Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

Service oriented Multi Model Network Inference Model for Identifying Denial of Service Attack in Network Immune System

Vasanthi S[1*], ThangarajK[2], Ilanchezhian P[3], Aldo Stalin JL[4]
[1,3]Associate Professsor/IT, Sona College of Technology, Salem, Tamilnadu, India
[2,4]Assistant Professsor/IT, Sona College of Technology, Salem, Tamilnadu, India

*vasanthi_sv@sonatech.ac.in

ABSTRACT

Identifying DDOS attacks has become more important task in network management and security where the immune system has responsibility of securing services and data available in the network. We propose a service oriented multi model (SOM) network inference model for identifying DDoS attacks, which consist of several phases. The SOM network inference model provides the solution for variety of services. Unlike other methodology available, the proposed model uses various metrics at various levels and combines the earlier models at required stages of identification process. The proposed model maintains the log trace where the features of packets are kept stored which are already received. The proposed approach extracts various features like ttl, payload, hop count, addresses, time, service details. Using those logs, the proposed approach splits them into time domain values for each of the distinct services available. The model maintains the protocol of services available and based on that the service access history according to each time window is split into different numbers, from which the flow approximation is computed using previous access history. Based on the results of time orient and flow approximation, the proposed model infers the packet signature. The proposed model produces efficient results and reduces the time complexity.

Keywords
DDOS, Service oriented multi model, Network metrics, Packet signature

Introduction

Modern communication and information systems have become more sophisticated due to increased solution. The organizations maintain their valuable resources at different locations of their network and in many computers. Also, there are service providers who provide services through which the user can access the required data to complete his task. Even though the service provider has security measures to access the service, even the genuine user initiates some malformed request to the service with the intention to degrade the service quality. Not only the service but also the channel gets disturbed due to some malicious users.

Generally, there are varieties of network attacks which can be of flow based network attack or connection based network attacks. In the case of flow based network attack the intruders tends to attack the channel capacity so that he floods enormous amount of packets to the channel. Similarly, in case of connection based attacks, the malicious user tends to attack the service throughput or network throughput. In the second case, a malicious user might hold number of connection for particular time without passing any information on that and the connection will be presented simply idle. In both the cases, the network and its services are getting affected hugely, which has to be avoided to improve the network performance. There are solutions for both, but the method focuses on any one of them, but only few solutions are there to handle both but misses various features of the request.

The service oriented architecture is one where the security measures are focused to secure the service from variety of attacks raised through the network. Generally the DDoS attacks are

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

focused toward a service point and with the intention to degrade the service quality. Our ultimate aim is to identify such attacks in wide spectrum to support network performance.

There are various methods has been discussed and available, but most of them suffers with the efficiency of DDoS detection. Some models uses only the hop details to identify the malicious user, some may use packet information to decide the packet status. All of them have problem with identifying the genuine packet from other packets. The inference model is one, which infers some conclusion using available history of records, packet signature, service details.

Literature Review

There exist various approaches for distributed denial of service detection and we discuss few of them here with the problem identified.

Haldar, N.A.H (2012) proposed an activity pattern for host based intrusion detection system [1], presents a wireless intrusion detection device that uses pattern recognition techniques to model authenticated users' usage habits and uses it to detect intrusions. The proposed intrusion detection system's main concept is to distinguish discriminative features from user activity data and use them to detect intrusions in wireless networks. The detection module employs the PCA technique to collect statistical variables of interest and compares them to thresholds obtained from user activity data. An alarm is triggered when the variables surpass the predicted thresholds, signalling a potential network intrusion. The proposed system is unique in that it has a light-weight architecture that needs fewer computing and memory resources and can be used in a real-time environment.

Yamini (2014) developed a method for Detecting DDOS Attacks by Circular Protection Network [2] , which tackles the DDos attack issue by using a firecol whose core is made up of a ring of Intrusion Prevention Systems (IPS), which defends by exchanging only a specific traffic. They also discuss DDoS attacks and present the circular security network's theoretical foundation, design, and algorithms. Intrusion prevention systems (IPSs) at the Internet service provider (ISP) level make up the heart. By exchanging selected traffic information, the IPSs form virtual security rings around the hosts to defend and collaborate.

Sridevi R (2012) suggested a Genetic algorithm and artificial immune systems [3], which is a new type of network security protection technology that can be used as a countermeasure to maintain data integrity and device availability in the event of an attack.An optimal IDS framework should be able to evolve over time in order to detect both known and unknown attacks. Algorithms involving Genetic Engineering and Immune Systems are known to evolve and learn from small examples. They proposed to investigate the efficacy of genetic search methods for feature selection and Immune system to classify threats and non threats.

JunyuanShen(2011)[4] proposed a Network intrusion detection based on artificial immune system. This approach uses genetic algorithm to generate detector which is then used to detect anomalous behaviour in the network. For the detection procedure, the Minkowski distance function is compared to the Euclidean distance. It has been shown that the Minkowski distance produces better results than the Euclidean distance, and that it can produce excellent results in

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

less time. The overall average detection rate is 81.74 percent, compared to 77.44 percent when using the Euclidean distance.

N.V. Poornima (2014) proposes Adaptive Discriminating Detection for DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient with Collective Feedback [5], There are two steps to this process of concentrating flash crowd and DDoS. First, using the Flash Crowd Detection Algorithm, distinguish normal traffic from flash crowd. Second, we must use the Flow Correlation Coefficient to distinguish between flash crowd and DDoS. (FCC). The proposed Adaptive discrimination algorithm is used to detect the DDoS from the flash crowd event using this FCC value. A sequential detection and packing algorithm was used to detect and filter out the attacked packets. We can increase the accuracy of filtering the attacked packets and reduce the amount of time it takes by using the algorithms described above.

Live Baiting for Service-Level DoS Attackers by Khattab et.al (2008) [6], is discussed in the aim of identifying defective members of the group. The live baiting is used to detect intruders using minimal state overhead without any models for neither legitimate behaviour nor anomalous behaviour. The amount of state required for live baiting is proportional to the number of attackers rather than the number of clients. This cost-cutting enables live baiting to expand to large-scale networks of millions of users.

Thai et.al [7] (2008) proposed a detection technique for identifying malicious Users Using Group Testing Techniques [38], discusses a theoretical model to provide security over service orient architecture. The proposed size constraint group testing (SCGT) works based on the size of the network and they discuss various approaches for different network scenarios.

JunhoChoi(2014) [8], framed a DDoS attack detection technique in cloud computing environment by making use of HTTP packet pattern and rule engine.For fast attack detection in a cloud computing environment, the DDoS attack detection technique proposes a method of integrating HTTP GET flooding among Distributed Denial-of-Service attacks and Map Reduce processing. Furthermore, experiments on processing time were carried out to compare the results with a pattern detection of attack features using Snort detection based on HTTP packet patterns and log data from a web server.

All the above discussed methods have the problem of time complexity and need proactive information and produce less efficiency in intrusion detection. We propose a multi model approach for detecting DDoS attacks which will enhance the network security.

Methodology

We propose a service oriented multi model network inference system to identify the DDoS attacks, the proposed approach has three functional modules namely:

- Packet Tracing
- Service Oriented Analysis
- DDoS attack detection.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

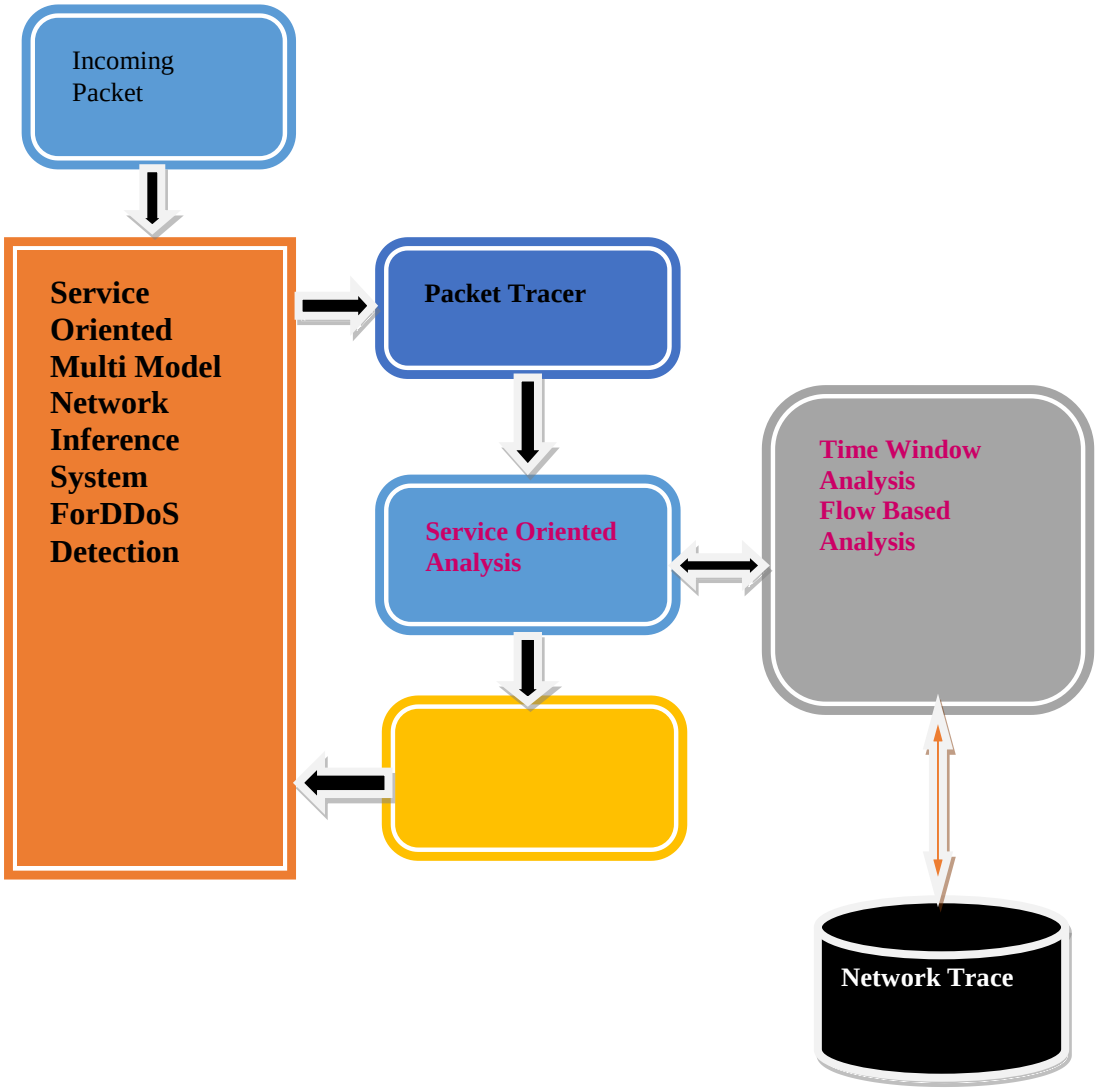

Figure.1 Proposed System Architecture.

Packet Tracing:

The packet which is entering the network is captured and the features information of the packet are extracted. The proposed method extract the following features from the incoming packet like TTL, PayLoad, Time, Source ip address, Destination ip address, Source Port value, Destination Port value, Hop Count, Hop Addresses, service Name, Service Id. From extracted features , a vector is constructed to be stored in the log trace. The proposed approach maintains two different logs as genuiness and malicious. The extracted feature will be given to the SOA for performing DDoS attack.

Algorithm:

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

Input: Raw Packet Rp.
Output: Feature vector v.
step1: IP Packet ipp = convert raw packet into ip packet.
step2: extract source ip, destination ip, source port, destination port, ttl values.
step3: extract hop count, hop addresses from communication header.
step4: Identify service id, service name.
step5: construct feature vector v = {Sip, Dip, Sport, Dport, Ttl, Haddrs, HopCount, ServiceID, Service Name}.
Step6:stop.

Service Oriented Analysis:

At this stage , the extracted features are used to identify whether the packet received is malicious or genuiness. The SOA retrieves the previous logs generated by system and splits them into different groups based on available services. There exists many services in the network and the logs of distinct services are grouped separately. The overall time window is split into number of windows of small size and based on the time window the logs of service groups are split into sub groups. Now we have small set of service groups where each has logs of distinct service. First we identify the service to which the packet is belongs and we separate the logs from others. Second we perform time orient analysis on the logs of specific service, with the flow approximation. We compute the service access weight of the packet using which further DDoS detection will be performed.

Pseudo Code:

Input: Feature vector v, Network Trace Nl.
Output: Service Access Rate SAR, Channel Access Rate CAR.
step1: for each time window Tw
Compute Total Number of service Accessed.
Compute service access rate using number of all services accessed from the hop and hop counts.
end.
Step2: For each time window
Compute total number of channel access.
Compute channel access rate
end.
Step3: stop.

The total number of channel access is computed using the following equation.

$$Tca = \int_{i=0}^{i=N} \sum Nl(Tw_{I,} \text{Haddress}) \text{ ---------- (1).}$$

The channel access rate can be computed using the equation (2):

$$CAR = \frac{\Sigma Tca}{\Sigma Nl(Twi, All\ Services) \times \emptyset} \times \frac{THC}{Tca} \text{ ---------- (2).}$$

Denial of Service Attack Detection

The DDoS attack detection is performed based on computed values of service access rate and channel access rate. With the malicious and genuiness history we compute the Service Denial factor which show the genuiness value using which we can infer that the packet received is

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

genuine or not. With the malicious history , we compare the pattern of feature and looks for the match to be found. We compute service denial factor for the packet received for the same source address. We collect all the malicious traces and identify the hop address and their pattern the we match with the pattern followed by the source packet. Based on that we compute the service denial factor and then based on pre computed access rates the final inference will be taken.

Algorithm:

Input: Malicious History Mh, Packet Feature v, SAR,CAR
Output: Boolean service-flag.
step1: for each history H_i from Mh
compute total Hops addresses matched using equation (3).
end
Step2: compute Hop similarity value Hsv using equation (4).
Step3: Compute Access Rate using service access rate and channel access rate.
Step4: if AR<ATh and Hsv<HTh then
return true.
else
Generate log in data base.
return false.
end

SHa= $\int_{j=0}^{N} \sum HopAddr(Hi) \in v(Haddr)$ ---------- (3).

Hsv = $\frac{SHa}{Total\ Number\ of\ packets\ received\ from\ Hop\ address}$----------(4).

Results and Discussion

The service oriented Multi model network inference model has generated good results. Unlike other immune systems, the proposed framework uses a service-oriented approach to counter both connection and packet-based attacks. We compute the service access rate and channel access rate for the packet being received and its hop from where the packet has been originated. Also we compute the hop similarity value for the packet being received with the trace list and finally we conclude the packet based on the thresholds used for access rate and hop similarity. As a result, the proposed method has a high success rate in detecting malicious packets and lowering the attack rate.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

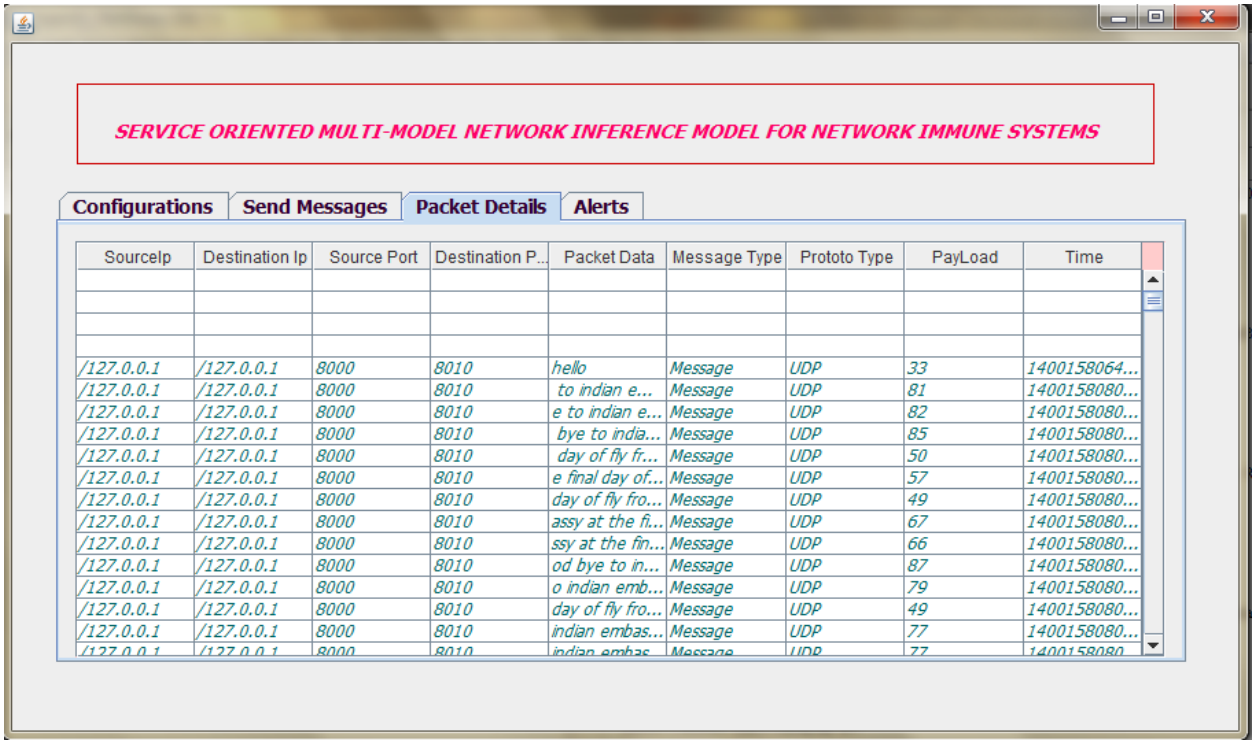

Figure.2: The packet features extracted from the received packet

Figure 2 shows the packet details extracted from the received packets through the gateway of the network. It is clearly visible that all the features mentioned in the paper have been extracted for the detection of genuiness of packet. The details displayed in the form has various parameters and the protocol name shows the service accessed and the payload details shows the payload details of the packet received. The source ip and destination ip values in the form shows the source address and destination address of the packet received.

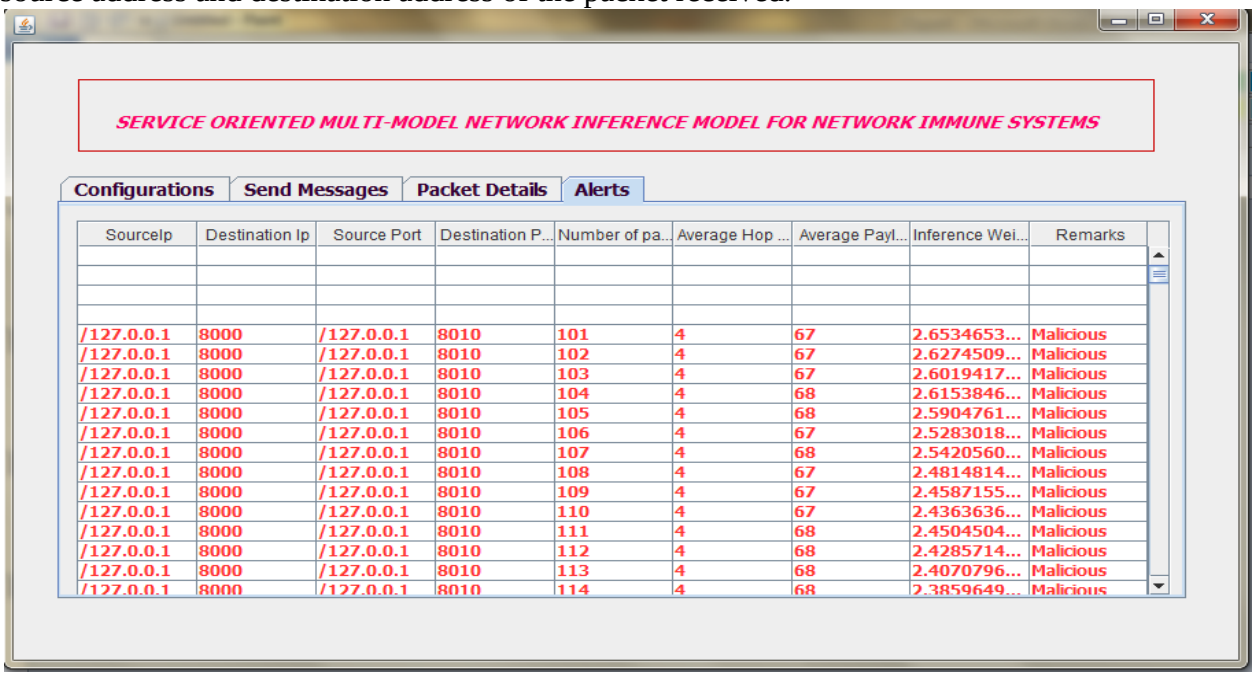

Figure.3: The result of proposed approach.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

The figure 3 shows the details of packets concluded as malicious packets. We have computed the inference weight for all the distinct nodes of the network and the details are furnished clearly.

Trace

ID	Slp	Sp	Dlp	Dp	Mess	Ptype	Payload	Hopcount	TTL
1	192.168.1.4	9000	146.128.3.7	9000	hello	TCP	92	17	23
2	192.138.4.90	9000	146.128.3.7	9000	raj	TCP	27	12	12
3	123.142.5.9	9000	146.128.3.7	9000	wellaodoc	TCP	13	4	23
4	192.168.1.4	9000	146.128.3.7	9000	heraldfsd	TCP	67	13	45
5	192.138.4.90	9000	146.128.3.7	9000	lsdfjs	TCP	87	5	6
6	123.142.5.9	9000	146.128.3.7	9000	weoruwjr	TCP	54	13	7
7	192.168.1.4	9000	146.128.3.7	9000	sdfhfs	TCP	33	55	8
8	192.138.4.90	9000	146.128.3.7	9000	dfgsgdfg	TCP	22	6	33
9	123.142.5.9	9000	146.128.3.7	9000	gdfgfdg	TCP	25	11	22
10	192.168.1.9	9000	146.128.3.7	9000	hello	TCP	74	45	12
11	192.168.2.4	9000	146.128.3.7	9000	fdgdfg	TCP	21	11	11
12	192.168.3.6	9000	146.128.3.7	9000	fhfgh	TCP	54	12	22
13	192.168.6.9	9000	146.128.3.7	9000	fghgfh	TCP	32	14	33
14	192.168.11.4	9000	146.128.3.7	9000	fghfghgjghjrert	TCP	55	41	44
15	192.118.11.14	9000	146.128.3.7	9000	rytrygh	TCP	11	17	55
16	192.168.1.4	9000	146.128.3.7	9000	hai	TCP	34	32	22
17	192.138.4.90	9000	146.128.3.7	9000	welcome	TCP	67	21	11
18	123.142.5.9	9000	146.128.3.7	9000	room	TCP	43	5	22
19	192.168.1.4	9000	146.128.3.7	9000	available	TCP	23	7	33
20	192.138.4.90	9000	146.128.3.7	9000	at cort	TCP	22	22	11
21	123.142.5.9	9000	146.128.3.7	9000	where is	TCP	43	12	11
22	192.168.1.4	9000	146.128.3.7	9000	sdfdsf	TCP	53	34	22
23	192.138.4.90	9000	146.128.3.7	9000	come with	TCP	24	5	33
24	123.142.5.9	9000	146.128.3.7	9000	key show	TCP	42	5	44
25	192.168.1.4	9000	146.128.3.7	9000	rowcks	TCP	52	6	5
26	192.168.1.4	9000	146.128.3.7	9000	sdfsdfdsf	TCP	21	9	22

Figure.4 Snapshot of network trace.

The figure 4 shows the network trace produced by the proposed method. It shows clearly that the proposed approach has extracted all the features of the packet and produced the trace to support intrusion detection.

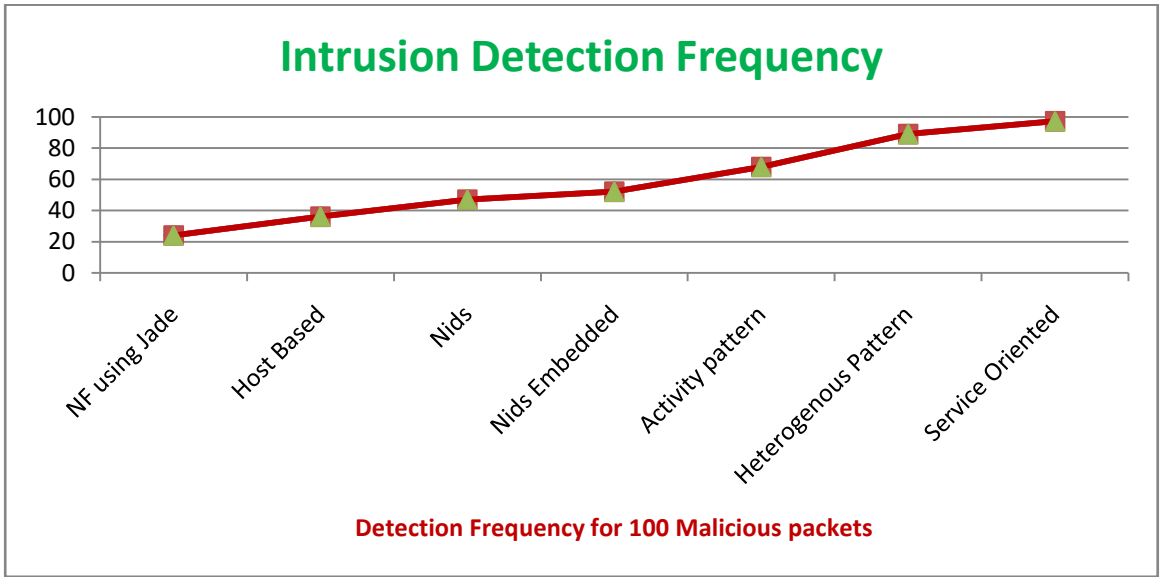

Figure.5: The frequency of detection of malicious packet.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

Figure 5 depicts the proposed system's performance in detecting malicious packets, and if 100 malicious packets arrive on time, the graph depicts the frequency of malicious packet detection. When compared to other host-based and activity pattern-based intrusion detection systems, it is apparent that the proposed system detects more malicious packets.

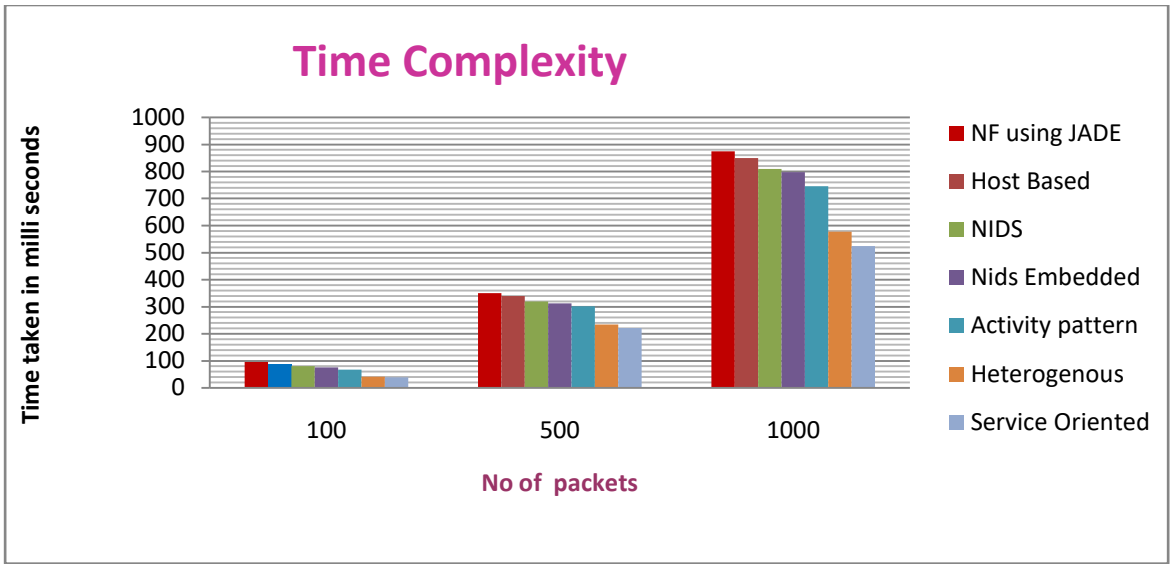

Figure.6: The time complexity of the proposed system.

Figure 6 compares the proposed system's time complexity to that of other methodologies. It clearly shows that the proposed system, when compared to other approaches for various numbers of packets, takes very little time. The other approaches take longer time to evaluate and detect the intrusion for a given number of packets than the proposed system.

Conclusion

The proposed service oriented Multi model network inference model compute the service access rate and channel access rate for the packet being received and its hop from where the packet has been originated. Also we compute the hop similarity value for the packet being received with the trace list and finally we conclude the packet based on the thresholds used for access rate and hop similarity. The proposed system has better approach for detecting malicious packets which in turn reduces the attacking rate.

References

[1.] Haldar, NAH 2012, 'An Activity Pattern Based Wireless Intrusion Detection System Information Technology', pp. 846-847.
[2.] Yamini, 2014, 'Detecting DDOS Attacks by Circular Protection Network', International Journal of Innovative Research in Computer and Communication Engineering , vol.2, Special Issue 1.
[3.] Sridevi, R 2012, 'Genetic algorithm and artificial immune systems:A combinational approach for network intrusion detection', Advances in Engineering sciences and Management, pp. 494-498.
[4.] JunyuanShen 2011, 'Network intrusion detection by artificial immune system', IECON, pp. 4716-4720.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 4427 - 4436
Received 25 April 2021; Accepted 08 May 2021.

[5.] Poornima, NV 2014, '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, no.1.

[6.] Khattab, S, Gobriel, S, Melhem, R &Mosse, D 2008, 'Live Baiting for Service-Level DoS Attackers', Proceedings of IEEE INFOCOM.

[7.] Thai, MT, Xuan, Y, Shin, I &Znati, T 2008, 'On Detection of malicious Users Using Group Testing Techniques', Proceeding of International Conference of Distributed Computing Systems (ICDCS).

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

[9.] Jothi G, Inbarani H. H, Hybrid Tolerance Rough Set–Firefly based supervised feature selection for MRI brain tumor image classification, Applied Soft Computing,Volume 46, , Pages 639-651,DOI: 10.1016/j.asoc.2016.03.014, September 2016

[10.] Inbarani H.H., Azar A.T., Jothi G. Supervised hybrid feature selection based on PSO and rough sets for medical diagnosis, Computer Methods and Programs in Biomedicine,Vol.113 (1) PP:175-185 DOI: 10.1016/j.cmpb.2013.10.007,2014

[11.] JE Jeyaswamidoss, K Thangaraj, K Ramar, M Chitra, "A rough set based rational clustering framework for determining correlated genes", ActaMicrobiologica et ImmunologicaHungarica 63 (2), 185-201.

[12.] P Ilanchezhian, K Thangaraj, J JebaEmilyn, S Vasanthi, JL Aldo Stalin, "Design of Nanotechnology Based Hazard Free Digital Circuit using Quantum Dot Cellular Automata", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ,ISSN: 2278-3075, Volume-9 Issue-1, November 2019.

[13.] B. Thiyaneswaran; K. Anguraj; S. Kumarganesh; K. Thangaraj, Early detection of melanoma images using gray level co-occurrence matrix features and machine learning techniques for effective clinical diagnosis, International Journal of Imaging Systems and Technology (IF 1.925), 2020, DOI: 10.1002/ima.22514