International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

A Hybrid Model for Detecting DDoS Attacks in Wide Area Networks

Mohammad Arshad, Mohammad Ali Hussain

Abstract*: *Wide Area Networks (WANs) are subjected massive Denial of Service (DoS) attacks known as Distributed Denial of Service (DDoS) attacks. There are many distributed computing use cases in the real world. They include banking, insurance, e-Commerce and a host of other applications. In distributed environments, these applications are targeted by adversaries for launching DDoS attacks of various kinds. Such attacks cause the servers to be very busy answering fake traffic from the compromised nodes used by attackers from behind the scene. Large number of computers over Internet are compromised by attackers and through such machines DDoS attack is made. The server machines that provide services to genuine users become victims of such attacks. Detecting DDoS attacks is difficult in the presence of flash crowds that resembles DDoS traffic. As there are different kinds of DDoS attacks, it is understood, from the literature, that there is need for further research to have a comprehensive framework for detecting different kinds of DDoS attacks. In this paper we proposed a hybrid approach for detecting various kinds of DDoS attacks and simulation study is made to have proof of the concept. The results of the experiments revealed that the proposed methodology is useful to detect DDoS attacks in wide area networks.

***Keywords*: Wide Area Network (WAN), Distributed Denial of Service (DDoS), DDoS attack detection, spoofed DDoS, sophisticated DDoS**

I. INTRODUCTION

Denial of Service (DoS) is the attack which sends attack traffic to the victim system so as to make it so busy. This will not enable the victim server to serve legitimate clients. When DoS attack is made in large scale in a WAN, it is named as Distributed Denial of Service (DDoS) attack. There are different types of DDoS attacks. One such kind id known as flooding attack [9] where large scale fake traffic is sent to a server machine. As shown in Figure 1, DDoS flooding attack is launched by adversaries by compromising multiple nodes in WAN. The attackers will hide behind as they do not directly attack. Instead they make use of bots and handlers to launch DoS attack in large scale and hide their own identity as well. In the literature, there are many approaches used to detect DDoS attacks. They are discussed in [4], [5] and [9]. A hybrid statistical model is employed in [4] for DDoS attack detection. Entropy based detection of DDoS attacks is explored in [5] while various defines mechanisms for flooding DDoS attacks is investigated in [9].

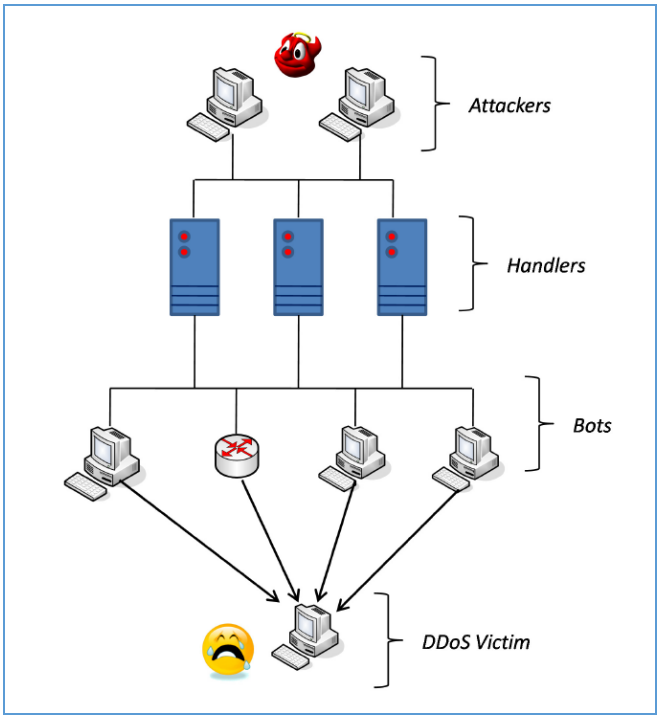

Figure 1: DDoS flooding attack scenario [21]

There are many solutions found in the literature. However, entropy based approaches are widely used to detect DDoS intrusions in wide area networks. Generally, attackers will work long time to launch DDoS attacks. They find various systems that can be compromised and used for launching attacks. The attackers are not known to public. It does mean that the source of attack is hidden. In other words, attackers will not use their machines to launch attacks. Instead, they compromise many systems through which they can reach the target server for making attacks. Therefore, it is difficult to identify attackers. However, attack can be detected and prevention measures can be taken care of. Our contributions in this paper are as follows.

1. We proposed a hybrid approach for detecting different kinds of DDoS attacks. Both source and traffic entropies are employed to achieve this.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author
Mohammad Arshad, Research Scholar, KLEF, Guntur District, A.P., India.
Dr. Mohammad Ali Hussain, Professor KLEF, Guntur District, A.P, India

2. A system model is designed for meaningful study of the problem in WAN environment which is distributed in nature.
3. We have made extensive simulations in NS-2 for evaluating the utility of the proposed approach in detection DDoS attacks. Experimental results revealed the usefulness of the proposed method.

The remainder of the paper is structured as follows. Section 2 presents literature review on various kinds of DDoS attacks and prevention measures. Section 3 on the other hand provides the proposed hybrid approach. Section 4 presents the distributed environment in which experiments are made. In other words, it provides system model followed. Section 5 provides experimental results. Section 6 concludes the paper and gives directions for future work.

II. RELATED WORK

This section reviews literature on different methods used for detecting DDoS attacks. Kasinathan et al. [1] considered Internet of Things (IoT) based on 6LoWPAN for detecting Denial of Service (DoS) attacks. Eslahi et al. [2] proposed characteristics of bots and botnets and provided valuable insights related to detection methods and challenges. Pandaa et al. [3] on the other hand proposed an intrusion detection method with a hybrid and intelligent approach. Girma et al. [4] used cloud computing environment for DDoS attack experiments. A hybrid statistical model is used for the empirical study. Navaz et al. [5] proposed an entropy based solution for DDoS attack detection. Anomaly in traffic is detected using entropy variations. Bots and botnets are used by adversaries to launch DDoS attacks.

Nadeem et al. [6] reviewed many intrusion detection methods that are investigated in the context of Mobile Ad Hoc Networks (MANET). The attacks are pertaining to network layer. Gendreau et al. [7] on the other hand explored intrusion detection systems that are used in the IoT use cases. Pan et al. [8] proposed a hybrid intrusion detection system for power systems using data mining approaches. It was found to be effective in detecting attacks. Zargar et al. [9] opined that there are many kinds of DDoS attacks. One such kind is known as DDoS flooding attacks. Sheikhan and Bostani [10] proposed a hybrid mechanism for intrusion detection with an architecture for IoT use cases. Multiple classifiers with supervised learning approach are used to detect attacks in [11].

Dilek et al. [12] discussed Artificial Intelligence (AI) techniques to detect cyber-attacks like DDoS. In [13] both AI and Genetic Algorithm (GA) are used in order to have protection from different attacks. Intrusion detection methods in IoT [14], [17] and cyber security mechanisms [15], botnet control traffic detection [16], attack detection in Wireless Sensor Networks (WSNs) [18], Hybrid approach in attack detection in MANET [19] and detection methods for virtual jamming methods [20] are other solutions found in literature. It is understood from the review that there is need for a hybrid approach for detecting different kinds of DDoS attacks in WAN. This paper proposes a methodology for the same.

III. PROPOSED HYBRID APPROACH

Our method for detecting DDoS attacks is the hybrid approach that makes use of source entropy and traffic entropy for classification of traffic into various kinds of DDoS attacks. Anomalous traffic patterns are identified and the detection is made. The network traffic is analysed for making well informed decisions. The packets when observed independently, they may look like genuine but when correlated with packets at different places, it is possible to identify attacks. DDoS attacks are caused by people or in other words, they are man-made attacks. Thus it is possible to identify certain patterns in the attack traffic. The variation in traffic or the degree of randomness or disorder in the traffic is called as entropy. This can be exploited to understand source IP distribution. The proposed hybrid approach is illustrated in Figure 1. It shows how the network traffic is monitored and classified to understand the dynamics of various kinds of DDoS attacks.

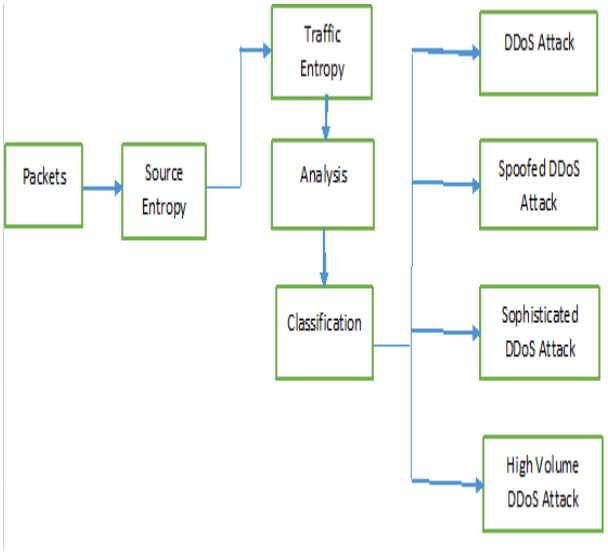

Figure 1: Overview of the hybrid approach

As DDoS attack is launched by an adversary, the network shows changes in traffic in time and space domain. When the traffic is low, there is no probability of DDoS attacks. However, when the traffic is unusually high, it is suspected as DDoS attack. In the temporal domain, it is possible to find the probability of attack. At the given time (initially) t1, there is no much traffic. After reaching the time t2, the traffic is more and the patterns reveal the probability of an attack. The time gap between t2 and t1 is denoted as detection delay. Source entropy is the measure to know the number of source IP addressed that are exploited by adversary to launch attacks. The term traffic cluster is used to denote the traffic from same network. The entropy measure that is related to the traffic clusters is called traffic entropy. The traffic analysis includes the volume of incoming traffic, source IP addressed that are found anew, the number of source IP addressed found and dynamics of traffic distribution. In order to reduce computational complexity, the concept of traffic cluster is used corresponding to entropy. In order to reduce false positives, the required thresholds are computed from traffic entropy.

When simulation is started, both source and traffic entropies are observed. Then packets are sent. The traffic may come actually from a normal user or attacker. The temporal domain is observed when traffic is increasing. Source and traffic entropies are computed. Both source and traffic deviations are also computed. Based on different conditions, it is possible to know whether it is a high volume DDoS attack or sophisticated DDoS attack or spoofed DDoS attack or simple DDoS attack. Different symbols and their definitions used in the proposed approach are provided in Table 1.

Symbol	Definition
H(SourceIP)	Represents source entropy
SourceIP	Represents source IP address
$p(SourceIP_t)$	Represents probability of source IP address
Same	Number of received packets
H(tr)	Represents traffic entropy
p(tr)	Represents probability of traffic
Y_i	Number of packets received
u,v	Integers
$(H_c(SourceIP))$	Represents current source entropy
$(H_c(tr))$	Represents current traffic entropy
$H_N(SourceIP)$	Represents initial Source entropy
$H_N(tr)$	Represents initial traffic entropy
H_N (SourceIP)+u* $\sigma_{SourceIP}$))	Represents upper threshold source entropy
$(H_N$ (SourceIP) $-u^*\sigma_{tc\ ID}))$	Represents lower threshold source entropy
$H_N(tr) - v^*\sigma_{tr}))$	Represents lower threshold traffic entropy
$H_N(tr) + v^*\sigma_{tr}))$	Represents upper threshold traffic entropy
$\sigma_{SourceIP}$	Represents standard deviation of source
σ_{tr}	Represents standard deviation of traffic

Table 1: Symbols used

Source IP address SourceIP is a 4-byte logical address used in the packets to represent its source IP. Traffic cluster is denoted as *t*. Source address entropy is denoted as H(SourceIP). Let the random variable H(SourceIP) take values Sc_IP_1, Sc_IP_2, Sc_IP_3,Sc_In_1 in different packets. Let the number of packets received per *src_IP* be $X_1, X_2, X_3, \ldots\ldots\ldots, X_n$.

H(SourceIP)=$-\sum_{i=1}^{N} p(SourceIPt)\ log_2(SourceIPt)$

$p(SourceIP_t)$={ $p(SourceIP_1)$ $p(SourceIP_2)$.....p $p(SourceIP_t)$

$p(SourceIP_t)=\frac{X_i}{s}$ where $S=\sum_{i=1}^{n} X_i$

Similarly traffic entropy is defined as

$H(tr)=-\sum_{i=1}^{M} p(tr)\ log2p\ ((tc\_ID_i)$

p(tr)= p(tr1) p(tr2)..... p(trnn)

$p(tr)=\frac{Y_i}{s}$ $S=\sum_{i=1}^{n} Y_i$

DDOS attack condition

$(H_c(SourceIP))>H_N(SourceIP)+u*\sigma_{SourceIP}))$

[current source entropy>upper threshold source entropy]

$(H_c(tr))>H_N(tr) + v^*\sigma_{tr}))$

[current traffic entropy > upper threshold traffic entropy]

Flash event condition

$(H_c(SourceIP))>H_N(SourceIP)+u*\sigma_{SourceIP}))$

[current source entropy>upper threshold source entropy]

$(H_c(tr))<H_N(tr) - v^*\sigma_{tr}))$

[current traffic entropy<lower threshold traffic entropy]

Spoofed DDOs Attack Condition

$(H_c(SourceIP))>H_N(SourceIP)+u*\sigma_{SourceIP}))$

[current source entropy>upper threshold source entropy]

$(H_c(tr))>H_N(tr) - v^*\sigma_{tr}))$

[current traffic entropy > lower threshold trafffic entropy]

High volume DDoS Attack condition

$(H_c(SourceIP))<H_N(SourceIP)+u*\sigma_{SourceIP}))$

[current source entropy<upper threshold source entropy]

$(H_c(sc_{IP})) > (H_N(sc_{IP}) - u^*\sigma_{sc\ IP})$

[current source entropy > lower threshold source entropy]

Sophisticated DDoS Attack Condition

$(H_c(SourceIP))<H_N(SourceIP)+u*\sigma_{SourceIP}))$

[current source entropy<upper threshold source entropy]

$(H_c(tr))>H_N(tr) + v^*\sigma_{tr}))$

[current traffic entropy > upper threshold traffic entropy]

Standard Deviation

The deviation value from the mean value is known as standard deviation. It is computed as in Eq. 1

$$\sigma=\sqrt{\frac{\sum(x-\bar{x})^2}{N}} \qquad (1)$$

The number of packets is denoted as N. The mean of packet values is represented as $\bar{x}$ and it is computed as in Eq. 2. The packet value is denoted by x.

$$\bar{x} = \sum\frac{x}{N} \qquad (2)$$

IV. SYSTEM MODEL AND ENVIRONMENT FOR EXPERIMENTS

A WAN mode is considered for empirical study. The model includes transit-stub which reflects the hierarchical nature of the Internet. As DDoS attacks are made on distributed environments, WAN is considered. In a WAN, many nodes are compromised by attackers prior to making DDoS attack. The WAN contains various domains. Every domain contains a stub network or a transit network. The stub network is used to have host nodes that are connected to Internet. A transit network is used in order to have inter-connection among many stub networks. The nodes linked to stub network are used to generate network traffic for experiments. The experiments are aimed at studying detection and prevention of DDoS attacks made on a server on which thousands of users get services. GT-ITEM model is used for network topology.

It has many Internet Service Provider (ISP) domains. There are as many as 12 transit routers. Legitimate nodes and DDoS traffic nodes are connected to those routers. DDoS is detected generally in an ISP domain. Around 400 nodes are employed for generating different kinds of traffic.

The simulation is made with the widely used NS-2 simulator. The simulation experiment continues for 70 seconds. The legitimate and DDoS traffics are generated with some interval time. HTTP protocol is used in order to generate genuine traffic while UDP is used for attack traffic. The nodes that are used for launching DDoS attack change TCP protocol for the sake of attack. The HTTP traffic is sent to servers in such a way that the server gets heavy attack traffic and will become busy serving the false requests. UDP flows are made with Constant Bit Rate (CBR) mode in the simulation environment. A time window is used in order to have temporal study with respect to DDoS attacks. For different sizes of window, traffic cluster entropy is computed. Server's capability is considered in order to make experiments on false positive rate, false negative rate, classification rate and detection rate. The attack is made for 30 to 35 seconds time.

V. RESULTS AND DISCUSSION

Experimental design is made using NS-2 as discussed in the Section 5. Logical AND or OR is used in order to have a detection metric for DDoS attacks. The metric is defined using source address entropy and traffic cluster entropy. There are many observations found in the simulation study. Source address entropy is found to be increased when DDoS attacks are made. The detection metric contains traffic cluster entropy in the majority part which will help in detecting DDoS attacks. Six sigma standard is used in order to compute threshold for source address entropy. ROC curve on the other hand is used in order to have traffic cluster entropy. The proposed methodology is employed to carry out simulations. A base line scenario is simulation with normal web traffic. Traffic cluster entropy in absence of attack is computed using source address entropy and corresponding standard deviation.

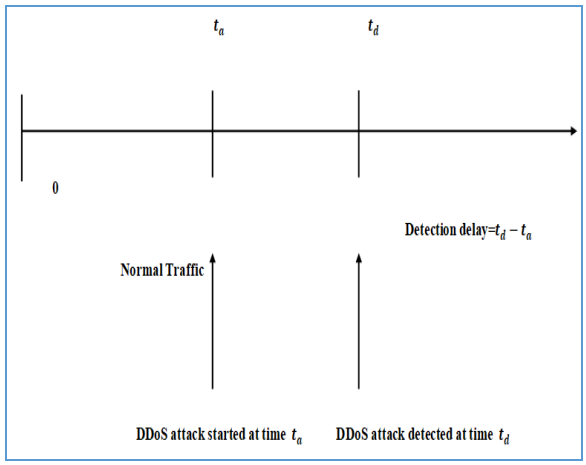

Figure 2: Time window for detection of DDoS attack

As presented in Figure 2, the DDoS attack start time appeared like normal traffic. However, as time is increased, the traffic is increased significantly and finally the detection of the attack is made. The delay in the detection of DDoS attack is computed using detection time and attack start time. The detection time is denoted as td while the attack start time is denoted as ta. The difference between them is considered to be delay in detection of DDoS attack as shown in Eq. 3.

$$\text{delay}=t_d - t_a \quad (3)$$

The detection delay is denoted as delay. Tolerance factor is another important variable that indicates the deviation in causing DDoS attack alarm. There are other variables such as normal detection, detection rate and false positive rate. In case of best detection rate, a low value is set for tolerance factor. Cluster entropy for normal traffic is set less in order to reduce false negatives and see that detection rate in increased. When tolerance factor is set high, it leads to high false positive rate. The range of entropy for classification is made broad for influencing false alarm rate and detection rate. In case of normal detection scenario, tolerance factor needs to be used as medium value. This will help in balancing false positives and false negatives. Tolerance factor is adjusted between 1 and 10 for making experiments. Normal and DDoS attack traffics are used to have different observations. The detection rate is computed as in Eq. 4.

$$D_{R=\frac{TP}{TP+FN}} \quad (4)$$

The false positive rate is computed as in Eq. 5.

$$FP_{R=\frac{FP}{TN+FP}} \quad (5)$$

The classification rate is computed as in Eq. 6.

$$C_{R=\frac{TP+TN}{TP+TN+FP+FN}} \quad (6)$$

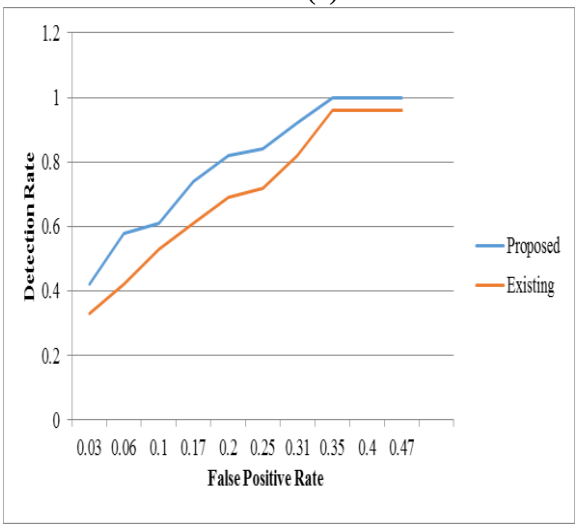

Figure 3: Detection rate comparison

As shown in Figure 3, the false positive rate is presented in horizontal axis. The values are taken from 0.03 to 0.47 with certain increment value. The results revealed that the false positive rate value has its influence on the detection rate. Another important observation is that the proposed system showed better performance over the state of the art in terms of detection rate.

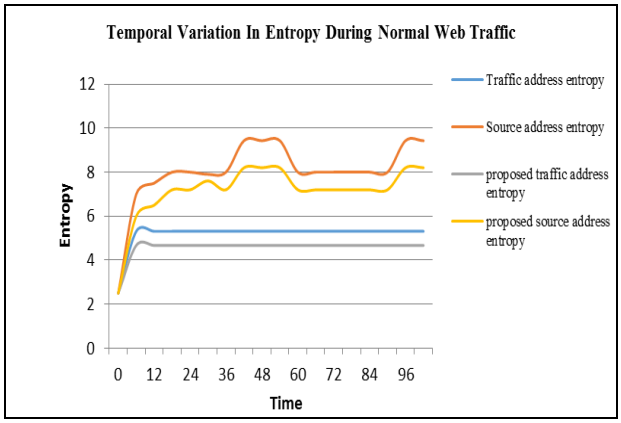

Figure 4: Temporal variation in entropy during normal web traffic

As shown in Figure 4, the time is considered in horizontal axis while the entropy values are shown in vertical axis. The traffic address entropy and source address entropy for existing and proposed methods are observed. The elapsed time has its impact on the entropy values. The proposed method has shown better performance than the state of the art.

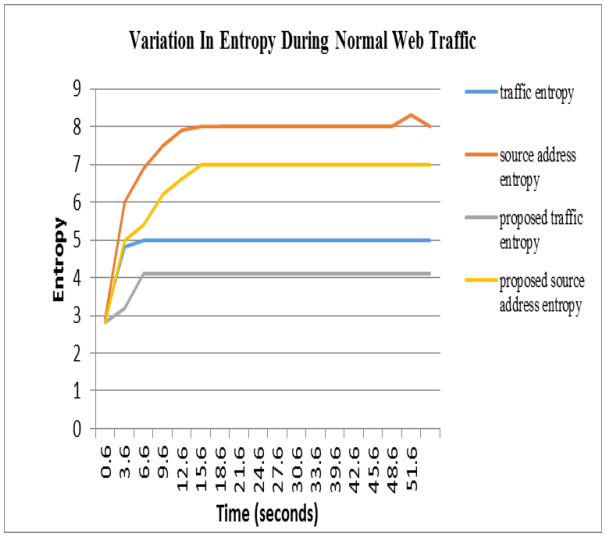

Figure 5: Variation in entropy during normal web traffic

As shown in Figure 5, the elapsed time is shown from 0.6 to 51.6 seconds with certain time interval in horizontal axis. The vertical axis showed entropy values. The time has its impact on the entropy. The proposed traffic and source address entropies showed better performance over state of the art.

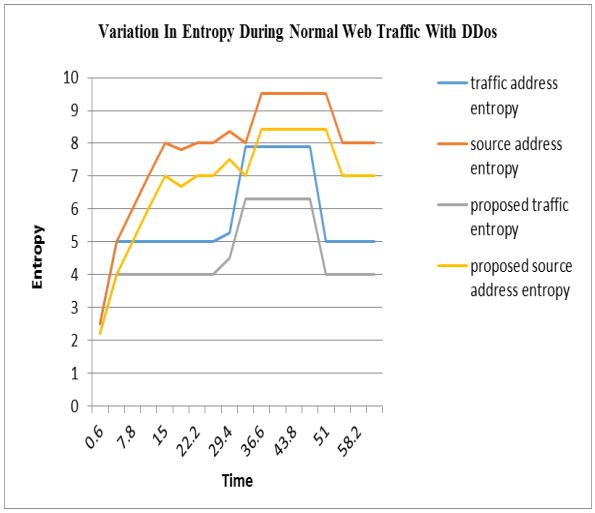

Figure 6: Variation in entropy during normal web traffic with DDoS attack traffic

As presented in Figure 6, the horizontal axis shows elapsed time while the vertical axis shows entropy values. The experiments are related to DDoS attack traffic. The time has its impact on the entropy values. The proposed method showed better performance over the state of the art.

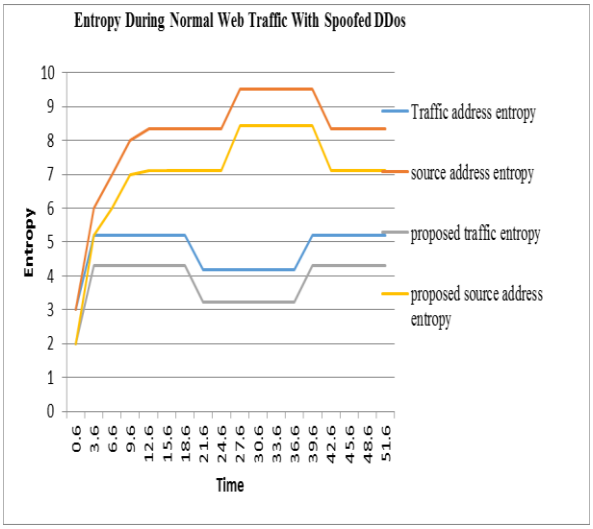

Figure 7: Entropy during normal web traffic with Spoofed DDoS attack

As shown in Figure 7, the elapsed time is taken in horizontal axis while the vertical axis shows the entropy values. The results with spoofed DDoS attack revealed that the time has its influence on the entropy values. The proposed method showed better performance over the state of the art.

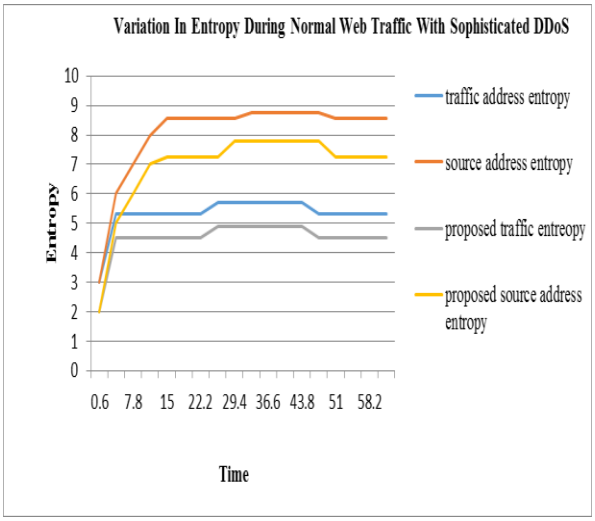

Figure 8: Entropy difference with normal web traffic containing sophisticated DDoS attack

As shown in Figure 8, the elapsed time is taken in horizontal axis while the vertical axis shows the entropy values. The results with sophisticated DDoS attack revealed that the time has its influence on the entropy values. The proposed method showed better performance over the state of the art.

VI. CONCLUSIONS AND FUTURE WORK

A hybrid approach is proposed in this paper for detecting different kinds of DDoS attacks. In presence of traffic that resembles DDoS attacks (like flash crowds), we investigated and found that it is difficult to identify DDoS attacks. Unlike existing approaches, we employed two kinds of entropy for better detection of such attacks. Both traffic cluster entropy and source address entropy are considered in the proposed methodology. A system model is designed for using a realistic distributed computing environment. Metrics like false positive rate, detection rate and classification rate are used for evaluating the proposed approach. Extensive study is made with NS-2 which is widely used network simulator (discrete event based). The experimental results showed that the proposed method is capable of detecting DDoS attacks in presence of realistic traffic environments. Besides it showed better performance over the state of the art. In future, we extend our methodology to deal with encrypted traffic (DDoS attack) launched by adversaries.

REFERENCES

1. Prabhakaran Kasinathan, Claudio Pastrone and Maurizio A. Spirito. 2013. Denial-of-Service detection in 6LoWPAN based Internet of Things. IEEE, P600-607.
2. Meisam Eslahi, Nor Badrul Anuar and Rosli Salleh.2012. Bots and Botnets: An Overview of Characteristics, Detection and Challenges. IEEE International Conference on Control System, Computing and Engineering, P349-354.
3. Mrutyunjaya Pandaa, Ajith Abrahamb and Manas Ranjan Patra.2012. A Hybrid Intelligent Approach for Network Intrusion Detection. International Conference on Communication Technology and System Design, P1-9.
4. Anteneh Girma, Moses Garuba, jiang Li and Chunmei Liu .2015. An Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment. International Conference on Information Technology, P212-217.
5. A.S. Syed Navaz, V. Sangeetha and C. Prabhadevi. 2013. Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud. International Journal of Computer Applications. 62, P42-47.
6. Adnan Nadeem, Member, IEEE and Michael P. Howarth.2013. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION, P1-19.
7. Audrey A. Gendreau, Ph.D.1, Michael Moorman, Ph.D.2 .2016. Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things. IEEE 4th International Conference on Future Internet of Things and Cloud, P84-90.
8. Shengyi Pan, Member, IEEE, Thomas Morris, Senior Member, IEEE, and Uttam Adhikari, Student Member, IEEE.2015. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. IEEE TRANSACTIONS ON SMART GRID, P1-10.
9. Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE. 2013. A Survey of Defence Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE COMMUNICATIONS SURVEYs, P1-24.
10. Mansour Sheikhan and Hamid Bostani.2016. A Hybrid Intrusion Detection Architecture for Internet of Things. International Symposium on Telecommunications, P601-606.
11. Michał Wo´zniaka,, Manuel Gra˜nab, Emilio Corchadoc.2014. A Survey of Multiple Classifier Systems as Hybrid Systems. Information Fusion, P1-30.
12. Selma Dilek, Hüseyin Çakır and Mustafa Aydın .2016. APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW. International Journal of Artificial Intelligence & Applications (IJAIA). 6, P21-39.
13. Fatemeh Barani. 2014. A Hybrid Approach for Dynamic Intrusion Detection in Ad Hoc Networks Using Genetic Algorithm and Artificial Immune System. Mobile ad hoc network, P1-6
14. Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani and Sean Carlisto de Alvarenga.2017. A Survey of Intrusion Detection in Internet of Things. Journal of Network and Computer Applications, P1-46.
15. Wenye wang, Zhuo Lu.2012. Cyber security in the smart grid: survey and challenges. ELSEVIER, P1344-1371.
16. Ibrahim Ghafir, Jakub Svoboda, Vaclav Prenosil .2015. A Survey on Botnet Command and Control Traffic Detection. International Journal of Advances in Computer Networks and Its Security– IJCNS. 5, P75-80.
17. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, MuttuKrishna Rajarajan.2013. A survey of intrusion detection techniques in cloud. Journal of network and applications, P42-57.
18. Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai-Choong Wong. 2013. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks. IEEE COMMUNICATIONS SURVEYS. 15, P1223-1237.
19. Masood Parvania, Georgia Koutsandria, Vishak Muthukumar, Sean Peisert, Chuck McParland, and Anna Scaglione.2014. Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems. Annual IEEE/IFIP International Conference on Dependable Systems and Networks, P774-779.
20. Diego Santoro, Ginés Escudero-Andreu, Konstantinos G. Kyriakopoulos, Francisco J. Aparicio-Navarro, David J. Parish and Michele Vadursi.2017. A Hybrid Intrusion Detection System for Virtual Jamming Attacks on Wireless Networks, P1-12.
21. Saman Taghavi Zargar, James Joshi and David Tipper. (2013). A Survey of Defence Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, p1-24.

AUTHORS PROFILE

Mohammad Arshad received the bachelor degree in Electronics and computer Engineering from Acharya Nagarjuna University, India and Master degree in Computer Science
Engineering from Jawahar Lal Nehru tecnnological University, India. He is Currently Pursuing

the Ph.D degree in Computer Science Engineering, from Koneru Lakshmaiah Education Foundation, India. His current research interests are computer networks ,Internet privacy, network security, and mobile network data analytics.

Dr. Mohammed Ali Hussain working as Professor in Department of Electronics and Computer Engineering, KL Deemed to be University, Guntur Dist., Andhra Pradesh, India. He has received 7 National Awards and 2 International Awards for his research contributions in various International Journals (Scopus & SCI). He is Editorial Board Member & Reviewer of various International Journals. He has published 6 patents to his credit and produced 8 PhD's under his supervision. His area of Interest includes Wireless Networks, Mobile Ad hoc Networks and Web Security. He is a member of various professional bodies FISEEE, ASDF, UACEE, IACSIT and IAENG.