A Slow DDoS Attack Detection Mechanism using Feature Weighing and Ranking

Yin Mon Swe
Department of Information Technology
Pyay Technological University
Myanmar
yimonswe24@gmail.com

Pye Pye Aung
Department of Information Technology
University of Technology-Yatanarpon Cybercity
Myanmar
pyepyeaung@gmail.com

Aye Su Hlaing
Department of Information Technology
Pyay Technological University
Myanmar
Ayesuhlaing.itptu@gmail.com

Abstract

A Denial of Service (DOS) attack is a continuous security risk in cyberspace. They are weaponized with advanced technologies and becoming more and more powerful as Distributed Denial of Service (DDoS) attacks. DDoS is one of the most occurring attacks nowadays and new methods are being needed to be able to detect such attacks. Attackers use many different techniques to perform DDoS attacks. Different DoS attack types has different characteristics and research is still needed to identify such attacks. In this paper, we analyse slow DDoS attack types (slowloris, slow http attack, etc) and propose a framework to detect them using machine learning techniques. We utilize gain-ratio and chi-squared ranking methods to select optimal feature subset for training detection mechanism. CICIDS2017 and CSE-CIC-*IDS* 2018 datasets are used to evaluate the proposed detection mechanism.

Keywords

Slow DDoS attacks, slowhttp, attack detection,classification, feature selection

1. Introduction

A denial-of-service attack(DoS) or Distributed Denial of Service (DDoS) is an attempt to make a machine or network resource unavailable to legitimate users. A Distributed Denial of Service (DDoS) attack can originate from multiple sources, making it far more difficult to detect and protect. Distributed Denial-of-Service (DDoS) attacks are a great threat on the Internet. Traditional DDoS attacks exhaust the bandwidth, CPU power, or memory of the victim host by flooding an overwhelming number of packets from thousands of compromised computers (zombies) to deny legitimate flows. On the other hand, slow or low-rate DDoS attacks are quite different from the traditional DDoS attacks, as their traffic pattern is similar to legitimate traffic. For example, a slow HTTP DDoS attack such as Slowloris does not rely on volume in causing denial-of-service, it will keep and hold as many connection ports opened as possible to prevent users from accessing the target servers. As a result, the attack can effectively cripple the target by sufficiently increasing the aggregated attack volume without being known by the detection systems. There are also other low-intensity attacks that do not seek to disrupt service entirely, but instead choose to degrade the service for a longer interval which effect the image of business.

A denial-of-service attack (DoS) or Distributed Denial of Service (DDoS) is an attempt to make a machine or network resource unavailable to its intended users. These attacks are occurred at various TCP/IP network layer with different behaviors and attacking techniques. Layer 3 DoS attacks generally focus on bandwidth consumption and have a variety of attack forms such as smurf attack, teardrop attack, TCP Syn flood attack, UDP attack, etc.

Traditional DoS attacks try to congest server with enormous amount of packets in a short period of time. In case of low-rate or slow DDoS, it tries to come in as normal traffic into the server and consumes server resources as long as possible while maintaining the connection active. Nowadays, there are also DoS attacks occurred at application layer (layer 7).

SlowHTTP attacks (Slow Header, Slowloris, Slow Read, Slow Post) - These attacks utilize HTTP request features and web server vulnerability to initiate DoS attacks. Attackers read or send data in small chunks, with intervals between reads and writes. It is familiar with normal request for web server and difficult to detect. Suroto 2017 explained how these attacks work in detail.

GoldenEye – It use both HTTP methods randomly. It sends HTTP headers with random quantity and normal values in Header content.

HULK (HTTP Unberable Load King) - HULK attack utilizes HTTP KeepAlive and NoCache features. HULK tool is designed to consume web servers' resources by continuously requesting single or multiple URL's from many source attacking machines.

Such kinds of slow or low rate DDoS attacks are difficult to detect since their traffic flow behaviour is similar to normal traffic. In this paper, we will explore in what way netflow features are useful to detect such kinds of attacks. We apply machine learning techniques to detect slow DDoS attacks.

1.1 Objectives

Traditional DoS attacks try to congest server with enormous amount of packets in a short period of time. In case of low-rate or slow DDoS, it tries to come in as normal traffic into the server and consumes server resources as long as possible while maintaining the connection active. Nowadays, there are also DoS attacks occurred at application layer (layer 7). Nowadays, slow application layer DoS attacks are becoming high risk and it needs effective mechanism to detect them accurately. In this paper, we focus on the slow DDoS attacks and use this data to detect slow rate DDoS attacks by using machine learning methods.

In recent years, attackers have moved towards the implementation of such application layer attacks because these are harder to be detected by the systems compared to network layer attacks. These attacks target specific application protocols being utilized by the target, many of which are prone to proven exploits. Research about detection of these kinds of attacks is still needed and therefore, in this paper, we build a detection mechanism that detect slow DDoS attacks. We analyse slow DDoS attacks in real-world dataset and build a mechanism that can classify slow DDoS attacks correctly. The experiments are done with real-world datasets.

2. Literature Review

Singh et al. (2017) used features like GET/POST requests and delta time to distinguish DDoS attack packets from normal ones. They used machine learning techniques and build a model based on their extracted feature data from simulated attacks. Zhou et al. (2017) proposed a slow DDoS attack detection method that is based on calculation of the expectation of future packet size and that is based on the distribution difference of the packet size of real DDoS attacks.

Rahman et. al. (2017) proposed a hybrid model that detect application layer DDoS attacks, HTTP-GET attack, HTTP-POST attack and Slow Read attack. They used clustering methods in their approach to identify attack traffic among normal traffic. Their approach was tested with attack datatset gathered from simulated attacks. Muraleedharan and Janet (2020) proposed a deep learning model to detects slow DoS attacks. His methods were evaluated with CICID 2017 dataset.

Siracusano et al. (2019) used TCP trace analysis tool and extracted 142 parameters from network traffic and used them to build attack detection models by using 6 machine learning algorithms. He used the CICID 2017 and his simulated dataset. Chad et al. (2019) tried to detect slow HTTP POST DoS attacks by using various machine learnging techniques. They performed attack in a live network and extracted Netflow features to be used in machine learning.

Dhanapal and Nithyanandam (2019), described the Slow HTTP Distributed Denial of Service Attack Detection in Cloud. The availability of cloud based online services is critical for businesses like financial services, e-commerce applications, etc.. Though cloud based applications are having potential threats of going down due to the slow HTTP Distributed Denial of Service (DDoS) attack in the cloud. The slow HTTP attacks intention is to

consume all the available server resources and make it unavailable to the real users. The slow HTTP DDoS attack comes with different formats such as slow HTTP headers attacks, slow HTTP body attacks and slow HTTP read attacks. Detecting the slow HTTP DDoS attacks in the cloud is very crucial to safeguard online cloud applications. This is a very interesting and challengingtopic in DDoS as it mimics the slow network. This paper proposed a novel method to detect slow HTTP DDoS attacks in thecloud. The solution is implemented using the OpenStack cloud platform.

There are many works done on CICID 2017 dataset but most works focus on finding methods to detect all attacks included in dataset by analyzing the flow data included in the dataset. Very few of them focus on the analysis of individual attack type. Since there are many types of DDoS attacks occurred nowadays and they have different behaviors and attacking forms, building a general detection mechanism that cover all kinds of DDoS attacks is not enough. Therefore, the purpose of this paper is to analyze various flow data extracted from slow DDoS attacks traffic and build a model that can detect slow DDoS attacks.

3. Methods

SlowHTTP attacks (Slow Header, Slowloris, Slow Read, Slow Post) - These attacks utilize HTTP request features and web server vulnerability to initiate DoS attacks. Attacker read or send data in small chunks, with intervals between reads and writes. It is familiar with normal request for web server and difficult to detect. Suroto (2017) explained how these attacks work in detail.

A slow HTTP Denial of Service attack (DoS), otherwise referred to as the Slowloris HTTP attack, makes use of HTTP GET requests to occupy all available HTTP connections permitted by a web server. It takes advantage of a vulnerability in thread-based web servers, which wait for entire HTTP headers to be received before releasing the open connection. A variation of this vulnerability is the slow HTTP POST vulnerability. In a slow HTTP POST attack, the attacker declares a large amount of data to be sent in an HTTP POST request and then sends it very slowly.

A malicious user can open many connections to the server by initiating HTTP requests but not closing them. If the attacker keeps every HTTP request open and feeds the server unreal data before the timeout is reached, the HTTP connection will remain open until the attacker closes it. Then, if the attacker occupies all available HTTP connections for a web server and keeps them busy waiting, new connections cannot be more processed by the server and this causes a denial of service to intended users.

This technique lets an attacker consume server resources and restrict access using very little bandwidth. This type of DoS attack is different from other DoS/DDoS attacks such as SYN flood attacks, which misuse the TCP SYN (synchronization) segment during a TCP three-way handshake. Therefore, this kind of attacks needs separate analysis and detection techniques. In this paper, we will find out what kind of flow data is important to detect these kinds of attacks and experiment and build a detection model by using machine learning techniques to classify various slow DDoS attacks.

The first step of our approach starts with analyzing and selection flow data features to know what feature is most significant to be able detect such attacks. We used CICIDS2017 (Sharafaldin et al. 2018) and (CSE-CIC-IDS2018) datasets to test our proposed approach. All flow data in the datasets are numerical types. The datasets consist of 82 flow features extracted by CIC Flow Meter tool. Using all features with a large dataset to build a classifier model is not cost effective and not all of 82 features is useful for our detection mechanism. Therefore, in order to build a slow DDoS detection mechanism by using machine learning algorithms, we start with optimal feature selection.

3.1 Optimal Feature Selection

The proposed system builds a classifier that can detect slow DDoS attacks by using machine learning techniques. According to Das and Behera (2017), machine learning is a learning process which creates a mathematical model to predict results or define a classification by using past data. Past data is fed to the learning process as large dataset and usually contains a lot of features.

Feature selection and feature engineering step is an important step in the machine learning process. Not all of features in a dataset is useful for machine learning. Using all features to build a prediction model is not only ineffective for cost of the system but also takes longer to build a model. First, data need to be normalized, de-duplicated or fix errors for unbalanced data as needed.

Choosing Optimal Attribute is important that distinguish abnormal traffic from normal ones. Dataset like DDoS attack traffic will be enormous in real world. And to train such large datasets with a lot of features, we need

to filter useless or unimportant attributes from the dataset. Moreover, useless or unimportant attributes can disturb the performance of detection mechanism. The CICIDS2017 and CSE-CIC-IDS2018 DDoS datasets have rather imbalanced class of attacks. The datasets contain features that are not useful for attack detection.

Therefore, as the first step of our machine learning process, we used gain ratio based feature selection method to choose optimal features among 80 features. Table 1 is the weights of 30 features. We chose 30 features with highest value first. In this way, we eliminate the unimportant features for detection. Table 1 list the 30 highest gain ratio weights of features.

Table 1. 30 Selected Features from Dataset

Feature	Weight	Feature	Weight
Fwd Seg Size Min	0.867	Subflow Fwd Pkts	0.49
Init Fwd Win Byts	0.705	Tot Fwd Pkts	0.49
SYN Flag Cnt	0.631	Subflow Bwd Pkts	0.474
Fwd PSH Flags	0.631	Tot Bwd Pkts	0.474
Active Std	0.575	Idle Std	0.452
TotLen Bwd Pkts	0.564	Fwd Pkt Len Max	0.435
Subflow Bwd Byts	0.564	TotLen Fwd Pkts	0.428
Init Bwd Win Byts	0.559	Subflow Fwd Byts	0.428
Bwd Pkt Len Max	0.555	Fwd Pkt Len Mean	0.42
Fwd Header Len	0.544	Fwd Seg Size Avg	0.42
Bwd Seg Size Avg	0.524	Fwd Pkt Len Std	0.4
Bwd Pkt Len Mean	0.524	Pkt Len Std	0.399
Bwd Pkt Len Std	0.523	Pkt Len Var	0.399
Bwd Header Len	0.508	Fwd Pkt Len Min	0.376
Pkt Len Max	0.502	PSH Flag Cnt	0.363

Then, as the second step, Dr. Janabi, and Kadhim (2018) chi-squared method is used to rank the features as of relevance. The purpose is to choose most relevant features to be used for training and eliminate otherwise. In machine learning, it evaluates the worth of an attribute by computing the chi-squared statistic regarding to the class. The higher the Chi-Square value, the feature is more dependent on the class and it can be selected for model training. Therefore, by ranking the features by chi-squared values, we can get the most outstanding features suitable for training classifiers.

In this paper, we select 10 features with highest chi-squared rank among 30 features from the previous step. Table 2 shows the Chi-Square weight of 10 selected features.

Table 2. Feature set with highest rank

Init Fwd Win Byts	8187840.196
Pkt Len Std	5596085.59
Pkt Len Var	5590878.238
Fwd Header Len	5128581.694
Fwd Pkt Len Max	5020564.179
Bwd Header Len	4953862.854
TotLen Fwd Pkts	4884683.308
Subflow Fwd Byts	4884683.308
Fwd Pkt Len Mean	4877617.503
Fwd Seg Size Avg	4877617.503

Figure 1 descries the system flow of the proposed detection mechanism. The proposed system will do preprocessing of the training data first. We remove useless features from the dataset according to their gain ration weights shown in Table 1. Then the next step is selection of more relevant features for attack detection by Chi-squared ranking values shown in Table 2. After this preprocessing step, the training dataset has the optimal features only which is relevant for attack detection, the next step is building classifier models by using various machine learning algorithms. And the final step is testing the classifiers with the test dataset to know the performance of the proposed mechanism.

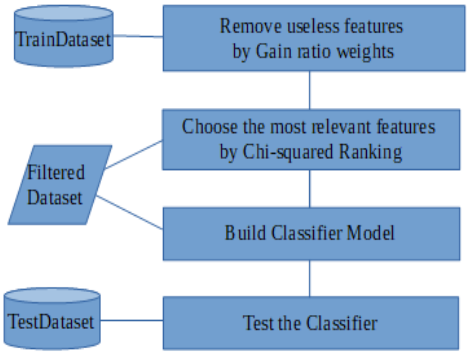


Figure 1. System Flow of the Detection Mechanism

3.2 Selection of Classifiers

After selecting optimal feature subsets, we use the dataset to build classification models by using different machine learning techniques. We run learning with common supervised learning techniques; J48, Random Forest (RF), KNN, MLP, PART to exploit the performance of different kind of learning models.

J48 Decision Tree classifier Mohammed et al.(2016) which is one of the widely-used algorithms in classification and regression problems. A decision tree creates a tree like structure where each node of the tree represents a feature, each link represents a decision (rule) and each leaf represents a possible outcome. Compared to other classifiers, Decision Tree is the easiest to understand and interpret.

Random forest, Mohammed et al.(2016), is a supervised learning algorithm. The "forest" it builds, is an ensemble of decision trees. In our experiment, we trained Random forest with the “bagging” method. The general idea of the bagging method is that a combination of learning models increases the overall result.

K nearest neighbor’s algorithm is a simple supervised learning algorithm that trains on all available cases and stores them and classifies a new case based on distance function between new case and stored cases. This algorithm works by classifying a new case on the basis of majority votes of its neighbors. Thus a case is assigned to a class most common among its ‘K’ nearest neighbors which are discussed in Mohammed et al.(2016).

According to Mohammed et al.(2016) ,Multilayer Perceptron are usually used in supervised learning. They train on a set of input-output pairs and try to learn the correlation (or dependencies) between those inputs and outputs.

PART is a separate-and-conquer rule learner, Vijayarani and Divya (2011). PART builds a partial C4.5 decision tree and makes the best leaf into a rule. PART is known as an efficient algorithm for generating rules.

3.3 Proposed System Set-up

1. Split 70% Dataset(D) for train and 30% test(T)
2. Perform Useless Feature Removal
   (i) Calculate gain-ratio weights of attributes
   (ii) Select 30 features with highest weights from D
3. Apply chi-squared feature ranking on the training dataset, D
   (i) Select 10 features with highest chi-squared value from D
4. Train a classifier model by using the training dataset, D
6. Test the classifier by using testing dataset, T
7. Evaluate performance and accuracy of classifier

4. Dataset

To train the proposed slow DDoS detection mechanism, we use the blended dataset of CICIDS2017 and *CSE*-CIC-IDS2018 datasets. These datasets contain the latest DDoS attack types. Both dataset includes various attacks not only DoS attacks. In this paper, we focus on various slow DDoS attacks only. The dataset contains net flow data extracted from PCAP files by CICFlowMeter. It is meant for research, as a benchmark for developing detection and mitigation methods.

CICIDS2017 is a dataset that contains various attacks such as Brute force FTP, Web Attack, Infiltration, DoS attacks, etc. We focus on DoS and DDoS attacks in this paper. The DDoS and DoS attacks are labeled DoS Slowloris, DoS Slowhttptest, DoS Hulk, DoS Goldeneye, and DDoS. Normal traffic is labeled as 'Benign'. Table 3 lists the numerical amount of traffic of these slow DDoS attacks.

Table 3. CICIDS2017 Statistics

Attack Type	Number of traffic
Benign	2,273,098
DoS Slowloris	5796
Slowhttptest	5499
DoS Hulk	231073
DoS GoldenEye	10293
DDoS LOIC-HTTP	128027

CSE-*CIC*-IDS2018 dataset contains the same attack types as *CICIDS2017* dataset with two additional DDoS attacks: DDoS LOIC and DDoS HOIC attacks. It also includes other attack types. Only DDoS attacks are shown here. The number of traffics included in the CSE-CIC-IDS2018 dataset is listed in Table 4.

Table 4. CSE-CIC-IDS2018 Dataset Statistics

Attack Type	Number of traffic
Benign	7372557
DoS Slowloris	10990
Slowhttptest	139890
DoS Hulk	461912
DoS GoldenEye	41508
DDoS LOIC-HTTP	576191
DDoS HOIC-HTTP	686012

As described in the tables Table 3 and Table 4, number of instances in attack types is rather imbalanced with the attack types. Especially the number of Benign traffic (normal traffic) in each dataset is significantly larger than the other attack traffics. Therefore, we use sampling method to get subset of Benign traffic since it is dramatically larger than that of other attacks. Then, to get a balanced dataset, we combined these two datasets as one dataset. And we use 70 % of dataset as training dataset and 30% as testing dataset. Table 5 describes the individual number of records in our combined dataset. The combined dataset is divided randomly into 70% for training and 30% for testing.

Table 5. Combined Dataset of Slow DoS Attacks

Attack Type	Number of traffic
Benign(normal)	446772
DoS Slowloris	16786
Slowhttptest	145389
DoS Hulk	692985
DoS GoldenEye	51801
DDoS attack-HOIC	686012
DDoS LOIC-HTTP	576190

5. Results and Discussion

Experiments are performed on a computer with corei7 processor and 8 GB RAM. We use Weka machine learning framework to implement classifiers. To evaluate performance and accuracy of classifiers, the precision, recall and F1 score are calculated.

Precision is the proportion of true positives from all instances that are predicted as positive and is given by

Precision = TP/(TP+FP).

Recall is the proportion of true positives from all instances that are actually positive and is calculated as

Recall = TP/(TP+FN).

F-measure is the weighted average of precision and recall and is calculated as

f_measure=2*(Recall * Precision) / (Recall + Precision)

where **TP (true positive rate)** is the number of DDoS attacks correctly detected as attacks by classifier, **FP (false positive rate)** is the number of normal traffic that is incorrectly classified as attacks and **FN (false negative rate)** is the number of attack traffic that is incorrectly classified as benign.

5.1 Numerical Results

Table 6 and Table 7 list precision and recall of each classifier model for the individual attack types. Among the tested classifier algorithms, it is found that j48, bagging with RF and PART classifiers got highest scores showing that it can detect the slow DDoS attacks well in combination with double feature selection process.

Table 6. Precision Values of Classifiers

Benign	1	1	0.996	1	1
DoS GoldenEye	0.996	0.996	0.981	0.996	0.869
DoS Slowloris	0.996	0.997	0.971	0.997	0.952
DoS Slowhttptest	1	1	0.971	1	0.985
DoS Hulk	1	1	0.948	1	0.993
DDOS attack-HOIC	1	1	0.998	1	1
DDoS attacks-LOIC-HTTP	1	1	1	1	1

Table 7. Recall Values of Classifiers

Benign	1	1	0.99	1	0.998
DoS GoldenEye	0.999	0.999	0.619	0.999	0.948
DoS Slowloris	1	1	0.731	0.999	0.749
DoS Slowhttptest	1	1	0.985	1	0.993
DoS Hulk	1	1	0.999	1	0.99
DDOS attack-HOIC	1	1	1	1	1
DDoS attacks-LOIC-HTTP	1	1	0.974	1	1

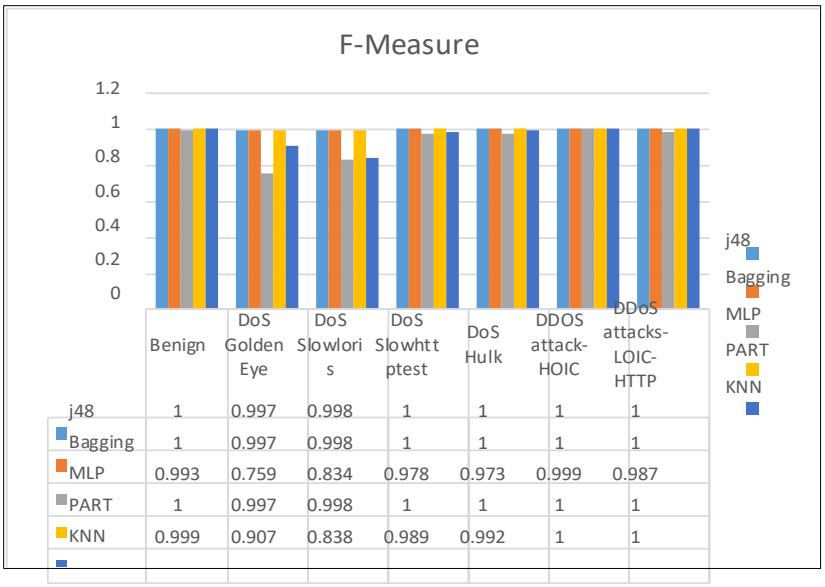
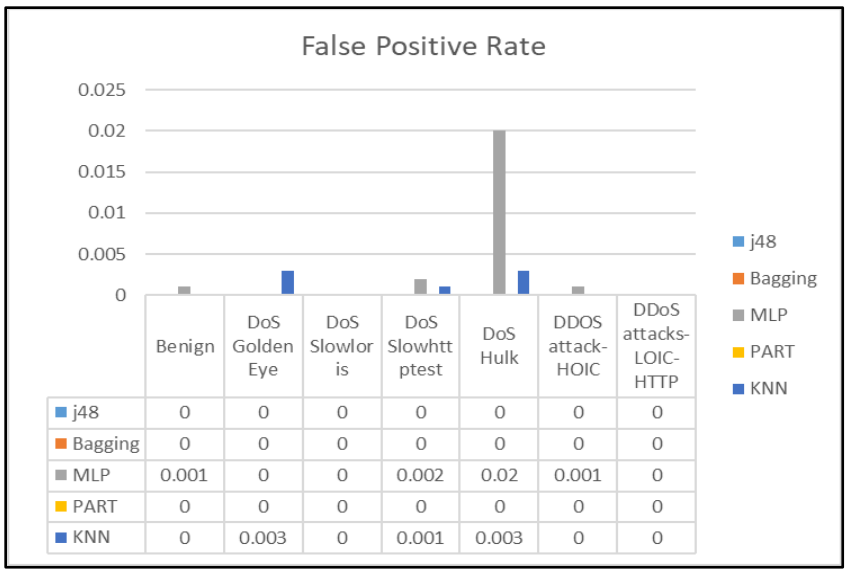


Figure 2. F-Measure of classifiers

As shown in Figure 2, all of the classifiers can detect fully DoS Hulk, DoS slowhttptest, DDoS attack-HOIC, LOIC-HTTP attacks with 0.99 to 1 F-measure values. There's some variation in detection of GoldenEye and Slowloris attacks such as 0.725 and 0.929 with MLP and 0.874 and 0.874 with KNN respectively.

When detecting network attacks, it is important to detect all attacks (true positive rate) and pass the normal traffic correctly. The number of normal traffic that incorrectly classified as attacks (false positive rate) and the number of attack traffic that incorrectly taken as normal traffic (false negative) play a vital role when measuring a detection mechanism. High false positive and false negative values could lead the lower performance as the system cannot serve the normal request. According to Figure 3 and Figure 4, the classifiers with double feature selection method in this paper have very few incorrect classification results. According to above statistics, J48, bagging with RF and PART classifiers outperforms MLP and KNN classifiers in terms of classification errors.

Figure 3. True Positive Rate (correctly classified instances in all attacks)



	Benign	DoS Golden Eye	DoS Slowloris	DoS Slowhttptest	DoS Hulk	DDOS attack-HOIC	DDoS attacks-LOIC-HTTP
j48	0	0	0	0	0	0	0
Bagging	0	0	0	0	0	0	0
MLP	0.001	0	0	0.002	0.02	0.001	0
PART	0	0	0	0	0	0	0
KNN	0	0.003	0	0.001	0.003	0	0

Figure 4. False Positive Rate (incorrectly classified attacks)

6. Conclusion

In this paper, slow DDoS attacks are analysed and a detection mechanism using netflow features is proposed. The proposed system used gain ratio and chi-squared ranking to select optimal subset of features from the large dataset with a lot of features. The proposed system was tested with the CSE-CIC-IDS 2017 and 2018 dataset and the experimental results shows that our proposed mechanism can detect slow rate attack with 99% accuracy and with very low false-negative rate. In the future, the proposed methods can be explored to test with different and real-world datasets. Moreover, slow DDoS mitigation techniques using the selected flow features can be explored.

Acknowledgements

I would like to express my deepest gratitude and sincere appreciation to the following persons, whose guidance aided towards the competition of this paper. First of all, I would like to thank **Dr. Pye Pye Aung** for her valuable suggestion and excellent comments. Special thanks are extended to **Dr. Aye Su Hlaing** for her kind permission, and precious guidance to conduct this paper. I would like to thank my parents, teachers and all of friends for their support and encouragement throughout this paper.

References

A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018), Available: https://registry.opendata.aws/cse-cic-ids2018/

Das, K., and Behera, R., N., A Survey on Machine Learning: Concept, Algorithms and Applications, *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no.2,pp.1301-1309, 2017 .

Dhanapal, A., and Nithyanandam, P., The Slow HTTP Distributed Denial of Service Attack Detection in Cloud, School of Computing Science and Engineering, VIT University,vol. 20, no. 2, pp. 285–297,2019.

Dr. Janabi, K. B. S. A and Kadhim, R**.**, Data Reduction Techniques: A Comparative Study for Attribute Selection Methods*, International Journal of Advanced Computer Science and Technology*, vol. 8, no. 1, pp. 1-13,2018

Mohammed , M. , Khan, B., M., and Bashier, E., B., M*., Machine Learning: Algorithms and Applications*, 1st edition, CRC Press, July 18,2016.

Muraleedharan, N., and Janet, B., A deep learning based HTTP slow DoS classification approach using flow data, *ICT Express,* https://doi.org/10.1016/j.icte.2020.08.005, 2020.

Rahman, M. A., Sarker, B. R., and Escobar, L. A., Peak demand forecasting for a seasonal product using Bayesian approach, *Journal of the Operational Research Society*, vol. 62, pp. 1019-1028, 2011.

Rahman, R., Tomar, D., S., and Jijin, A.,V., Application Layer DDOS Attack Detection Using Hybrid Machine Learning Approach**,** *International Journal of Security and Its Applications*, vol. 11, no. 4 , pp.85-96, 2017.

Sharafaldin, I., Lashkari, A., H., and Ghorbani, A. Ali ,Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization, *In Proceedings of the 4th International Conference on Information Systems Security and Privacy* , pp. 108-116,2018.

Singh, K., J., and De, T., An Approach of DDOS Attack Detection Using Classifiers, *Emerging Research in Computing, Information,Communication and Applications*, pp. 429-437,2017.

Suroto, A Review of Defense Against Slow HTTP Attack, *International Journal on Informatics Visualization*, vol.1, no. 4, pp. 127-134,2017.

Siracusano, M., Shiaeles, S., and Ghita, B., Detection of LDDoS Attacks Based on TCP Connection Parameters, Available:https://www.researchgate.net/publication/330945504_Detection_of_LDDoS_Attacks_Based_on_TCP_Connection_Parameters,2019.

Vijayarani, S. and Divya, M., An Efficient Algorithm for Generating Classification Rules, *International Journal of Computer Science And Technology*, vol.2, no.4, pp.512-515,2011.

Zhou, L., Liao, M., Yuan, C., and Zhang, H., Low-Rate DDoS Attack Detection Using Expectation of Packet Size, *Security and Communication Networks*, pp 1-14, 2017.

Yin Mon Swe is working as an associate professor at Pyay Technological University, Myanmar, having research and teaching experiences of more than 8 years. She graduated Bachelor of Engineering (Information Technology) from Technological University (Pathein) in 2006.And then, she received Master of Engineering (Information Technology) at Mandalay Technological University in 2011 where she received Ph.D degree in 2015. She has research interests mainly concern DDoS attack detection, machine learning, digital image processing and Information technology engineering.

Dr. Pye Pye Aung received B.E in Engineering (Information Technology) from Technological University (Toungoo) in 2006 and also received M.E in 2009. She holds Ph.D degree in Information Technology (IT) from University of Technology (Yatanarpon Cyber City) in 2014 where she currently serves as an associate professor in Faculty of Information and Communication Technology(ICT). She has a research interest in machine learning, networking and security, Information technology engineering.

Dr. Aye Su Hlaing is currently working as a professor at IT Department in Pyay Technology University. She received her bachelor, master and doctoral degrees at Mandalay Technological University and Yangon Technological University in 2002, 2004 and 2007 respectively. She is giving advice to graduate and post graduate students in networking and network security fields. Moreover she is a member in Board of Subjects for Technological Universities in myanmar and also a Technical Member of ICICSP 2018 and ICICSP2019 (IEEE International Conference on Information Communication and Signal Processing (ICICSP)