Malware Attack Detection using Machine Learning Methods for IoT Smart Devices

Chaw Su Htwe
Cyber Security Research Lab
University of Computer Studies,
Yangon, Myanmar
chawsuhtwe@ucsy.edu.mm

Mie Mie Su Thwin
Cyber Security Research Lab
University of Computer Studies,
Yangon, Myanmar
drmiemiesuthwin@ucsy.edu.mm

Yee Mon Thant
Cyber Security Research Lab
University of Computer Studies,
Yangon, Myanmar
yeemonthant@ucsy.edu.mm

***Abstract*— The malware attacks are targeting IoT devices as the rapid development of these devices. The limited resource of IoT devices is attracting malware developers. The strong security mechanisms cannot be deployed on these devices because of their computational capabilities. Therefore, there are malicious attacks challenging these devices, especially botnet attacks. After infection to these devices, they tried to attack the victim user by launching the distributed denial of service (DDoS). Although machine learning methodologies can support to detect these attacks, their heavyweight processing is challenging to implement the prompt response to the attack actions. Therefore, this paper intends to reduce the processing time by using the information-gain feature selection method for implementing the malware attack detection system with the CART learning algorithm, and its results are compared the performance with Naïve Bayes. The experiment results indicate that the proposed methodology is effective in detecting malware attacks with up to 100% accuracy.**

Keywords*— *IoT, Malware, Botnet, Feature Selection, Machine Learning

I. INTRODUCTION

In recent years, there are many IoT devices rapidly growing in several environments, such as smart homes, smart cars, smart industries, and so on. The report predicted [1] that the IoT devices connection will be 24 billion, and its market will be 1.5 trillion USD in 2030. Figure 1 shows the botnet attack challenges between 2019 and 2020 Q1 [2]. Due to the challenges of the attacks, the IoT security market will grow to 36,600 million USD by 2025 [3]. There are many malware families captured by the security analysts, and the popular malware families are Mirai, Hajime, Bashlite and etc. [4]. Among them, Mirai and its variances have infected many IoT devices around the world since 2016. Figure 2 shows the Mirai botnet attacks flow to the victim host through the botnets infected IoT nodes [5]. They launched the distributed denial of service (DDoS) attacks through the IoT devices in 164 countries, and they were mostly targeting CCTV cameras

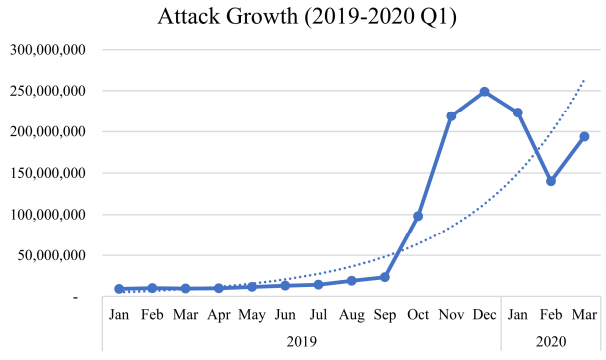

Figure 1. The attacks attempt between 2019 and 2020 Q1

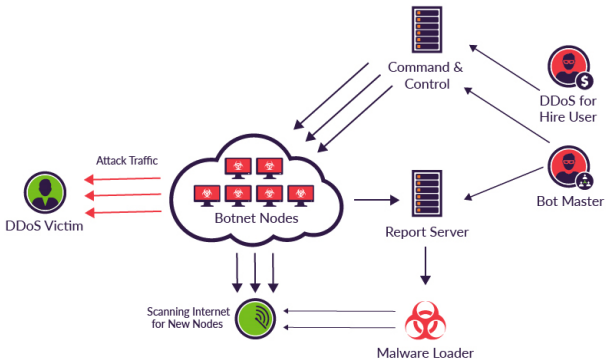

Figure 2. The Mirai attacks flow to the victim host

by their botnet [6]. After infecting their botnets, the IoT devices became bots that can control through the C&C server for launching the attacks to the victim hosts.

There are two possible ways to detect the attacks, such as host-based detection system and a network-based detection system. However, it is difficult to implement the computational attack detection system in the resource constraint devices. Thus, most attack detection systems are based on the network-based architecture for this environment. As the detection methodologies, the main two ways are possible. The first one is signature-based detection systems. These systems are based on the pre-recorded attack signatures by matching their signatures to investigate the attacks. Thus, these are not possible to detect unknown attacks. These are also called rule-based detection systems because they are based on the rules which are generated by the attack signatures.

Another way is the anomaly-based detection system, and these are based on the benign traffic of the dedicated networks. These systems are really effective not only to detect the known attacks but also the unknown attacks. However, the challenge of these systems in the IoT environment is the different nature of the IoT devices. The different nature of devices works with a different benign traffic manner. The machine learning methods can support detecting botnet attacks, but the computation demand of these methodologies is a challenge for the prompt response to the attacks defending system. Therefore, the paper used the feature selection method to reduce the high demand for computation. The information-gain method is applied for the feature selection purpose. The CART algorithm and Naïve Bayes are implemented to detect the attacks after getting the most important features from the dataset which is captured by running the Mirai botnet to the IoT device.

The remaining parts of the paper are organized as the related work in Section 2. After that, the background methodologies, including the feature selection method and the classification approach in Section 3. The proposed attack detection flow and experiment results are presented in Section 4. Finally, the conclusion will be included in Section 5.

II. Related Works

Many attacks detection works were based on the well-known datasets, such as KDD CUP 99 [7], its improvement (KDD-NSL), and Kyoto [8], but these datasets are only eligible for the attacks detection in conventional networks because of the lack of the malware attacks which are infected in the smart devices. Some recent attack detection works are also based on the modern dataset, called Bot-IoT [9], but its records are captured in the simulated environment.

The signature-based attack detection works [10], [11] are not eligible for detecting the malware attacks on smart devices. The attack detection system [10] was proposed to get an efficient attack detection mechanism for extending original Snort rules by using the honeypot. The study [11] proposed the signature-based detection system with a module that was performing the parallel tasks with a small database. These types of attack detection systems can only be effective for detecting the known attacks because of the pre-defined attack signature rules.

The study [12] investigated the performance of the public signature-based detection systems. They observed that Suricata would use more computational resources than Snort. They also proposed the extension of Snort with machine learning methods to improve the attack detection accuracy. The attack detection work is based on the machine learning methodologies, but the dataset that is applied in their works is not related to smart devices. The research [13] focused on the rules generation framework with machine-learning methodologies. They applied Random Forest to discover the rules for implementing the real-time detection system. Whatever the systems with signature-based attack detection methodologies were implemented, it is difficult to detect the unknown attacks. Although many studies were trying to implement effective attack detection systems with machine learning methods, they are mostly based on outdated datasets. They are not focused on detecting malware attacks on smart devices.

III. Background Methodologies

The attack classification and detection process will be performed with the tree-based algorithm, called CART, and Naïve Bayes. The feature selection method called the information-gain approach would be used to remove the irrelevant features and to reduce the computation process for attack detection.

A. CART

The classification algorithm, called CART, is introduced in 1984. A tree is developed by recursive parceling, beginning from the root hub; every hub can be part of the left and right youngster hubs. These hubs would then be able to be additionally part, and they when all is said and done, become parent nodes of their subsequent nodes. Arrangement and relapse trees are for developing expectation models from the information. The models are obtained by recursively dividing data space and fitting a direct gauge model inside each fragment. Hence, the distributing be addressed graphically as a decision tree. Plan trees are planned for subordinate factors that take a predetermined number of unordered characteristics, with desire botch assessed the extent that misclassification cost and besides for subordinate factors that take steady or mentioned discrete characteristics, with gauge bungle ordinarily assessed by the squared differentiation between the watched and foreseen characteristics [14].

$$Gini = 1 - \sum (Pi)^2 \tag{1}$$

CART uses a generalization of the binomial variance called the Gini index; it is shown in equation (1). It stores the sum of squared probabilities of each class, and i is from 1 to the number of classes.

B. Naïve Bayes

It is a simple but powerful algorithm for predictive modelling. Its classifier belongs to the category of probability classifier, using the Bayesian theorem. It is called 'Naïve' because it requires strong (naive) independence assumptions between the features [15]. The main process of Naïve Bayes is based on equation (2). Its training process is fast and easy. It can also perform even better than other statistical models.

$$\mathrm{P(A|B)} = \frac{P(B|A)P(A)}{P(B)} \tag{2}$$

C. Information-Gain

It is an entropy-based feature selection method [16]. It can be used as the filter-based approach, which means the feature selection process will perform before the classification process. Each feature is evaluated by the measurement of the gain values, which is shown in equation (3). C denotes the target class, and A denotes the attribute of the dataset. Where IG (C, A) represents the information gain for the dataset, H (C) is the entropy of the dataset before changing, and H (C|A) represents the conditional entropy for the dataset for the given attribute A. It can evaluate the binary or nominal class, and it can handle missing class values.

$$IG\ (C, A) = H\ (C) - H\ (C\ |A) \tag{3}$$

IV. Proposed Detection System and Experiment Results

There are two main parts of the proposed malware attack detection system, which is shown in Figure 3. The first one is the training part, and the second one is the attack detection part. The public dataset, called N-BaIoT [17], is used in the experiment to build the detection system. It is captured by

running the Mirai botnet to the IoT smart devices, like a smart home security camera. There are 115 features included in the original dataset, the benign traffic records, and a total of 4 kinds of attack classes in the Mirai records which are used in the experiment, such as ack, scan, syn, and udpplain attacks. These are included in the most challenging attacks, DDoS. Two-third of the dataset is applied for training, and the remaining part of the dataset is used for evaluating the proposed detection system.

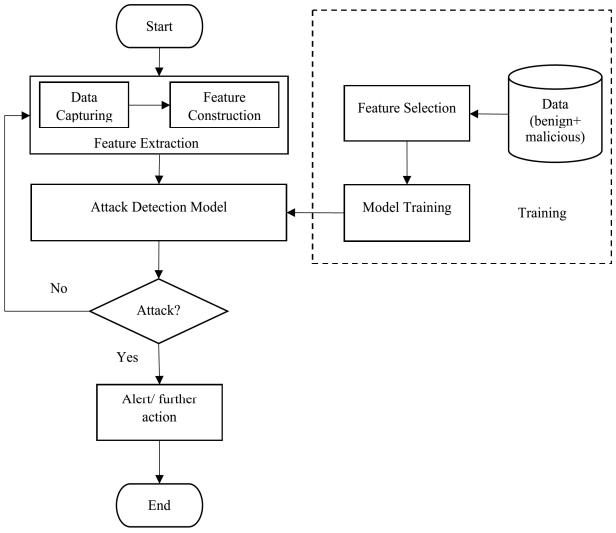

Figure 3. The proposed attack detection flow

Before performing these two parts, the feature selection has to be done for deciding which features should be selected. The information-gain feature selection approach is applied for the selection of the most important features from the dataset, after getting the gain values of each feature, by ascending order and selected half of the features which possess the highest gain values. Thus, there are 58 features selected according to the gain values of each feature. After getting the most important features, the training process is performed by using the CART and Naïve Bayes algorithms. After preparing the trained model for attack detection, the system performs the attack detection with selected features.

A. Performance Evaluation

The performance evaluation processes are done by using the confusion matrix, which is based on recall and precision. The recall is important to identify the performance of the system the correctly classify the network pattern as the attack. Moreover, precision is also necessary to identify the performance of the system, which reflect correctly classify the network pattern as the attack, with of all attack actually having it. Equation (4) and (5) shows how to identify the recall and precision, where, TP means the network pattern is identified as an attack, and it is actually attacking, FN means the network pattern is identified as benign, but it is actually attacking, and FP means the network pattern is identified as an attack, but it is actually benign.

$$recall = \frac{TP}{TP + FN} \tag{4}$$

$$precision = \frac{TP}{TP + FP} \tag{5}$$

B. Experiment Results

The comparison of performance results is shown in Figures 4, 5, 6, and 7. Figures 4 and 5 compare the results of recall values, using CART and Naïve Bayes (NB), between all features (All-F) and selected features (S-F). In Figure 4, all of the results are not different; even half of the original features are removed from the experiment. In Figure 5, the Naïve Bayes algorithm could not support to detect the attacks when using all original features. However, the results are improved when using the selected features, especially in the SCAN attack detection. That can greatly support the protection of the devices because the scanning attack is an initial critical attack on the devices.

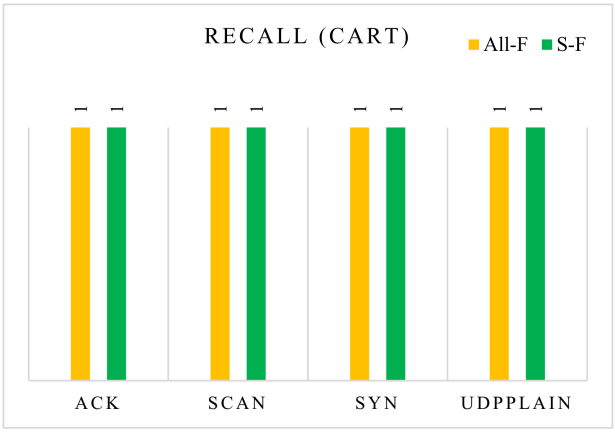

Figure 4. The recall values with CART, using all features vs selected features

Figure 6 and 7 show the comparison of the results of precision values, using CART and Naïve Bayes (NB), between all features (All-F) and selected features (S-F) which is selected using information gain approach. The precision results using the CART algorithm are shown in Figure 6. The results between using all features and selected half of the features are the same. Moreover, the results of recall and precision values using CART are almost 100% whether using all features or not, but the processing resource demand will be significantly reduced by using the selected features. Besides, the precision values using Naïve Bayes with selected features are significantly higher than the values of using all features. Therefore, the detection of attacks using selected features is better than using all features in all cases of these two algorithms.

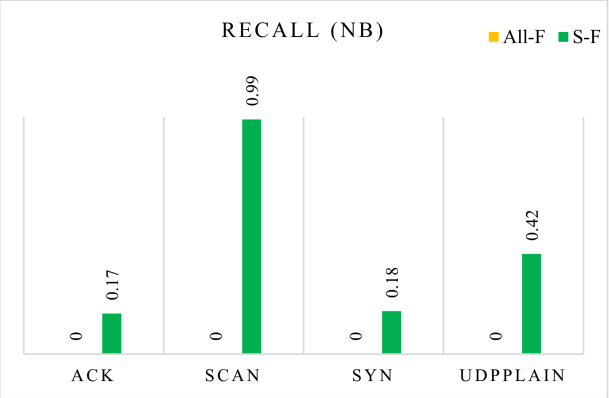

Figure 5. The recall values with Naïve Bayes, using all features vs selected features

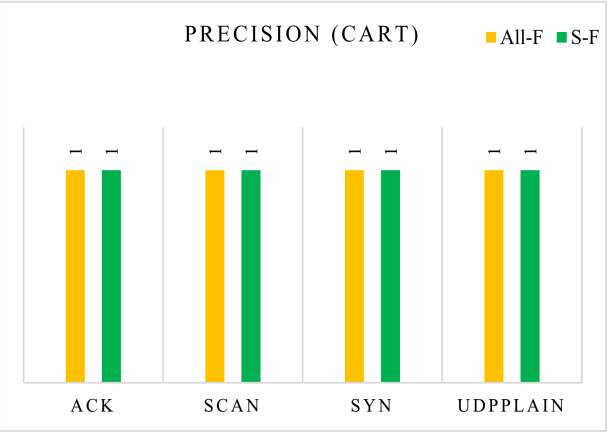

Figure 6. The precision values with CART, using all features vs selected features

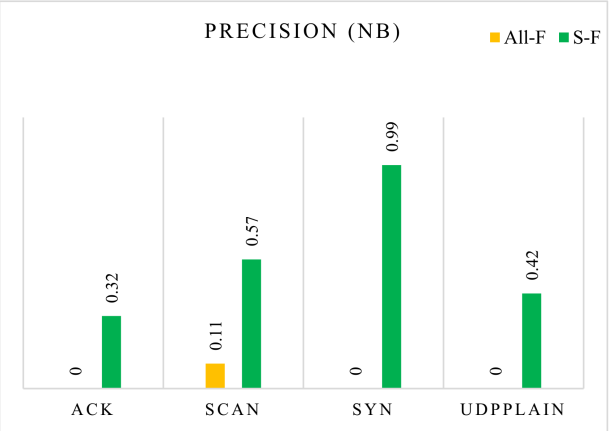

Figure 7. The precision values with Naïve Bayes, using all features vs selected features

C. *Contributions*

According to the experiment results, the following contributions can be found.

- CART algorithm is more suitable than Naïve Bayes in the detection of the malware attacks that can be found in the smart environments.
- The feature selection method, called Information-Gain, is useful to reduce the number of features significantly.
- The detection accuracy with CART is still high, even removing many features from the dataset.
- In the situation of using Naïve Bayes, the accuracy is not high enough as the usage of CART, but the results are improved when using the selected features by feature ranking method, Information-Gain.
- The machine learning methods, both of the classifier (CART) and the feature selection method (Information-Gain) are useful to implement the malware attack detection system of smart devices.

V. Conclusion

As the growth of the IoT and its developments are found everywhere. On the other side, these devices are facing malware attacks and becoming bots which can be controlled by the bot-master. They launched the attacks on the victim host through the infected IoT devices. Thus, an effective attack detection mechanism is necessary for protecting these devices and their connected network devices. This paper proposed the malware attack detection with machine learning method, CART with the selected features. The results indicated that it could support detecting the attacks with up to 100% accuracy with the CART algorithm. Moreover, the performance of Naïve Bayes becomes better with the selected features. In future work, the detection system will perform with other different learning algorithms.

References

[1] M. Hatton, “IoT News - The IoT in 2030: 24 billion connected things generating $1.5 trillion - IoT Business News,” 2020. [Online]. Available: https://iotbusinessnews.com/2020/05/20/03177-the-iot-in-2030-24-billion-connected-things-generating-1-5-trillion/. [Accessed: 10-Nov-2020].

[2] Help Net Security, “New wave of attacks aiming to rope home routers into IoT botnets.” [Online]. Available: https://www.helpnetsecurity.com/2020/07/17/home-routers-iot-botnets/. [Accessed: 10-Oct-2020].

[3] L. Wood, “Global Internet of Things (IoT) Security Market Outlook 2020-2025 - Increasing Ransomware Attacks on IoT Devices and Growing IoT Security Regulations Driving Market Growth.” .

[4] A. Costin and J. Zaddach, “IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies,” *BlackHat USA*, pp. 1--7, 2018.

[5] A. Shoemaker, “How to Identify a Mirai-Style DDoS

Attack," *Imperva Incapsula Blog*, 2017. [Online]. Available: https://www.incapsula.com/blog/how-to-identify-a-mirai-style-ddos-attack.html. [Accessed: 30-Oct-2020].

[6] Devry Jane, "Mirai Botnet Infects Devices in 164 Countries - Cybersecurity Insiders," *Cybersecurity Insiders*, 2019. [Online]. Available: https://www.cybersecurity-insiders.com/mirai-botnet-infects-devices-in-164-countries/. [Accessed: 06-Nov-2020].

[7] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in *Proceedings of the Second IEEE International Conference on Computational Intelligence for Security and Defense Applications*, 2009, pp. 53–58.

[8] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation," in *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, 2011, pp. 29–36.

[9] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset," 2018.

[10] H. Altwaijry and K. Shahbar, "(WHASG) automatic SNORT signatures generation by using honeypot," *J. Comput.*, vol. 8, no. 12, pp. 3280–3286, 2013.

[11] A. H. Almutairi and N. T. Abdelmajeed, "Innovative Signature Based Intrusion Detection System," pp. 114–119, 2017.

[12] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Futur. Gener. Comput. Syst.*, vol. 80, no. March, pp. 157–170, 2018.

[13] M. Domb, E. Bonchek-Dokow, and G. Leshem, "Lightweight adaptive Random-Forest for IoT rule generation and execution," *J. Inf. Secur. Appl.*, vol. 34, pp. 218–224, 2017.

[14] L. Breiman, J. H. Friedman, R. A. Olshen, and C. J. Stone, "Classification and regression trees," *Classif. Regres. Trees*, vol. 1, no. February, pp. 1–358, 2017.

[15] S. Taheri and M. Mammadov, "Learning the naive bayes classifier with optimization models," *Int. J. Appl. Math. Comput. Sci.*, vol. 23, no. 4, pp. 787–795, 2013.

[16] S. Lei, "A feature selection method based on information gain and genetic algorithm," in *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, 2012, vol. 2, pp. 355–358.

[17] Y. Meidan *et al.*, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," vol. 13, no. 9, pp. 1–8, 2018.