Bulletin of Electrical Engineering and Informatics
ISSN: 2302-9285
Vol. 6, No. 2, June 2017, pp. 140~148, DOI: 10.11591/eei.v6i2.605

Review of Detection DDOS Attack Detection Using Naive Bayes Classifier for Network Forensics

Abdul Fadil[1], Imam Riadi[2], Sukma Aji*[3]
[1]Department of Electrical Engineering Ahmad Dahlan University, Yogyakarta, Indonesia
[2]Department of Information System Ahmad Dahlan University, Yogyakarta, Indonesia
[3]Master Program of Information Technology Ahmad Dahlan University, Yogyakarta, Indonesia
*Corresponding author, e-mail: fadlil@mti.uad.ac.id[1], imam.riadi@is.uad.ac.id[2], sukma.aji@staff.uad.ac.id[3]

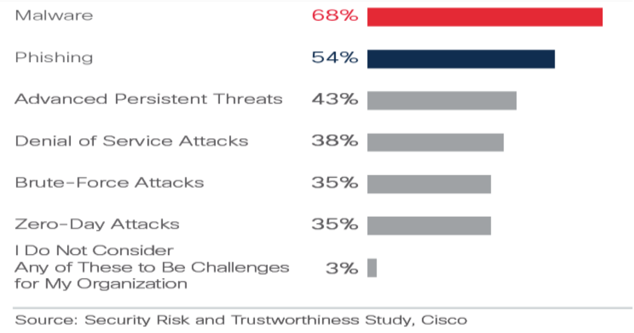
Abstract

Distributed Denial of Service (DDoS) is a type of attack using the volume, intensity, and more costs mitigation to increase in this era. Attackers used many zombie computers to exhaust the resources available to a network, application or service so that authorized users cannot gain access or the network service is down, and it is a great loss for Internet users in computer networks affected by DDoS attacks. This research proposed to develop a new approach to detect DDoS attacks based on network traffic activity were statistically analyzed using Gaussian Naive Bayes method. Data will be extracted from training and testing of network traffic in a core router at Master of Information Technology Research Laboratory Ahmad Dahlan University Yogyakarta (MITRLADUY). The new approach in detecting DDoS attacks is expected to be a relation with Intrusion Detection System (IDS) to predict the existence of DDoS attacks based on average and standard deviation of network packets in accordance with the Gaussian method.

Keywords: *DDoS, Gaussian, Naive Bayes, average, standard deviation*

1. Introduction

Cisco 2016 Annual Security Report [1] showed DoS attacks still top the External Challenges Faced. Respondent does not Consider any of these to be challenges in the organization with 3 %, Zero-Day Attacks and Brute Force with 35 %. Whereas DoS leads the chart of the External Challenges Faced with 38 %, ahead Advanced Persistent Threats 43 %, Phishing 54 %, and Malware 68 %. It shows that DDoS attacks are still interesting to investigate. Figure 1 shows the Cisco statistic about External Challenges Faced.



Source: Security Risk and Trustworthiness Study, Cisco

Figure 1. External challenges faced

Jasreena Kaur Bains et al [2] propound model used Naive Bayes Classifier with K2 Learning process on reduced NSL KDD data set for each attack class. In this method, every layer is individually trained to detect a single type of attack category and the outcome of one layer to increase the detection rate and for better categorization of both the majority and minority attacks.

Received March 3, 2017; Revised May 4, 2017; Accepted May 18, 2017

Mangesh D. Salunke and Ruhi Kabra [3] used Naive Bayes Classifier and Artificial Neural Network to detect the DDoS attack. They are proposed system is divided into two modules. First Training Set Generation, create a database for future use. All incoming packets are going through each level of training set generation and create dynamic data set and mark the incoming packet as “OK packet” or “Attack”. And then the second module is Real-Time Layered Intrusion Detection System, applying K-means clustering and Naive Bayes algorithm for data mining and classification algorithm to classify the attack as SYN flood, PING flood, UDP flood.

Kanagalakshmi R. and Naveenantony Raj [4] used Hidden Naive Bayes Multiclass Classifier Model on network Intrusion Detection System for struggling progressively sophisticated network attacks. Bharti Nagpal et al [5] comparing many software DDoS attacks that showing complete information of the software DDoS attacks. V. Hema and C. Emily Shin [6] used Naive Bayes to calculate DoS attacks comparing Detection Rate and rate False Positive with the achievements by the proposed and existing systems. Mangesh Salunke at al [7] used K-means Clustering and Naive Bayes to classifying DDoS attacks with number of the malicious packets correctly classified as malicious in True Positive (TP), number of normal traffic falsely classified as malicious in False Positive (FP), when the malicious traffic is classified as normal traffic in False Negative (FN), and number of benign packets correctly classified as benign in True Negative (TN),

Gnanapriya N. And Karthik R. [8] showed superiority Naive Bayes detection method compared with Information Gain and Gain Ratio. Niharika Sharma et al [9] used K-Means Clustering, Naive Bayes, Neural Network, Fuzzy Logic, and Genetic Algorithm to review anomaly DoS attacks to IDS by language Machine Learning. Mohammed Alkasassbeh et al [10] incorporates three well-known classification techniques: Multi-Layer Perceptron (MLP), Bayes, and Random Forest. That show MLP achieved is the highest accuracy. S.H.C. Haris et al [11] had been observed and analyzed in IP header for the first experiment. There are five main fields that are important in order to detect threats. The experiment is focusing on Internet Protocol Version 4 (IPV4), so the IPV must be 4 and IP header length must be equal or above than 20 bytes and equal or below than 60 bytes.

Nikhil S. Mangrulkar et al [12] proposed Intrusion Detection System and Intrusion Prevention System using Naive Bayes Classifier. Preprocessing part, Classification part, and Protection part became part of the principal. Majed Tabash and Tawfiq Bathroom [13] compared many methods to detecting and preventing the network from DoS attacks. The methods are K-NN with K=3, Decision Tree, SVM, and Naive Bayes. Navdeep Singh et al [14] compared Analysis of different DDoS detection Technique with Statistical Method, IDS, IDS based Dempster-Shafer Theory, Packet information Gathering and Preprocessing, Network Detection, and Real-time Detection System. Primula Is Armani and Imam Radi [15] used K-Means Clustering to classify DoS attacks in three danger levels Low, Medium, and High.

Previous papers describe different techniques to detect DoS/DDoS attacks. We proposed to conduct further research on network testing, network processing, and analytical methods to achieve better detection accuracy with different network traffic and make the detection systems based on average and standard deviation according to the Gaussian method.

2. Basic Theory

2.1. Three-way Handshake

Communication between computers requires a standard protocol called a three-way handshake as seen in Figure 2. The communication contains a protocol exchange between the server and the attacker [16].

Three-way handshake from a normal TCP connection initiates transmission from an attacker by sending SYN to the server, and the server will allocate a buffer to the user and reply with SYN and ACK packet. This stage, the connection is in a half-open state, waiting for an ACK response from the attacker to complete the connection settings. When the connection is completed, this is called three-way handshake. But TCP SYN Flood attacks manipulate this three-way handshake by making server busy with a SYN request. TCP SYN Flood is a common form of Denial of Service attack. TCP SYN Flood can be observed with a Packet Capture application by using a spanned link to observe a copy of server activity. TCP SYN Flood features are often the emergence of the incoming IP Address to the server. IP Address that always appear to the server is calculated within a certain time range and used as feature extraction as a DDoS attack [11].

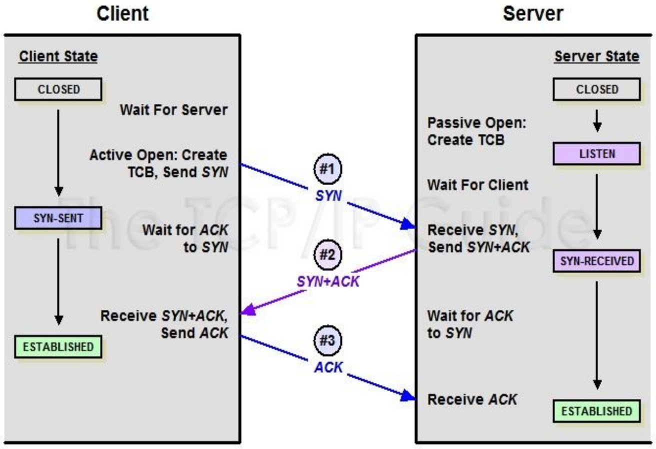


Figure 2. Three way handshake

2.2. Gaussian Distribution

The Gaussian distribution is one of the common and important methods in probability calculation and statistics, introduced by Gauss in his study of error theory [17]. Gauss uses it to describe errors. Experience shows that many random variables, the height of adult males, and reaction time in psychological experiments, all of which can be solved by the Gaussian distribution [18]. The Gaussian distribution is:

$$P(x) = \frac{1}{\delta\sqrt{2\pi}} e^{\frac{(x-\mu)^2}{2\delta^2}} \tag{1}$$

where, μ is average and δ is standard deviation, to calculate μ and δ values for numerical attributes using formula

$$\mu = \frac{\sum_{i-1}^{n} xi}{n} \tag{2}$$

$$\delta^2 = \frac{\sum_{i=1}^{n}(xi-\mu)^2}{n-1} \tag{3}$$

2.3. Naive Bayes Algorithm

Bayes theorem is stated mathematically as the following equation [2]

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{4}$$

where: *A* and *B* are events

P (*A*) and P (*B*) are the probabilities of *A* and *B* independent of each other

P (*A*|*B*), a conditional probability, is the probability of *A* given that *B* is true

P (*B*|*A*), is the probability of *B* given that *A* is true

Based on Gaussian distribution and Naive Bayes algorithm, we proposed to calculate incoming IP Address and packet length using packet capture application as numerical input to be displayed in the 2-dimensional graph. After obtaining numerical input, the data is processed using Gaussian Naive Bayes method based on a calculation of average and standard deviation.

3. Proposed Methodology

3.1. Architecture Diagram

Figure 3 Architecture Diagram, where the client is a router in MITRLADUY and connected to an investigator with a spanned link.

a. Capture IP Packets

Network traffics is collected using packet capture application. The input packets traffic is resized for further operation.

b. Analyzing the IP/Data Packet

IP packets are processed and analyzed to find out the normal network traffic and in case of under attack

c. Features Extraction

In the stage where implemented data processing which originally shaped log file into a form that can be processed further, so that the data can be retrieved from the important information.

d. Training Set Formation

Training set formation is a stage where the training implemented with naive Bayes method of log data file result processing to recognize the pattern of attacks

e. Apply Gaussian Naive Bayes (Classify)

Classify is the stage where the results of the training, tested with data test to know the success of introduction of DDoS attacks

f. Classification Predictor

The system provides output in the form of a normal traffic or under attack. The system will produce the output of an attacker's IP address

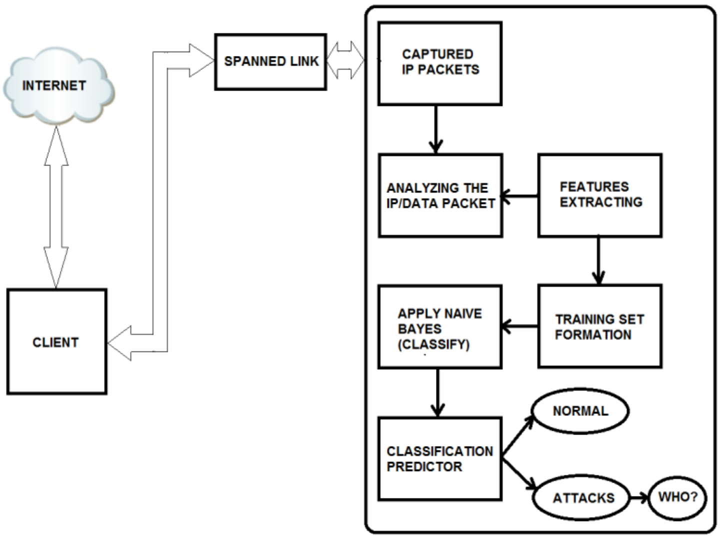


Figure 3. Architecture diagram of proposed research on MITRLADUY

3.2. Topology

Figure 4 shows the distribution of Computer network in MITRLADUY, that router serves 8 users to access the internet. In this proposed research, DDoS attacks will be captured by the investigator as data input through the spanned link. Simulations were done by 6 attackers from outside the laboratory to the victim IP Address 172.10.64.250 using DDoS application Low Orbit Ion Cannon (LOIC) and Wireshark packet capture application to observe network traffic activity.

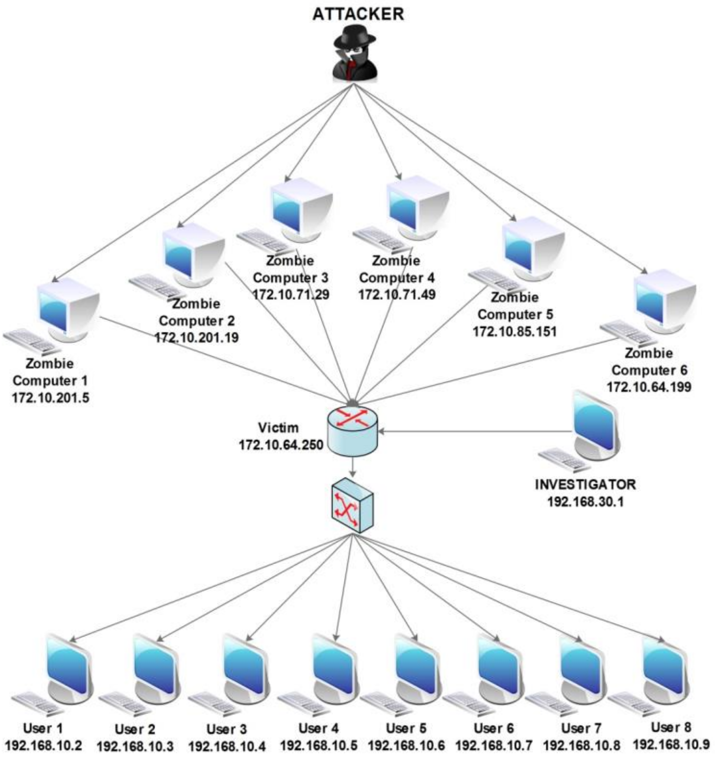

ATTACKER
Zombie Computer 1 172.10.201.5
Zombie Computer 2 172.10.201.19
Zombie Computer 3 172.10.71.29
Zombie Computer 4 172.10.71.49
Zombie Computer 5 172.10.85.151
Zombie Computer 6 172.10.64.199
Victim 172.10.64.250
INVESTIGATOR 192.168.30.1
User 1 192.168.10.2
User 2 192.168.10.3
User 3 192.168.10.4
User 4 192.168.10.5
User 5 192.168.10.6
User 6 192.168.10.7
User 7 192.168.10.8
User 8 192.168.10.9

Figure 4. Network topology

3.3. Classification

Numerical data input will be processed by Gaussian Naive Bayes Classifier and give decision result in the form of normal access or attack. Figure 5 shows the proposed classification process using the Gaussian Naive Bayes method.

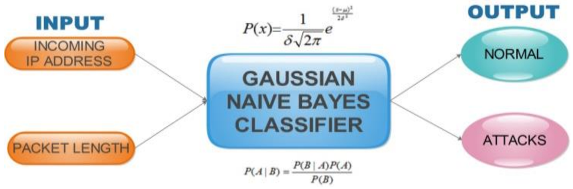

INPUT
INCOMING IP ADDRESS
PACKET LENGTH
$P(x)=\frac{1}{\delta\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\delta^2}}$
GAUSSIAN NAIVE BAYES CLASSIFIER
$P(A|B)=\frac{P(B|A)P(A)}{P(B)}$
OUTPUT
NORMAL
ATTACKS

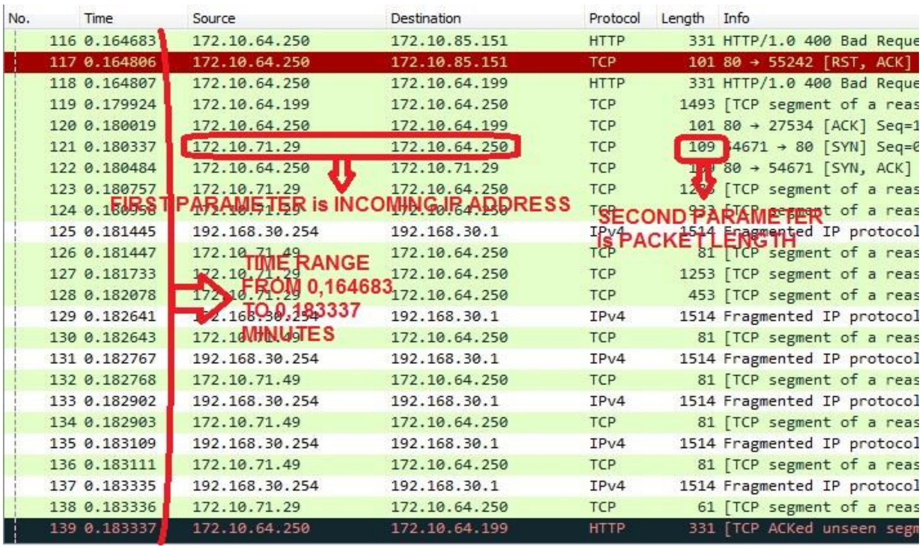
Figure 5. Classification process

4. Result and Discussion

Attack scenario is done in accordance with the topology in Figure 4, namely IP address 172.10.64.199, 172.10.85.151, 172.10.71.29, 172.10.71.49, 172.10.201.5, and 172.10.201.19 perform DDoS attacks using LOIC application to the victim with IP address 172.10.64.250. Attacks are performed within 3 minutes and captured using packet capture application.

4.1. Input Parameters

Packet capture determines network traffic activity data in form of time range, incoming IP address packet length, and so on. We observe network traffic within 3 minutes caused by storage limit and calculate the incoming IP address and packet length to serve as input parameters of numerical data that can be visualized in the classification process. Figure 6 shows the capture result for the input parameter.


FIRST PARAMETER is INCOMING IP ADDRESS
SECOND PARAMETER Is PACKET LENGTH
TIME RANGE FROM 0,164683 TO 0,183337 MINUTES

No.	Time	Source	Destination	Protocol	Length	Info
116	0.164683	172.10.64.250	172.10.85.151	HTTP	331	HTTP/1.0 400 Bad Reque
117	0.164806	172.10.64.250	172.10.85.151	TCP	101	80 → 55242 [RST, ACK]
118	0.164807	172.10.64.250	172.10.64.199	HTTP	331	HTTP/1.0 400 Bad Reque
119	0.179924	172.10.64.199	172.10.64.250	TCP	1493	[TCP segment of a reas
120	0.180019	172.10.64.250	172.10.64.199	TCP	101	80 → 27534 [ACK] Seq=1
121	0.180337	172.10.71.29	172.10.64.250	TCP	109	54671 → 80 [SYN] Seq=0
122	0.180484	172.10.64.250	172.10.71.29	TCP	[illegible]	80 → 54671 [SYN, ACK]
123	0.180757	172.10.71.29	172.10.64.250	TCP	[illegible]	[TCP segment of a reas
124	0.180958	172.10.71.29	172.10.64.250	TCP	933	[TCP segment of a reas
125	0.181445	192.168.30.254	192.168.30.1	IPv4	1514	Fragmented IP protocol
126	0.181447	172.10.71.49	172.10.64.250	TCP	81	[TCP segment of a reas
127	0.181733	172.10.71.29	172.10.64.250	TCP	1253	[TCP segment of a reas
128	0.182078	172.10.71.29	172.10.64.250	TCP	453	[TCP segment of a reas
129	0.182641	192.168.30.254	192.168.30.1	IPv4	1514	Fragmented IP protocol
130	0.182643	172.10.71.49	172.10.64.250	TCP	81	[TCP segment of a reas
131	0.182767	192.168.30.254	192.168.30.1	IPv4	1514	Fragmented IP protocol
132	0.182768	172.10.71.49	172.10.64.250	TCP	81	[TCP segment of a reas
133	0.182902	192.168.30.254	192.168.30.1	IPv4	1514	Fragmented IP protocol
134	0.182903	172.10.71.49	172.10.64.250	TCP	81	[TCP segment of a reas
135	0.183109	192.168.30.254	192.168.30.1	IPv4	1514	Fragmented IP protocol
136	0.183111	172.10.71.49	172.10.64.250	TCP	81	[TCP segment of a reas
137	0.183335	192.168.30.254	192.168.30.1	IPv4	1514	Fragmented IP protocol
138	0.183336	172.10.71.29	172.10.64.250	TCP	61	[TCP segment of a reas
139	0.183337	172.10.64.250	172.10.64.199	HTTP	331	[TCP ACKed unseen segm

Figure 6. Input parameters

Packet capture determines network traffic activity data in form of time range, incoming IP address packet length, and so on. We observe network traffic within 3 minutes caused by storage limit and calculate the incoming IP address and packet length to serve as input parameters of numerical data that can be visualized in the classification process. Figure 6 shows the capture result for the input parameter.

Table 1 shows the results of calculating incoming IP addresses and packet lengths to be the coordinate point values on the x-axis and y-axis in 3 minutes time range.

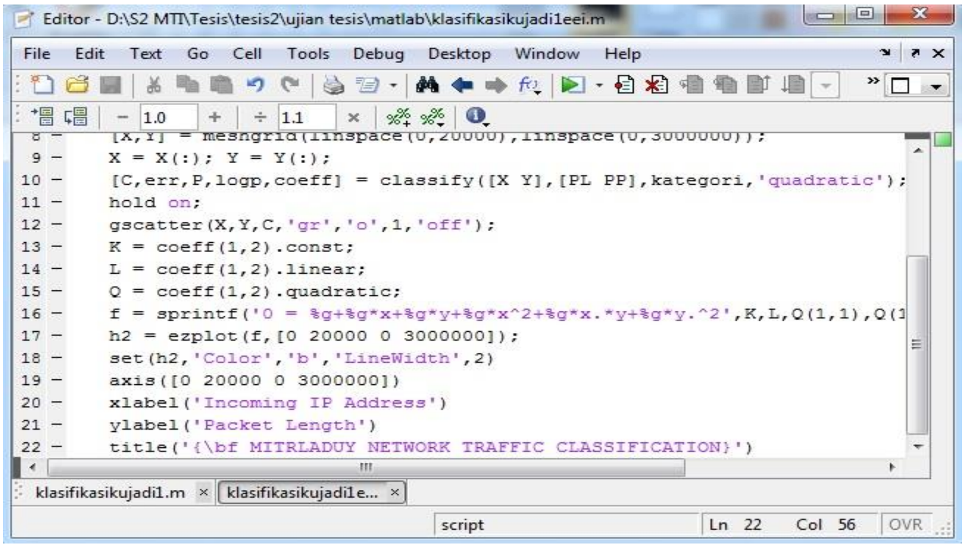
Table 1. MITRLADUY Network Traffic 3 minutes Time Range

IP address	Incoming IP (IIP) in time range (x-axis)	Packet length (PL) in time range (y-axis)	Access	Time Range (minutes)
192.168.10.2	36	10048	Normal	3
192.168.10.3	2449	384809	Normal	3
192.168.10.4	786	111132	Normal	3
192.168.10.5	1003	140340	Normal	3
192.168.10.6	1174	160075	Normal	3
192.168.10.7	1118	148707	Normal	3
192.168.10.8	1200	161525	Normal	3
192.168.10.9	1606	226306	Normal	3
172.10.64.199	4515	1527368	Attack	3
172.10.85.151	14320	2522499	Attack	3
172.10.201.5	9811	2044024	Attack	3
172.10.201.19	4407	1014119	Attack	3
172.10.71.29	8338	2356408	Attack	3
172.10.71.49	11206	1694624	Attack	3

4.2. Current Classification with Naive Bayes in Matlab

We use Matlab software for classification process because this software is very familiar for users and also very good for displaying the graph.

Matlab provides Naive Bayes classification facility for data processing. Network traffic can also use this facility to know the class. In the process of classification, using K, L, Q, and also function f. It will make difficult for many people to understand. Figure 7 shows the Matlab code of Naive Bayes classification with many coefficients.


Editor - D:\S2 MTI\Tesis\tesis2\ujian tesis\matlab\klasifikasikujadi1eei.m
File Edit Text Go Cell Tools Debug Desktop Window Help
1.0
1.1
klasifikasikujadi1.m
klasifikasikujadi1e...
script
Ln 22 Col 56 OVR

```
    [X,Y] = meshgrid(linspace(0,20000),linspace(0,3000000));
    X = X(:); Y = Y(:);
    [C,err,P,logp,coeff] = classify([X Y],[PL PP],kategori,'quadratic');
    hold on;
    gscatter(X,Y,C,'gr','o',1,'off');
    K = coeff(1,2).const;
    L = coeff(1,2).linear;
    Q = coeff(1,2).quadratic;
    f = sprintf('0 = %g+%g*x+%g*y+%g*x^2+%g*x.*y+%g*y.^2',K,L,Q(1,1),Q(1
    h2 = ezplot(f,[0 20000 0 3000000]);
    set(h2,'Color','b','LineWidth',2)
    axis([0 20000 0 3000000])
    xlabel('Incoming IP Address')
    ylabel('Packet Length')
    title('{\bf MITRLADUY NETWORK TRAFFIC CLASSIFICATION}')
```

Figure 7. Naive Bayes code in Matlab

The result of network traffic classification is shown in Figure 8, the normal class set is limited by the quadratic curve on the blue line with the green circle set member. The other is the attack class with a red square set member.

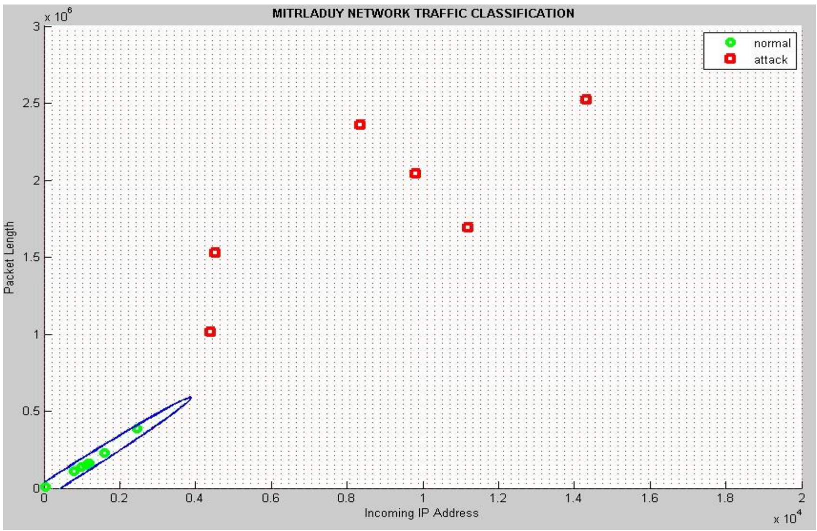


Figure 8. Result of classification in Matlab facility

4.3. Proposed Classification with Gaussian Naive Bayes in Matlab

Based on table 1, the formulas (2), and (3), we can calculate the average and standard deviation of the normal class and attack class. The average and standard deviation are:

- Incoming IP's average of normal class	=1172
- Incoming IP's average of attack class	=8766
- Packet length's average of normal class	=167868
- Packet length's average of attack class	=1859840
- Incoming IP's standard deviation of normal class	=686
- Incoming IP's standard deviation of attack class	=3877
- Packet length's standard deviation of normal class	=106791
- Packet length's standard deviation of attack class	=560838

The set of each class is based on the average and match standard deviation μ+(xδ) to get the best accuracy, so the set can shelter its members. Average of each class to be the center of the set and coupled with the match standard deviation that states the extent of the set of each class. We have calculated the match standard deviation to get the best accuracy with the set area μ+(3δ) for the normal class and μ+(2,5δ) for the attack class. Figure 9 shows the set of normal classes and set of attack classes based on average and standard deviation.

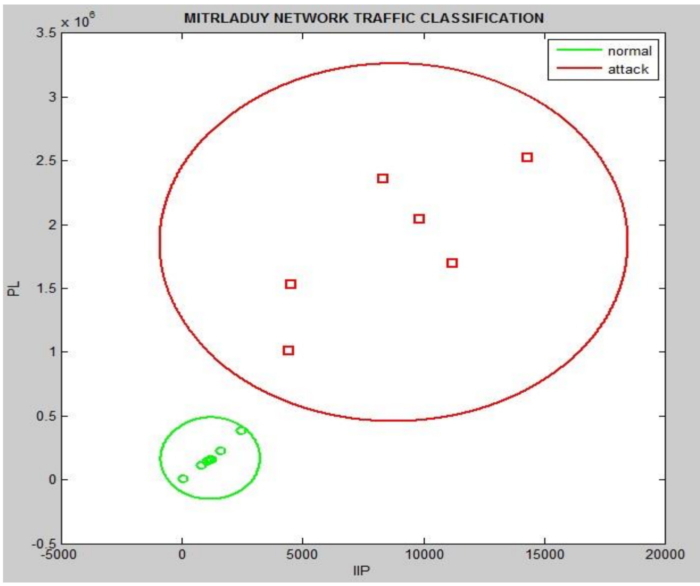


Figure 9. Gaussian Naive Bayes classification based on the average and standard deviation

Finally, formula (1) and formula (4) are used to predict network traffic activity so that it can be known IP address that attacks to the victim. Table 2 shows the IP addresses that perform normal activities and IP addresses that perform attacks.

Table 2 also shows the IP addresses that perform normal activities are 192.168.10.2, 192.168.10.3, 192.168.10.4, 192.168.10.5, 192.168.10.6, 192.168.10.7. 192.168.10.8, and 192.168.10.9. IP addresses that perform the attack activities are 172.10.64.199, 172.10.85.151, 172.10.201.5, 172.10.201.19, 172.10.71.29, and 172.10.71.49.

Table 2. Network Traffic Prediction of MITRLADUY Activities

No	IP Address	Incoming IP (IIP) in time range (x axis)	Packet length (PL) in time range (y axis)	Access	P(normal|IP)	><	P(attack|IP)	CLASS
1	192.168.10.2	36	10048	NORMAL	1.4688E-09	>	1.96172E-11	NORMAL
2	192.168.10.3	2449	384809	NORMAL	1.2666E-09	>	3.26734E-11	NORMAL
3	192.168.10.4	786	111132	NORMAL	1.8679E-09	>	2.3003E-11	NORMAL
4	192.168.10.5	1003	140340	NORMAL	1.9175E-09	>	2.40365E-11	NORMAL
5	192.168.10.6	1174	160075	NORMAL	1.9305E-09	>	2.47967E-11	NORMAL
6	192.168.10.7	1118	148707	NORMAL	1.927E-09	>	2.4442E-11	NORMAL
7	192.168.10.8	1200	161525	NORMAL	1.9306E-09	>	2.48799E-11	NORMAL
8	192.168.10.9	1606	226306	NORMAL	1.8575E-09	>	2.71337E-11	NORMAL
9	172.10.64.199	4515	1527368	ATTACK	6.3477E-14	<	6.20552E-11	ATTACK
10	172.10.85.151	14320	2522499	ATTACK	4.9321E-30	<	5.33277E-11	ATTACK
11	172.10.201.5	9811	2044024	ATTACK	1.029E-20	<	6.92607E-11	ATTACK
12	172.10.201.19	4407	1014119	ATTACK	1.7146E-11	<	5.29461E-11	ATTACK
13	172.10.71.29	8338	2356408	ATTACK	3.309E-22	<	6.59322E-11	ATTACK
14	172.10.71.49	11206	1694624	ATTACK	1.5572E-19	<	6.76054E-11	ATTACK

5. Conclusion and Future Work

The average and standard deviation can be used as a reference to create a set of classes using Gaussian Naive Bayes method. The average indicates the center of the class set, whereas the standard deviation shows the extent of the class set. The width of the set of each class is more specific to all members of the set. The Gaussian Naive Bayes method can also predict accurately and precisely. Further research is expected to process more data so that it can test the accuracy of the Gaussian Naive Bayes method.

References

[1] Cisco, Cisco 2016 Annual Security Report, 2016.

[2] JK Bains. Intrusion Detection System with Multi-Layer using Bayesian Networks. *International Journal of Computer Applications*. 2013; 67(5): 1–4.

[3] MD Salunke, R Kabra. Denial-of-Service Attack Detection. *International Journal of Innovative Research in Advanced Engineering*. 2014; 1(11): 16–20.

[4] R Kanagalakshmi, VN Raj. Network Intrusion Detection Using Hidden Naive Bayes Multiclass Classifier Model. *International Journal of Science, Technology & Management*. 2014; 3(12): 76–84.

[5] B Nagpal, P Sharma, N Chauhan, A Panesar. *DDoS Tools : Classification, Analysis, and Comparison*. Proceeding of the 2nd International Conference on Computing for Sustainable Global. 2015: 2–6.

[6] V Hema, CE Shin. DoS Attack Detection Based on Naive Bayes Classifier. *Middle-East Journal of Scientific Research*. 2015; 23: 398–405.

[7] M Salunke, R Kabra, A Kumar. Layered architecture for DoS attack detection system by combined approach of Naive Bayes and Improved K-means Clustering Algorithm. *International Research Journal of Engineering and Technology.* 2015; 2(3): 372–377.

[8] Gnanapriya, KR. Denial of Service Attack by Feature Reduction Using Naive Bayes Classification. *International Journal of Science and Engineering Research*. 2016; 4(1).

[9] N Sharma, A Mahajan, V Malhotra. Machine Learning Techniques Used in Detection of DOS Attacks : A Literature Review. *International Journal of Advance Research in Computer Science and Software Engineering*. 2016; 6(3): 100–105.

[10] M Alkasassbeh, ABA Hassan, G Al-any mat. Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. *International Journal of Advanced Computer Science and Applications*. 2016; 7(1): 436–445.

[11] SHC Haris. Anomaly Detection of IP Header Threats. *International Journal of Computer Science and Security*. 2011; 4(5): 497–504.

[12] NS Mangrulkar. Network Attacks and Their Detection Mechanisms : A Review. *International Journal of Computer Applications*. 2014; 90(9): 36–39.

[13] M Tabash, T Barhoom. An Approach for Detecting and Preventing DoS Attacks in LAN. *International Journal of Computer Trends and Technology*. 2014; 18(6): 265–271.

[14] N Singh, A Hans, K Kumar, M Pal, S Bird. Comprehensive Study of Various Techniques for Detecting DDoS Attacks in Cloud Environment. *International Journal of Grid Distribution Computing*. 2015; 8(3): 119–126.

[15] A Iswardani, I Riadi. Denial of Service Log Analysis Using Density K-Means Method. *Journal of Theoretical Applied Information Technology*. 2016; 83(2): 299-302.

[16] AS. Tanennbaum, *Computer Networks*, 5th ed. Pearson, 2011.

[17] J Yang, X Yu, Z Xie, J Zhang. A Novel Virtual Sample Generation Method Based on Gaussian Distribution. *Knowledge-Based Syst.* 2011; 24(6): 740–748.

[18] E Balkanli. *Supervised Learning to Detect DDoS Attacks*. IEEE Int. Conf. Comput. Commun. Informatics, 2014.