ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 72-76 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

Detection of DDoS and DRDoS using Entropy based Approach and Comparative analysis with RCD approach in Networks

Thasneem Abdul Jaleel
Dept. of Computer Science and Engineering
KMEA Engineering College
thasneemj@gmail.com

A.Neela Madheswari
Professor, Dept. of Information Technology
KMEA Engineering College
neela.madheswari@gmail.com

***Abstract*— Network security is an important field in the area of computer science. Since everybody make use of computer networks in some form and makes maximum utilization of the networks, the study of attacks in network security is essential. Distributed reflection Denial of Service attacks (DRDoS) and Distributed Denial of Service (DDoS) attack are major threats to the network security. In the proposed system the volume of network traffic is pre-processed by entropy-based methods. Then, by using analysis on the entropy of source IPs and destination IPs, DDoS attacks and DRDoS attacks are detected. In this procedure, a variation fromLyapunov exponent is used to detect attacks. In order to express the rate of separation between source IPs and destination IPs, a variation of Lyapunov exponent of these entropies have been introduced to detect the anomalies in traffic. The system focus on analysing the efficiency of entropy based method against the efficiency of Rank Correlation based detection against DRDoS attacks.**

Key words-DRDoS, DDoS, Entropy, Lyapunov exponent

INTRODUCTION

Threats are common in wired and wireless networks. The potential threats to network security are always evolving. Therefore constant network monitoring and security should be the priority of the network administrator.

If the security of the network is compromised, there could be serious consequences, such as loss of privacy, and theft of information. Main objective of network security is to ensure that the network is unavailable for unauthorizedaccess. The business transactions and other activities carried over the internet makes the network more vulnerable to attacks and misuse. We need to implement solutions that are flexible, transparent and flawlessly integrated to the networking system.

Network security threats mainly evolve in the form of different types of attacks.

Network attack tools and methods have evolved. Back in the days when a hacker had to have sophisticated computer, programming, and networking knowledge to make use of rudimentary tools and basic attacks.

Nowadays, network hackers, methods and tools has improved tremendously, hackers no longer required the same level of sophisticated knowledge, people who previously would not have participated in computer crime are now able to do so.

Threats to the networks evolve in the form of attacks. Different types of attacks like Black hole, worm hole and sink hole disrupts the network as described in [4].Denial of Service attacks like Distributed DoS (DDoS) and Distributed Reflected DoS (DRDoS) are also emerging .

DDoS occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. This is the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behaviour of each attack machine can be stealthier, making it harder to track and shut down.

Distributed Reflection Denial of Service (DRDoS) attacks include attackers using DNS servers as reflectors to send bogus packets to the target systems

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 72-76 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

The work proposed in [2] focus on detecting these attacks using the Rank Correlation based detection (RCD) method.

The proposed approach focus on detecting DDoS and DRDoS using entropy based analysis. The work further analyse the efficiency of entropy based approach against RCD method.
The basis for detection is Lyapunov exponent and Tsallis entropy as described in [1].

RECENT RESEARCHES

Distributed denial-of-service (DDoS) attacks pose an immense threat to the Internet, and many defence mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. The DDoS field is quickly becoming more and more complex, and has reached the point where it is difficult to see the forest for the trees. On one hand, this hinders an understanding of the DDoS phenomenon.
The variety of known attacks creates the impression that the problem space is vast, and hard to explore and address. On the other hand, existing defence systems deploy various strategies to counter the problem, and it is difficult to understand their similarities and differences assess their effectiveness and cost, and to compare them to each other. The paper [4] describes that one frequently exercised manner to perform a DDoS attack is for the attacker to send a stream of packets to a victim; this stream consumes some key resource, thus rendering it unavailable to the victim's legitimate clients. Another common approach is for the attacker to send a few malformed packets that confuse an application or a protocol on the victim machine and force it to freeze or reboot.
The increasing practicality of large-scale flow capture makes it possible to conceive of traffic analysis methods that detect and identify a large and diverse set of anomalies. However the challenge of effectively analysing this massive data source for anomaly diagnosis is as yet unmet. The argument in [5] is that the distributions of packet features (IP addresses and ports) observed in flow traces reveals both the presence and the structure of a wide range of anomalies.
Using entropy as a summarization tool, it is able to show that the analysis of feature distributions leads to significant advances on two fronts: (1) it enables highly sensitive detection of a wide range of anomalies, augmenting detections by volume-based methods, and (2) it enables automatic classification of anomalies via unsupervised learning. In [5] it is demonstrated the utility of treating anomalies as events that alter traffic feature distributions. It is shown that treating anomalies in this manner yields considerable diagnostic power, in detecting new anomalies, in understanding the structure of anomalies, and in classifying anomalies.
The work proposed in [5] showed that entropy is an effective metric to capture unusual changes induced by anomalies in traffic feature distributions.
The work in [6] has demonstrated the utility of treating anomalies as events that alter traffic feature distributions. It shows that treating anomalies in this manner yields considerable diagnostic power, in detecting new anomalies, in understanding the structure of anomalies, and in classifying anomalies. It also shows that entropy is an effective metric to capture unusual changes induced by anomalies in traffic feature distributions.

The work proposed in [5] uses the theory of network self-similarity to differentiate DDoS flooding attack traffic from legitimate self-similar traffic in the network. It observed that DDoS traffic causes a strange attractor to develop in the pattern of network traffic. From this observation, a neural network detector trained by DDoS prediction algorithm was developed. The preliminary experiments and analysis indicate that the proposed chaotic model in [4] can accurately and effectively detect DDoS attack traffic. The approach has the potential to not only detect attack traffic during transit, but to also filter it.
Once a DDoS attack has been identified by the victim via detection algorithms, the victim then initiates the pushback tracing procedure. The traceback algorithm first identifies its upstream routers where the attack flows came from, and then submits the traceback requests to the related upstream routers. This procedure continues until the most far away zombies are identified or when it reaches the discrimination limitation of DDoS attack flows. Extensive experiments and simulations have been conducted, and the results demonstrate that the proposed mechanism works very well in terms of effectiveness and efficiency. Compared with previous works, the proposed strategy in [7] can traceback fast in larger scale attack networks.
The work in [8] proposes two new and effective information metrics for low-rate DDoS attacks detection: generalized entropy and information distance metric. The experimental results show that these metrics work effectively and stably.
As the proposed metrics can increase the information distance (gap) between attack traffic and legitimate traffic, they can effectively detect low-rate DDoS attacks early and reduce the false positive rate clearly. The proposed information distance metric overcomes the properties of asymmetric of both Kullback–Leibler and information divergences. Furthermore, the proposed IP traceback scheme based on information metrics can effectively trace all attacks until their own LANs (zombies).

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 72-76 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

ENTROPY BASED DETECTION ALGORITHM

During a Denial of Service attack there will be changes in the nature of distributions of source IPs and destination IPs in the traffic. The dispersal nature could be captured using entropy based measurements. As a statistic metric, entropy has been used in anomaly detection by many researchers. It describes the degree of concentration and dispersal characteristic of traffic. We can perform the analysis of the entropy of source IPs and destination IPs in order to detect DDoS attacks. A variation from Lyapunov exponent is used for attack detection.
Lyapunov exponent can identify the rate of separation between the source and destination IPs and thereby detect anomalies in the traffic.

Basis of Entropy

Given a distribution of probabilities P = {p1, p2... pN} with N elements, where $0 \leq pi \leq 1$ and $\sum i\ pi=1$, entropy$Hq$is defined as

$$H_q = \frac{1-\sum_{i=1}^{N} p_i^q}{q-1} \quad (1)$$

In general, $Hq$is called Tsallis entropy or non-extensive entropy. Here, q is called the entropic parameter. The variation of q modifies the relative contribution of a given event to the whole. Actually, Tsallis entropy is one-parametergeneralization of the well-known Shannon entropy. When the value of q is equal to 1, they have the same expression.In the proposed work$N$ identifies the number of packets in the dataset, and pi is the probability of each packet feature. The value of entropy may range from 0 toH_{max}^{q} which represents maximum concentration and maximum dispersion.The maximum entropy $H_{max}^{q}$is defined as

$$H_{max}^{q} = \frac{1-N^{1-q}}{q-1} \quad (2)$$

Lyapunov Exponent

Lyapunov exponent is a quantity that characterizes the rate of exponent separation between two trajectories in phase space [14].

$$e^{\lambda t} \approx \frac{\Delta xt}{\Delta x0} \quad (3)$$

When $\lambda<0$, the orbit attracts to a stable fixed point or stable periodic orbit. Negative Lyapunov exponents mean the merger degree between two trajectories. The more negative the exponent, the smaller distance they have. In our case, negative exponents represent the dispersal trend in the distribution of destination IPs.

When $\lambda = 0$, the orbit is a neutral fixed point (or an eventually fixed point). A Lyapunov exponent of zero indicates that the system is in some sort of steady state mode. In our case, zero exponent represents source IPs and destination IPshave the same distribution, which is normal traffic in most times.

When $\lambda >0$, the orbit is unstable and chaotic. Positive Lyapunov exponents mean the separation degree between two trajectories. The more positive the exponent, the bigger distance they have. In our case, positive exponents representthe dispersal trend in the distribution of source IPs.

Exponent Separation algorithm

Tsallis entropy and Lyapunov exponent are combined to propose the detection algorithm. In this approach, the entropy of the observed traffic is normalized with respect to the maximum entropy. The normalized entropy H_{norm} is given by

$$H_{norm} = \frac{Hq}{H_{max}^{q}} \quad (4)$$

The proposed approach first captures the details regarding the flow information of the network traffic. Every packet contains the source IP and destination IP. Now the entropies of source and destination IPs can be calculated. We can then preprocess these entropy sequences using AutoRegressive model. The rate of exponent separation between source and destination IPs can be analysed. Finally we need to specify a threshold λ_k which is dependent on the simulation environment as in [1].

SYSTEM ENVIRONMENT

The network simulations are being done in java. The reflectors, clients and attackers are created during runtime. We created a default network topology.

SYSTEM DESCRIPTION

The system can be developed in 4 phases-Simulation environment creation, DDoS and DRDoS simulation, DDoS and DRDoS detection using entropy based approach and comparison of RCD based approach with Entropy based approached.

Simulation Environment creation

simulations are carried out using java.The network topology consisting of 16 client and attacker nodes and 17 reflector nodes are

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 72-76 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

created.The client nodes and reflectors are created in the simulation window.

The simulation created is assumed to be under a static network. Each client and reflector is given an IP address and an identifier. We can select the source and destination node and send the message from source to destination. A single click on each node reveals all its details like its name, IP and the coordinate position.

To simulate the actual packet flow in the network, we have to first create the topology. Each node knows their neighbours. The source and destination nodes are to be identified for very flow. Each node has two modes - normal mode and attacking mode. In the normal mode, the desired message can be send from source to destination nodes at any point of time. The source and destination are selected, and the desired messages are created and send.

DDoS and DRDoS Simulation.

Once we choose a node to be in attacking mode, for DRDoS the source node (attacker) chooses various reflector paths and send the data simultaneously. This flow is indicated using different colored lines successively for the ease of understanding. This continues and eventually the target gets overloaded. In case of DDoS attack, an attacker node make use of an available path and send packets, then the next attacker sends packet through its possible route and overloads the victim.

DDoS and DRDoS Detection

The attack detection can be carried out using the entropy based method described in section III. We calculated the entropy separation of source and destination IP addresses. The obtained entropy is normalized with respect to maximum entropy.

The flow details from the source and destination nodes were pre-processed using the Auto Regression model. The rate of exponent separation is calculated based on this observation. Now we specify a threshold $-0.3 \leq \lambda \leq 0$ for genuine traffic as observed under different simulation scenarios. The rest of the flows that fall beyond the threshold are classified as attack flows.

Comparison of RCD based approach with Entropy based analysis.

This is a comparative analysis of the attack detection methods based on Rank correlation based detection and Entropy based approach. The delay in in finding the attack packets using the entropy based approach is found to be lower than that incurred in RCD based approach.

EXPERIMENTAL RESULTS

The attack throughput of DRDoS attack was found to be higher than that of DDoS as in [2].This is described in fig 1.The throughput vs. number of attackers graph states that the intensity of DRDoS is higher than that of DDoS.This observation is due to the use of reflector nodes in DRDoS which is clearly stated in [2]

Fig.1.Attack throughput graph

The entropy threshold was found to be $-0.3 \leq \lambda \leq 0$ for genuine flows as shown in fig 2. The flows that fall beyond this threshold are found to be malicious.

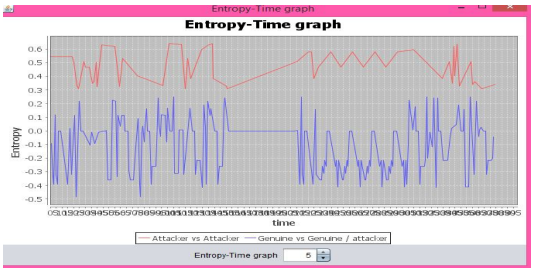

Fig .2 Entropy –Time graph.

Fig 3 describes the entropy separation between the source and destination.

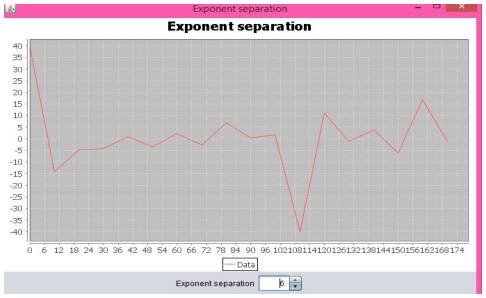

Fig 3.Entropy separation between source and destination nodes.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 72-76 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

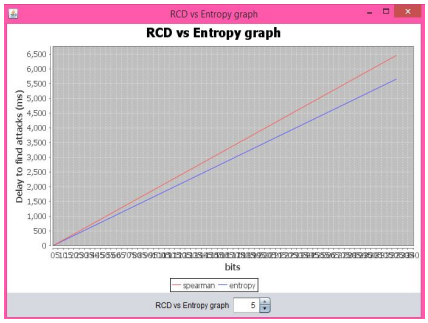

Fig 4.Comparison of RCD and Entropy based approaches

Consider the graph given in fig 4.The delay in packet transmission is found to be higher in the system when RCD based approach is used when compared to entropy based approach. Delay is greater in spearman because of the computational complexity to find spearman coefficient from flows. Entropy calculation is comparatively simple due to the use of AR model.

CONCLUSION

The proposed anomaly detection method is based on the Tsallis Entropy and Lyapunov exponent. In this approach, the entropy between Source IPs and Destination IPs can be compared by analysing the rate of exponent separation. The detection of DDoS and DRDoS attacks can be performed. Weanalysed the intensity of the attacks. The exponent separation between source ip and destination ip in both the attacks are analysed.The delay in the system running with Entropy based approach for detecting DRDoS and DDoS was found to be lower than the system that uses Rank Correlation based Detection approach. Hence Entropy based approach is better compared to RCD based approach for detecting DDoS and DRDoS attacks.

REFERENCES

[1]XinleiMa,YonghongChen,"DDoS Detection method based on chaos analysis of network traffic entropy",IEEE commun.lett,2014.

[2]Thasneem Abdul Jaleel, A.Neela Madheswari,"RCD based detection of Distributed Reflection Denial of Service attacks with a comparative analysis of DDoS over DRDoS " In the Proceedings of National Conference on Information and Communication Technologies (NCICT 2014) held at Baselios Poulose II Catholicos College, Baselios Mount, Piravom, 4.03.2014

[3]Wei Wei, Yingjie Xia, Guang Jin"Rank Correlation Based Detection against Distributed Reflection DoS Attacks"IEEE Commun.Lett.Vol.17 no.1, 2013.

[4]LijaJoy,Sheena Kurien k,"Black Holes Detection in Adhoc Wireless Networks"In the Proceedings of National Conference on Information and Communication Technologies (NCICT 2014) held at Baselios Poulose II Catholicos College, Baselios Mount, Piravom, 4.03.2014.

[5] Y Chen, X. Ma, and X. Wu, "DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory," *IEEECommun.Lett.*, vol. 17, no. 5, pp. 1052–1054, 2013.

[6]S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3,pp. 412–425, Mar. 2011

[7]Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE Trans. Inf. Forensicsand Security*, vol. 6, no. 2, pp. 426–437, June 2011

[8]Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Commun. Lett.*, vol. 13, no. 9,pp. 717–719, 2009