Volume-1
Issue-3
March-2016

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com

DDOS Attack Detection Mechanism to Avoid Network Performance Issues

Amit Dogra

Department of CSE BGSB University, Rajouri

ARTICLE DETAILS

Article History
Received: 22 February 2016
Accepted: 04 March 2016
Published Online: 10 March 2016

Keywords:
DDOS, Throughput, Transmission time, delay

ABSTRACT

Network traffic management results in effective packet transmission and resource utilization. All the major stakeholders of the network service providers work to increase the traffic flow by fair or unfair means. To this end, unfair means results in attackers to attack the resources over the network. This generally is accomplished by forming the similar identities for accessing the resource on behalf of other nodes. In addition, heavy traffic is generated by the fake or formulated node. This heavy traffic causes resource unavailability and denial of service. This type of attack is also termed as distributed denial of service attack. The performance of network degrades through this aspect of attack and optimization strategies are required to overcome this issue. This paper discussed some of the effective strategies that could be employed for the detection and prevention of DDOS attack. The parametric comparison of those techniques is also presented comprehensively. Parametric comparison includes throughput, packet drop ratio, transmission time and delay.

1. Introduction

[1]DDOS attack can hamper the performance of the system and causes performance degradation. To tackle the issue,[2] DDOS attack must be detected at the early stage and block the node that is being suspected to be malicious. The process of detection of DDOS attack and nodes blocking that are indulged within the problem. [3]The mechanism of detection generally involved machine learning process. This process of detection has number of different phases. All of these phases are discussed as under:

- Pre-processing

[4]This mechanism is used in order to remove the noise if any from the dataset. The mechanism could increase classification accuracy of detection of the attack.

- Segmentation

[5]Segmentation is the process of dividing the entire dataset into critical and non-critical parts. Critical parts are retained and non-critical parts are rejected from the simulative parts. The result will be greatly impacted through this phase.

- Classification

[6]Classification is the mechanism that is used in order to determine the final result as a result of testing and training operation performed. [7]The mechanism ensures that better classification accuracy is achieved by removing the noise if any from the dataset.

All of these processes are followed in sequence to achieve the desired result. Rest of the paper is organised as under: section 2 gives the literature survey of the existing mechanisms used to detect DDOS attack, section 3 gives the comparative analysis of the parameters used within different techniques, section 4 gives the conclusion and future scope, section 5 gives the references.

2. Literature Survey

This section gives the details of the techniques that are used to detect the DDOS attack. The different mechanisms are discussed as under.

[8] Conducted survey on DDOS attacks within cloud related platform. The cloud related platform was often comes into direct contact with different types of attacks. This paper discussed mining related attack detected strategies along corrective measure. [9]proposed a DDOS attack detection through network encryption mechanism. Network encryption mechanism uses the cryptography to convert plain text into cipher text. The cipher text is encrypted text that is being transferred towards the destination. [10]discussed clone based attacks detection strategy through machine learning. Machine learning mechanism uses series of phases for

the detection of attack from the dataset. [11]proposed cloud based security issues and detect the problem from the vast majority of domain by securing the process of packet transmission. The mechanism although decrease the throughput of the data transmission. [12]proposed a security based mechanism to detect the issues within the cloud based system. The mechanism used for the detection was known as intrusion detection system. The intrusion based system allows better throughput and response time as compared to existing system. [13]proposed a mechanism to detect the abrupt change in entropy of the network through security procedures. The security based mechanism ensures better stability of the network through packet transmission towards the base station. Packet drop ratio was reduced considerably using this mechanism.

All of the discussed mechanism works towards detection of problems from the cloud and networked environment. The problem however of packet drop ratio and latency exists as a result of DDOS attack.

3. Comparative Analysis

The comparative analysis of the techniques used to detect the DDOS attack from the network is given as under

Technique	Number of Packets	Transmission Time(ms)	Delay	Throughput	Packet Drop ratio(%)
KNN	1000	8	2	187	10
SVM	1000	12	5	156	12
Genetic Algorithm	1000	20	15	123	25
K Means	1000	18	12	145	14
Random Forest	1000	11	13	140	15

Table 1: Parametric comparison

From the comparative analysis it is clear that KNN generates best possible result as compared to other approaches in terms of transmission time and throughput.

4. Conclusion and Future scope

The proposed approach provided comparative analysis of the techniques that are used to detect the DDOS attack from the provided environment. The environment that is used could be networked or cloud environment. Most of the discussed work performs the operation within the cloud based environment. The network based environment is also greatly impacted by the DDOS attack. The DDOS attack hampers the performance by causing deadlock within the system. Resource unavailability reduced the profit of the network service provider. To overcome this issue, in future KNN approach can be merged along other mining based mechanism to detect the attack at early stage and increase the performance of the cloud or networked system.

References

[1] L. . Li and G. . Lee, "DDoS Attack Detection and Wavelets," *Telecommunication Systems*, vol. 28, no. 3, pp. 435-451, 2005.

[2] R. . Xunyi, W. . Ruchuan and W. . Hai-yan, "Wavelet analysis method for detection of DDoS attack on the basis of self-similarity," *Frontiers of Electrical and Electronic Engineering in China*, vol. 2, no. 1, pp. 73-77, 2007.

[3] B. . Xiao, W. . Chen and Y. . He, "A novel approach to detecting DDoS Attacks at an Early Stage," *The Journal of Supercomputing*, vol. 36, no. 3, pp. 235-248, 2006.

[4] M. . Kim, H.-J. . Na, K. . Chae, H. . Bang and J.-C. . Na, "A Combined Data Mining Approach for DDoS Attack Detection," *Lecture Notes in Computer Science*, vol. , no. , pp. 943-950, 2004.

[5] K. . Lu, D. . Wu, J. . Fan, S. . Todorovic and A. . Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," *Computer Networks*, vol. 51, no. 18, pp. 5036-5056, 2007.

[6] T. . Ni, X. . Gu, H. . Wang and Y. . Li, "Real-time detection of application-layer DDoS attack using time series analysis," *Journal of Control Science and Engineering*, vol. 2013, no. 2013, p. 4, 2013.

[7] B. . Kashyap and S. K. Jena, "DDoS Attack Detection and Attacker Identification," *International Journal of Computer Applications*, vol. 42, no. 1, pp. 27-33, 2012.

[8] S. M. Lee, D. S. Kim, J. H. Lee and J. S. Park, "Detection of DDoS attacks using optimized traffic matrix," *Computers & Mathematics With Applications*, vol. 63, no. 2, pp. 501-510, 2012.

[9] Y. . Chen, K. . Hwang and W.-S. . Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 12, pp. 1649-1662, 2007.

[10] S. T. Zargar, J. . Joshi and D. . Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046-2069, 2013.

[11] H. . Rahmani, N. . Sahli and F. . Kamoun, "DDoS flooding attack detection scheme based on F-divergence," *Computer Communications*, vol. 35, no. 11, pp. 1380-1391, 2012.

[12] Y. . Xiang, K. . Li and W. . Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 426-437, 2011.