ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Prevention of DDOS Attack Using Entropy Variations in Data Centers

P Mallika [1], G Manjula [2], M Muthumani [3], S Rubini [4]

Assistant Professor Department of CSE, Jai Shriram Engineering College, Tirupur, Tamilnadu, India[1]

Students Department of CSE, Jai Shriram Engineering College, Tirupur, Tamilnadu, India[2,3,4]

ABSTRACT: Distributed Denial of service attack (DDOS) is One of the major security threat to the internet.An essential strategy for halting DDOS attacks is to recognize aggressors and handlers. Identification of DDOS attacks is a testing issue for system security identifying DDOS attacks in the server system utilizing Entropy Based Anomaly Detection Algorithm. The estimation of entropy is figured regarding time and parcel windows. The outcomes demonstrate that amid typical action that is just genuine activity is streaming, Estimation of entropy lies in a restricted range however in the event of attack, it increments or reductions significantly. In this way, attack can without much of a stretch be distinguished. Botnet is one of the significant causes that dispatch DDOS attack. Botnet is really a system of bots or zombie PCs that are under the control of assailant.

KEYWORDS: DDOS, entropy, botnet, packet sniffer

I. INTRODUCTION

Distributed Denial-of-Service (DDOS) attacks are one of the most common threats to the internet. However, the unreliable communication is made through routing system that formulate which is very tough to trace the source of these attacks. Distributed Denial-of-Service (DDOS) is the most dreadful network threats in recent years. The vulnerabilities of IPv6/IPv4 environment in the occurrence of DDOS have been obtainable in and they have proposed a distributed defense system for IPv6/IPv4. The most familiar implementation of DDOS attack is the attack is distributed because it is a coordinate attack on the availability of given target system or network that use the computing power of thousands of compromised machines known as “zombies” to a target a victim. A DDOS attack is carried out in several phases. To lunch a DDOS attack malicious user first searches for some compromised hosts. This process is usually performed automatically through scanning of remote machines, looking for security holes. Consequently the malicious user installs attack tools on the compromised host. In a typical DDOS attack, Zombies are collected to send useless service requests, packets at the same time.

DDOS Attacks are launched for a variety of reasons, including monetary gain, maliciousness, fraud, warfare and to gain an economic advantage. Attacks are directed at compromising the confidentiality, integrity and availability of networks and their resources fall into the following four general categories are Modification attack,

Repudiation attack, Denial of service attack and access attacks. Today’s more critical infrastructures are increasingly reliant upon the Internet for operations.

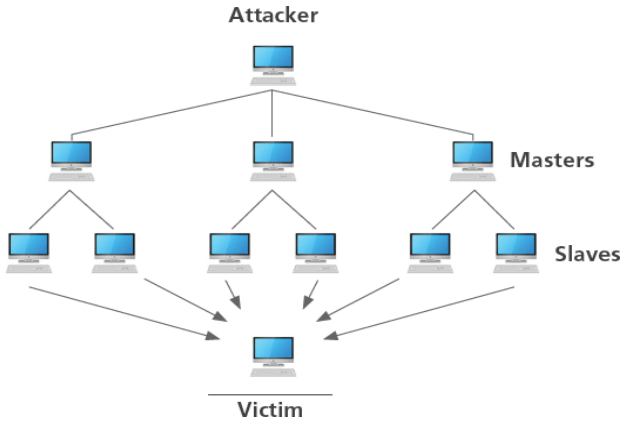
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019



.

Fig 1. The structure of DDOS attack

II. LITERATURE SURVEY

An Efficient and Reliable DDOS Attack Detection Using a Fast Entropy Computation Method

Conventional entropy is known as the efficient algorithm to monitor changes of network conditions. It needs time to calculate probabilities of distinct packet types; computing probabilities of distinct packets take very long computational time. In this paper, we have proposed the fast entropy approach that combines the lossless compression entropy of the FOEC method, and the entropy calibration that uses the number of packet types and the number of packets based on the idea that DDOS attacks rely mainly not on packet types alone as in conventional entropy, but both the packet types and traffic volume (the number of packets). We report that our Fast Entropy scheme reduced computational time by 90% of conventional entropy scheme while maintaining detection accuracy. Fast Entropy is even faster than compression entropy scheme in computing entropy values with same or better detection accuracy. For our future work, we have been developing an adaptive fast entropy algorithm that will further reduce the false positives as well as false negatives without adding overhead by introducing dynamic moving average and detection threshold value with respect to behavior of attacks.

Entropy Based Detection of DDOS Attacks

In this paper they proposed an effective and efficient IP Traceback scheme against DDOS attacks based on entropy variations. Here the packet marking strategies is avoided, because it suffers a number of drawbacks. This paper employs by storing the information of flow entropy variations at routers. Once the DDOS attack has been identified it performs pushback tracing procedure. The Traceback algorithm first identifies its upstream router where the attack flows comes from and then submits the Traceback request to the related upstream router. This procedure continues until the most far away zombies are identified. But in my existing case I used the static value to determine to determine the entropy rate. But in my proposed strategies I used dynamic value to determine the entropy rate which is based upon the packet size of the client's behavior.

Reliable Determination of Zombies Based on Entropy Variation

Zombie is a computer, connected to the internet that has been cooperated by a cracker. Zombie computers are frequently used to launch distributed denial-of-service attacks. Distributed denial-of-service (DDOS) attacks are a significant threat to the internet. IP traceback schemes are considered successful if they can recognize the zombies from whom the DDOS attack packets come into the Internet. Research on DDoS detection improvement and filtering has been conducted pervasively. However, the efforts on IP traceZback are limited. A number of IP traceback approaches

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

have been recommended to discover attackers and there are two major methods for IP traceback, the probabilistic packet marking (PPM) and the deterministic packet marking (DPM). Both of these strategies require routers to inject marks into individual *packets*

III. PROPOSED SYSTEM

Entropy Based TCP/IPv6/IPv4 Worm Detection

The proposed system going to be implemented using the entropy variation techniques. Entropy variation is used to find out the source of the attack with the help of entropy variation in dynamic by calculating the packet size, which shows the variation between normal and DDOS attack traffic. For DDoS attack detection, it is needed to compare the distribution of packet flows, which are out of the control of attackers once the attack is launched.

A typical scenario is to send out TCP/IP packets to random hosts, while keeping very little state information for each target, or none at all if the attack can be executed by sending a single TCP/IP packet. In IPv6/IPv4, TCP worms are high and there will be failure to detect the worms. The proposed system uses the **entropy variations for finding and detecting TCP worms**. Entropy maintains the threshold level for incoming packets; if the data flow reaches the maximum threshold level, the entropy detects the worm and also keeps away from the malicious users' request. The Entropy system makes the **TCP/IP communication is more secure and uninterrupted service** provided by the data transfer.

Entropy Variations

This TCP/IP is based on the notion of packet dynamics, rather than packet content, as a way to deal with the increasing complexity of attacks. We utilize a concept of entropy to measure time-variant packet dynamics. The entropy of network traffic should vary immediately on the router.

Entropy variation is a technique for identifying the vulnerable request from the attacker. It monitors the packet flows in router, and when the packet count exceeds the prescribed limit, the vulnerability is detected. The entropy maintains the threshold level for providing uninterrupted communication in the internet.

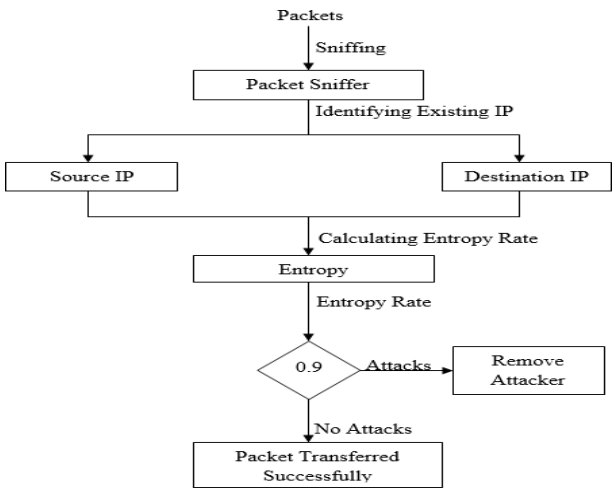


Fig 2. Proposed method

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Normalized Entropy

The entropy attains its minimum value of zero when all the items coming over the stream are the same and its maximum value of log (N0) when each item in the stream appears exactly once.

Across measurement intervals we might observe a different number of distinct items (N0). Thus, we normalize H to be between zero and one by computing the normalized entropy:

NE=H/ logN0.

This normalization measures the relative randomness within each measurement interval, and allows us to quantitatively compare entropy values across time. For the remainder of the discussion we will use this definition of normalized entropy.

Entropy management

Network events not caused by worms that trigger the detector. A worm detector based on entropy has to be calibrated for certain outbreak strength and the specific port profile of the worm. The source port can be variable or fixed, and mainly depends on the worm implementation details. The destination port can be variable or fixed, depending on the vulnerabilities(s) used to compromise target systems. It uses partial removal of the worm traffic in order to evaluate detector sensitivity for a detector that has had its sensitivity increased by dividing all thresholds by a factor larger than one**.**

Detector Design Methods

We use two independent methods for time series worm detection. We do so primarily to avoid any biases arising from a particular worm detection technique

1. Wavelet analysis

This technique treats measurement data (e.g., number of packets per five minute interval) as a generic time series signal. Using wavelet decomposition, the time series is then decomposed into different sub-components consisting of the low, mid-range, and high-frequency components.

2. Threshold-based detection

Entropy maintains the threshold level for incoming packets; if the data flow reaches the maximum threshold level, the entropy detects the worm and also keeps away from the malicious user'srequest.

The Entropy system makes the IPv6 UDP communication is more secure and uninterrupted service provided by the data transfer.

Entropy based DDoS detection algorithm

1. Collect sample TCP/IP flows for a time window T on the edge routers.
2. Calculate router entropy $H(x) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$
3. Calculate Normalized router Entropy (NE) = $(H / \log n0)$
4. If NE < threshold ($\delta 1$), identify the suspected attack flow.
5. Calculate the entropy rate H (X) = lim

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

1 H (x1, x2… xn) of the suspected flow in that router and the routers on downstream.

1. Compare Hi (x) i entropy rates on routers.
2. If Hi (x) threshold (δ2),

Legitimate traffics.
Else
It is a DDOS attack

3. Discard the attack flow.

Entropy Based DDOS Detection

1. Collect sample TCP/IP flows for a time window T on the edge routers.

The system has to collect the UDP data packet flows from the IPv6 network. The Packet Sniffer operation allows capturing UDP packets travelled through network adapter and also sniffing complete conversation between the network elements. This system can capture the source and destination machine complete information like IP address, port number, date and time of travelling and duration of packet traveling between the systems. Run the packet sniffer system for N hour of time in IPv6 network. This Capture the complete packet transfer details of both legitimate user data flow and attacker data flow. All the captured flows are removing the attacker host by using entropy based system in the packet capture and analysis system.

2. Calculate router entropy

The entropy H (x) of a random variable x with possible values of {1, 2…, n} and distribution of probabilities P = {p1, p2, . . . , pn} with n elements, where $0 \le pi \le 1$ and $\sum P = 1$ can be calculated as

$$H(x) = -\sum_{i=1} P(xi) \log P(xi)$$

$$P(xi) = \frac{\text{Number of packets with } X_i \text{ as source (destination) address}}{\text{Total number of packets}}$$

Here total number of packets is the number of packets travelled for a time *T*. likely we can estimate probability for each source (destination) port as

$$P(xi) = \frac{\text{Number of packets with xi as source (destination) port}}{\text{Total number of packets}}$$

3. Calculate Normalized router Entropy (NE) = (H / log n0)

Normalized entropy calculates the over all probability distribution in the captured flow for the time window *T*.

Normalized entropy = (H / log n0)

Here n0 is the number of distinct xi values in the given time window. In a DDoS attack from the captured traffic in time window *T*, the attack flow dominates the whole traffic, as a result the normalized entropy of the traffic decreased in a detectable manner. But it is also possible in a case of massive legitimate network accessing. To confirm the attack we have to again calculate the entropy rate. Here flow is packages which share the same destination address/port. In this

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

mechanism we have taken one assumption that the attacker uses same function to generate attack packets at "zombies", and it is a stationary stochastic process. According to for a stochastic processes the entropy rate H (c) of two random processes are same.

4. If NE < threshold (δ1), identify the suspected attack flow

To check the normalized value is less/greater than the threshold detection rate. If the entropy rate is less than the threshold limit, it will consider as normal flow. Otherwise, it will consider as attacker flow.

5. Calculate the entropy rate H (X) = lim

$$\square \to \infty$$

$\frac{1}{\square}$ H (x_1, x_2… x_n) of the suspected flow in that router and the routers on downstream

6. Compare the entropy rate

IV. IMPLEMENT THE RESULTS

DDOS Security System

The simulation is based on three situations considering normal flow, attack flow and entropy based prevention. In the first case the packets are send without any attack or performance enhancement, the normal flow of the packets are observed.

In the second case a set of anonymous data are send as attack packets to the destination which significantly reduces the overall system performance as well as connected nodes.

The third case, the system is equipped with the attacking data using entropy variation technique which analyses the previous history of data flow and compares it with the current flow and when maximum flow of data is found, the pattern is monitored which prevents the attack data and improves overall system performance

The graph Effect of DDOS Attack

The following graph1 depicts the normal flow of packets without any system degradation. The X axis represents the time involved in throughout the data flow and the Y axis represents packet count. It is observed that the packets achieved a stable flow throughout packet count 135 in IPv6-UDP networks

Entropy Rate	0.04	0.08	0.45	0.52	0.68	0.6
Time (MSec)	0	.5	1	1.5	2	2.5

Entropy Rate	0.32	0.48	0.53	0.58	0.46	0.49
Time (MSec)	4.5	5	5.5	6	6.5	7

Table: Sample Entropy Rates and Time

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

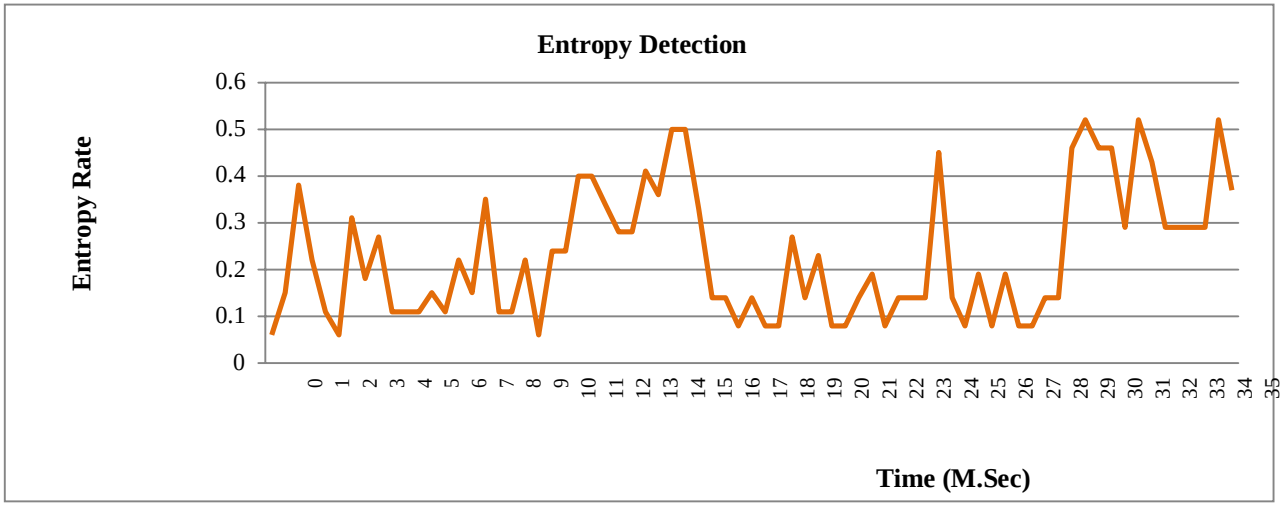


Fig 3. Normalized TCP flow entropy

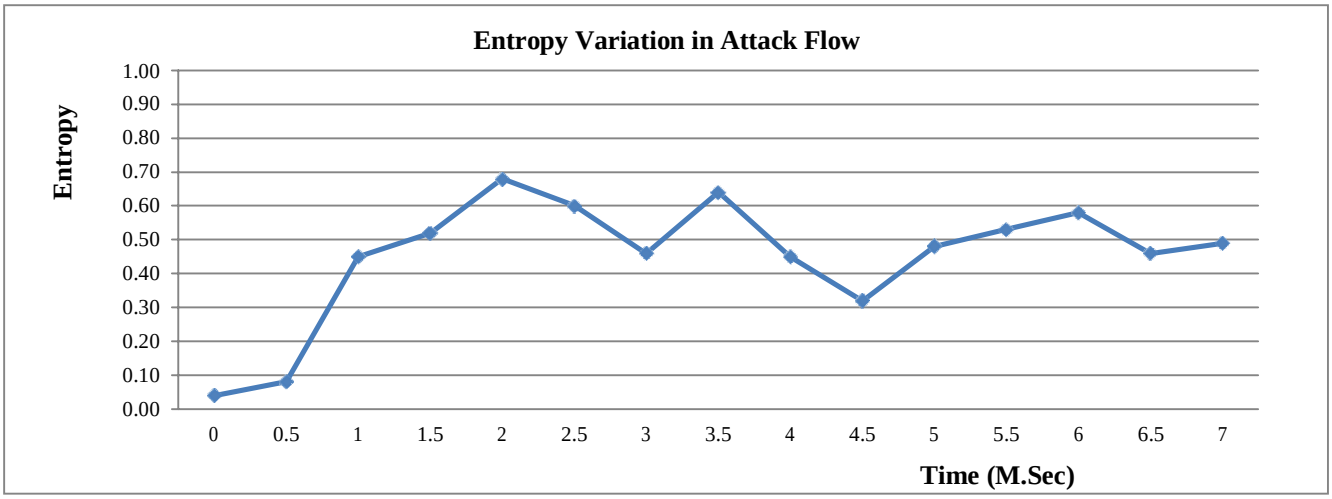


Fig4. Entropy Variation in Attack Flow

V. CONCLUSION

The proposed technique is an effective and efficient one for detecting UDP based DDoS attacks in IPv6 networks, based on entropy variations. This technique stores the information of flow entropy variations at routers. Once the DDoS attack has been identified it performs to delete the attacker request. Experimental results show that this system detects UDP worms in IPv6 networks very effectively. However, since the UDP data flow is very large in nature, it also results in higher false positive rates. In the future this algorithm could be enhanced to reduce the false positive rates and also to discriminate legitimate flash crowd from attack packets.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

REFERENCES

1. Balamurugan D. Chandrasekar S. Jaya Prakash D. Usha M. (2013) 'Analysis of Entropy Based DDoS Attack Detection to Detect UDP Based DDoS Attacks in IPv6 Networks' International Journal of Information & Computation Technology (IJICT) ISSN 0974-2239 Vol-3 PP 25-28
2. Khanna S. Venkatesh S.S. Fatemieh O. Khan F. Gunter C.A. (2012) 'Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks' Networking, IEEE/ACM Transactions PP. 715 – 728
3. Anitha G. (2012) 'Reliable Determination of Zombies Based on Entropy Variation', Journal of Computer Applications ISSN on Network security PP.257-260
4. K.Malarvizhi1 S.Saravanan2 (2012) Entropy-Based Detection of DDoS Attacks using HSM Model, International Journal of Communications and Engineering Volume 05– No.5, PP – 38-42
5. Shui Yu. Wanlei Zhou. Doss R. Weijia Jia. (2011) 'Traceback of DDoS Attacks Using Entropy Variations' IEEE Transactions on Parallel and Distributed Systems PP.412 – 425
6. You-ye Sun. Cui Zhang. Shao-qing Meng. Kai-ning Lu. (2011) 'Modified Deterministic Packet Marking for DDoS Attack Traceback in IPv6 Network' Computer and Information Technology (CIT), IEEE 11th International Conference on Digital Object Identifier PP.245–248
7. Anusha J. (2011) 'Entropy Based Detection of DDOS Attacks' International Journal of Soft Computing and Engineering (IJSCE) PP.564-567
8. Ting Ma. (2009) 'A link signature based DDoS attacker tracing algorithm under IPv6' International Journal of Security and Its Applications PP.27-36
9. Caicedo C.E. Joshi J.B.D. Tuladhar S.R. (2009) 'IPv6 Security Challenges' Published by IEEE PP. 36 – 42
10. Giseop No and Ilkyeun Ra (2009) 'An Efficient and Reliable DDoS Attack Detection Using a Fast Entropy Computation Method', ISCITPP-PP-1228
11. Velarde-Alvarado P Vargas-Rosales C Torres-Roman D (2008) 'Entropy Based Detection of DDOS Attacks' Advances in Computer Science and Engineering Research in Computing Science. PP-225-235
12. Sumit Kar. (2009) 'An Anomaly Detection Scheme for DDoS Attack in Grid Computing' International Journal of Computer Applications In Engineering Technology and Sciences (Ij-Ca-Ets) ISSN: 0974-3596 Vol 1 PPs 553-557
13. Shui Yu. Wanlei Zhou. (2008) 'Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks' Sixth Annual IEEE International Conference on Pervasive Computing and Communications PP. 566571
14. Khanna S. Venkatesh S.S. Fatemieh O. Khan F. Gunter C.A. (2008) 'Adaptive Selective Verification' 27th Conference on Computer Communications Published by IEEE PP.529 – 53
15. Xinyu Yang. Ting Ma. Yi Shi. (2007) 'Typical DoS/DDoS Threats under IPv6', Computing in the Global Information Technology, International Multi-Conference on Digital Object Identifier PPs. 55
16. Jun Bi, Jianping Wu, and Xiaoxiang Leng (2007) 'IPv4/IPv6 Transition Technologies and Univer6 Architecture' IJCSNS Int 232 ernational Journal of Computer Science and Network Security, VOL.7 PP-432- 442
17. W. Timothy Strayer. (2004) 'SPIE-IPv6: Single IPv6 Packet Traceback', Local Computer Networks, 29th Annual IEEE International Conference on Digital Object Identifier PP. 118 – 125
18. Waddington D.G. Fangzhe Chang. (2002) 'Realizing the Transition to IPv6' Communications Magazine on Digital Object Identifier PP. 138 – 147