Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FLOW BASED MULTI FEATURE INFERENCE MODEL FOR DETECTION OF DDOS ATTACKS IN NETWORK IMMUNE SYSTEM

[1]S.VASANTHI, [2]S.CHANDRASEKAR

[1]Associate Professor/IT, Sona College of Technology, Salem, Tamil Nadu, INDIA.
[2]Principal, Gnanamani College of Engineering, Namakkal , Tamil Nadu, INDIA.
E-mail: [1]vasanthiphd123@gmail.com

ABSTRACT

Network immune systems have been developed in many ways but differ with the feature set used and suffer with identifying network threats in efficient manner. We propose a multi feature inference model which uses various parameters of network flow. Unlike earlier approaches, the proposed method infers valuable knowledge from the packet flow and packet details to detect DDOS attacks. The proposed method uses, hop count, hop details, payload, Time to live with time variant information's. The network packets are monitored about their traversal, through which they forwarded towards destination. We consider the botnet attacks, which is supported by dedicated nodes distributed throughout intermediate network. Whenever a new packet received at the network various features are extracted and we compute the probability of genuine value according to the features. The proposed immune system maintains packet trace for each of the packet received at various time domains. At each time window, for each distinct traversal path an probability value is computed using the features extracted from traffic trace. The inferred results are applied do denial the service for the malicious nodes. The result will be inferred using computed probability value to allow or deny the packet into the network.

Keywords: *Intrusion Detection System, Network Immune System, Botnet, Flow Based Inference Model, Denial of Service Attacks.*

1. INTRODUCTION

The growth of internet technology increases the growth of network attacks, also the type of threats are increasing every day. The network threats can be broadly classified as flow based or connection based threats. In flow based approach, the malicious user could generate enormous number of packets towards a service point, which is greater than the capacity of the service. Whereas in case of connection based attack, malicious node may hold many number of connections without performing any data transfer on that. We focus on the previous one, also it becomes more complicated to distinguish the genuine packets from malicious one.

There are various approaches has been proposed in literature, which uses packet details like pay load, hop count and ttl values. Most of the methods suffers with identifying the host which generate malicious packet and will not be effective where there are dynamic addressing nodes present. The growth of internet technology leads the support for malicious nodes to group compromised nodes to perform flow based attacks. The botnets are set of nodes to form a network with dedicated compromised nodes using which the nodes can generate malicious packets.

DDOS-Distributed denial of service attacks, the more dominating kind of attack generated in networks with the intension to reduce the throughput of the network and reduce the service performance. The DDOS attacks are initiated from various nodes of the network and sends malicious packets towards the servicing node. Whenever a servicing node receives a malicious packet, it spends some time on that and drop the packet finally. What happens is, the servicing node could not spend time on genuine nodes and the frequency of getting allocated to the genuine node reduces. Such a malicious nodes and their packet has to be identified and dropped, and performing that process is named as distributed denial of service. By adapting DDOS approach, the malicious nodes will not be provided service and whatever the packets comes from the malicious nodes will be dropped so on.

Because of the presence of botnets, the network immune systems could not take any decision about the packet and the decision making becomes more complicated. Even though every packet approaches the network through different traversal path, identifying them as malicious is impractical. Flow based inference model, is the process of generating the probability value to infer some valuable knowledge using which the packet can be allowed or denied. The flow of packet per each time window can be identified and their payload, ttl values can be used to generate the probability of trustworthy of the packet.

2. RELATED WORKS

There are various approaches have been discussed in the literature, we explore few of them according to the problem. For the immune system, various researchers proposed many methodologies and they each have their own merits and demerits and discuss a few of them here.

FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks [1], address the problem of DDoS attacks and presents the theoretical foundation, architecture, and algorithms of FireCol. The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information.

A DDoS attack by flooding normal control messages in Kad P2P networks [2], introduces a new DDoS attack by flooding control messages from normal users in Kad network, which is DHT-based P2P network. The proposed attack can make normal nodes participated into the Kad network to act as if they were zombies to generate numerous control messages destined to a target system unintentionally. With the flooded control messages from those nodes, it can cause a DDoS effect to a certain system.

In DDoS Attack Detection and Attacker Identification [3], they first identified the types of DoS and DDoS attack. Then we have provided the solution for those attacks on the basis of attacker's identification. Main focus of this paper is to identify the actual attacker, who has performed attack by sitting behind a forged System. For that purpose first we prevent IP forgery by using sender authentication process, then calculate TCP flow rate and from it we identify whether packets are nor- mal packet or malicious packet. We detect attack on receiver proxy server by using entropy and normalize entropy calculation on receiver proxy server. If attack is detected then we drop packets, get their mark value and trace them back to the source. Finally we use the concept of ISP and IANA to identify the actual attacker.

DDoS Detection Algorithm Based on Preprocessing Network Traffic Predicted Method and Chaos Theory [4], pre-process network traffic by cumulatively averaging it with a time range, and using the simple linear AR model, and then generate the prediction of network traffic. Secondly, assuming the prediction error behaves eechaoticallyee, we use chaos theory to analyze it and then propose a novel network anomaly detection algorithm (NADA) to detect the abnormal traffic. With this abnormal traffic, we lastly train a neural network to detect DDoS attacks.

A collaborative detection of DDOS attacks [8], propose a distributed methodology which involves installing the attack detectors at various parts of the network. Each router in the network will monitor the traffic flowing through it and if any anomaly in the traffic pattern is detected, it will raise an alarm to the nearby routers. The alarm propagates to all the routers through which the attack flows. By this way a tree like construct is made, which will have information about number of alarms raised and the path of the attack flow. If the construct shows any converging pattern then it is declared as DDoS attack.

Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art [9], present a comprehensive study to show the danger of Botnet-based DDoS attacks on application layer, especially on the Web server and the increased incidents of such attacks that has evidently increased recently. Botnet-based DDoS attacks incidents and revenue losses of famous companies and government websites are also described. This provides better understanding of the problem, current solution space, and future research scope to defend against such attacks efficiently.

Detecting And Analyzing DDoS Attack Using Map Reduce In Hadoop [11], proposed a new approach to handle Big data Hadoop technology takes cardinal part in analysis. They proposed detection of DDoS attack by using Counter based algorithm and Access Pattern algorithm which will implemented in Hadoop framework. Along this we can provide future prediction functionality using analytics. Dashboard provides visual view which will help to unveil the attacker and loyal user along with statistics.

Adaptive Discriminating Detection for DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient with Collective Feedback [12], concentrating flash crowd and DDoS there are two steps involved, first it is necessary to differentiate normal traffic and flash crowd by using Flash Crowd Detection Algorithm. Second we have to differentiate flash crowd and DDoS by using Flow Correlation Coefficient (FCC). By using this FCC value, algorithm proposed called Adaptive discrimination algorithm is used to detect the DDoS from the flash crowd event. And a sequential detection and packing algorithm used to detect t he attacked packets and filter it out .By using above mentioned algorithms we can improve the accuracy in filtering the attacked packets and also the time consummation is reduced.

A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment [13], proposes a method of integration between HTTP GET flooding among Distributed Denial-of-Service attacks and Map Reduce processing for fast attack detection in a cloud computing environment. In addition, experiments on the processing time were conducted to compare the performance with a pattern detection of the attack features using Snort detection based on HTTP packet patterns and log data from a Web server.

Detecting DDOS Attacks by Circular Protection Network [14], addresses this problem by using the firecol whose core is composed of a ring of Intrusion prevention systems(IPS) defends by exchanging only a selected traffic. Also they address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of the circular protection network. The core is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information.

Novel DoS/DDoS Attack Detection and Signature Generation [15], presents a light-Weight mechanism to detect novel DoS/DDoS (Resource Consumption) attacks and automatic

Signature generation process to represent them in real time. Experimental results are provided to support the proposed mechanism.

All the above discussed approaches have used variety of DDOS detection approach but suffer with the newly arriving attacks. We propose such a naval approach to handle future attacks and increase the throughput of the network.

3. PROPOSED METHOD

The proposed method has four stages namely: Packet Capturing, Feature Extraction, Log Generation, Time variant multi Feature Inference Generation.

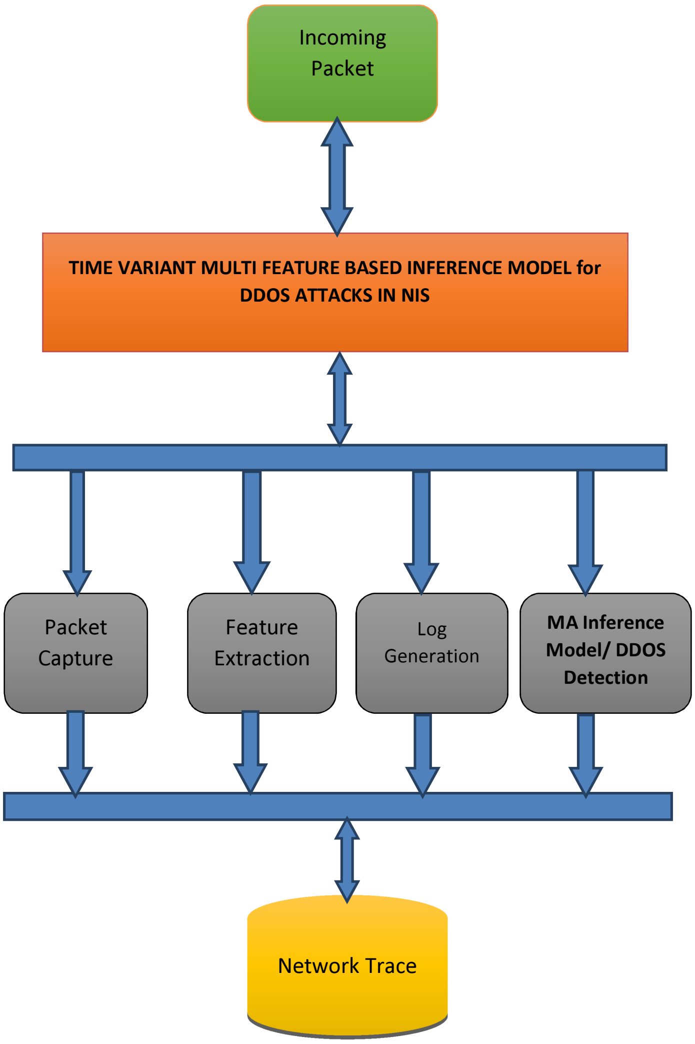

Incoming Packet
TIME VARIANT MULTI FEATURE BASED INFERENCE MODEL for DDOS ATTACKS IN NIS
Packet Capture
Feature Extraction
Log Generation
MA Inference Model/ DDOS Detection
Network Trace

Figure1: Proposed Method Architecture.

3.1 Packet Capturing:

The packets approaches the network is captured in distributed manner to support intrusion detection. The network level packets are monitored and captured at the interfaces and adapters attached to the nodes of the network. Whenever a new packet reaches the network gateway or general node will be captured and handover to the intrusion detection procedure.

```
Input: Packet P
Output: Packet P.
Step1: Initialize Malicious node list Ml.
Step2: Extract packet Address from P
Step3:verifiy the presence of packet address in Ml.
Step4: If found then
            Add Packet address to malicious list Ml
        else
            continue;
        end.
Step5: Stop.
```

3.2 Feature Extraction:

For each packet received the following features are extracted as ; pay load, sequence number, hop count , hop addresses, time to live. The packet is converted into IP packet to extract the address of packet and its pay load size is extracted using the packet format and ttl value is computed using the time available at the time slot of the packet. Extracted packet is converted into a feature vector which represents the packet information in computational form.

```
Algorithm:
Input: Packet P.
Output: Feature Vector V.
Step1: initialize V.
```

```
Step2: convert raw packet into IP Packet
        Extract packet source Address Saddr.
Step3: Extract Communication Header CMN_HDR.
        HopCount = CMN_HDR(hcount).
        TTL = CMN_HDR(ttl).
        Hop Address Set Hs = CMN_HDR(ha).
Step4: Extract payload from p.
Step5: V = {Saddr, Daddr, HopCount, TTL, payload, Hs}.
Step6: Stop.
```

3.3 Log Generation:

The proposed method generates log for each packet received at the network interface of the node attached to the network. Whenever a packet is received, a distinct log will be generated using the feature extracted. For each log , an distinct time value will be assigned to represent the time at which the packet is received. The feature extracted from the previous procedure is used and a new time value will be assigned for the packet received. The log with new time value and feature set will be inserted into the network log trace.

```
Input:Feature Vector v.
Output: Log l.
Step1: read network log Nl.
Step2:initialize timer T.
Step3: generate current time Ct.
Step4: construct log Cl = ∑ Fv.Feature, Ct.
Step5: insert log to L.
        L = ∑l+cl.
Step6: stop.
```

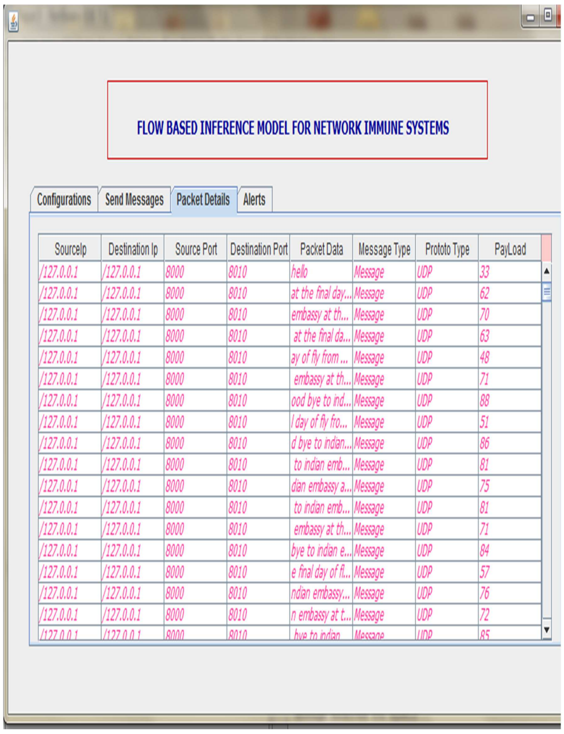
3.4 Time Variant Multi Feature Inference Model & Ddos Attack Detection:

At this stage the logs from the trace where taken for processing. First, the traces will be split based on time window. The time will be divided into small time frames and the logs split will be named accordingly. For each log of the time window, we compute the common nodes present in the traversal path of packet and then access rate will be computed. The packet will be identified only based on the network access rate and if its greater than threshold then the particular node will be identified as malicious node. Further the packets received from such a node will be dropped.

```
Input: Network Log L.
Output: Inference Value.
Step1: initialize inference value, Network Access Rate NARS, Malicious Node list Ml.
Step2: For each time window $T_i$
        Extract logs Tl = $\int_1^{size(L)} L \times Ti$
        Extract common nodes present in Tl.
                CN = Ω(Tl).
        For each path p from Cn
    Compute network access rate NAR = $\int (Np *$Payload)/TTL
    NARS(i) = NARS(i)+NAR.
        End.
      End.
Step3: For each Time window $T_i$
    If NARS($T_i$)> Threshold
     Infernce=false
    Mark packet source address as malicious node.
    Add node address to malicious list. Ml = ΣNodes(Ml)+Saddr.
          End
         End.
Step4: stop.
```

4. RESULTS AND DISCUSSION

The proposed flows based multi feature inference model has been implemented and evaluated for its efficiency. The proposed method has been tested with variety of node sets and traces. The proposed method has produced efficient results compared to other approaches. This approach has increased the frequency of DDOS attack detection and supports increasing the throughput of the network.

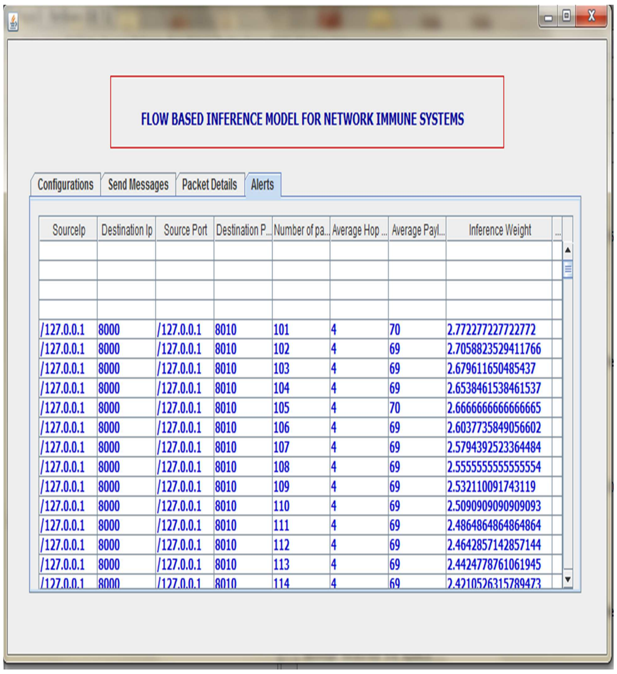


FLOW BASED INFERENCE MODEL FOR NETWORK IMMUNE SYSTEMS

SourceIp	Destination Ip	Source Port	Destination Port	Packet Data	Message Type	Prototo Type	PayLoad
/127.0.0.1	/127.0.0.1	8000	8010	hello	Message	UDP	33
/127.0.0.1	/127.0.0.1	8000	8010	at the final day...	Message	UDP	62
/127.0.0.1	/127.0.0.1	8000	8010	embassy at th...	Message	UDP	70
/127.0.0.1	/127.0.0.1	8000	8010	at the final da...	Message	UDP	63
/127.0.0.1	/127.0.0.1	8000	8010	ay of fly from ...	Message	UDP	48
/127.0.0.1	/127.0.0.1	8000	8010	embassy at th...	Message	UDP	71
/127.0.0.1	/127.0.0.1	8000	8010	ood bye to ind...	Message	UDP	88
/127.0.0.1	/127.0.0.1	8000	8010	l day of fly fro...	Message	UDP	51
/127.0.0.1	/127.0.0.1	8000	8010	d bye to indian...	Message	UDP	86
/127.0.0.1	/127.0.0.1	8000	8010	to indian emb...	Message	UDP	81
/127.0.0.1	/127.0.0.1	8000	8010	dian embassy a...	Message	UDP	75
/127.0.0.1	/127.0.0.1	8000	8010	to indian emb...	Message	UDP	81
/127.0.0.1	/127.0.0.1	8000	8010	embassy at th...	Message	UDP	71
/127.0.0.1	/127.0.0.1	8000	8010	bye to indian e...	Message	UDP	84
/127.0.0.1	/127.0.0.1	8000	8010	e final day of fl...	Message	UDP	57
/127.0.0.1	/127.0.0.1	8000	8010	ndian embassy...	Message	UDP	76
/127.0.0.1	/127.0.0.1	8000	8010	n embassy at t...	Message	UDP	72
/127.0.0.1	/127.0.0.1	8000	8010	bye to indian...	Message	UDP	85

Figure2: Snapshot Of Packet Capture Results And Packet Details

The figure2 shows the result of packet captured and features of packet received. It shows all the features of packet received at the inference node.

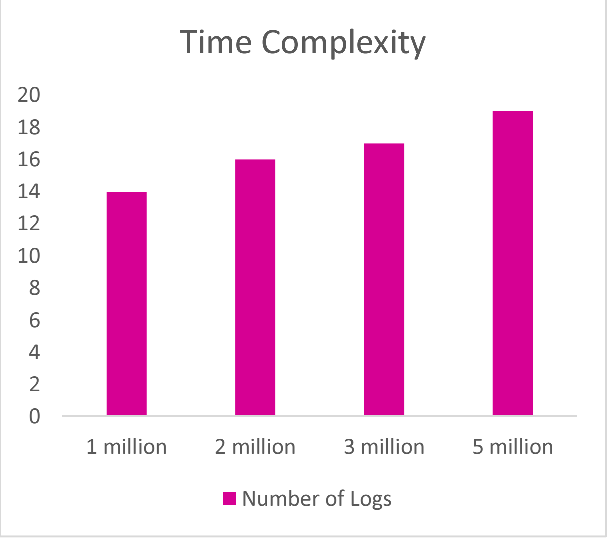


FLOW BASED INFERENCE MODEL FOR NETWORK IMMUNE SYSTEMS

SourceIp	Destination Ip	Source Port	Destination P...	Number of pa...	Average Hop ...	Average Payl...	Inference Weight	...
/127.0.0.1	8000	/127.0.0.1	8010	101	4	70	2.772277227722772	
/127.0.0.1	8000	/127.0.0.1	8010	102	4	69	2.7058823529411766	
/127.0.0.1	8000	/127.0.0.1	8010	103	4	69	2.679611650485437	
/127.0.0.1	8000	/127.0.0.1	8010	104	4	69	2.6538461538461537	
/127.0.0.1	8000	/127.0.0.1	8010	105	4	70	2.6666666666666665	
/127.0.0.1	8000	/127.0.0.1	8010	106	4	69	2.6037735849056602	
/127.0.0.1	8000	/127.0.0.1	8010	107	4	69	2.5794392523364484	
/127.0.0.1	8000	/127.0.0.1	8010	108	4	69	2.5555555555555554	
/127.0.0.1	8000	/127.0.0.1	8010	109	4	69	2.532110091743119	
/127.0.0.1	8000	/127.0.0.1	8010	110	4	69	2.5090909090909093	
/127.0.0.1	8000	/127.0.0.1	8010	111	4	69	2.4864864864864864	
/127.0.0.1	8000	/127.0.0.1	8010	112	4	69	2.4642857142857144	
/127.0.0.1	8000	/127.0.0.1	8010	113	4	69	2.4424778761061945	
/127.0.0.1	8000	/127.0.0.1	8010	114	4	69	2.4210526315789473	

Figure3: Result Of Proposed Approach.

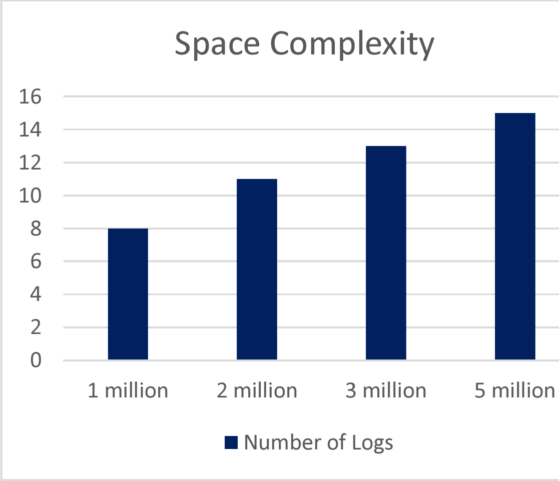
The figure3, shows the result generated by the proposed approach and it shows the computed legitimate weight of all the packets and distinct nodes of the network.



Graph1: Time Complexity Of Proposed Method.

The graph 1 shows the time complexity generated by the proposed method, and the proposed method has produced less time complexity at different number of logs available.

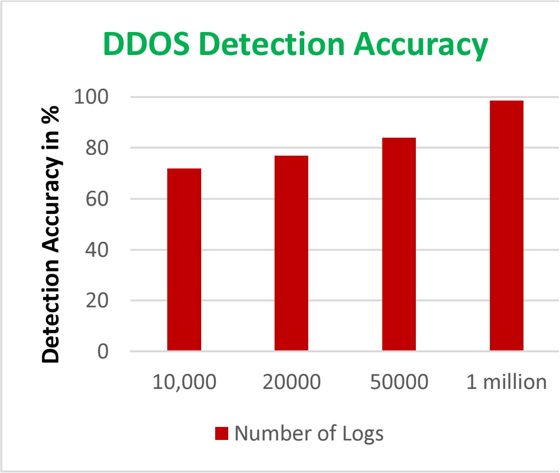
It shows that the proposed method has produces less time for many numbers of logs.



Graph2: Space Complexity Of Proposed Method.

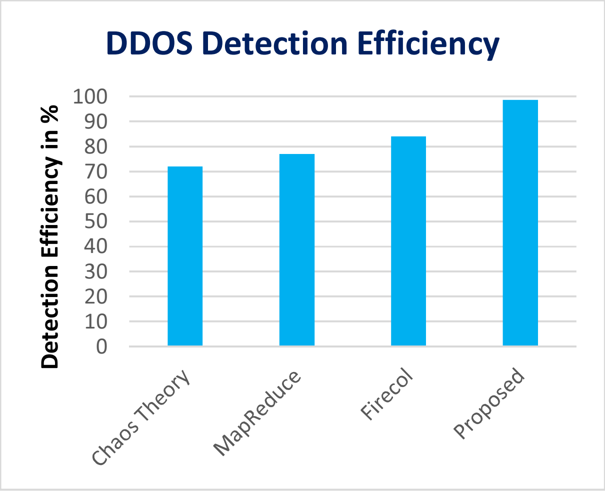
The graph2 shows the time complexity value generated for different number of logs available. It shows that the proposed method has produces less space complexity even at higher number of logs.

The distribute denial of service attack detection accuracy is computed according to the number of malicious packets arrived at particular time window and number of packets analyzed as malicious.



Graph3: Shows The Accuracy Of Time Values.

The graph3, shows the accuracy of DDOS attack detection and it shows that the proposed approach has produced efficient results.



Graph4: Shows The Comparison Of Ddos Detection Efficiency.

The graph4 shows the comparison of results on detection efficiency produced by different algorithms and it is clear that the proposed method has produced higher efficiency than previous approaches.

5. CONCLUSION

We proposed a flow based multi feature inference model for DDOS attack detection in immune systems. The proposed method captures the packet and extracts various features to generate the time variant log. For each time window, we identity the set of distinct traversal paths and compute network access rate using the logs generated. The generated network access rate is used to compute the inference value, using which the packet will be allowed or denied from the network. The proposed method reduces the frequency of threats compared to other approaches and produces less time and space complexity values.

REFERENCES

[1] Francois.J, FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks , IEEE Transaction on Networking, Vol.20,issue.6,pp.1828-1841,2012.

[2] Hyelim koo, A DDoS attack by flooding normal control messages in Kad P2P networks, International conference on advanced communication technology, pp.213-216, 2012.

[3] Brajesh Kashyap and S K Jena. Article: DDoS Attack Detection and Attacker Identification. International Journal of Computer Applications 42(1):27-33, March 2012.

[4] Chen, Yonghong, DDoS Detection Algorithm Based on Preprocessing Network Traffic Predicted Method and Chaos Theory , IEEE Transaction on communications, vol.17, issue.5, pp.1052-1054,2012.

[5] Yang Xiang,Wanlei Zhou, “Low-Rate DDOS Attack Detection and Traceback with New Information Metrics”, IEEE transactions on information forensics and security, vol. 6-no. 2, june 2011.

[6] Rizwan Khan , A. K. Vatsa, “Detection and Control of DDOS Attacks over Reputation and Score Based MANET”, Journal of Emerging Trends in Computing and Information Sciences, vol. 2, No 11, October 2011.

[7] S.Raja Ratna, Mitigating Denial of Service Attacks in Wireless Networks, International Journal of Advanced Research in Computer Engineering & Technology, Volume 2, No 5, May 2013..

[8] Shalinie S.M, CoDe — An collaborative detection algorithm for DDoS attacks, International conference on recent trends in information technology, pp.113-118,2011.

[9] Esraa Alomari, Selvakumar Manickam, B B Gupta, Shankar Karuppayah and Rafeef Alfaris. Article: Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications 49(7):24-32, July 2012.

[10] Moti Geva, Amir Herzberg, Yehoshua Gev, "Bandwidth Distributed Denial of Service: Attacks and Defenses", IEEE Security & Privacy, vol.12, no. 1, pp. 54-61, Jan.-Feb. 2014.

[11] G.S. Navale, Detecting And Analyzing Ddos Attack Using Map Reduce In Hadoop, International Journal of Industrial Electronics and Electrical Engineering, Volume- 2, Issue- 2, Feb.-2014.

[12] N.V. Poornima, Adaptive Discriminating Detection for DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient with Collective Feedback, International Journal of Innovative Research in Computer and Communication Engineering , Vol.2, Special Issue 1, March 2014.

[13] Junho Choi, A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Springer, Soft Computing, 2014.

[14] Yamini, Detecting DDOS Attacks by Circular Protection Network , International Journal of Innovative Research in Computer and Communication Engineering , Vol.2, Special Issue 1, March 2014.

[15] Vijay Katkar and S G Bhirud. Novel DoS/DDoS Attack Detection and Signature Generation. International Journal of Computer Applications 47(10):18-24, June 2012.

[16] Prajeet Sharma, Niresh Sharma and Rajdeep Singh. Article: A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. International Journal of Computer Applications 41(21):16-21, March 2012.