Botnets Attack Detection Using Machine Learning Approach for IoT Environment

Chaw Su Htwe¹, Yee Mon Thant¹ and Mie Mie Su Thwin²

¹Cyber Security Lab, University of Computer Studies, Yangon, Myanmar.
²Department of Information Science, University of Computer Studies, Yangon, Myanmar.
Email: {chawsuhtwe, yeemonthant, drmiemiesuthwin}@ucsy.edu.mm

Abstract. The era of the Internet of Things (IoT) is very rapidly developing with millions of devices that are useful in the smart home, smart city, and many other smart systems for education, organization and so on. On the other side, attackers are mostly targeting these devices. After infecting the malware attacks on these devices, they become bots that are controlled by attackers, and these will be targeted to the organizations not only for stealing important information but also for breaking down the network. Although some security mechanisms have developed to protect against cyber-attacks, most such systems are rule-based systems, like public IDS systems. And also, the formal rule-based detection could be circumvented by the malware attackers’ knowledge. Therefore, the machine learning-based detection scheme is the replacement for the lack of previous detection techniques. The proposed detection architecture is based on machine learning methodology, like the CART algorithm and public IDS dataset, named N-BaIoT. The experimental results indicate that the detection accuracy of the selected classifier, CART is significantly better than that of the Naïve Bayes classifier, and the overall detection rate using CART is reached up to 99%.

1. Introduction
In recent years, there are much malware is targeting IoT devices. Therefore, it is needed to develop and implement an effective detection system. Although there are many previous detection systems, it is not enough to detect all kinds of attacks effectively because of the emergence of the new variant type of malware. In general, they are classified into two main categories, such as misused and anomaly-based detection systems. According to the detection architecture, it can be classified by a host-based detection system and the network-based detection system.

IoT (Internet of Things) has already been implemented and our world will become more comfortable and more efficient. According to the Cisco Visual Network Index (VNI), the Compound Annual Growth Rate (CAGR) of mobile data traffic will grow at 47 percent from 2016 to 2021, reaching 49 exabytes per month by 2021 [1]. In the growth of mobile and IoT infrastructure, the more challenging of cyber-security problems occur. Internet of Things devices are being targeted by cyber-attacks over 2016, the average of IoT device was attacked once every two minutes.[2]. The interest of Cybercriminals in IoT devices continues to grow, and many malwares attacking for smart devices picked up to three times in 2017. Kaspersky Lab has collected 121,588 malware samples in 2018 [3].

Misuse based detection also called signature-based detection that is implemented by monitoring network activities and looking for matches with the existing attack signatures. Most of the public detection system used that kind of detection system. Basically, the misused-based detection system can detect the attack based on the attack signatures which is already stored in their database. This detection scheme can’t recognize the unknown attacks. Another detection mechanism, anomaly
detection systems can identify unknown attack detection capability. However, this mechanism has a high number of false-positive alarm, and it is really hard for implementing in the IoT environment because of the complex nature of the IoT devices.

The machine learning-based detection is the possible detection mechanism because it can detect the essential differences of attacks. Although there are many previous kinds of research were implemented by using machine learning methodologies, most of them are using outdated datasets, mainly KDDCUP 99 and KDD NSL. These datasets have outdated records, and there is a lack of IoT attack records. Therefore, the modern dataset [8], called N-BaIoT can also be used to build the detection model. This dataset has ten attack classes and one benign class that are captured on the IoT devices by running the malware (botnets) such as Mirai and Gafgyt.

Machine learning is a subset of Artificial Intelligence (AI) in the field of computer science that frequently utilizes factual strategies to enable computer to learn with information. It could understand how to program them to learn, to improve automatically with experience, and its impact would be dramatic. Decision tree (CART algorithm) is one of the popular machine learning methods to get high detection rates and light processing for the cyber-attack protection system.

The proposed detection system is intended to develop an effective detection system using machine learning methodology. It is also intended to implement the detection system by using the effective features from public datasets which were captured by running malware samples on real IoT devices. The primary objective of the research is to get an effective detecting system which is the highest detection accuracy for protecting the smart environment.

The paper is organized with five sections. The current challenging of cyber-attacks and the detection systems were introduced in this section. The related work of the cyber-attack detections researches will be addressed in section 2. Moreover, the background methodology will be presented in section 3. The experiment results will be discussed in section 4. Finally, the discussion will be concluded in section 5.

2. Related Work
Most of the previous IDS researches [4–6] used KDDCUP 99 dataset and machine learning algorithms were used for implementing the detection system. Another popular dataset, the variant of KDDCUP 99, named KDD-NSL dataset was also used in IDS researches [5,7,8]. Obviously, such datasets are too outdated and not enough for the modern attack distribution of the data. In recent years, as more and more IoT devices are actually deployed, IDS in IoT environments has been attracting attention from many researchers and developers. The researches [9,10] addressed specific types of threats targeting specific devices.

The previous signature-based IDS systems were implemented by many kinds of research [11–13], there is still needed to get the effective system for IoT devices. The studies [14,15] showed that formal snort rules are not sufficient for the detection system, and their proposals were focused on a traditional network. Although the rule generation proposals [16,17] were for the IoT environment, their work was based on static analysis.

Some previous researches are based on artificial neural networks (ANN) such as the back-propagation algorithm [15,18] and anomaly-based replicator neural network [16]. Some anomaly-based IDS were implemented with k-nearest neighbour (KNN) [6,13], the random forest (RF) algorithm [6], and Naïve Bayes (NB) [19]. Moreover, these datasets are for traditional networks and not for the IoT environment. Although there are many types of research for the detection of the cyber-attack, it is still needed an effective system of IoT environment because of the heterogeneous nature of IoT devices and the current challenges of botnet attacks.

3. Methodology
The well-known machine learning algorithm, classification and regression tree (CART) algorithm was used as the detection model. To evaluate the proposed detection system, Python libraries, especially the scikit learn was used. Firstly, the selected dataset is loaded to the learning program which is implemented by Python language. The one-third of the dataset is used for testing/validation and the remaining two-thirds is used for training. And then, the classification results which are based on the
CART algorithm are extracted by this tool. Finally, the evaluation results are calculated by equation (1).

\[
\text{Acc} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}
\]

Where, TP is true positive which indicates the number of attack class correctly classify, TN is true negative which indicates the number of benign/normal class correctly classify, FP is false positive which indicates the number of attack class wrongly classify and FN is false negative which indicates the number of benign/normal class wrongly classify. The python scripts with scikit-learn library are prepared for the performance evaluation. It can support to implement many machine-learning algorithms, including CART and NB.

3.1. CART

Leo Breiman et al. introduced the CART algorithm in 1984. A decision tree is constructed by recursive partitioning, starting from the root node, each node can be split into left and right child nodes. These nodes can then be further split and they themselves become parent nodes of their resulting children nodes. Classification and regression trees are for constructing prediction models from data. The models are gotten by recursively parcelling the information space and fitting a straightforward forecast model inside each segment. Thus, the parcelling can be spoken to graphically as a choice tree. Arrangement trees are intended for subordinate factors that take a limited number of unordered qualities, with expectation mistake estimated as far as misclassification cost and furthermore for subordinate factors that take consistent or ordered discrete qualities, with forecast blunder normally estimated by the squared distinction between the watched and anticipated qualities [20]. The pseudo-code for tree construction is shown in Figure 1.

Figure 1. The pseudo-code for tree construction

\[
\text{Gini} = 1 - \sum(P_i)^2 \tag{2}
\]

CART uses a generalization of the binomial variance called the Gini index; it is shown in equation (2). It stores the sum of squared probabilities of each class, i is from 1 to the number of classes.

3.2 Naïve Bayes

Naïve Bayes is a simple but surprisingly powerful algorithm for predictive modelling. The Naïve Bayes Classifier belongs to the family of probability classifier, using the Bayesian theorem. The reason why it is called ‘Naïve’ because it requires strong (naive) independence assumptions between the features [21]. Naïve Bayes Equation is shown in equation (3).

\[
P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{3}
\]

Naïve Bayes classifier can be trained easily and fast and can be used as a benchmark model. When variable selection is carried out properly, Naïve Bayes can perform as well as or even better than other statistical models.

4. Experiments

The experiments are done by using python language to implement the detection architecture with machine learning classifier, and the IoT botnet attacks dataset, N-BaIoT is used for evaluation the proposed system.
4.1. Proposed Detection Architecture
The architecture of detection is shown in Figure 1. There are three main parts in this system. Firstly, the system extracts the features from incoming traffic pattern. After extracting the required features, these features will pass through the detection phase. It is the main part of the proposed system. For the detection phase, CART algorithm is used to build the detection model, and also it is used for classification the incoming patterns/features as attack or normal. The desirable number of instances from selected dataset are used for building the detection model with machine learning classifier, CART algorithm. Finally, it will generate the alert if the system decided the incoming traffic pattern as attack. The high true-positive rate is very essential, and also the false alarm rate is need to be cautious for the implementation of effective detection system.

![Figure 2. The botnets attack detection architecture](image)

4.2. Dataset
The selected dataset, called N-BaIoT [22], was used for the detection system. This dataset has 115 features which are including output class. The output class one benign class and ten types of attacks class. The traffic data were collected by running two botnet attacks, Mirai and BASHLITE. There are 115 features involved in the N-BaIoT dataset [22]. Although there are nine kinds of IoT devices records in this dataset, Home_XCS7_1002_WHT_Security_Camera is selected for this analysis. This dataset has 859,255 traffic records, including 111k ack, 45k scan, 125k syn, 151k udp, 78k udpplain, 54k combo, 28k junk, 27k scan, 88k tcp, 103k udp and 42k benign.

4.3. Evaluation Results
The experiment results are based on the implemented program which is created by python language for the CART and Navie Bayes algorithm. The detection approach is separately done on each kind of attack class. The 34% (292,147 records) of the dataset is randomly selected for testing by the scikit-learn library and the remaining part (567,108 records) are for training.

The confusion matrices of the two classification algorithms for Mirai and Gafgyt attacks are listed in Figure 3 and 4. These results show that there are true-positive, true-negative, false positive and false negative values by using the CART and NB algorithm for the detection of botnet attacks on IoT. The detection for the Mirai botnet attack using Naïve is shown in Figure 3 (a). This algorithm can only correctly classified as the 108 out of 8,536 benign traffics. This means there are large amount of false-positive alarms will be generated if the Naïve Bayes classifier is applied the proposed system. Moreover, the system cannot generate alarm for 32 out of 22,211ack attack, 21 out of 9,166 of scan attack, 29 out of 25,131 syn attack, 40 out of 30,459 udp attack, and 42 out of 15,668 udpplain class, respectively. This means, this will occur the significant false-negative classification on this system. Moreover, there are much amount of misclassification on each attack class even though the system classified as attack. As an example, there are 26 ack pattern as scan attack, and 22,153 ack pattern as udp class. Other attack classes classification is also same like the ack attack detection results. Therefore, it can be decided as Naïve Bayes classifier is not suitable for the proposed system.
Figure 3. Confusion Matrix of Mirai attacks detection using (a) Naïve Bayes, or (b) CART

According to the results show that the detection performance of CART is significantly better than that of using Naïve Bayes classifier. There is no false alarm in this experiment, and it can decide all benign traffic as benign. It has just a little rate for false detection, like one scan attack is classified as syn attack and two udpplain attack is classified as udp attack class. However, these results are acceptable because it just a misclassification on the attack classes, and these are detected as attack correctly. Therefore, the proposed system with CART is the best choice for detecting the Mirai botnet attack.

Figure 4. Confusion Matrix of Gafgyt attacks detection using (a) Naïve Bayes, or (b) CART

The Gafgyt attack detection performance with Naïve Bayes is shown in Figure 4 (a) and the performance of the system with CART is shown in Figure 4 (b), respectively. Naïve Bayes can only correctly classify 92 out of 8,713 benign traffic, but CART can correctly classify all of benign traffic. This means that there is no false alarm rate with CART implementation for detection Gafgyt attacks. Moreover, there is no false classification for all attack classes of Gafgyt on CART implementation. It has only small amount of misclassification between attack classes, e.g., two of combo attack class, three of junk attack class, five of tcp attack class and two of udp attack class, respectively. All of the results form Figure 3 and 4 show that the detection accuracy with CART implementation is significantly better than the implementation with Naïve Bayes algorithm.

According to the results, the average detection accuracy of Naïve Bayes is 58%, and the average detection accuracy of CART is 99% on the implementation of the detection system. All of the results show that the proposed system with CART is the suitable for the botnets attacks detection of IoT environment.
5. Conclusion
The IoT devices are very rapidly developed in recent years. On the other side, the attackers are more targeting these devices. They made the botnet attacks and the infected devices become bots that are controlled by bot-master. After that, they made a serious attack on the targeted systems and devices. Therefore, it is needed to implement an effective detection system for these devices. However, the most of popular systems, like public IDS are based on the signature-based system. That is, the bot-masters can circumvent the formal rule-based system. This paper compares the role of machine learning techniques for identifying and detecting the most challengeable attacks, botnets on the IoT environment. The proposed detection architecture is implemented by a simple decision tree algorithm, CART. The performance comparison of this algorithm is compared with the Naive Bayes algorithm. According to the accuracy results, the implemented system using machine learning of the CART algorithm is beneficial for detecting the cyber-attack on the smart environment.

6. References
[1] Cisco 2017 Cisco Visual Networking Index (VNI) Glob. Forecast Updat. 1–35
[2] Symantec 2017 Internet Security Threat Report
[3] Mikhail Kuzin, Yaroslav Shmelev V K 2018 New trends in the world of IoT threats Securelist Kaspersky Lab
[4] Aggarwal P and Sharma S K 2015 An empirical comparison of classifiers to analyze intrusion detection Int. Conf. Adv. Comput. Commun. Technol. ACCT 2015-April 446–50
[5] Samdani S and Shukla S 2017 A novel technique for converting nominal attributes to numeric attributes for intrusion detection 8th Int. Conf. Comput. Commun. Netw. Technol. ICCCNCT 2017 1–5
[6] Kushwaha P, Buckchash H and Balasubramanin R 2017 Anomaly based intrusion detection using filter based feature selection on KDD-CUP 99 Proc. 2017 IEEE Reg. 10 Conf. (TENCON), Malaysia 839–44
[7] Haddad Pajouh H, Javidan R, Khayami R, Ali D and Choo K-K R 2016 A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks IEEE Trans. Emerg. Top. Comput. 6750 1–1
[8] Subba B, Biswas S and Karmakar S 2016 A Neural Network based system for Intrusion Detection and attack classification 2016 22nd Natl. Conf. Commun. NCC 2016
[9] Cervantes C, Poplade D, Nogueira M and Santos A 2015 Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015 606–11
[10] Guo Z, Harris I G, Jiang Y and Tsaur L F 2017 An efficient approach to prevent battery exhaustion attack on BLE-based mesh networks 2017 Int. Conf. Comput. Netw. Commun. ICNC 2017 1–5
[11] Dhanabal L and Shantharajah D S P 2015 A Study On NSL-KDD Dataset For Intrusion Detection System Based On Classification Algorithms Int. J. Adv. Res. Comput. Commun. Eng. 4 446–52
[12] Ullah I, Shah M A, Wahid A and Waheed A 2017 Protection of enterprise resources: A novel security framework Int. Conf. Commun. Technol. ComTech 2017 98–103
[13] Bay S D, Kibler D, Pazzani M J and Smyth P 2000 The UCI KDD archive of large data sets for data mining research and experimentation ACM SIGKDD Explor. Newsl. 2 81–5
[14] Ganesan A, Parameshwarappa P, Peshave A, Chen Z and Oates T 2019 Extending Signature-based Intrusion Detection Systems WithBayesian Abductive Reasoning
[15] Shah S A R and Issac B 2018 Performance of intrusion detection systems and application of machine learning to Snort system Futur. Gener. Comput. Syst. 80 157–70
[16] Domb M, Bonchek-Dokow E and Leshem G 2017 Lightweight adaptive Random-Forest for IoT rule generation and execution J. Inf. Secur. Appl. 34 218–24
[17] Alhanahnah M, Lin Q, Yan Q, Zhang N and Chen Z 2018 Efficient signature generation for classifying cross-architecture IoT malware 2018 IEEE Conf. Commun. Netw. Secur. CNS 2018
[18] Kumar R and Sharma D 2018 HyINT: Signature-Anomaly Intrusion Detection System 2018 9th
Int. Conf. Comput. Commun. Netw. Technol. 1–7

[19] Smyth S D B D F K M J P P 2000 The UCI KDD Archive of Large Data Sets for Data Mining Research and Experimentation SIGKDD Explor. 2 81

[20] Breiman L, Friedman J H, Olshen R A and Stone C J 2017 Classification and regression trees Classif. Regres. Trees 1 1–358

[21] Taheri S and Mammadov M 2013 Learning the naive bayes classifier with optimization models Int. J. Appl. Math. Comput. Sci. 23 787–95

[22] Mirsky Y, Doitshman T, Elovici Y and Shabtai A 2018 Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection 18–21