DoS/DDoS Detection Using Random Forest with Wavelet Decomposition

Ying-Feng Hsu [0000-0002-5335-4510] and Morito Matsuoka

Cybermedia Center, Osaka University, Osaka, Japan
{yf.hsu, matsuoka}@cmc.osaka-u.ac.jp

Abstract. As DoS/DDoS attacks become increasingly sophisticated and diverse, the need for attack detection models with both high detection rates and the ability to respond to new types of attacks has increased. In this study, we proposed a DoS/DDoS attack detection model which combines machine learning, wavelet decomposition, and a widely used feature extraction algorithm in an attempt to improve the detection accuracy of current machine learning models. The performance of our proposed model is compared to the models without wavelet decomposition, and the usefulness of feature selection on our proposed model is assessed. Based on our evaluation, the proposed model achieved a higher recall of 99.99% while still maintaining accuracy of 98.57%.

Keywords: DoS detection, DDoS detection, Wavelet, Feature Selection, Machine Learning

1 Introduction

Denial-of-service (DoS) is a cyber-attack that aims to make network services such as websites and web applications unavailable to its intended users by disrupting the targeted host and/or network resources [1][2]. A typical service disruption attack is made by flooding the target with huge loads of requests. A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource. Recent trends have revealed that DDoS attacks contribute to the majority of overall network attacks. The most common DDoS mitigation approach is to block all traffic from those attacker sources. However, due to the massive load of requests in question originates, this strategy is not effective against DDoS attacks. As DoS/DDoS attacks become increasingly sophisticated and diverse, distinguishing between legitimate and malicious flows is always a challenging task. Meanwhile, the need for attack detection models with both high detection rates and the ability to respond to new types of attacks has increased.

In general, two types of Network Intrusion Detection Systems (NIDS) have been used for the task of DDoS mitigation. The Signature-based NIDS (S-NIDS) detect intrusions based on a pattern-matching algorithm that inspects and identifies threats from the incoming packet by comparing a preinstalled attacked signature database. SNIDS

has good detection capabilities for known attacks, with fewer false alarms. However, it requires a preinstalled signature and is not aware of unknown threat patterns. When using SNIDS for network protection, frequent maintenance, and routine updates are required. In contrast, anomaly-based NIDS (ANIDS) focuses on deviations of the traffic pattern and uses those deviations to analyze incoming traffic to determine outliers as anomalous, even when faced with unknown attacks. Machine learning techniques have been widely used for ANIDS based on a wide range of statistics-based algorithms that recognizes patterns in large amounts of network traffic data. As recent machine learning algorithms have reached a level where they can sometimes detect abstract patterns with greater accuracy than human experts [3], the performance of machine learning-based intrusion detection systems is promising.

In this paper, we propose a model for the detection of DoS/DDoS attacks which combines machine learning with wavelet decomposition, a widely used feature extraction algorithm, in an attempt to improve the detection accuracy of current machine learning models. The rest of this paper is organized as follows. In section 2, we present recent related works on anomaly detection using wavelet decomposition and machine learning methods. In section 3, we elaborate on the proposed model and its procedures for DoS/DDoS detection. To validate the advantages and performance of the proposed approach, we provide a comprehensive evaluation in section 4. We conclude this paper and discuss future directions for research in section 5.

2 Related Works

Various machine learning researches have been conducted for network intrusion detection or DoS/DDoS detection such as using reinforcement learning [21], and ensemble learning [22] and, GAN [23]. However, only a few approaches use wavelet as data feature extraction. In this section, we provide a detailed summary of those related works in the area of DoS/DDoS detection using machine learning classifiers, DoS/DDoS detection using wavelet techniques, and combined machine learning and wavelet techniques.

The work of [4] proposed a model for early detection of DDoS attacks using the k-nearest neighbor classifier and achieved an overall accuracy of 91.886% when tested against the 2000 DARPA dataset. They came to the conclusion that their method can classify the DDoS phases correctly and efficiently detect DDoS attacks early. Pei [5] tested the detection accuracy of random forest and support vector machine against three subtypes of DDoS attacks, including TCP flood attacks, UDP flood attacks, and ICMP flood attacks. Random forest outperformed support vector machine in terms of accuracy in all cases regardless of the ratio of normal traffic to attack traffic. Bindra and Sood [6] performed a comparison of machine learning techniques using the DDoS part of the CIC-IDS 2017 dataset and achieved a mean accuracy of 82.48% using logistic regression,94.36% using k-nearest neighbor 81.04% using Gaussian NB, 96.13% using random forest 82.35% using linear SVM. They concluded that the random forest classifier is a good choice in the case of DDoS detection. Another work of [7] proposed a method that utilizes energy distribution based on wavelet analysis to detect DDoS

attack traffic. This is one of the early attempts to detecting DDoS attacks using wavelet analysis techniques, and they succeeded in detecting UDP flooding attacks in simulation using their proposed approach. As for the wavelet and machine learning hybrid method, Liang et al. [8] proposed an improved DDoS attack detection method by combining the traditional wavelet analysis method with the Isomap dimension-deduction method. They claimed that their approach is able to detect some DDoS attacks that traditional wavelet analysis methods do not become sensitive to. He et al. [9] proposed a low-Rate DoS (LDoS) detection method based on feature extraction using wavelet transform and backpropagation neural network. They compared the variance ratio (before and during the attack) of feature metrics using different wavelets and concluded that the db4 wavelet is sensitive to LDoS attacks. They achieved an accuracy of 99.3%, recall of 99.1%, and precision of 99.5% in their simulation. A semi-supervised learning model using wavelet features by [20], naive Bayes, and decision tree are used to classify unlabeled entities, and the entities are labeled based on their agreement. The labeled entities are then used as input to a support vector machine classifier which makes the final judgment. When testing their method using the CAIDA dataset, they achieved a detection rate of 97.955%, false positive rate of 1.75%, and a false negative of 2.34%. The use of semi-supervised learning in the proposed model provided a reasonable trade-off between supervised learning and the unavailability of the labeled dataset, and the proposed model is very useful in scenarios where training using a real-time generated dataset is important.

From the previous work listed above, we can clearly see that DoS/DDoS detection using machine learning and wavelet analysis techniques has been successful in many scenarios. However, previous researches did not thorough considering the facts that (i) only either wavelet analysis or machine learning techniques were used and researches on combining the two are still limited, (ii) many studies use outdated datasets for evaluation which cannot reflect the current situation, and (iii) no research we found has used multiresolution analysis and stationary wavelet transform for DoS/DDoS detection purposes. In this study, we aim to investigate these scenarios and reflect on these challenges.

3 Proposed Model

In this section, we propose an anomaly-based DoS/DDoS detection model as illustrated in Fig 1. The proposed model utilizes supervised learning, so the network traffic flow features used for training are supposed to have labels of “benign” or “attack” attached to them. The proposed model consists of three major components to process the network flow data: the wavelet decomposition using stationary wavelet transform (SWT), feature selection, and supervised machine learning by random forest.

3.1 Feature extraction: Wavelet Transform and Decomposition

In this step, the network flow signal is decomposed into multiple parts corresponding to different sub-frequency bands of the original features. One widely used technique of

signal analysis is Fourier transform (FT), the result of which shows the frequency components of a given signal in the form of a frequency spectrum. The main drawback of the Fourier transform is that it sacrifices all information about time for absolute precision on frequency. Thus, Fourier transform makes it inappropriate for analysis of signals where information about temporal information is important, i.e., signals of network traffic which property changes over time.

Unlike Fourier transform, Wavelet transform (WT) keeps a balance between time information on the frequency and temporal spread of a signal. In general, Wavelet transform (WT) is divided into three categories: continuous wavelet transform (CWT), discrete wavelet transformation (DWT), and stationary wavelet transform (SWT). DWT samples the signal in different resolutions (frequency) when it is decomposed. It generates different length of wavelet coefficients in each scale which cause the difficult for the later step of machine learning. For example, as the wavelet coefficients generated by DWT are not 1-to-1 mapped to the sample data points of the original signal, they cannot be directly used as input to machine learning classifiers. SWT does not downsample the signal at each scale and provides a solution to the aforementioned problem of DWT. The wavelet coefficients generated at each level of SWT are time-invariant and retain the same number of samples as the original signal, and therefore can be directly used as input to machine learning classifiers together with original machine learning labels. As DoS/DDoS is a type of attack that shows strong temporal characteristics, it is likely that wavelet transforms for time-series analysis are effective for extracting DoS/DDoS-related features from the original network flow features. We adopt the concept from [12] and apply SWT to our model due to the fact that it's a time-invariant transform, and the output wavelet coefficients can be directly used as input features to machine learning classifiers.

3.2 Feature Selection: Recursive Feature Elimination (RFE)

A dataset may contain a number of features, of which some are relevant to solving the target problem while the others are redundant or irrelevant. Feature selection is the process of identifying and selecting a subset of features that is relevant to solving the target problem from a dataset [10], and selecting the appropriate features as input to a machine learning model can improve the accuracy and shorten the execution time of the model [11]. Recursive feature elimination (RFE) is a wrapper method, and it works by eliminating a given number of features with the lowest weights according to the weights assigned by a user-specified estimator at each step. RFE repeats the process until the desired number of features is selected. The reason for using RFE instead of selecting features directly according to the weights assigned by estimators is that weights (especially that of comparatively relevant features) calculated with the presence of less relevant features might be imprecise. By gradually eliminating comparatively irrelevant features and recalculate the weights, the weights assigned to comparatively relevant features are likely to be more accurate. Besides, RFE can be used directly with the random forest classifier using the classifier's built-in feature importance as assigned weights. As the built-in feature importance is closely related to the random forest classification model and RFE can help assign weights to comparatively relevant features

more accurately, it has been shown [11] that using RFE with random forest's built-in feature importance will perform well in selecting relevant features.

3.3 Machine Learning for DoS/DDoS Detection

The third step is classification using machine learning classifiers. We chose to use the random forest classifier because (i) the random forest classifier performed well in DDoS in a number of previous researches including [5] and [6], and (ii) the random forest classifier is known for its good generalization performance [13] which is likely to help detect new, unknown types of DoS/DDoS attacks, and (iii) coefficients generated by SWT can be directly used as input to machine learning classifiers, making the whole DoS/DDoS detection model straightforward and easy to apply. In this study, the random forest classifier will take the features selected by feature selection and classify each record as either "Attack" or "Benign."

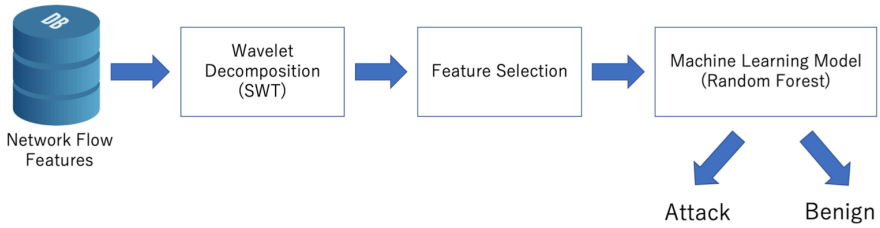

Fig. 1. Purposed model.

4 Experiment

In this section, we evaluate the performance of our proposed DoS/DDoS attack detection method. We first introduce the evaluation dataset and metrics used for evaluation and then present and analyze the evaluation results of our proposed models. In order to ensure the feasibility of our proposed method, we conducted three evaluation plans, as shown in Fig. 2.

4.1 Experimental Dataset

We used the DoS and DDoS part of the CIC-IDS 2017 dataset in our experiment. The CIC-IDS 2017 dataset consists of full packet payloads in pcap format as well as network flow features generated by CICFlowMeter [14] (along with labels) that can be used for machine learning in csv format. The benign flow in the dataset is generated using the B-Profile system [15] that profiles the abstract behavior of human interaction and generates naturalistic benign background traffic, while the attack flow in the DoS and DDoS part of the dataset is generated using actual DoS/DDoS attack tools including slowloris, slowhttptest, hulk, goldeneye and LOIT [16]. We chose to use this dataset for our evaluation task due to the following characteristics:

- It includes many recent types of DDoS, which is better reflects the real-world situation than older datasets.
- The numbers of attack records and benign records are relatively balanced compared to other DoS/DDoS datasets like CIC-DDoS2019 [17].
- The attack flow is generated using real-world DDoS attack tools.
- The total number of records of the DoS and DDoS parts (918,448 records) is reasonable for the experiment.

We removed a few records from both the train/validation dataset and the test dataset due to the fact that the SWT is only defined on record numbers that are multiples of 2^n, where n is the maximum decomposition level. After this step, the train/validation dataset has 425,984 records and the test dataset has 491,520 records, which are both multiples of 2^{15}. Therefore, 15 levels of wavelet decomposition using SWT can be done on our dataset.

4.2 Evaluation Metrics

The DoS/DDoS attack detection models we proposed in this paper perform binary classification, that is, classifying each network flow record as either "Attack(DoS/DDoS)" (positive) or "Benign" (negative). Our evaluation method is based on the confusion matrix described in Table I. Common evaluation metrics that can be calculated based on TP (true positive), TN (true negative), FP (false positive), and FN (false negative) include accuracy, precision, recall and F1 score, etc. In our experiment, we chose to use accuracy as an evaluation metric since it can directly interpret the model performance, and our dataset (the DoS/DDoS part of CIC-IDS 2017) is not highly imbalanced. We also chose to use recall as an evaluation metric due to the fact that in most intrusion detection scenarios, false negatives (predict attack as benign) lead to much more serious consequences compared to false positives (predict benign as an attack), and therefore reducing false negatives is more crucial than reducing false positives. The definitions of both metrics are listed below.

Table 1. Confusion matrix for DoS/DDoS dection

Positive = A (Dos/DDoS attack) Negative = N (normal)		Actual Label	
		A	N
Predicted Label	A	TP	FP
	N	FN	TN

- Accuracy:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}}$$

Accuracy shows the ratio of correct predictions to all predictions. It is an intuitive, easy-to-interpret metric and works well in many scenarios. However, it may fail to reflect the real performance of a classification model when the input data is extremely unbalanced. For example, a model that only makes positive predictions will still achieve high accuracy when almost all the records in the input data are positive.

- Recall:

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

Recall shows the ratio of positive records that are classified as positive to all positive records. In the case of network intrusion detection, the higher the recall of a model is, the less likely it will miss a positive record (by predicting DoS/DDoS traffic as benign traffic). The recall is important when reducing the number of false negatives is crucial.

4.3 Evaluation Plans and Results

Fig. 2 illustrates our three evaluation plans, and the experiment is performed mainly using an HPC server, which includes dual Intel Xeon E5-2690 v4 processors (56 cores in total), 768 GB of main memory. Python with Keras is used as the developing and evaluation platform, and all evaluation models are subject to optimize the hyperparameter Through a library named Hyperas. In the experiment, we first create a baseline for comparison by creating a random forest model without SWT decomposition. This is shown as plan (1) in Fig. 2. Next, we perform the SWT decomposition using the haar, coif3, and sym5 wavelet basis functions and create random forest models using the output of the SWT decomposition. For each wavelet basis function, we will try five decomposition levels, so 15 random forest models are generated in this step. This is shown as plan (2) in Fig. 2. The three wavelet basis functions are selected based on the study of [18], which states that the Daubechies wavelets (harr), symlets and coiflets are reasonable choices for DDoS detection. Finally, we perform feature selection after SWT decomposition using RFE based on the feature importance of the random forest classifier and generate models using the selected features. Accuracy of models generated using different numbers of features is compared, and the model with the highest accuracy is chosen for each wavelet basis function decomposition level combination. This step will also generate 15 random forest models and is shown as the procedure (3) in Fig. 2. By comparing models generated in plan (1) and (2), it is possible to reveal what influence SWT decomposition has on the performance of the random forest classifier, and by comparing models generated in procedures (2) and (3), we explore that if feature selection after SWT decomposition can improve the performance of the random forest classifier.

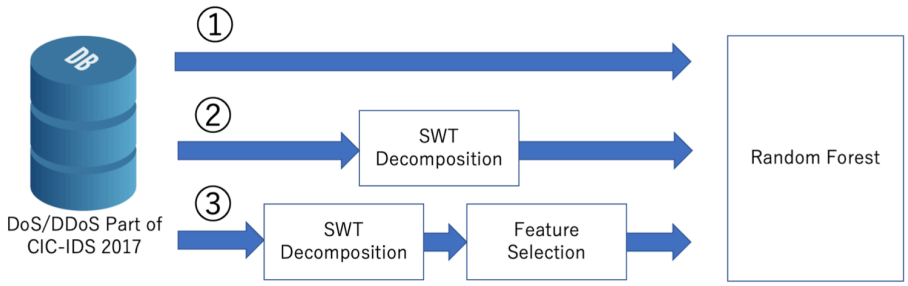

Fig. 2. Proposed Model

Results of Plan (1): baseline model
We first created a model without wavelet decomposition as a baseline for comparison, and test accuracy and precision of the model are 99.14% and 99.91%, respectively. This part of the experiment corresponds to plan (1) in Fig. 2.

Results of Plan (2): Models with SWT Decomposition:
The test accuracy and precision of the models are shown in Fig. 7 and Fig. 8. respectively. It can be seen that the accuracy of all the models with SWT decomposition is lower than that of the model without SWT decomposition, and the accuracy tends to drop as the decomposition level increases. However, the recall of some models with SWT decomposition is higher than the recall of the model without SWT decomposition, especially in the case of using haar as the wavelet basis function and decomposition level 3, where recall of 99.99% is achieved. The recall of models with SWT decomposition using different wavelet basis functions denotes the same tendency of increasing from decomposition level 1, reaching the maximum value around decomposition levels 3 to 4, and then starting to drop.

When comparing the performance of different wavelet basis functions, it is clear that haar outperforms both coif3 and sym5 because it records the highest accuracy at all decomposition levels and the highest recall at all decomposition levels except level 2. As sym5 outperforms coif3 in both accuracy and recall at all decomposition levels, coif3 has the worst performance of the three wavelet basis functions. We summarize five observations as follows.
<1> Models with SWT decomposition have lower accuracy compared to the model without SWT decomposition regardless of accuracy and decomposition levels.
<2> SWT decomposition can increase the recall of the DoS/DDoS detection model if proper accuracy and decomposition level are chosen.
<3> Of the three wavelet basis functions, haar has the best performance while coif3 has the worst performance.
<4> Accuracy tends to drop as the decomposition level increases.
<5> Recall increases and then drops as decomposition level increases, reaching the maximum value around decomposition levels 3 to 4.

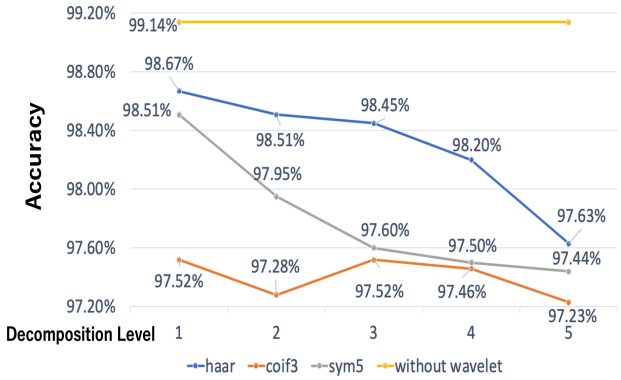

Fig. 3. Accuracy of Models with SWT Decomposition

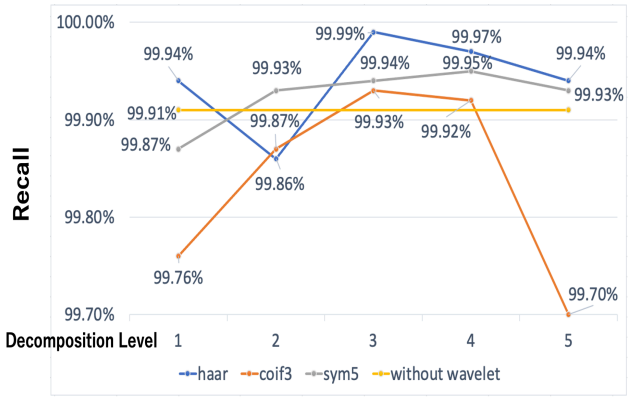

Fig. 4. Recall of Models with SWT Decomposition

Results of Plan (3): Models with SWT Decomposition and Feature Selection

Finally, we created models with both SWT decomposition and feature selection applied, which corresponds to plan (3) in Fig. 2. The test accuracy and precision of the models are shown in Fig. 5 and Fig. 6. It can be seen from these figures that although feature selection improved the accuracy and recall of the models to some extent, the five observations from the plan (2) stay applicable to models with feature selection applied. In addition, we include the observation <6> as

(6) Feature selection can slightly (but not significantly) improve the performance of models with SWT decomposition.

Discussions:

The observation <2> from above is likely due to the fact that SWT decomposition is able to help capture the characteristics of DoS/DDoS attack flows. However, considering observation <1>, it is possible that SWT decomposition somewhat destroys the characteristics of normal(benign) flows as normal flows that do not have strong time-related characteristics as DoS/DDoS attacks. These reasons can also explain observations <4> and <5>. The fact that recall increases and accuracy drops as decomposition level increases at first means that benign flows are increasingly misclassified. This is possible because the characteristics of normal(benign) flows are gradually lost as SWT decomposition proceeds. The characteristics of DoS/DDoS attack flows, on the other hand, become more evident as SWT decomposition proceeds and increases the value of recall. The reason why recall of the models starts to drop beyond decomposition levels 3 to 4 might be that the characteristics of DoS/DDoS attack flows are the most evident at these decomposition levels, and further decomposition starts to damage the network traffic signal. observation <3> might be due to the fact that haar has compact support, and DoS/DDoS attack flows are usually closely spaced because wavelets with compact support generally work well in the detection of closely spaced features [19]. The fact that haar has sharp filter transition bands and is therefore robust against edge effects might also have helped haar perform better than the other two wavelet basis functions. Observation <6> might be due to the fact that the machine learning model used this time, random forest, already performs some sort of feature reduction internally as only part of the input data is used to build the decision trees. Feature selection is likely to be more effective when used with classifiers that make use of all input data.

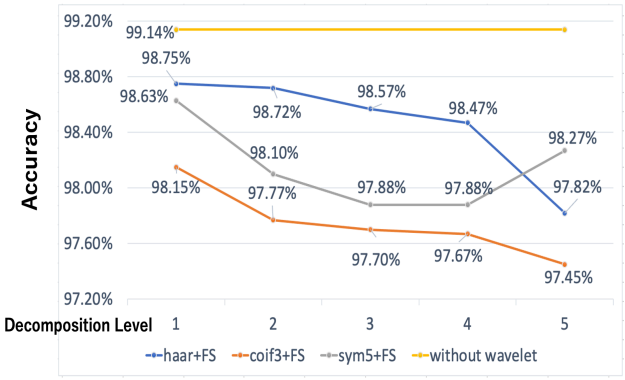

Fig. 5. Accuracy of Models with SWT Decomposition and Feature Selection

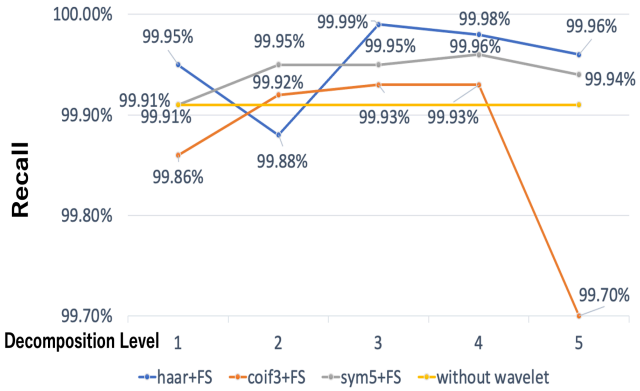

Fig. 6. Recall of Models with SWT Decomposition and Feature Selection

5 Conclusion

In this thesis, we proposed a DoS/DDoS attack detection model that combines the random forest classifier with wavelet decomposition based on stationary wavelet transform. We achieved 99.99% for the value of recall while still maintaining an accuracy of 98.57% when testing our proposed model using the DoS/DDoS part of the CIC-IDS 2017 dataset. Two future research tasks related to this research. First, we plan to extend our model to differentiate different types of DoS/DDoS. There are numerous different types of DoS/DDoS attacks, and each might have unique characteristics. Testing our proposed models against different types of DoS/DDoS attacks can reveal the performance of our proposed models against different known(trained) DoS/DDoS types and also unknown(untrained) types of DoS/DDoS. Next, although we used the random forest classifier in this research, the random forest classifier is not specifically designed to retain time-related characteristics of the input data. Therefore, combining SWT decomposition with other classifiers that retain time-related characteristics of input data better might achieve even better results and is worth experimenting with.

References

[1]. "Oracle and KPMG Cloud Threat Report 2019." available at https://www.oracle.com/a/com/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf.

[2]. "Cyber Attack - What Are the Most Common Cyber Attacks? - Cisco." available at https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[3]. J. A. Nichols, H. W. Herbert Chan and M. Baker, "Machine learning: applications of artificial intelligence to imaging and diagnosis," Biophysical reviews, vol.11(1), pp. 111-118, Feb. 2019.

[4]. H.-V. Nguyen and Y. Choi, “Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDoS framework,” World Academy of Science, Engineering and Technology, vol. 39, pp. 640-645, Mar. 2009.
[5]. J. Pei, Y. Chen and W. Ji, “A DDoS Attack Detection Method Based on Machine Learning”, Journal of Physics: Conference Series, vol. 1237, no. 3, pp. 032040, Jun. 2019.
[6]. N. Bindra and M. Sood, “Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset,” Automatic Control and Computer Sciences, vol. 53, pp. 419-428, Sep. 2019.
[7]. L. Li and G. Lee, “DDoS Attack Detection and Wavelets,” Telecommunication Systems, vol. 28, pp. 435-451, Mar. 2005.
[8]. L. F. Lu, M. L. Huang, M. A. Orgun and J. W. Zhang, “An Improved Wavelet Analysis Method for Detecting DDoS Attacks,” Proceedings of 2010 Fourth International Conference on Network and System Security, pp. 318-322, 2010.
[9]. Y.X. He, Q. Cao, T. Liu, Y. Han and Q. Xiong, “A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform”, Journal of Software, vol. 20(4), pp. 930-941, 2009.
[10]. L. Rokach, B. Chizi and O. Maimon, “Feature Selection by Combining Multiple Methods,” Advances in Web Intelligence and Data Mining, pp. 295-304, 2006.
[11]. K. Kurniabudi, D. Stiawan, Dr. Darmawijoyo et el., “CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection,” IEEE Access, vol. 99, pp. 1-12, Jul. 2020.
[12]. Fouladi, T. Seifpoor and E. Anarim, “Frequency characteristics of DoS and DDoS attacks,” Proceedings of 2013 21st Signal Processing and Communications Applications Conference (SIU), pp. 1-4, 2013.
[13]. H. Hitoshi, “Random Forests: Fundamentals and Recent Trends,” The Journal of the Institute of Image Information and Television Engineers, vol. 70, no. 9, pp. 788-791, 2016.
[14]. “CICFlowMeter.” available at https://github.com/ISCX/CICFlowMeter.
[15]. A. Gharib, I. Sharafaldin, A. Habibi Lashkari and A. A. Ghorbani, “An evaluation framework for intrusion detection dataset,” Proceedings of 2016 International Conference on Information Science and Security (ICISS), pp. 1-6, 2016.
[16]. I. Sharafaldin, A. Habibi Lashkari and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, Proceedings of 4th International Conference on Information Systems Security and Privacy (ICISSP), pp. 108-116, Jan. 2018.
[17]. I. Sharafaldin, A. Habibi Lashkari, S. Hakak and A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy”, Proceedings of IEEE 53rd International Carnahan Conference on Security Technology, pp. 1-8, 2019.
[18]. V. Srihari and R. Anitha, “DDoS detection system using wavelet features and semi-supervised learning,” Proceedings of International Symposium on Security in Computing and Communication, pp. 291-303, Sep. 2014.
[19]. “Choose a Wavelet - MATLAB & Simulink.” available at https://www.mathworks.com/help/wavelet/gs/choose-a-wavelet.html.
[20]. V. Srihari and R. Anitha, “DDoS detection system using wavelet features and semi-supervised learning”, Proceedings of International Symposium on Security in Comput- ing and Communication, pp. 291-303, Sep. 2014
[21]. Y. Hsu and M. Matsuoka, “A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System”, Proceedings of IEEE International Conference on Cloud Networking (CloudNet), November 2020

[22]. Y. Hsu, Z. He, Y. Tarutani, and M. Matsuoka, “Toward an Online Network Intrusion Detection System Based on Ensemble Learning”, Proceedings of IEEE International Conference on Cloud Computing (IEEE Cloud), July 2019

[23]. G. Caminero, M. Lopez-Martin and B. Carro, "Adversarial environment reinforcement learning algorithm for intrusion detection," Computer Networks, vol. 159, 2019.