International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S4, December 2019

Bit-and-Piece DDoS attack Detection based on the Statistical Metrics

T. Subburaj, K. Suthendran

***Abstract:** on each successive day, the DDoS attacks are increasing, improving and becoming more critical than ever before. In 2018, CISCO predicted that DDoS attack traffics may reach to 3.1 billion during 2021. Bit and Piece DDoS attack is an emerging attacking technique was found and reported by Nexusguard. This attack mainly targets the communication service providers and it injects unwanted junk information in to the legitimate traffic and thus bypasses the detection techniques. This work is aimed to propose a novel approach for detecting bit and piece attack using statistical metrics. Here, the packet flow is monitored at every second and the variations in the data flows easily identified as an attack.*

***Keywords :** DDoS attack, Entropy, Bit and Piece, security.*

I. INTRODUCTION

DDoS attacks cause disturbance in the day to day business of large information technology companies, organizations, educational institutions, social media companies and government sectors. This result in data theft, revenue loss, broken infrastructure, productivity loss, spoils the brand and etc.In 2018, NETSCOUT, a Cyber Security Company has reported a 20% increase in the DDoS attacks rate compared to the previous year [1]. The Nexusguard reported the invention of a new type of DDoS attack was invented by the attackers, named as Bit-and- Piece DDoS attacks.

A. Bit and Piece attack

Figure.1 shows the Bit-and-Piece attack structure. In Bit-and-Piece attack, the attacker controls a number of local systems through the Internet Service Provider. The attacker sends the attacking commands through ISP. All the local systems connected with ISP's are attacked based on the master’s commands.

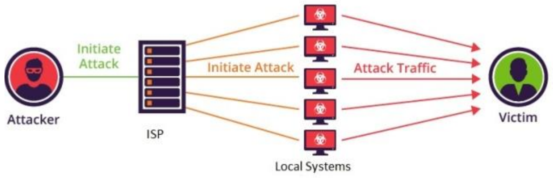

Fig. 1.Bit-and-Piece attack structure

Manuscript published on 30 December 2019.
***** Correspondence Author (s)

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

Volumetric attacks are performed through ISP. Here, the attackers are sending some unwanted junk information in to the legitimate traffic causing a failure in the existing attack detection mechanism to sense the attack, due to; instead of attacking are destinations or one machine attacking all the machines which are connected to that ISP [2]. Therefore, all the systems connected with a particular ISP are attacked at different time intervals. Finally, it brings down all the machines connected in particular ISP.

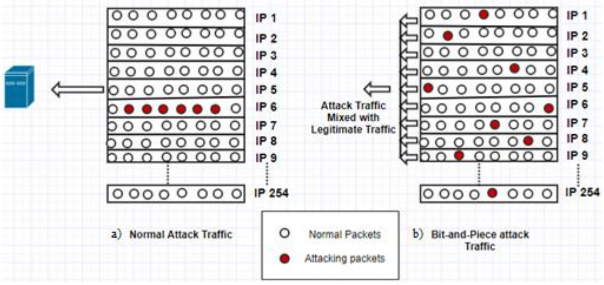

Fig. 2.Normal atatck and Bit-and-Piece attack

Figure.2 shows the difference between a normal attack flow and a Bit-and-Piece attack flow. In general, a normal attack is performed in one or more IP addresses in a network. In a Bit-and-Piece attack, the attackers spread malicious packets along with normal packets on every IP address during various time periods. In Figure.2, the malicious packets are marked in red and normal packets in blue. Figure.2 (a) shows a normal attack flow. Here, the attackers send the malicious packets in a single IP address 6. Figure.2 (b) shows a Bit-and-Piece attack. Here, the attackers send the malicious packet to all IP address at various time periods. This type of attack is a bit-and-piece attack. It is related to the pulse wave attacks.

II. LITERATURE SURVEY

The authors [3] have proposed an imaginative idea to detect DDoS attack and Flash events based on the set of information theory metrics called φ-Entropy and φ-Divergence metrics. It detects the variations between the legitimate traffics and the attack traffics. In 2017, Hoque et.al projected an approach to smell the real-time DDoS attack based on Field Programmable Gate Arrays (FPGA) [4]. The proposed method uses the correlation value for identifying the attacks. An attack alarm is generated, when the estimated correlation value is smaller than a user-defined threshold. The author [5] has proposed an innovative approach for detection of the DDoS attack and its detection efficiency based on Multilayer observation with a Genetic Algorithm (MLP-GA). It detects DDoS attack in application layer. This result in reduced false positive and also provides the detection efficiency as 98.04%.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

S. Behal et.al [6] have proposed an idea that helps detection of the presence of DDoS attack and Flash events used by the D-FACE approach. This approach senses the attack at the ISP level. A attack sensing is based on distributed, flexible, automated and collaborative defense systems. In this method early detect the DDoS attacks. The authors [7] have proposed a concept for detecting DDoS attack and the Flash events based on the 3 key parameters, flow similarity, pages referred, and client legitimacy. The result of proposed method achieves reduced false positive and false negative. In [8], the authors have proposed a detection and trace back mechanism for DDoS attack based on the hybrid approach of the logging method and the packet marking method. This approach resulted in reduced storage requirements and access time.

Cui et al [9] have proposed a new concept for DDoS attack detection based on SD-anti-DDoS mechanism. Here, the DDoS attack is detected based on the trigger method and the wrongdoer source address was also identified. The proposed approach takes minimum computational time to sense attack detection and also for tracing the attack source. Kalkan et al [10] have proposed a ScoreForCore approach for filtering out the network attack traffics. This approach deploys proactive and collaborative filtering techniques. The ScoreForCore method uses statistical calculations for identification and prevention of the attack.

In 2014, the authors [11] demonstrated the DDoS attack detection mechanism based on data mining algorithms such as advanced All Repeated Patterns Detection (ARPaD) Algorithm. This method senses the repeated patterns in the traffic quickly and reports those as an attack. Xiao [12] have proposed a brand new DDoS attack detection concept based on the CKNN (K-nearest neighbour's traffic classification with correlation analysis). It also includes the method called the r-polling method. The proposed method effectively detects the DDoS attack with improved classification accuracy.

An improved DDoS attack detection method was presented by Lee [13] in 2012. The attack sensing rate was improved by tuning the traffic matrix parameters of a Genetic Algorithm (GA). In addition, the traffic matrix was modified by altering the hash function to avoid hash collisions. The packet-based window size was applied instead of time-based window size with the aim to minimize computational overheads.

Jazi, et al [14] have proposed a novel idea to detect the seventh layer DoS attacks based on nonparametric CUSUM algorithm. The real time traffic was used for analysis of the effectiveness of this approach. Their study also revealed the impact of sampling approach for attack detection. To overcome the existing problems in detecting the LDDoS flows Zhang et al., [15] proposed an imaginative approach that calculates a metric named Congestion Participation Rate (CPR). Here, a predefined threshold value is compared with CPR value to categorize the attack flows and normal flows. When the CPR value falls above the threshold, the corresponding packets are marked as attack and the same is dropped. Their study also presents the guidelines to choose CPR threshold value in real time.

In practice, most of the times, the known and unknown attacks are a threat to the networks. Saied et al [16] have proposed a solution for the above based on artificial neural network algorithms.

A novel DDoS detection approach based on fuzzy estimation was proposed by Shiaeles [17]. The estimation is based on the average value of the packet inter arrival times. This approach succeeded in DDoS attack detection and traceed the offending machine. However it found difficulty in attack detection for the sites with a large average number of hits, thereby resulting in a large false positive.

In [18], authors have proposed an idea to detect DDoS attack and trace back the source of an attack based on statistical metrics. In this approach, the detection process was based on the threshold value comparison with entropy values. The threshold value is calculated based on the statistical mean value or median value [19], and six sigma value. During the attacking time, the entropy values which are less than the threshold value is identified as an attack. The authors [20] proposed an innovative solution for Digital Watering Hole attack detection based on the sequential pattern in data mining techniques. Through the examples authors have demonstrated how digital watering hole attack is happening and how to mitigate the same.

The above literature alarm us about the continuous happening of DDoS attack and its damages in many business places, Institution, Private and Public sectors. This work offers suggestion for the DDoS attack detection and identifying the wrongdoer.

Bit-and-Piece attack is a new type of DDoS attack. We propose for accurately detection of the Bit-and-Piece attack based on the statistical approach with less amount of time.

III. Attack Detection Process

In general, the Communication Service Provider (CSP) offers the internet for any network. During, Bit-and-Piece DDoS Attack, the attackers target mostly the CSPs in networks. Here, the attackers do not send the malicious packets to a single IP continuously, but instead they spread the malicious packets to various IP addresses at different times. The statistical calculation is used to identify the presence of attacks in the detection process. The information about the entire packet is stored in the nearest router of the server. So, the detection process begins at nearest router of the Server.

A. 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 attacker creates the new type of DDoS attacks on every day. Bit and Piece attack is also one new DDoS attack, this attack launched on 2018. When this Bit and Piece attack happens the attacker's throughput gets increased, and the normal user's throughput gets reduced. Statistical metrics are used for effective detection of Bit and Piece attack. In this detection process every second all routers involved the monitoring the data packets flow and identify the variations of the flow at a time of attacks. In detection process use the entropy calculation for monitoring the packet flows and use the standard deviation, average entropy and six-sigma for set the threshold value.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

B. Entropy

Let X = {x_1, x_2...x_n} represent a packet rates on communication packets. X = {x_1, x_2... x_n} variables are used to calculate the entropy values based on the following equation:

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

H(X) denotes entropy values, P(x_i) denotes probability values.

C. Threshold

The average entropy values in calculated as follows:

$$AE = \frac{1}{n}\sum_{i=1}^{n} H(x_i) \qquad (2)$$

where, AE denotes Average Entropy, based on the AE value the Standard Deviation value and six-sigma (6σ) value is calculated.

$$Threshold\ value = AE \pm 6\sigma \qquad (3)$$

D. Attack Detection

In the detection process, the current entropy value is compared with the threshold value for identifying the attacking packets. In this comparison, normal packet flow values are less than the threshold value; whole attacking packet values are higher than the threshold values.

IV. EXPERIMENT AND DISCUSSION : CASE STUDY

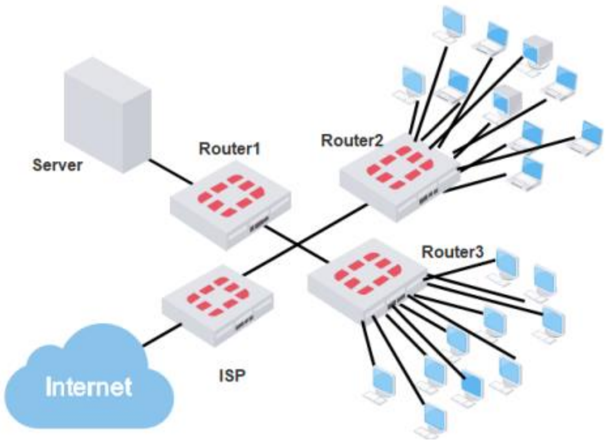

Fig. 3. Expermental Architecture

A. Experimental Environment

The experimental setup of the proposed work is shown in Figure.3. LAN has 20 systems, 3 routers, one ISP and server. Router1 maintains all packet information viz., Source IP, Destination IP, Packet rates, Time, Protocol etc.

B. Attack Detection Process

In attack detection process every second all packet flows are monitor and also calculate the entropy value.

1) Monitoring packets

Table.I shows the collected packet rates from the various time slots at every IP used by Wireshark tool. It has 20 time slots and 20 IP addresses. At first, it collects ten time slot values for calculating the entropy value and threshold value from the Table.

2) Entropy

Table.II shows the normal packet flow rates. The entropy values are calculated on every time slot at each IP address using equation 1.

3) Threshold

Table.III shows the entropy values of all IP address on ten-time slots. The threshold value for the detection process is calculated using equation 3.

Average Entropy value (AE)	= 0.2146
Standard Deviation value (σ)	= 0.029
Six-Sigma value (6σ)	= 0.180
Threshold value (AE + 6σ)	= 0.394

Based on the calculations, the threshold value is fixed as 0.394. Now another ten-time slot on all IP's is obtained from the Table.I.

4) Attack detection

Table.IV shows another ten-time slot packet rates. The entropy values are calculated for all IPs. Entropy values, after calculation are compared with the threshold value and decisions are taken accordingly.

Table.V shows the entropy values for the T_11 to T_20 time slots. A comparison between the entropy values with the threshold value is carried out for identifying the variations in the packet flows in networks. Based on the comparison, all IP's are as having the attacking packets, due to the entropy values of all IP's being greater than the threshold value on some time slots. Table.V, shows the entropy values as greater than the threshold marked as red. These entropy values are reported as an attacking packet.

Figure.4 is the comparison chart between entropy and threshold values. X axis denotes the IP addresses and Y axis indicates the calculated entropy values. The threshold value is marked in sky blue. Each time slot is marked in a separate color. During normal time, entropy values are less than the threshold values. In attacking time alone, the entropy values cross the threshold value. In a Bit-and-Piece attack, the attack happens in all the machines at different time slots instead of attacking single machine continuously.

Here, all the machines connected with ISP suffer by this attack as the attacker the passies the commands only through ISP. During the trace back, the verification begins at Internet service provider. A machine who communicates often with the ISP is reported as a Zombie or Master of the attacker. The offender is identified using the log information available in ISP and it is removed from the network for security reasons.

C. Benefits of Detection process:

- Our detection process easily detects the any new type of DDoS attacks. Example Bit and Piece and Ransom ware attacks.
- Monitoring the packets every second, so detection and trace out the attackers are quickly.
- Using the threshold comparison is accurately detecting the attacks with less amount of time.

D.Prevention of Bit-and-Piece DDoS attack:

- Fit the Firewall between ISP server and Local ISP and also update it regularly.
- ISP should be configured with access control lists.
- Maintain the log information in ISP.

V. CONCLUSION

The usage of Internet is unavoidable in the current scenario. However, most of the users do not have enough awareness of how to safeguard themselves from the cyber wrongdoers. So, the cyber criminals take this as an advantage and they easily compromise the unsecured systems in both the private and the public sectors. Bit and Piece attack is an emerging DDoS attack threatening the universe. This paper offers the solution for the above issue based on the statistical approach. It senses the attack quickly using the threshold value. The computational time complexity of the method is $O (log_2n)$. This method involves effective increase in the security in local network. Experimental results prove accurate detection of the Bit-and-Piece attacks by the proposed method.

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.windstreamenterprise.com/insights/security/ddos-attacks-are-escalating-and-financial-institutions-are-especially-vulnerable/?utm_source=win-ambassador&utm_medium=social-media&utm_content=blog&utm_campaign=2019-WIN-Ambassadorhttps://nltimes.nl/2019/02/01/school-system-hit-ddos-attack-hundreds-schools-affected

[2] https://gbhackers.com/ddos-attack-bit-and-piece/

[3] S. Behal, and K. Kumar, K. "Detection of DDoS attacks and flash events using novel information theory metrics", Computer Networks, Vol. 116(4), pp.96–110, 2017.
DOI: 10.1016/j.comnet.2017.02.015.

[4] N. Hoque, H. Kashyap, D.K. Bhattacharyya, "Real-time DDoS attack detection using FPGA", Computer Communications 110, pp: 48–58, 2017.

[5] K.J.Singh and T.De, "MLP-GA based algorithm to detect application layer DDoS attack", Journal of Information Security and Applications, Vol. 36, pp. 145–153, 2017.

[6] S.Behal, K.Kumar, M.Sachdeva, "D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and Flash Events", Journal of Network and Computer Applications. DOI: 10.1016/j.jnca.2018.03.024

[7] R. Saravanan, S. shanmuganathan, Y. Palanichamy, "Behavior-based detection of application layer distributed denial of service attacks during flash events", Turkish Journal of Electrical Engineering and Computer Sciences, pp- 510-523, 2013.

[8] S. Malliga, C. S. Kanimozhi selvi AND S. V. Kogilavani "Low Storage and Traceback Overhead IP Traceback System" Journal of Information Science and Engineering , Vol. 32, pp. 27-45 , 2016.

[9] Y.Cui, L. Yan, S. Li, H. Xing, W. Pan, J. Zhu, J. and X. Zheng, "SD-anti-DDoS: fast and efficient DDoS defense in software-defined networks", Journal of Network and Computer Applications, Vol. 68(6), pp.65–79, 2016.

[10] K. Kalkan and F. Alagoz, "A distributed filtering mechanism against DDoS attacks: ScoreForCore", Computer Networks, Vol. 108, (10), pp.199–209, 2016.

[11] K. Xylogiannopoulos, P. Karampelas, and R. Alhajj, "Early DDoS detection based on data mining techniques", Information Security Theory and Practice. Securing the Internet ofThings, Springer , pp.190–199, 2014

[12] P. Xiao, W. Qu, H. Qi and Z. Li, "Detecting DDoS attacks against data center with correlation analysis", Computer Communications, Vol. 67(8), pp.66–74, 2015.

[13] S.M. Lee, D.S. Kim, D.S., J.H. Lee, and J.S. Park, "Detection of DDoS attacks using optimized traffic matrix", Computers & Mathematics with Applications, January, Vol. 63(2), pp.501–510, 2012.

[14] H.H. Jazi, H. Gonzalez, N. Stakhanova, and A.A. Ghorbani, "Detecting http-based application layer dos attacks on web servers in the presence of sampling", *Computer Networks*, Vol. 121(7), pp.25–36, 2017.

[15] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, "Flow level detection and filtering oflow-rate DDoS", Computer Networks, Vol. 56(15), pp.3417–3431, 2012.

[16] A. Saied, R.E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using artificial neural networks", Neuro computing, Vol. 172(1), pp.385–393, 2016.

[17] 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.

[18] 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.

[19] 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.

[20] T. Subburaj and K.Suthendran, "Digital Watering Hole Attack Detection Using Sequential Pattern", Journal of Cyber Security and Mobility, Vol. 7 (1), pp-1–12, 2018.

TABLE I. TRANSFERRED PACKET RATES ON VARIOUS TIME SLOTS IN EXPERIMENTAL

Address	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_10	T_11	T_12	T_13	T_14	T_15	T_16	T_17	T_18	T_19	T_20
IP 1	20	25	30	40	20	25	40	20	40	35	20	25	30	40	280	25	40	20	40	35
IP 2	20	25	30	35	40	35	35	40	35	40	250	25	30	35	40	35	35	40	35	40
IP 3	30	35	40	35	30	35	35	30	40	35	30	35	40	35	30	350	35	30	40	35
IP 4	20	25	30	35	40	35	35	40	35	40	20	25	30	35	40	35	35	40	400	40
IP 5	35	40	35	20	25	30	20	25	35	25	350	40	35	20	25	30	20	25	35	25
IP 6	30	35	40	35	30	40	20	30	35	40	30	350	40	35	30	40	20	30	35	40
IP 7	20	25	30	40	20	25	30	35	40	35	20	25	30	40	250	25	30	35	40	35
IP 8	35	40	35	25	30	40	30	35	40	35	35	40	35	25	30	40	30	35	400	35
IP 9	35	40	35	30	35	40	35	40	20	25	35	40	35	300	35	40	35	40	20	25
IP 10	40	20	25	30	35	40	35	30	35	40	40	20	25	30	35	40	35	30	35	300
IP 11	25	30	35	40	35	30	35	40	40	20	25	300	35	40	35	30	35	40	40	20
IP 12	20	25	30	40	20	25	30	35	35	40	20	25	30	40	20	25	250	35	35	40
IP 13	40	20	25	25	30	40	35	40	35	30	40	20	25	25	30	40	35	40	350	30
IP 14	35	40	35	25	30	35	40	35	35	40	350	40	35	25	30	35	40	35	35	40
IP 15	30	35	40	35	40	20	25	30	20	25	30	35	40	35	40	20	25	300	20	25
IP 16	35	40	35	40	35	40	35	40	20	25	35	40	35	400	35	40	35	40	20	25
IP 17	20	25	30	40	20	25	30	35	40	35	20	25	30	40	20	280	30	35	40	35
IP 18	35	40	35	40	35	40	35	40	20	25	35	40	35	40	35	40	35	40	250	25
IP 19	20	25	30	35	40	35	30	35	40	35	20	250	30	35	40	35	30	35	40	35
IP 20	35	40	35	40	20	25	30	35	40	35	35	40	350	40	20	25	30	35	40	35

TABLE II. **NORMAL PACKET FLOWS**

Address	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_10
IP 1	20	25	30	40	20	25	40	20	40	35
IP 2	20	25	30	35	40	35	35	40	35	40
IP 3	30	35	40	35	30	35	35	30	40	35
IP 4	20	25	30	35	40	35	35	40	35	40
IP 5	35	40	35	20	25	30	20	25	35	25
IP 6	30	35	40	35	30	40	20	30	35	40
IP 7	20	25	30	40	20	25	30	35	40	35
IP 8	35	40	35	25	30	40	30	35	40	35
IP 9	35	40	35	30	35	40	35	40	20	25
IP 10	40	20	25	30	35	40	35	30	35	40
IP 11	25	30	35	40	35	30	35	40	40	20
IP 12	20	25	30	40	20	25	30	35	35	40
IP 13	40	20	25	25	30	40	35	40	35	30
IP 14	35	40	35	25	30	35	40	35	35	40
IP 15	30	35	40	35	40	20	25	30	20	25
IP 16	35	40	35	40	35	40	35	40	20	25
IP 17	20	25	30	40	20	25	30	35	40	35
IP 18	35	40	35	40	35	40	35	40	20	25
IP 19	20	25	30	35	40	35	30	35	40	35
IP 20	35	40	35	40	20	25	30	35	40	35

Retrieval Number: A10861291S419/2019©BEIESP
DOI:10.35940/ijeat.A1086.1291S419
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

TABLE III. ENTROPY VALUES ON FIRST TEN TIME SLOTS

Address	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_10
IP 1	0.1675	0.1847	0.2027	0.2393	0.1617	0.1789	0.2500	0.1481	0.2404	0.2247
IP 2	0.1675	0.1847	0.2027	0.2192	0.2578	0.2247	0.2293	0.2382	0.2203	0.2451
IP 3	0.2210	0.2317	0.2451	0.2192	0.2137	0.2247	0.2293	0.1967	0.2404	0.2247
IP 4	0.1675	0.1847	0.2027	0.2192	0.2578	0.2247	0.2293	0.2382	0.2203	0.2451
IP 5	0.2444	0.2525	0.2247	0.1488	0.1889	0.2027	0.1563	0.1734	0.2203	0.1789
IP 6	0.2210	0.2317	0.2451	0.2192	0.2137	0.2451	0.1563	0.1967	0.2203	0.2451
IP 7	0.1675	0.1847	0.2027	0.2393	0.1617	0.1789	0.2070	0.2182	0.2404	0.2247
IP 8	0.2444	0.2525	0.2247	0.1743	0.2137	0.2451	0.2070	0.2182	0.2404	0.2247
IP 9	0.2444	0.2525	0.2247	0.1977	0.2366	0.2451	0.2293	0.2382	0.1496	0.1789
IP 10	0.2661	0.1580	0.1789	0.1977	0.2366	0.2451	0.2293	0.1967	0.2203	0.2451
IP 11	0.1955	0.2092	0.2247	0.2393	0.2366	0.2027	0.2293	0.2382	0.2404	0.1529
IP 12	0.1675	0.1847	0.2027	0.2393	0.1617	0.1789	0.2070	0.2182	0.2203	0.2451
IP 13	0.2661	0.1580	0.1789	0.1743	0.2137	0.2451	0.2293	0.2382	0.2203	0.2027
IP 14	0.2444	0.2525	0.2247	0.1743	0.2137	0.2247	0.2500	0.2182	0.2203	0.2451
IP 15	0.2210	0.2317	0.2451	0.2192	0.2578	0.1529	0.1827	0.1967	0.1496	0.1789
IP 16	0.2444	0.2525	0.2247	0.2393	0.2366	0.2451	0.2293	0.2382	0.1496	0.1789
IP 17	0.1675	0.1847	0.2027	0.2393	0.1617	0.1789	0.2070	0.2182	0.2404	0.2247
IP 18	0.2444	0.2525	0.2247	0.2393	0.2366	0.2451	0.2293	0.2382	0.1496	0.1789
IP 19	0.1675	0.1847	0.2027	0.2192	0.2578	0.2247	0.2070	0.2182	0.2404	0.2247
IP 20	0.2444	0.2525	0.2247	0.2393	0.1617	0.1789	0.2070	0.2182	0.2404	0.2247

TABLE IV. PACKET RATES ON T_11 TO T_20

Address	T_11	T_12	T_13	T_14	T_15	T_16	T_17	T_18	T_19	T_20
IP 1	20	25	30	40	280	25	40	20	40	35
IP 2	250	25	30	35	40	35	35	40	35	40
IP 3	30	35	40	35	30	350	35	30	40	35
IP 4	20	25	30	35	40	35	35	40	400	40
IP 5	350	40	35	20	25	30	20	25	35	25
IP 6	30	350	40	35	30	40	20	30	35	40
IP 7	20	25	30	40	250	25	30	35	40	35
IP 8	35	40	35	25	30	40	30	35	400	35
IP 9	35	40	35	300	35	40	35	40	20	25
IP 10	40	20	25	30	35	40	35	30	35	300
IP 11	25	300	35	40	35	30	35	40	40	20
IP 12	20	25	30	40	20	25	250	35	35	40
IP 13	40	20	25	25	30	40	35	40	350	30
IP 14	350	40	35	25	30	35	40	35	35	40
IP 15	30	35	40	35	40	20	25	300	20	25
IP 16	35	40	35	400	35	40	35	40	20	25
IP 17	20	25	30	40	20	280	30	35	40	35
IP 18	35	40	35	40	35	40	35	40	250	25
IP 19	20	250	30	35	40	35	30	35	40	35
IP 20	35	40	350	40	20	25	30	35	40	35

TABLE V. ENTROPY VALUES ON T_11 TO T_20

Address	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_10
IP 1	0.0857	0.1015	0.1545	0.1533	0.5025	0.1142	0.2059	0.1164	0.1150	0.1794
IP 2	0.4386	0.1015	0.1545	0.1392	0.1739	0.1461	0.1880	0.1910	0.1041	0.1967
IP 3	0.1164	0.1303	0.1890	0.1392	0.1417	0.5160	0.1880	0.1563	0.1150	0.1794
IP 4	0.0857	0.1015	0.1545	0.1392	0.1739	0.1461	0.1880	0.1910	0.4688	0.1967
IP 5	0.4960	0.1436	0.1723	0.0918	0.1241	0.1307	0.1262	0.1371	0.1041	0.1413
IP 6	0.1164	0.4960	0.1890	0.1392	0.1417	0.1607	0.1262	0.1563	0.1041	0.1967
IP 7	0.0857	0.1015	0.1545	0.1533	0.4858	0.1142	0.1689	0.1742	0.1150	0.1794
IP 8	0.1303	0.1436	0.1723	0.1087	0.1417	0.1607	0.1689	0.1742	0.4688	0.1794
IP 9	0.1303	0.1436	0.1723	0.4864	0.1583	0.1607	0.1880	0.1910	0.0678	0.1413
IP 10	0.1436	0.0857	0.1355	0.1244	0.1583	0.1607	0.1880	0.1563	0.1041	0.5272
IP 11	0.1015	0.4715	0.1723	0.1533	0.1583	0.1307	0.1880	0.1910	0.1150	0.1201
IP 12	0.0857	0.1015	0.1545	0.1533	0.1051	0.1142	0.5181	0.1742	0.1041	0.1967
IP 13	0.1436	0.0857	0.1355	0.1087	0.1417	0.1607	0.1880	0.1910	0.4448	0.1610
IP 14	0.4960	0.1436	0.1723	0.1087	0.1417	0.1461	0.2059	0.1742	0.1041	0.1967
IP 15	0.1164	0.1303	0.1890	0.1392	0.1739	0.0966	0.1484	0.5244	0.0678	0.1413
IP 16	0.1303	0.1436	0.1723	0.5223	0.1583	0.1607	0.1880	0.1910	0.0678	0.1413
3IP 17	0.0857	0.1015	0.1545	0.1533	0.1051	0.4861	0.1689	0.1742	0.1150	0.1794
IP 18	0.1303	0.1436	0.1723	0.1533	0.1583	0.1607	0.1880	0.1910	0.4150	0.1413
IP 19	0.0857	0.4386	0.1545	0.1392	0.1739	0.1461	0.1689	0.1742	0.1150	0.1794
IP 20	0.1303	0.1436	0.5306	0.1533	0.1051	0.1142	0.1689	0.1742	0.1150	0.1794

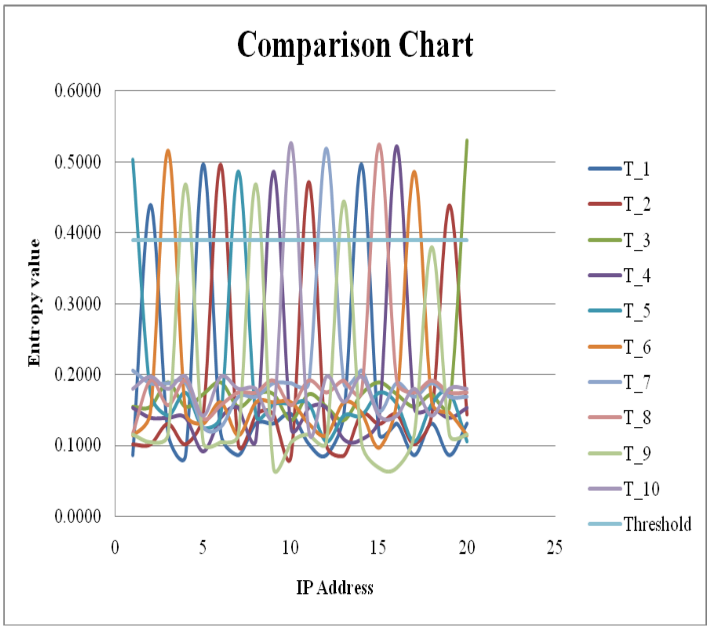

Fig. 4.Comaprison Chart

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..