Chi-Square and Entropy (CS-E): A Hybrid Method for DDoS Attack Detection and Trace Back

T. Subburaj, K. Suthendran

Abstract: — Internet becomes unavoidable and it provides us with a wealth of information and allows us to keep in touch with the outside world. However, there can also be risks on the internet that is, for example, even a naive hacker can access information and easily learn to generate a large scale DDoS attack with the help of downloadable user-friendly attacking tools. Nowadays, this has made even small businesses in trouble. One of the extensive DDoS attacks was done on October 2016 which is called "Mirai botnet". In that, the attackers send 30 million packets per second to attack the financial department, industries, home system, etc. were affected. In the future, the attackers may hit the hardest even as banks, government sectors, and corporate sectors, etc. On DDoS attack time, the attackers are sending a lot of malicious packets to the server/victims. So the attacker's throughput is increased and legitimate user throughput is decreased on time of the attack. In this paper, a novel approach is proposed to detect the DDoS attacks using Chi-Square method which compares the normal packets and current packets statistics to discriminate whether the particular flow is DDoS or not. Further; it identifies the IP address of attacking source using entropy statistic. The proposed method can be used to control internet crimes. The experimental results show that the proposed method outperforms the existing approaches by detecting the DDoS attack and also by identifying the wrongdoer IP address. In addition, it takes minimum time to perform the above.

Keywords: Chi-Square, Critical value, DDoS attack, Entropy, Time complexity.

I. INTRODUCTION

Nowadays, the internet users face many problems in the form of attacks viz., Browser attacks, Brute force attacks; Distributed Denial of Service attack (DDoS), Secure Socket Layer (SSL) attack, Domain Name System (DNS) attack, and Back Door attack. At present, the most popular attack is a DDoS attack. Many useless packets or messages are being sent to the target systems through compromised computers (Botnet) using DDoS attacks. The main aim of this attack is to disable the system from responding to internet services. These DDoS attacks are launched by sending the malformed packets to crash the target systems and creating a massive volume of useless traffic to occupy all the resources. Every time the attackers invent the new techniques for attacking the systems.

DDoS attacks are classified into Synchronize (SYN) attack, Ping of Death attack, Smurf attack, Flooding attack, and Teardrop attack. In a SYN attack, the attacker sends lot of SYN request to the targeted systems making it unavailable to legitimate users. In a Ping of Death attack, the attackers attempt to crash the target systems by sending malware packets. In a smurf attack, attackers use the spoofed IP address for sending a lot ICMP messages to the target systems. Flooding attack, the target system's service is forced down by flooding it with a large amount of traffic. In the teardrop attack, the attacker sends the fragmented message repeatedly to the target system.

The motivation for this attack is to extract money from individual or an organization, or to disrupt some organizations or government sectors. Many researchers are still working an effective the solution to this DDoS attack. However, with the available technologies, hackers are getting strong day by day creating new types of attacks.

In January 2019, 500 million packets per second massive DDoS attacks were generated by attackers based on the SYN flood attack on GitHub [1]. However, the attackers have also performed the small size attack. This was also caused the damages in server. In 30th January 2019, More than 500 schools were hacked by the DDoS attacks at Netherland [2]. As the result, thousands of pupils or students were unable to access the study materials, books, assignments etc. The pupils, government sectors, and banking systems etc. were affected by DDoS attacks.

To overcome this DDoS attack issues, we propose an imaginative idea to sense the DDoS attack and also to trace out the attackers based on mathematical statistical calculations. During non-attacking period, each router table stores the information about all the packets pass through it. During the process of attack identification, the packet flow rate is compared with threshold value and the decision is made as an attack when the flow rate exceeds the threshold. Further, the attacking packets and its relevant information available on the subsequent upstream routers play crucial role in identifying the attacker source IP address based on entropy calculations.

Revised Manuscript Received on December 05, 2019.

***** Correspondence Author

T. Subburaj, Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India. E-mail:shubhurajo@gmail.com

K. Suthendran*, Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India. E-mail:k.suthendran@klu.ac.in

Retrieval Number: D11001284S219/2019©BEIESP
DOI: 10.35940/ijrte.D1100.1284S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. RELATED WORKS

Shiaeles et al.,[3] proposed a novel method to detect DDoS attack and identify by wrongdoer IP address. Further, their evaluation shows that the proposed method success rate is over 80%. However, in the case of flash crowds; this method identifies only the presence of DDoS attack but, not the offending IPs. This is still one of the open research issues. Kashyap and Bhattacharyya [4] have discussed about DDoS attack defence method. In addition, the authors have validated the proposed detection method by using two real times and one benchmark dataset and proved higher accuracy than the existing approaches. The authors Jiang et al. [5] have proposed a secure method to safeguard our systems from DoS attack based on flow trust values. Here the flow trust values are calculated at all routers which obviously compared with network data flow. The data flow with higher trust values are identified as legitimate whereas the flows with lower trust values are reported as malicious. Kaur et al. [6] have proposed a method for the detection of DDoS attacks based on the statistical techniques by monitoring the incoming flows and describing the unwanted traffics. This work utilized the existing KDD dataset. Using this approach the author has demonstrated the detection of DDoS attack and its occurrence time.

MinLee et al. [7] have introduced DDoS detection approach using Genetic Algorithm. In this work, the traffic matrix parameters are fine-tuned to increase success detection rate. The experiments are performed with different datasets viz., DARPA 2000 LLDOS 1.0, LBL-PKT-4 of Lawrence Berkeley Laboratory and generated attack datasets. The result shows the detection accuracy and speed of the proposed approach. The Statistical based DDoS attack detection and trace back method is proposed by author (Arumugam et al. [8]). In this work, by monitoring the flow of the packets every second at every router the DDoS attack is detected. Here the attack identification is based on the threshold value of the normal data flow. The experimental results show that the proposed method outperforms the existing packet marking method. However, it results in high false positive. To overcome this issue, the authors Subburaj and Suthendran [9] have proposed DDoS detection and trace back approach in which the threshold value was calculated based on median calculations instead of mean Calculations as in paper [8].

SkyShield, a method is a new defence of DDoS attack proposed by Wang et al. [10]. This method is used to quickly detect the DDoS attack in an application layer. This detection process is done automatic. The used the Hellinger distance is used to calculate the variance between the two types of transactions. Secondly identify the malicious packets effectively. Finally, used by the bloom filter and the CAPTCHA are guaranteed the detection of the malicious nodes. Cheng et al. [11] have proposed an IP address features value (IAFV) method for DDoS attacks screening based on identifying the feature changes in the network flows. SVM classifier is utilized to compute the variance of the normal flow and the attacking flows. This method catches malicious data flow and increases the effect of the normal flow and thus reduces the false alarm rate. The authors [12] proposed most recent approach for DDoS attack detection by monitoring all incoming packets, verifying count variation with respect to the threshold value. This work finished the job in less time compared with the other detection process because it didn’t maintain the list of source IP’s and it uses non-parametric change point modelling technique for smelling the flooding attacks on a real-time process. The author [13] has proposed the new concept for detection the DDoS attack using pattern matching process in the flow of the packets and also used for improving the firewall services. This method is successfully filtered the unwanted attacking packets.

Feinstein et al [14] have modified the snort pre-processor using Chi-square and entropy statistics. In this work, the attack detection is possible with the help of packet header information. There are three filter rules viz., constant, random and allows are used for attack detection. The rules are also applied to the IP header of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP). The constant and random rules may treat the normal packets as attack packets and drops the same. The allow rule, sometimes predicts the attack packets as normal data packets even when the rule matches. In snort based detector having a false positive and false negative.

Kim et al. [15] have combined two data mining approaches viz., decision tree algorithm and neural networks to detect the DDoS attacks. The decision tree algorithm uses an automatic feature selection mechanism. The other automatic feature selection uses chi-square or entropy for selecting the attribute. The selected attributes are used as input to neural networks. In the neural network, the detection of the DDoS attack process is done based on the classifier generation module. So, this combined data mining approach results in a processing overhead for the selection of attributes and identification of the attacks.

Singh and De [16] have proposed the DDoS attack detection technique based on the mathematical model. This work considered Statistical parameters viz., inter-arrival time of the packets. Based on inter-arrival time the bandwidth depletion and memory exhaustion is calculated. When the attacker’s inter-arrival time is a small mean then the buffer size of the legitimate user is high. The Total attack is estimated based on the bandwidth probability and memory usage probability. Next, the throughput value is Calculated based on the arrival time. Finally, clustering the packets based on inter-arrival time. The Clustering packet uses the method of Self-Organizing Map (SOM). After clustering, the coefficients of clusters are calculated. Finally, identified the low inter-arrival time clusters are reported as attacked clusters.

This method has lots of calculations for attack detection. In some situations, a normal user who frequently communicating the server means; it’s also identified as the attack based on the above method. So, this method will increase the false positive. Another issue, the attackers may not send packets continually, they may send the packets in specific time interval, and therefore this method does not detect the presence of attack. So, false negative also increased.

Processing overhead of this method is also high. Because, this method performs more calculations viz, inter-arrival time based on arrival packet rates, bandwidth depletion and memory exhaustion based on the packet rate and inter-arrival time, mean value calculation based on inter-arrival time, throughput calculation, clustering the packet and also co-efficient calculation from the inter-arrival time packets.

The above reviews witness the availability of different attack detection methods which may vary in their performance to detect the attacks. Most of the existing DDoS detection and trace back methods are focused on the following metrics: packet loss on particular time, throughput calculation is based on the legitimate and attacked user, packet marking, request and reply delay on the communications, processing time and also resource allocation based on the inter-arrival time. There are few disadvantages viz., Processing overhead increased, amplified the false positive and false negative, low detection efficiency and high cost with low throughput. However, all methods are used to detect the presence of attacks very well. With the advent of new technology is the attackers are generating variety of attacks so there is a great demand for a system which prevents the same.

To overcome the above issues; this work proposes an innovative hybrid approach based on the Chi-Square and Entropy statistical calculation. In proposed work, Chi-square statistic is used to detect the attack and also identify the upstream routers at server nearby router. Entropy statistics are used to identify the attacker in LAN. A novel approach is to detect the attacks and trace out the offending source and block the attackers IP address. The calculations' are required to identify the attacks are done at each router so it reduces the time computation complexity and traces back time on comparing with previous detection approaches.

III. SYSTEM MODELING FOR DETECTION PROCESS

A DDoS attack is a very simple technique used in the performance of an attack on the systems, but detection of DDoS attack is a highly critical work. So, the attackers choose these DDoS attacks frequently. When the DDoS attack happens the attacker's throughput gets increased, and the normal user's throughput gets reduced. Statistical methods are used for effective detection of DDoS attacks. Statistical methods like Chi-Square statistic and Entropy are used for the detection process.

A. CS-E (Chi-Square & Entropy)

In this section, a combination of two statistical calculations is used for speedy identification of the attackers. Here chi-square approach is applied to each parental router which is close to the target system to identify the attack based on the packet rates from the various upstream routers. The trace back process begins following the identification of the presence of the attacks. It is based purely on entropy calculations. Application of an entropy calculation is easier in small network connections otherwise the chi-square calculation suits all other networks. Detection and trace back process are done in parallel and distributed. So the processing time is reduced for the detection and trace back process.

a. Chi-Square Statistic

Chi-Square test is used for goodness of the fit. The chi-square statistic is applied in the evaluation of the relationship between categorical values. The calculation of the chi-square statistic is relatively simple and sensitive:

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \qquad (1)$$

ted Data:

The statistics gives the relationship between the observed data and expected data which are named as chi-square statistic value.

Chi-square test is used in the detection of the DDoS attacks from the group of communications. It analyses the packet on the basis of the variations in upstream routers. On every second, packets are collected from the various connections and the chi-square value is calculated. The critical value based on the chi-square critical table is fixed following [17]. This critical value is the threshold value of this detection process.

b. Entropy Statistic

Entropy is a Statistical concept; it is used in the detection of the changes in the randomness of flow at each router for some time intervals. Before calculating the entropy, find the probability for all values. The changes in randomness of flow at routers are computed as follows:

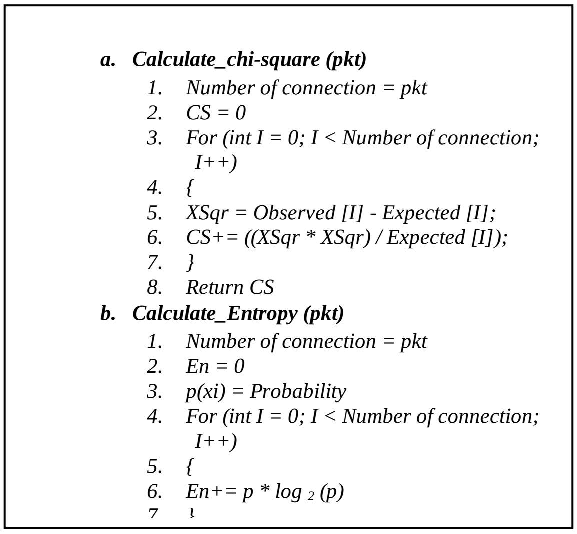
$$H(X) = -\sum_{i=1}^{n} P(x_i) * \log_2 P(x_i) \qquad (2)$$

B. Work Flow of Detection Process

Figure.1 shows the working flow of CS-E (Chi-Square & Entropy) model. All packets information like, upstream router, downstream router and arrival time is stored inside the routing table.

C. Pseudo code

```
Chi-Square & Entropy (CS-E)
    1. 'N' number of packets from Source to Destination.
    2. Repeat for all packets 'pkt'
    3. CS= Calculate_chi-square(pkt)
    4. Th =CriticalValue( CS)
    5. If CS <Th
           a.Attack is generated
               i. Find the path of the attacked packets
               ii. 'N' number of packets send from
                   source to destination
               iii. Repeat for all packets 'pkt'
               iv. En= Calculate_entropy(pkt)
               v. If En < threshold value
                   Find the IP address of the attacker
                   Else
                   No attack generated
           b.Else
           c.No attack generated
    6. End
```



```
a. Calculate_chi-square (pkt)
    Number of connection = pkt
    CS = 0
    For (int I = 0; I < Number of connection;
      I++)
    {
    XSqr = Observed [I] - Expected [I];
    CS+= ((XSqr * XSqr) / Expected [I]);
    }
    Return CS
b. Calculate_Entropy (pkt)
    Number of connection = pkt
    En = 0
    p(xi) = Probability
    For (int I = 0; I < Number of connection;
      I++)
    {
    En+= p * log 2 (p)
    }
```

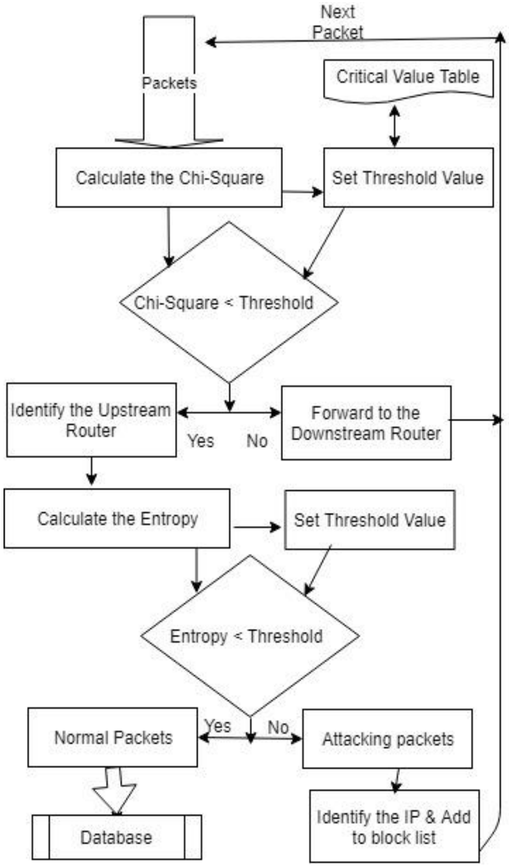


Fig. 1. Work flows of CS-E (Chi-Square & Entropy)

IV. EXPERIMENT AND DISCUSSION: CASE STUDY

In DDoS attacks, wrongdoers send unwanted data of enormous volume to a server, with an intention to make the server unavailable for innocent users. During this time, the attackers may access or change the secured information of the server. Example; on 30th January 2019, in Netherland more than 500 schools were hacked by the DDoS attacks. As a result, thousands of pupils or students were unable to access the study materials, books, assignments etc.

We have chosen our environment as college with only four departments. Experiments are being conducted only for 4 departments viz., Department of Computers, Department of Mechanical, Department of Civil and Department of Science. There were five intermediate routers and one server. Each router monitors all incoming and outgoing packets. Table.1 shows the departments, number of users and its corresponding IP addresses.

TABLE I. SAMPLE EXPERIMENTAL ENVIRONMENT

Department	Number of Users	IP Addresses
Computers	3	192.168.1.1 – 192.168.1.3
Mechanical	3	192.168.2.1 – 192.168.2.3
Civil	3	192.168.3.1 – 192.168.3.3
Science	3	192.168.4.1 – 192.168.4.3

The experiments are made as sample DDoS attacks had happened in Netherland. The attackers hacked the server to find out some juicy information or to change the documents or to change the mark statements etc. Our proposed method is used to identify such DDoS attacks and also identifies the wrongdoer IP addresses.

Figure.2 shows the experimental architecture simulated by NS3. The Wireshark tool is used to monitor all the packet flows. In our simulation, four department systems are connected with the server through the routers. Normal users and attackers are included in the experiment.

Table.2 shows the ten-time slots from T_1 to T_10. At each time slot, all incoming packet rates to the server are monitored by the router and the same is shown in Table. 2.

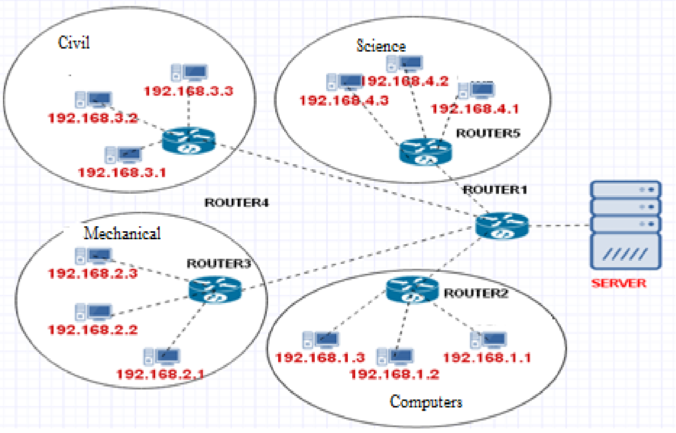


Fig. 2. Configutaion of experimental architecture

Singh and De [16] have calculated the packets Inter-arrival time to detect the presence DDoS attack. Table.3 shows the packet rates and also inter-arrival time of the transferred packets at particular time intervals. The presence of attack was identified during the detection process when the packets inter-arrival time was low.

Table.3 shows Mechanical department inter-arrival time as very low compared with all other departments on all time slots. The attacked packets rates are easily detected on the basis of the packets inter arrival time screening. After applying this concept on the above table, the attacked packets have been identified as coming in to the server from the mechanical department. Sometimes this detection may not be correct. Because the normal packets are also reported the attacked packets, so this method results in increased the false positive and false negative.

This method also has a lot of computational processes and compares the results with the other detection approach. To overcome these existing issues, we proposed the hybrid approach of the DDoS attack detection based on the Statistical metrics.

By applying the Chi-Square statistics on the server nearby router the attacked flow direction is determined. We simulated experimental setup and recorded the details for 10 seconds initially; on 3rd, 6th, and 8th second only the Department of Mechanical is sending the packets and department of science are idle. In our detection process, firstly the average values of all time slots are calculated and finally the relative frequencies are computed as follows.

$$\text{Relative Frequency} = \frac{\textit{Average Number of packets in a single Departm}}{\textit{Avearge number of packets for all departmen}} \quad (3)$$

Using the above formula the relative frequency for all departments has been calculated and the same is presented in time slot-wise in Table.3. For example, on time slot T_1, the relative frequency of departments viz., COMPUTERS=0.19, MECHANICAL=0.46, CIVIL=0.19 and SCIENCE=0.14. The maximum relative frequency of all events at the same time slot is equal to 1. Based on these relative frequencies the Chi-Square statistics are calculated for all time slots.

Table.3 shows the Chi-Square (χ^2) values of T_1 is 10.52, T_2 is 10.54, T_3 is 103.09, T_4 is 9.17, T_5 is 9.88, T_6 is 114.55, T_7 is 12.05, T_8 is 112.26, T_9 is 9.22, and T_10 is 12.38. In that, the critical value of Chi-Square is 16.266 with 1% of significance [10]. This critical value is fixed as the threshold value for the detection of attacks.

Now, compare all Chi-Square value with a threshold value, the values which are higher than the threshold value that values are reported as high rate attacks. Based on this comparison, Three-time slot are having the higher values like: T_3 = 103.09, T_6 = 114.55 and T_8 = 112.26.

Figure.3 shows the Chi-Square and threshold value comparison chart based on Table.3. In Figure.5, the red color line denotes threshold value and black color denote Chi-square. It has three peak values during T_3, T_6 and T_8which are reported as high rate attacks. This experiment shows that the only from Mechanical department the attacking flow packets were originated. So, any one person was sending the attacking packets from Mechanical department.

After that, as a novelty, the entropy Calculation is performed only on the Mechanical department to find out the IP addresses of the attacker instead of Calculating entropy values at every router.

Table.4 presents the entropy Calculations for attacked time slot T_3, T_6, and T_8. Entropy is the main role in the identification of the attacker. In entropy calculation, first, calculate the Probability of the communication's packets. Then calculate the Entropy value using the entropy formula equation 2. After Calculating the entropy fixes the threshold value used by the average in entropy Calculation. Now fixed 0.10 is a threshold value.

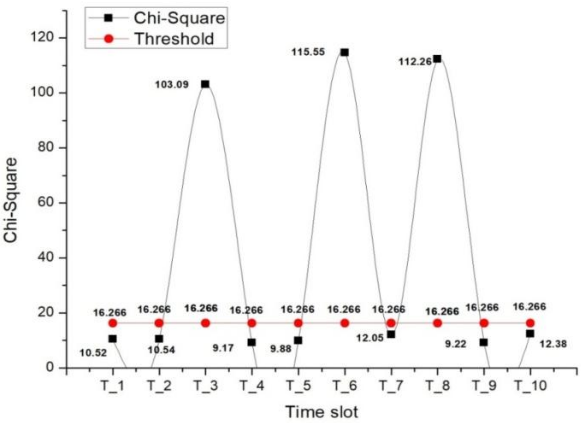


Fig. 3. Chi-square and threshold value comparison chart

The Calculated entropy value at the identified router is compared with the threshold value to determine the offending node. That is when the calculated entropy value lesser than the average entropy means it is decided as attack flow otherwise normal data flow. Based on the observations from Table 5, it is clear that the IP address 192.168.2.1 is having the entropy values 0.08, 0.07 and 0.09 during the time slots T_3, T_6 and T_8 which are lesser than the threshold value**.**

Figure.4 shows the entropy and threshold value chart based only on the Time slots T_3, T_6 and T_8. Here threshold value is highlighted by green color and attack flow is marked with Black color. From the above, it is decided that the IP address 192.168.2.1 is attacking the server and the same is blocked. Now the normal or legitimate user is freely communicated to the server.

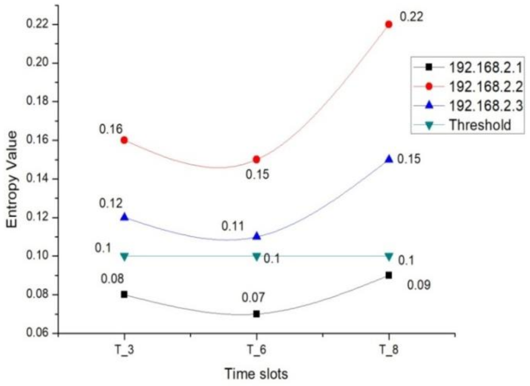


Fig. 4. Entropy and threshold value chart during attacking time

Figure.5 shows the throughput effects of the DDoS attack based on the packet rates. Throughput is calculated based on the packet rate and the inter arrival time of the packets. In normal time throughput of all communication packets are same levels but attacking time the line level will be changed. When Redline changed to the high level all other line levels are move to the idle level. The Mechanical department throughout is increased and it is marked in red line, normal users like Computers, Civil and Science throughput is decreased to low and it is represented in other 3 lines

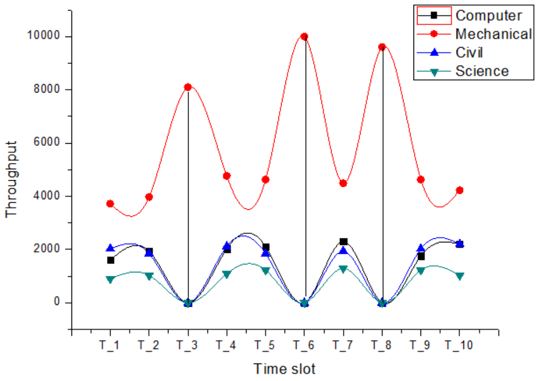


Fig. 5. Throughput plot for all departments during Simulation time

In the existing method, the detection and trace back of the offending node is done based on packets inter-arrival time with correlation method was applied to all the packets for all time slots denoted as *n* and the corresponding time complexity is *O (n)*. But in the proposed method Chi-square Calculation is computed on server nearby router for every time slots denoted as T_{1}, T_{2}… T_{Kn}, i.e. *K* - total number of time slots for the single router. After that, the entropy is calculated on the remaining selected router to identify the source of an attack. The overall all-time complexity for the proposed method is *O (log* $_2$ *n)*. So proposed method take less amount of computation time.

V. CONCLUSION

DDoS attacks are very complex and serious problem consequently in the IoT infrastructure by computers using real damages in the system of individual or organization. Quality of the service also affected during the presence of DDoS attacks i.e throughput of the user will be decreased, the delay also increased. It's difficult to detect the DDoS attacks. Because, the attacker does not involve directly in attacks, through the compromised system they generates the attack. So it's difficult to point out the origin of the attacks. To handle this issue, a novel approach was proposed by using Chi-Square Statistics and entropy calculation to detect the DDoS attack and trace back the attack source. The NS3 experimental results show that the proposed method performs the detection and trace back of attacking source. The proposed method effectively does this job than the existing approach with a reduced computation complexity. The computational complexity of the existing approach is *O (n)* whereas the proposed model complexity is *O (*$\log_2$ *n)*. So the time complexity is reduced more than 50% than the existing approach. Our future work aims to solve this issue using other statistical metrics in wireless and ad-hoc domain.

ACKNOWLEDGMENT

The author would like to thank the management of Kalasalingam Academy of Research and Education for supporting the research through University Research Fellowship and also thank to National Cyber Defence Research Centre for supporting laboratory facility for research.

REFERENCES

[1] https://www.darkreading.com/attacks-breaches/massive-ddos-attack-generates-500-million-packets-per-second/d/d-id/1333766

[2] https://nltimes.nl/2019/02/01/school-system-hit-ddos-attack-hundreds-schools-affected

[3] S.N. Shiaeles, V. Katos, A.S. Karakos., and B.K. Papadopoulos, "Real time DDoS Detection Using Fuzzy Estimators", Computer and Security, Vol. 31(6), pp. 782–790, 2012.

[4] H.J. Kashyap, and D. Bhattacharyya, "A DDoS Attack Detection Mechanism Based on Protocol Specific Traffic Features", In Proceedings of the Second International Conference on Computational Science Engineering and Information Technology, ACM, pp. 194–200,2012.

[5] X. Jiang, J. Yang, G. Jin, and W. Wei, "RED-FT: A scalable Random Early Detection Scheme with Flow Trust against DoS Attacks", IEEE Communications Letters, Vol, 17(5), pp. 1032–1035, 2013.

[6] G. Kaur, S. Varma, and A. Jain, "A Novel Statistical Technique for Detection of DDoS Attacks in KDD Dataset", IEEE, pp. 393–398, 2013.

[7] S. MinLee, D.S. Kim, J. HakLee, and J. SouPark, "Detection of DDoS attacks using optimized traffic matrix", Computers and Mathematics with Applications, Vol. 63(2), pp. 501–510, 2012.

[8] T. Subburaj, K. Suthendran, and S. Arumugam, "Statistical Approach to Trace the Source of Attack Based on the Variability in Data Flows", Lecture Notes in Computer Science, Vol 10398, pp. 392–400, 2017.

[9] T. Subburaj, K. Suthendran, "Detection and Trace Back of DDoS Attack Based on Statistical Approach", Journal of Advanced Research in Dynamical and Control, Vol, 13-Special issue, pp. 66-74, 2017.

[10] C. Wang, T. Tony, N. Miu, X. Luo, and Wang, J., "SkyShield: A Sketch-Based Defense System against Application Layer DDoS Attacks", IEEE Transactions on Information Forensics and Security, Vol, 13(3), pp. 559 – 573, 2018.

[11] Y. Chen, S. Das, P. Dhar, A. El Saddik. and A. Nayak, "Detecting and Preventing IP-spoofed Distributed DoS Attacks", International Journal of Network Security, Vol. 7(1), pp. 70–81, 2018.

[12] R.C. Baishya, N. Hoque and D.K. Bhattacharyya, "DDoS Attack Detection Using Unique Source IP Deviation", International Journal of Network Security, Vol. 19(6), pp. 929-939, 2017.

[13] A. Sanmorino and S. Yazid, "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow" , International Conference of Information and Communication Technology, IEEE, pp. 12-16, 2013.

[14] L. Feinstein., D. Schnackenberg., R. Balupari and D. Kindred,. "Statistical Approaches to DDoS Attack Detection and Response", Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), IEEE Computer Society, 2003.

[15] M. Kim., H. Na., K. Chae, H. Bang and J. Na, "A combined data mining approach for DDoS attack detection", International Conference on Information Networking, LNCS, Springer, pp. 943-950, 2004.

[16] K.J. Singh and T. De., "Mathemetical modelling of DDoS attack and detection using correlation", Journal of Cyber Security Technology, 2017, DOI:10.1080/23742917.2017.1384213.

[17] http://www.itl.nist.gov/div898/handbook/eda/section3/eda 3674.htm

TABLE II. TRANSFERRED PACKET RATES AND INTER-ARRIVAL TIME

	No of packets per seconds				Inter-Arrival Time			
Time slot	**Computers**	**Mechanical**	**Civil**	**Science**	**Computers**	**Mechanical**	**Civil**	**Science**
T_1	40	61	45	30	0.025	0.016393	0.022222	0.033333
T_2	44	63	43	32	0.022727	0.015873	0.023256	0.03125
T_3	0	90	0	0	0	0.011111	0	0
T_4	45	69	46	33	0.022222	0.014493	0.021739	0.030303
T_5	46	68	43	35	0.021739	0.014706	0.023256	0.028571
T_6	0	100	0	0	0	0.01	0	0
T_7	48	67	44	36	0.020833	0.014925	0.022727	0.027778
T_8	0	98	0	0	0	0.010204	0	0
T_9	42	68	45	35	0.02381	0.014706	0.022222	0.028571
T_10	47	65	47	32	0.021277	0.015385	0.021277	0.03125
Average	**31.2**	**74.9**	**31.3**	**23.3**				

TABLE III. CHI-SQUARE CALCULATION FOR ALL TIME SLOTS

Time Slot	*Department*	*Relative Frequency*	*Observed Frequency*	*Expected Frequency*	x^2
T_1	COMPUTERS	**0.19**	40	34.1705	**10.52**
	MECHANICAL	**0.46**	61	82.0311	
	CIVIL	**0.19**	45	34.28	
	SCIENCE	**0.14**	30	25.5184	
T_2	COMPUTERS	**0.19**	44	35.3354	**10.54**
	MECHANICAL	**0.46**	63	84.8276	
	CIVIL	**0.19**	43	35.4487	
	SCIENCE	**0.14**	32	26.3883	
T_3	COMPUTERS	**0.19**	0	17.4736	**103.09**
	MECHANICAL	**0.46**	90	41.9477	
	CIVIL	**0.19**	0	17.5296	
	SCIENCE	**0.14**	0	13.0492	
T_4	COMPUTERS	**0.19**	45	37.4711	**9.17**
	MECHANICAL	**0.46**	69	89.9546	
	CIVIL	**0.19**	46	37.5912	
	SCIENCE	**0.14**	33	27.9832	
T_5	COMPUTERS	**0.19**	46	37.2769	**9.88**
	MECHANICAL	**0.46**	68	89.4885	
	CIVIL	**0.19**	43	37.3964	
	SCIENCE	**0.14**	35	27.8382	
T_6	COMPUTERS	**0.19**	0	19.4151	**114.55**
	MECHANICAL	**0.46**	100	46.6086	
	CIVIL	**0.19**	0	19.4773	
	SCIENCE	**0.14**	0	14.4991	
T_7	COMPUTERS	**0.19**	48	37.8594	**12.05**
	MECHANICAL	**0.46**	67	90.8867	
	CIVIL	**0.19**	44	37.9807	
	SCIENCE	**0.14**	36	28.2732	

T_8	COMPUTERS	**0.19**	0	19.0268	**112.26**
	MECHANICAL	**0.46**	98	45.6764	
	CIVIL	**0.19**	0	19.0877	
	SCIENCE	**0.14**	0	14.2091	
T_9	COMPUTERS	**0.19**	42	36.8886	**9.22**
	MECHANICAL	**0.46**	68	88.5563	
	CIVIL	**0.19**	45	37.0068	
	SCIENCE	**0.14**	35	27.5482	
T_10	COMPUTERS	**0.19**	47	37.0828	**12.38**
	MECHANICAL	**0.46**	65	89.0224	
	CIVIL	**0.19**	47	37.2016	
	SCIENCE	**0.14**	32	27.6932	

TABLE IV. ENTROPY CALCULATION FOR ATTACKED TIME SLOT

Time Slot	***Mechanical***	***Flow***	***Sum***	***$p(x_i)$***	***$\log_2 p(x_i)$***	***Entropy***
T_3	192.168.2.1	85	90	0.94	-0.08	0.08
	192.168.2.2	3	90	0.03	-4.91	0.16
	192.168.2.3	2	90	0.02	-5.49	0.12
T_6	192.168.2.1	95	100	0.95	-0.07	0.07
	192.168.2.2	3	100	0.03	-5.06	0.15
	192.168.2.3	2	100	0.02	-5.64	0.11
T_8	192.168.2.1	90	98	0.92	-0.12	0.09
	192.168.2.2	5	98	0.05	-4.29	0.22
	192.168.2.3	3	98	0.03	-5.03	0.15

AUTHORS PROFILE

T. Subburaj, received B.Sc Computer Science degree from Madurai Kamaraj University, his MCA degree from Anna university and also ME CSE degree from Anna University. He is pursuing Research work in Kalasalingam Academy of Research and Education in the area of Cyber security.

K. Suthendran received his B.E. Electronics and Communication Engineering from Madurai Kamaraj University in 2002; his M.E. Communication Systems from Anna University in 2006 and his Ph.D Electronics and Communication Engineering from Kalasalingam University in 2015. He was a Research and Development Engineer at Matrixview Technologies Private Limited, Chennai for a couple of years. He is now the Head, Cyber Forensics Research Laboratory and Associate Professor in Information Technology, Kalasalingam Academy of Research and Education. His current research interests include Cyber Security, Communication System, Signal Processing, Image Processing, etc..