TRIBHUVAN UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

CENTRAL DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

DDOS ATTACKS, ITS DETECTION AND PREVENTIVE MEASURES: A STUDY REPORT

By

Brihat Ratna Bajracharya

19/075

SUBMITTED TO THE CENTRAL DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE MASTER'S DEGREE IN COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

CENTRAL DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

KIRTIPUR, KATHMANDU

December, 2019

TRIBHUVAN UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
CENTRAL DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

CERTIFICATE OF APPROVAL

The undersigned certify that they have read, and recommended to the Institute of Science and Technology for acceptance, a seminar report entitled "**DDoS attacks, its detection and preventive measures: A study report**" submitted by **Brihat Ratna Bajracharya** in partial fulfillment of the requirements for the Master's degree in Computer Science and Information Technology

---

Mr. Jagdish Bhatta
Supervisor
Central Department of Computer Science and Information Technology

---

Mr. Bikash Balami
Coordinator
Central Department of Computer Science and Information Technology

---

Mr. Nawaraj Paudel
Head of Department
Central Department of Computer Science and Information Technology

DATE OF APPROVAL:

TABLE OF CONTENT

CERTIFICATE OF APPROVAL....ii
LIST OF ABBREVIATIONS....iv
LIST OF FIGURES....v
LIST OF TABLES....vi
ACKNOWLEDGMENT....vii
ABSTRACT....viii
1. INTRODUCTION....1
1.1. Denial of Service (DoS) Attack....1
1.2. Distributed Denial of Service (DDoS) Attack....1
1.3. DDoS vs Flash Events....1
2. Detection of DDoS Attacks....2
2.1. Classification Based....2
2.2. Entropy based system....2
2.3. Regression Based Network Traffic Analysis....3
2.4. Using Artificial Neural Network....4
3. PREVENTING FUTURE DDOS ATTACKS....5
3.1. By maintaining the blacklist of source IP addresses....5
3.2. By simply dropping the detected attack packets....5
4. PERFORMANCE OF DETECTION SYSTEM....6
4.1. Performance of Classification based DDoS detection....6
4.2. Performance of Entropy based system....7
4.3. Performance evaluation of Regression based approach....8
4.4. Performance evaluation of ANN based approach....9
5. DISCUSSION AND CONCLUSION....10
REFERENCES....11

LIST OF ABBREVIATIONS

ANN	Artificial Neural Network
DDoS	Distributed Denial of Service
DoS	Denial of Service
FBI	Federal Bureau of Investigation
FSM	Finite State Machine
HTTP	Hyper Text Transfer Protocol
IAT	Inter Arrival Time
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LS-SVM	Least Square Support Vector Machine
PNN	Probabilistic Neural Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

LIST OF FIGURES

Figure 1: DDoS Attack.....1
Figure 2: Blacklisting of IPs from abnormal packet.....5
Figure 3: Six fold cross-validation result.....7
Figure 4: Proposed approach of [6] for classification of DDoS attack.....7
Figure 5: Malware Traffic Detection Result (Source: Divakaran et al.[*5*]).....8

LIST OF TABLES

Table 1: Classification Performance Average (Single Source of Attack).....6
Table 2: Classification Performance Average (Multiple Sources of Attack).....6
Table 3: Comparison of ANN with other approaches.....9
Table 4: Comparision between old and up-to-date dataset.....9

ACKNOWLEDGMENT

I would like to express my indebted gratitude and sincere thanks my supervisor Mr. Jagdish Bhatta for his continuous support, guidance and supervision by which this seminar has been possible. I would also like to thank Central Department of Computer Science and Information Technology for arranging such a schedule for the academic course.

Every attempt has been made to most of the details in each and every aspects of the seminar in this documentation so that the reader can clearly understand about the seminar. We would be pleased to get the feedback on this report. Finally I would like to express our gratitude to my family, friends and well wishers for encouraging and supporting me.

Brihat Ratna Bajracharya
19/075

ABSTRACT

In the present day digital world, most of our electronic devices have become smart and most of them have capability to connect to the internet. This capability has both pros and cons. The benefit is that we can control those devices from anywhere but possess a serious risk of being attacked and compromised. Those attack may have different intentions behind it like for fun, for ransom, theft of data, exploitation of privacy, and personal reasons. So, it has been crucial that we detect those attack before the attack could do any damage and also prevent similar attack in the future. In this report, we mainly focus in distributed denial of service (DDoS) because it is one of the most common type of attack. The victim's machine is attacked from multiple systems across the internet using infected botnets of networks. The attacker controls those infected botnet and is programmed to launch attack packet flood. In this report, we studied some of the researches relating to evidence gathering, attack detection using proposed system and some preventive measure like maintaining blacklist and dropping packet to avoid future attacks. We organized this report to briefly describe the proposed system of some authors and also interpret their experimental result analysis and performance evaluation. Finally, discussion section compares all performances and proposed system to conclude this report.

Keywords: ***network security, DDoS attack, flash event, classification, evidence gathering***

1. INTRODUCTION

1.1. Denial of Service (DoS) Attack

A DoS attack is a denial of service attack where a computer (or computers) is used to flood a server with TCP or UDP packets. In this attack, the service is put out of action as the packets sent overload the server's resources and make the server unavailable to other devices and users throughout the network.

1.2. Distributed Denial of Service (DDoS) Attack

A DDoS attack is the most common type of DoS attack in which multiple systems target a single system with a DoS attack. The targeted network is bombarded with packets from multiple locations. DDoS attack is more complicated to recover. DDoS attacks are not only a widespread attack but also the second most common cybercrime attack to cause financial losses [3] according to the United States Federal Bureau of Investigation (FBI) and since the attack is generated from multiple computers across distributed network, it becomes very hard to differentiate DDoS attack from the genuine traffic.

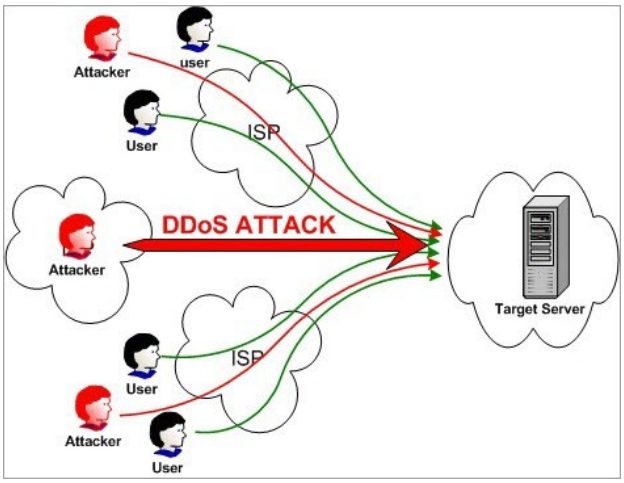

Figure 1: DDoS Attack

DDoS attacks can be done in two different ways, direct and indirect. Direct attack target the victim's machine in its weakness of the system while in indirect attack, attacks are performed on the elements associated with the victim's machine.

1.3. DDoS vs Flash Events

DDoS attacks corresponds to large number of compromised systems flood requests to one or more servers in distributed environment while Flash events corresponds to large number of genuine traffic that occurs due to certain flash events. Flash events how ever resembles to that of DDoS traffic. The main difference between two is that the access intent in case of flash event is genuine and shows natural flow pattern.

2. DETECTION OF DDOS ATTACKS

Many researchers have contributed their time in research of effectively detecting the DDoS traffic differentiating from genuine traffic. Researchers have dived into detection using various methodologies and techniques. This section briefly points out some of the detection techniques used for the detection of DDoS attacks and to correctly identify flash events

2.1. Classification Based

Sahi et al. [1] has proposed a new classifier system for the detection as well as prevention of DDoS TCP flood attacks in their paper. Their proposed system can identify these attacks regardless of the form of in which these attacks comes to the system. In this classification based system, the detection sub-system collects the incoming packet within a time frame, and then passed through the blacklist checker where the source IP of the packet is checked with the database of blacklist. If the source IP is matched in blacklist, it is directly sent to prevention for safety, If the packet passed the blacklist check, it is then passed through the classifier which decides whether the packet is normal or abnormal (from attacker). The normal packets are forwarded to the destination IP while the abnormal packets' source IP is added to the blacklist thus simplifying future detection and the packet is sent to prevention sub-system

2.2. Entropy based system

Gera et al. [6] has proposed the system based on the anomaly of traffic patterns to differentiate between DDoS flood packets and genuine flash event traffic. This system is based on the fact that DDoS are artificial packets generated with the sole purpose of attacking the victim to flood its resources. So, this attack must have some kind of pattern. On the other hand, flash events pattern are more genuine and random and this randomness factor between two can be used for the detection of DDoS flood packets. Some of the parameters that can be used for this kind of detection are as follows:

a. Time Interval – before the DDoS attack, the network traffic is generally low. Suppose at time t1 the network shows less traffic and when the DDoS attack starts, the network traffic will spike up. Let this time be t2. In DDoS attack the network traffic abruptly increase while in case of flash event, the traffic will increase gradually (i.e. spread of a breaking news takes place in gradually increasing pace and end in same fashion)

b. Source entropy – It is the number of source IP addresses from which attack is launched. The traffic that comes from the same network is considered traffic cluster. A threshold entrophy is defined. Then while analysing the incoming traffic, if it is found that there are more source IPs but less traffic cluster, it is considered a flash event (i.e. more number of people pinging the news some few times). Similarly, if there are more source IPs and more traffic cluster, it is considered as a DDoS attack (spoofed) (i.e. attackers are using multiple IPs to attack the victim's machine and these multiple source IPs are used multiple times). Finally if the source IP is same and the traffic cluster is same, it is also considered DDoS attack (i.e. attackers attacking the victim's machine from the same IP; non-spoofed).

2.3. Regression Based Network Traffic Analysis

Divakaran et al. [5] proposed a framework of gathering evidences to detect traffic sessions related to attacks and malicious activities. They applied regression models to detect fundamental anomalous patterns. Their framework include three stage approach for evidence gathering.

a. Modeling and analyzing sessions to detect anomalous patterns – they defined a flow as a set of packets localized in time, and studied the inter-arrival time (IAT) of the flows in a session. Attack bots are likely to generate flows in fixed interval of time, i.e. the randomness in the arrival time is lesser than in normal scenario. The flow size is also another vital parameter to distinguish anomalous session with normal genuine session. Another parameter is the degree of the end host (number of distinct IP addresses that an end host communicates to). DoS attack can be detected using the modeling session using the degree of destination IP address.

b. Detecting scans and illegitimate TCP state sequences – The anomaly can also be detected using the TCP state sequence, the normal flow of a TCP packet can be modeled in a finite state machine with SYN, SYN+ACK, DATA and FIN packet. Any other flow that does not corresponds to this normal flow is considered illegitimate. From this FSM, we can say TCP flow is either legitimate or illegitimate is a binary decision depending on the FSM.

c. Evidence correlation and decision making – Spacial correlation is performed in this stage i.e. using IP addresses to correlate the anomalous pattern. One example is to look for the flows with the same IP address. Instead of spacial correlation, correlation in time can also be

used but spacial correlation technique is more natural option as attacker may be passive for a while after successful exploit.

After the framework stages are completed, the analyzed data is processed to remove the outlier using a threshold for higher accuracy. The attack count if found nearly same will definitely raise suspicion. Also increasing count of attack packet with respect to time is also another type of anomaly detection technique. Regression models are then used to detect anomalous pattern. Authors have used linear regression to find the relationship between destination IP addresses with time. Quadratic regression is also used to detect anomalies using polynomial fit.

2.4. Using Artificial Neural Network

Saied et al. [2] used supervised ANN (feed forward, error back propagation) approach on three different type of packets: TCP, UDP and ICMP. The ANN ICMP uses three input nodes (source_ip, icmp_sequence, and icmp_ip) with four hidden layer nodes to get the result in one output node. Similarly, ANN TCP uses five input nodes (source_ip, tcp_sequence, source_port, destination_port, and tcp_flags) and four hidden layer nodes to get outpur output in one output node. And in ANN UDP, four input layer nodes (source_port, destination_port, source_ip, and packet_length) are taken with three hidden layer to get result in one output layer node. The ANN is trained to get output in either 0 or 1 indicating whether the packet is normal or abnormal respectively.

The basic flow for ANN based supervised learning is as follows:

1. DDoS detectors are installed in different network, each detector registering the IP of neighboring detectors and communicate via encrypted messages and continuously monitors the number of passing packets

2. If the number of packets are greater than certain threshold, then there is suspicion of the attack. The packets are sorted and IP of the victim is identified. The ANN retrieves the required patterns and prepares for the ANN engine. The trained ANN engine takes the input and produces the output.

3. The second step is repeated for three times and majority result is considered final out of the three outcomes.

This ANN engine needs to be trained regularly for detecting up-to-date DDoS attacks.

3. PREVENTING FUTURE DDOS ATTACKS

Preventing the attacks is another step after the detection of such attacks are performed so that we could be safe from such attacks in the future. Actually preventing DDoS attack means not allowing the attack packets to its destined address. For this obvious response to such attack will be to drop such packet and take some action against those attack packet. Some approaches that the researches tried are also similar to this concept and some authors have presented some preventive measures for the DDoS attack (and other attack packets) after detection. Two prevention measure include maintaining the blacklist of such source IP that initiates DDoS attack packet and simply dropping the attack packet so that those packet will never damage intended victims.

3.1. By maintaining the blacklist of source IP addresses

The classification based proposed model by [1] has the prevention subsystem that first alerts the system administrator of the attacks. Then on the second step, the subsystem adds the attacking source address to the blacklist which is later used by detection subsystem. And after all these steps, the attacking packet is finally dropped so that it does not reach the destination (i.e. victim's machine).

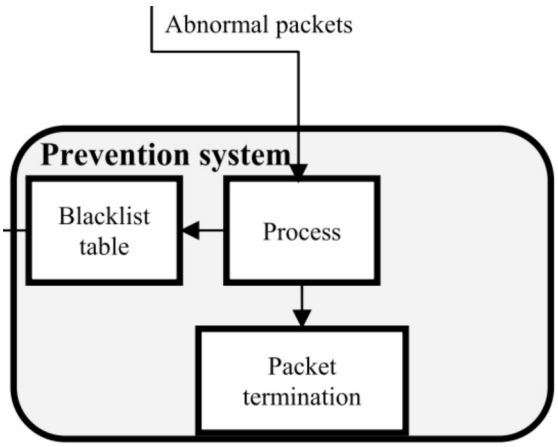

Figure 2: Blacklisting of IPs from abnormal packet

3.2. By simply dropping the detected attack packets.

In the Artificial Neural Network based approach by [2], if the output of the ANN is 1, then the incoming packet is classified as attack packet. In this case, the defense component activates and drops the attack packet. They have implemented the defense mechanism as a separate plugin based on the Snort signature Intrusion Detection System Project [7] and integrated the plugin with Snort-AI [4]. Later the output from the detection system is coupled with destination IP to instruct iptables [8] to mitigate forged packets while allowing genuine traffic to pass through.

4. PERFORMANCE OF DETECTION SYSTEM

The efficiency and performance of the detection system described in section 2 is presented in this section. The performance related data is extracted from the related researches and presented here as the information.

4.1. Performance of Classification based DDoS detection

[1] used four commonly used classification algorithms and validation is done using K-fold cross validation technique. The authors used LS-SVM, Naive Bayes, K-nearest and Multi layer perceptron for the classification and experimented for two different scenario. The first table is the Classification performance average for the algorithm under single source of attack while Table 2 is the classification performance average of the same algorithm for multiple source of attacks.

	Classifiers	Average			
		Accuracy	Sensitivity	Specificity	Kappa coefficient
1	LS-SVM	97%	97%	97%	0.8875
2	Naïve Bayes	88%	94%	94%	0.765
3	K-nearest	81%	96%	95%	0.7275
4	Multilayer perceptron	93%	98%	97%	0.69

Table 1: Classification Performance Average (Single Source of Attack)

	Classifiers	Average			
		Accuracy	Sensitivity	Specificity	Kappa coefficient
1	LS-SVM	94%	95%	94%	0.9025
2	Naïve Bayes	88%	92%	94%	0.7825
3	K-nearest	84%	92%	93%	0.735
4	Multilayer perceptron	88%	95%	95%	0.725

Table 2: Classification Performance Average (Multiple Sources of Attack)

For the validation using K-fold, the dataset was divided into six equal sized chunks and five out of six chunks were used to train the model and remaining one chunk was used to test the model. This process was repeated for total of six times each with different set to test the model. And the result of six fold cross validation are almost the same which proved that the classification results are stable and accurate [1]. Also the proposed system showed 97 % accuracy in LS-SVM classification.

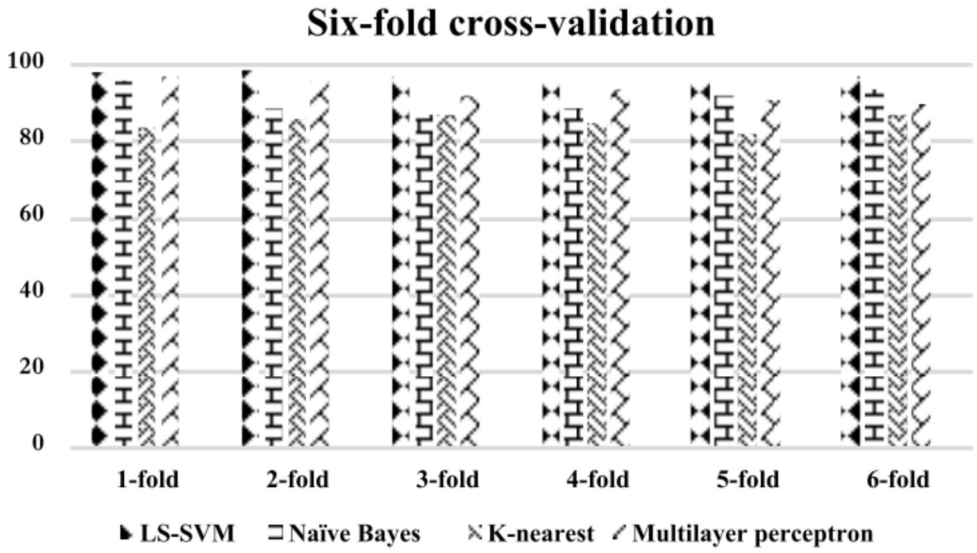

Figure 3: Six fold cross-validation result

4.2. Performance of Entropy based system

[6] used traffic cluster entropy as major part of detection metric which served two purpose of detecting a DDoS attack and also differentiating DDoS traffic from flash event traffic.

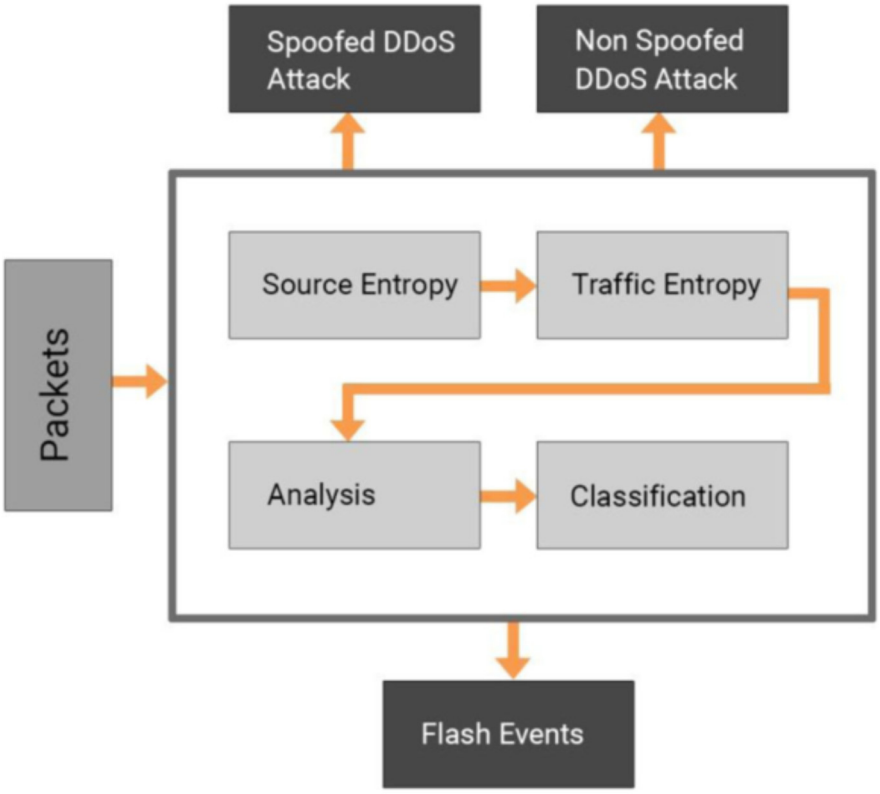

Figure 4: Proposed approach of [6] for classification of DDoS attack

The author took two variables as design parameter and after multiple simulation the two parameters are found to be 3 and 4 for best detection rate, 5 and 6 for normal defense and higher values for false positive rate. This shows that when the tolerance value is taken lower values, it will ensure reduction of false negative and thus increase the detection rate. The author in the paper compared the result with the result of his previous work and found out that the current proposed system performed better in terms of detection rate.

4.3. Performance evaluation of Regression based approach

First component of the performance evaluation is the data. Divakaran et al. [5] constructed data from multiple benign and malicious traffic because these are the kind of data involved in different types of attack including DDoS. And the author limited their scope of study to HTTP traffic only. There are two type of network traffic in their study. Normal traffic in which they used genuine network traffic captured from the co-authors and other set from publicly available source.

Related botnet	Total number of sessions	Detected sessions	Detection rate
Andromeda	148	132	89.2%
Barys	16	16	100.0%
Emotet	95	95	100.0%
Geodo	63	44	69.8%
Htbot	287	171	59.6%
Miuref	82	44	53.7%
Necurse	19	19	100.0%
Sality	440	435	98.9%
Vawtrak	40	40	100.0%
Yakes	39	25	64.1%
Zeus	168	133	79.2%

Figure 5: Malware Traffic Detection Result (Source: Divakaran et al.[5])

Another type of network traffic is malware traffic which is obtained from Stratosphere IPS Project (2016) which include data traffic generated by botnets like Andromeda, Emotet, Geodo, Miuref, Sality, Yakes and Zues. Finally they normalize the regression output in range [0,1] and defined 0.7 as borderline between malicious and genuine traffic where higher than 0.7 denotes high score and lower than 0.7 are considered low scores. From their analysis, the detection result obtained is tabulated below.

4.4. Performance evaluation of ANN based approach

Saied et al. [2] evaluated the ANN based solution on the basis of accuracy, precision, sensitivity (ability to identify positive result) and specificity (ability to identify negative result). They also compared their result with other approach like Snort[4], PNN, Chi-square, and found that this approach performed better in all four basis.

Approach	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)
Our approach	98	96	100	100
Snort	93	90	97	96
PNN [7]	92 (P1); 97 (P2)	NA	NA	NA
BP [6]	90 (BP)	NA	NA	NA
Chi-square [25]	94	92	NA	NA
K-PCA-PSO-SVM [26]	NA	96	NA	NA

Table 3: Comparison of ANN with other approaches

Also the comparison between old dataset and up-to-date dataset also affected the result in which up-to-date dataset solution produced an accuracy of 98 %. The performance is tabulated in table 3 and 4.

Our approach	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)
Old datasets	92	88	96	96
New datasets	98	96	100	100

Table 4: Comparision between old and up-to-date dataset

Table 4 shows that if the ANN is trained with up-to-date dataset, the accuracy of detecting new attacks in the future improves which is obvious and new dataset contain new signatures for new attacks and thus increase of detecting more attacks during detection phase. Further discussion is done in Section 5 with final remark of the report.

5. DISCUSSION AND CONCLUSION

The classification based proposed system by [1] has designed a good classifier using LS-SVM technique with promising accuracy but does not consider for spoofed IP addresses while the Entropy based system of [6] considers both spoofed as well as non spoofed IP addresses to detect the DDoS attacks and also distinguish attack traffic from the genuine flash event. Although [6] has considered their previous work and current proposed system and presented in favor of proposed system in terms of accuracy, the proposed system of [6] is only tested in simulated environment and the result may deviate from the result obtained when testing in the real environment.

The evidence detection of [5] using regression analysis only searched for the evidence of attack of different malware and does not provide concrete way around on how to prevent after the evidence has been obtained. Their framework has further scope of building an enhanced solution that not only gathers the evidence of the attack but also identify and classify the attack based on their profile (signature).

Finally the ANN based approach has few limitation as listed by the author themselves which all of the described system lacked. It is that if the attack packet's protocol headers are encrypted, then there is no any possible way to analyze the encrypted information from the headers. We require source IP, packet length, source port, destination IP, destination port, protocols used etc to analyze the packet for anomaly.

Another thing is that attacker is using newer and newer techniques of attack so we need to be up-to-date with our system of detecting and preventing such attack. For this the ANN based approach needs constant periodic training of the models so as to cover all the available attack techniques and provide maximum result for each future attacks.

Among the limitations described above, the limitation due to encrypted packet headers can be most challenging topic for future researches.

REFERENCES

[1] A. Sahi, D. Lal, Y. Li, and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment", in *IEEE Access*, vol. 5, pp. 6036-6048, 2017.

[2] A. Saied, R. E. Overhill, T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks", in *Neurocomputing 172*, pp. 385-393, 2016.

[3] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, The Economic Impact of Cyber-Attacks, document CRS RL32331, *Congressional Research Service Documents*, Washington, DC, USA, 2004.

[4] C. Bedon, A. Saied, Snort-AI (Version 2.4.3), "Open Source Project", 2009. Available from: http://snort-ai.sourceforge.net/index.php/

[5] D. M. Divakaran, K. W. Fok, I. Nevat, and V. L. L. Thing, "Evidence gathering for network security and forensics", in *Digital Investigation 20*, pp. S56-S65, 2017.

[6] J. Gera, and B. P. Battula, "Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds", in *EURASIP Journal on Information Security,* doi:10.1186/s13635-018-0079-6, 2018.

[7] M. Roesch, Snort (Version 2.9), "Open Source Project", 1998. Available from: http://www.snort.org/.

[8] R. Russell, Iptables (Version 1.4.21), "Open Source Project", 1998. Available from: http://ipset.netfilter,org/iptables.man.html/.