DDoS Attack Detection Using Moment in Statistics with Discriminant Analysis

Pradit Pitaksathienkul[1]
and Pongpisit Wuttidittachotti[2]
King Mongkut's University of Technology North Bangkok, Thailand
[1]praditp9@gmail.com
[2]pongpisit.w@it.kmutnb.ac.th

Abstract **- The research objectives are to create discriminant analysis functions using moment of aggregate traffic packets on victims to classifying attack situations and detect DDoS attacks on the network. To simulate the network model, the DDoS attack simulation model over wired networks was conducted to keep data packets from the victim and then analyze to find the attributes from the attack. In order to achieve a more accurate classification, discriminant analysis was used to find the characteristics of harmful traffic. In this research, the discriminant analysis function was created by using four moments of the traffic. Accurately detection was found to at 92.5%.**

Keywords **- DDoS Attack Detection, Discriminant Analysis, Wilks' Lambda Statistic**

I. INTRODUCTION

Today's computer networks play a significant role in diverse areas such as business, education, communication and other services.

There are many advantages from a computer network such as flexibility and ease of connection. Moreover, Internet usage and computer networks are wildly spread nowadays.

Howover, security issues have become significant and attacks can threaten a whole computer network. One attack is conducted by sending large amounts of packets to computer hosts on the Internet. This is one of the most common computer network attacks which can effect network devices and any computer connected, known as the Distributed Denial-of-Service (DDoS). A recent report [1] revealed the largest attack in 2015 was 500 Gbps, which surprisingly increased 833.33% in attack size since 2012.

Research on DDoS detection has been able to identify DDoS attack packets from traffic flows by using two methods, statistical and heuristic analysis, to identify attacks in progress. While statistical-based detection system [2, 3] has the ability to learn and distinguish normal from abnormal network, the heuristic-based detection system [4-6] is based on threshold decisions.

In this paper, a solution to discriminate DDoS using the pattern behaviour of traffic sources by observing packet arrivals as the moment in statistics, mean, variance, skewness and kurtosis is proposed. These features are classified into three groups (normal, normal but sometimes abnormal and attack) using the developed discriminant function.

The rest of the paper is organized as follows. Section 2 provides background knowledge on definition of discriminant analysis functions. The research methodologies are described in Section 3. The results and discussion are given in Section 4. Section 5 covers the conclusion of this research.

II. BACKGROUND KNOWLEDGE

A. Objective

The objectives of this research are to find discriminant analysis functions with moment in statistics to classify and detect DDoS attacks over wired networks.

B. Definition

Discriminant analysis is a statistical approach to classifying objects based on their set of features which can be placed in two or more charactistic groups. A feature must be defined as an observation, property, attribute or measurement of an object.

Moment in statistics are the constants of a population. These constants help in deciding the characteristics of the population and on the basis of these characteristics of data by calculating the normal moment statistically. In this paper, this technique is used to decide the situation of network as one attribute of traffic [7].

III. METHODOLOGY

This section describes the process of this research used for the network simulation, log file of traffic storage, log file forwarding to find the moment of attributes such as the characteristic of traffic to create the discriminant analysis function, as shown in Fig. 1.

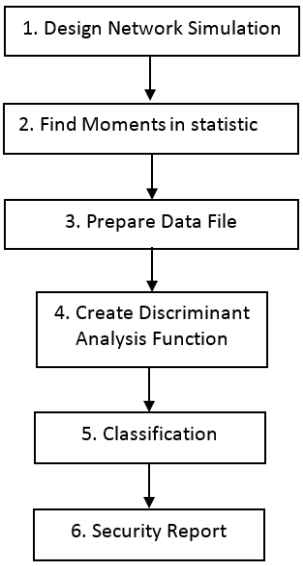

Fig. 1 Framework of the Discriminant Analysis System

There are six steps as follows:

Step 1: Design the network simulation using Network Simulation (NS2), generate a network model of about 200 nodes including random attack nodes and victims, random time attacks and generation of packets sent to victims.

Table I presents the network simulation model that will be used to simulate the attack of approximately 80 seconds. Traffic arrivals at the victim's computer are collected every 0.1 seconds in Mbps. The simulation ran 30 normal, 30 normal but abnormal samples and 60 attack sample datasets.

TABLE I
THE EXAMPLE OF EACH TRAFFIC DATA FROM NS2

	time	traffic
1	11.30	.13
2	11.40	.20
3	11.50	.20
4	11.60	.20
5	11.70	.20
6	11.80	.19
7	11.90	.22
8	12.00	.21
9	12.10	.22
10	12.20	.18

The normality of traffic from the sample datasets were examined.

TABLE II
THE MOMENTS OF DATA

Descriptives

			Statistic	Std. Error
traffic	Mean		.3829	.00840
	95% Confidence Interval for Mean	Lower Bound	.3664	
		Upper Bound	.3994	
	5% Trimmed Mean		.3774	
	Median		.2080	
	Variance		.049	
	Std. Deviation		.22036	
	Minimum		.13	
	Maximum		.72	
	Range		.59	
	Interquartile Range		.44	
	Skewness		.386	.093
	Kurtosis		-1.818	.186

Step 2: Find the characteristics of data by calculating the normal moment statistically as shown in Table II.

The 1th moment (Mean) = $\sum \frac{(X-\bar{X})}{N}$ (1)

The 2nd moment (Variance) = $\sum \frac{(X-\bar{X})^2}{N}$ (2)

The 3rd moment (Skewness) = $\sum \frac{(X-\bar{X})^3}{N}$ (3)

The 4th moment (Kurtosis) = $\sum \frac{(X-\bar{X})^4}{N}$ (4)

Step 3: After the dataset collection, the data file format was prepared as shown in Table III.

TABLE III
THE EXAMPLE OF FOUR MOMENTS AND CASE USED TO MODEL THE DISCRIMINANT ANALYSIS FUNCTION

Mean	Variance	Skewness	Kurtosis	case
0.199	0.000	-1.023	12.38	1
0.199	0.000	0.706	3.422	1
0.199	0.000	-0.293	9.934	1
0.199	0.000	-0.526	9.357	1
0.199	0.000	0.299	4.203	1
0.199	0.000	0.657	3.771	1
0.199	0.000	-0.15	4.244	1
0.199	0.000	-1.948	28.395	1
0.199	0.000	0.222	2.061	1
0.199	0.000	-0.961	13.609	1
0.251	0.008	1.073	-0.693	2
0.222	0.002	1.136	-0.185	2
0.277	0.017	1.087	-0.737	2
0.256	0.005	0.521	-1.555	2
0.262	0.007	0.639	-1.447	2
0.248	0.004	0.507	-1.539	2
0.265	0.008	0.639	-1.47	2

Step 4: Create the discriminant analysis function. The statistical model can be given by the following equation:

$$D = ß0 + ß1 \,.\, X1 + ß22 \,.\, X2 + \ldots + ßi \,.\, Xi \quad (7)$$

Where

D is the discriminant score
$ß_i$ denotes discriminant coefficients
X_i are predictor variables

TABLE IV
THE COEFFICIENTS OF CANONICAL DISCRIMINANT FUNCTION

Canonical Discriminant Function Coefficients

	Function	
	1	2
Mean	12.781	.712
Variance	.248	.364
Skewness	1.161	-.593
Kurtosis	-.043	.061
(Constant)	-5.568	-.378

Unstandardized coefficients

From Table IV, the discriminant equation can be written as follows:

D = (-5.568) + (12.781 * Mean) + (0.248 * Variance) + (1.161 * Skewness) + (-0.43 * Kurtosis) (8)

Function 1 was chosen because of the Eigenvalues from Table V. Three cases were used, so the discriminant analysis process generated 2 functions. Function 1 has Eigenvalue 5.804 greater than 1 while Function 2 had Eigenvalue 0.215 less than 1.

TABLE V
THE EIGENVALUES OF DISCRIMINANT FUNCTION

Eigenvalues

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	5.804[a]	96.4	96.4	.924
2	.215[a]	3.6	100.0	.421

a. First 2 canonical discriminant functions were used in the analysis.

This model used the Wilks' lambda statistic [8] to evaluate significant functions which discovered that both discriminant functions in Table VI had significant vaules less than 0.05 indicating a highly significant function (Sig. = .000). Thus concluded that predictor variables have a certain discriminant power to reach.

TABLE VI
THE WILKS' LAMBDA OF DISCRIMINANT FUNCTION

Wilks' Lambda

Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 2	.121	243.980	8	.000
2	.823	22.499	3	.000

Step 5: Classification, the Classification

results as shown in Table VII were investigated.

TABLE VII
THE CLASSIFICATION RESULT TABLE

Classification Results[a]

		Case	Predicted Group Membership 1.00	2.00	3.00	Total
Original	Count	1.00	30	0	0	30
		2.00	0	30	0	30
		3.00	0	9	51	60
	%	1.00	100.0	.0	.0	100.0
		2.00	.0	100.0	.0	100.0
		3.00	.0	15.0	85.0	100.0

a. 92.5% of original grouped cases correctly classified.

The classification table is a table in which the rows are the observed categories of the dependent and the columns are the predicted categories. The percentage of cases on the diagonal is the percentage of correct classifications.

The classification results (Table VII) reveal that a rate of 92.5% (footnote) respondents were classified correctly into 'normal', 'abnomal' or 'attack' groups. This overall predictive accuracy of the discriminant function from Case 1 and 2, normal and anomaly, was classified with slightly better accuracy (100%) than Case 3, attack (85%).

This means the legitimate flow has unique behaviour regarding unpredictable packet transmission as well as a high accuracy for detecting DDoS attack flow that can protect the host computer system.

Step 6: After a decision has been made by the classification results, an action command or message is then generated to inform the security system.

IV. RESULTS AND DISCUSSIONS

Results of the classification process derived from the train data which come from Network Simulation were collected. The test data set by simulation normal, normal but abnormal sample and attack sample datasets with random time attack were prepared and divided into slots of time (10 seconds) and then passed to the discriminant equation (8) for prediction, as shown in Table VIII.

TABLE VIII
THE EXAMPLE OF TEST DATA

Mean	Variance	Skewness	Kurtosis	case	time slot	case predict
0.192	0.002	-3.067	10.526	1	10-20	1
0.197	0	0.345	-0.209	1	21-30	1
0.199	0	0.745	0.596	1	31-40	1
0.201	0	-0.215	-0.726	1	41-50	1
0.199	0	0.684	1.17	1	51-60	1
0.2	0	0.176	-0.042	1	61-70	1
0.613	0.153	-0.077	-1.986	3	71-80	3
0.192	0.002	-3.067	10.526	1	10-20	1
0.197	0	0.345	-0.209	1	21-30	1
0.199	0	0.745	0.596	1	31-40	1
0.201	0	-0.215	-0.726	1	41-50	1
0.199	0	0.684	1.17	1	51-60	1
0.954	0.028	-3.908	14.34	3	61-70	3

The discriminant equation (8) can accurately discriminate the legitimate flow 100% of the time. However, the attack flow can only be detected with a rate of 85% accuracy. This means the legitimate flow has a unique behavior, the attack flow might be normal but sometime send abnormal packets (DDoS attack).

According to the discriminant function using moment in statistics of aggregate traffic packets at the victim are attributes, the accuracy of classification equals 92.5%. This means that the discrimination process has a high level of differentiation in the attack flow.

V. CONCLUSION AND FUTURE WORK

In this paper, an effective approach with using moment in statistics of aggregate traffic to increase the performance of classifying in discriminant function was proposed. This gained an accurately of classifying at 92.5%. This is useful to apply for the process of DDoS detection.

For future work, an improvement to the accuracy in the discriminant function with moments of characteristics of traffic packets should be investigated, this may provide more accuracy.

VI. ACKNOWLEDGMENT

Thanks to Assoc. Prof. Dr. Somchai Prakarncharoen for useful information and suggestions and Mr. Gary Sherriff for editing.

REFERENCES

(Arranged in the order of citation in the same fashion as the case of Footnotes.)

[1] Arbor Networks. (2016). "Worldwide Infrastructure Security Report". Arbor Networks, Vol. 11, pp. 24. <https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf>.

[2] Yi, F., Yu, S., Zhou, W., Hai, J., and Bonti, A. (2008). "Source-Based Filtering Algorithm Against DDOS Attacks". International Journal of Database Theory and Application, Vol. 1, No. 1, pp. 9-20.

[3] Xie, Y. and Yu, S.Z. (2009). "Monitoring the Application-Layer DDoS Attacks for Popular Websites". IEEE/ACM Transactions on Networking, Vol. 17, No. 1, pp. 11.

[4] Khan, L., Awad, M., and Thuraisingham, B. (2007). "A new intrusion detection system using support vector machines and hierarchical clustering". The VLDB Journal, Vol. 16, pp. 507-521.

[5] Oikonomou, G. and Mirkovic, J. (2009). "Modeling Human Behavior for Defense against Flash-Crowd Attacks". in Proceedings of IEEE International Conference on Communications 2009 (ICC'09), pp. 1-6.

[6] Yu, S., Thapngam, T., Liu, J., Wei, S., and Zhou, W. (2009). "Discriminating DDoS Flows from Flash Crowds Using Information Distance". in Proceedings of the 3rd 171 IEEE International Conference on Network and System Security (NSS'09), pp. 351-356.

[7] Yu, S., Thapngam, T., Liu, J., and Wei, S. (2012). "DDoS Discriminatation by Linear Discriminant Analysis (LDA)". in Proceedings of the IEEE International Conference on Computing, Networking and Communications, Green Computing, Networking and Communication Symposium.

[8] Todorov, V. and Filzmoser, P. (2010). "Robust Statistic for the One-way MANOVA". in Computational Statistics & Data Analysis, ELSEVIER, Vol. 54, Issue 1, pp. 37-48, <http://dx.doi.org/10.1016/j.csda.2009.08.015>. Accessed 1 January 2010.