and 853.9 seconds to train ANN-1, ANN-2 and ANN-3, Respectively. As this time is only needed for training and not for the production environment, it is irrelevant to our choice of which model to use. Therefore, the ANN is still the best model because it showed greater tolerance to noise than J48 did.

REFERENCES

[1] V. G. M. and U. S. K. Mainanwal, "A survey on wireless body area network: Security technology and its design methodology issue," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015.

[2] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," Future Generation Computer Systems, vol. 78, pp. 956–963, 2018.

[3] A. Bengag, O. Moussaoui and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), Marrakech, Morocco, pp. 1-5, 2019, doi: 10.1109/ICDS47004.2019.8942268.

[4] T. V. P. Sundararajan and A. Shanmugam, "A novel intrusion detection system for wireless body area network in health care monitoring," Journal of Computer Science, vol. 6, no. 11, p. 1355, 2010.

[5] D. K. Anguraj and S. Smys, "Trust-based intrusion detection and clustering approach for wireless body area networks," Wireless Personal Communications, vol. 104, no. 1, pp. 1-20, 2019.

[6] M. Feurer, A. Klein, K. Eggensperger, J. Springenberg, M. Blum, and F. Hutter, "Efficient and robust automated machine learning," in Advances in neural information processing systems, 2015.

[7] J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," Big Data & Society, vol. 3, no 1, 2016.

[8] K. T. Butler, D. W. Davies, H. Cartwright, O. Isayey, and A. Walsh, "Machine learning for molecular and materials science," Nature, vol. 559, no. 7715, p. 547, 2018.

[9] M. A. E. Bhuiyan, E. I. Nikolopoulos, and E. N. Anagnostou, "Machine learning-based blending of satellite and reanalysis precipitation datasets: A multi-regional tropical complex terrain evaluation," Journal of Hydrometeorology, vol. 20, no. 11, pp. 2147–2161, 2019.

[10] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, et al., "Tensorflow: A system for large-scale machine learning," 12th {USENIX} Symposium on Operating Systems Design and Implementation, 2016.

[11] F. K. Hamey and B. Göttgens, "Machine learning predicts putative haematopoietic stem cells within large single-cell transcriptomics datasets," Experimental Hematology, vol. 78, pp. 11-20, 2019.

[12] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," Journal of Sensors, vol. 2016, article ID 4731953, 2016, doi:10.1155/2016/4731953.

[13] A. I. Al-issa, M. Al-Akhras, M. S. ALsahli ,and M. Alawairdhi, "Using machine learning to detect DoS attacks in wireless sensor networks," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, pp. 107-112, 2019.

[14] E. Frank, M. A. Hall, and I. H. Witten, "The WEKA Workbench," in Data Mining: Practical Machine Learning Tools and Techniques, 4th ed.. City: Morgan Kaufmann, 2016.

[15] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software: An update," SIGKDD Explorations, vol. 11, no. 1, 2009.

[16] M. AL-Akhras, H. Zedan, R. John, and I. ALMomani. "Non-intrusive speech quality prediction in VoIP networks using a neural network approach," *Neurocomputing*, vol. 72, no. 10-12, pp. 2595-2608, June 2009.