International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(2), pp.267-269
DOI: http://dx.doi.org/10.21172/1.102.42
e-ISSN:2278-621X

DISTRIBUTED DENIAL OF SERVICE ATTACKS AND VARIOUS COUNTER MEASURES-A REVIEW

Sumanjit Kaur[1], Mohit Marwaha[2], Guresh Pal Singh[3]

Abstract- Data Security in the world of digital computing is the most challenging aspect. Since most of the services now days are online and information and data can be accessed anytime and anywhere so it requires almost unlimited storage capacity. However security becomes a typical issue that need to be addressed while talking about such a huge amount of data and information. Such an emerging technology known as cloud computing uses a huge volume of storage, its data and services are also distributed worldwide. As the users for these technologies are increasing rapidly therefore safeguarding the data and its users is quite essential. The major possible attack in such an era that threatens the IT industries is Distributed Denial of Service (DDoS) attack, a variant of Denial of Service (DoS) attacks. DDoS is the single largest threat to internet and internet of things. This paper provides a wide survey on various DDoS attacks, their vulnerabilities and mitigating policies proposed against them. Through the analysis done in this paper about the DDoS attacks and various mitigation policies, one can think of designing a secured cloud infrastructure which will prevent the DDoS attackers to breach the security measures.

Keywords –Cloud Computing, DDoS Attacks, Zombies, Artificial Neural Network.

1. INTRODUCTION

The word ‘Security’ in the world of digital computing is the practice of securing and protecting the information that is being accessed over the internet. Digital computing such as cloud computing enables a network which provides configurable computing resources such as servers, storage, applications and services to the users anytime and anywhere. Since, provided services are automated and demand large volumes of data or storage, so security still remains a typical issue that has to be addressed. The major possible attack in such environment is DDoS, a variant of DoS attacks, by which most of the legitimate users are affected without servicing. Because of its distributed nature, computing resources have become easy targets for the intruders to exploit the information. In Distributed environment, the computing is decentralized where several computers are able to communicate over a network to achieve a common goal independently while retaining transparency, integrity and making the data available all the time to legitimate users. Denial of Service (DoS)[13,14] is a prominent class of attacks where an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, ultimately denying legitimate user access to a machine [15]. There are different ways to launch DoS attacks:

- Abusing the computers legitimate features.
- Exploiting the system’s misconfigurations.
- Targeting the implementations bugs.

DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users [16, 17].

Distributed Denial of Service (DDoS) attacks are a scaled form of DoS attacks where multiple attack bots (Zombies) under the control of an attacker (Master) are employed in a coordinated fashion to form an attack network for attacking a specific target(Victim). DDoS attacks are catastrophic particularly when implemented to extremely sensitive targets such as Critical-Information Infrastructure. Various types of DDoS attacks are Application Level Attacks, Degradation of Service Attacks, Multi-Vector Attacks, Nuke, Peer-to-Peer Attacks, Ping of Death, Reflected Attack, Slow Loris, SYN Flood, UDP Flood (User Datagram Protocol), Unintentional DDoS, Zero Day DDoS [18]

2. EXISTING WORK TO PREVENT DDOS ATTACKS

Bo Wen has introduced an optical WDM network simulation tool known as optical WDM network simulator (OWns), that facilitates the study of switching and routing schemes in WDM networks. OWns is designed as an extension to the network simulator NS2, a multi-protocol network simulator that is widely-used for networking research and available in the public domain. Author’s goal is to incorporate the key characteristics of WDM networks in the simulator, such as optical switching nodes, multi-wavelength links, virtual topology constructions, related switching schemes and routing algorithms.[1]

Byung-Chul Kim has investigated the performance of reservation mechanisms for optical burst switching (OBS) in multiple

[1] Department of Computer Science and Engineering, Beant College of Engineering and Technology, Gurdaspur, Punjab, India
[2] Department of Information Technology, Beant College of Engineering and Technology, Gurdaspur, Punjab, India
[3] Department of Information Technology, Beant College of Engineering and Technology, Gurdaspur, Punjab, India

hop network environments. The author first review current research on wavelength reservation schemes for OBS, and investigate the path length priority effect of existing just-enough-time (JET) scheme. Then, author propose a novel hop-by-hop priority increasing (HPI) scheme. The simulation results showed that the proposed scheme could avoid the path length priority effect and enhance the end-to-end throughput in multiple hop network environments.[2]

Craig Cameron has introduced a new routing protocol for Optical Burst Switching, Shortest Path Prioritized Random Deflection Routing (SP-PRDR),that aims to lower burst loss probabilities while only using limited state information from traditional Internet Protocol technologies. The author show, through analysis and simulation, that loss in OBS networks is significantly reduced by SP-PRDR for loads that previously gave moderate or low losses in the unmodified case. [3]

S.Selvakani has applied Genetic Algorithm to generate rules for training the IDS. Rules are generated for only Smurf (DoS) attack and Warzemaster (Remote_to_Local) attack. This performance of this methodology detection rate is low. This survey shows that the proposed Intrusion Detection models for R2L (Remote_to_Local), U2R (User_to_Root), Probe attacks get low detection rates using KDD CUP dataset. This paper introduced two types of attacks for each category i.e., DoS, R2L, U2R and Probe. Author has designed the KDD CUP dataset to detect the attacks. [4],

Amit Kumar Garga, and R.S.Kaler, have proposed an effective way for improving channel utilization in several optical burst switching networks. In the proposed method, a specific burst is signified by a specific interval of time. The procedure of scheduling a number of bursts, accordingly, turns out to be a procedure of fitting a group of the equivalent time intervals on a specific channel timeline, which also characterizes a particular channel-time resource. By doing so, the scheduling procedure could be expressed as a combinatorial optimization issue. Then, graph-theory is implemented to plan as many non-overlapping intervals as probable onto the particular channel-timeline. The fundamental model of the proposed scheduling approach is that of momentarily postponing the scheduling of a specific burst so that a much better judgment/decision could be made about a number of bursts all-together. This approach is presented, through various simulations, so as to enhance its performance in terms of burst_loss_probability, fairness-control channel utilization, along with proper data throughput over existing approaches. Thus the proposed scheme is well suited for high performance networks in terms of reliability.[5]

Amit Kumar Garga has projected a novel burst dropping policy based on even selection of burst in conjunction with an appropriate technique to make available differentiated service so as to support the Quality of Service (QoS) necessities of various dissimilar applications. In the proposed approach of burst_dropping policy, the dropped_parts are carefully chosen uniformly from both of the competing bursts as well as the truncated_bursts are assured to be much larger as compared to the smallest burst-length that is permitted by the specific network. Moreover, the proposed approach is improved by using a flow_control approach. The simulation results displays that the performance of suggested policy is much better as compared to existing burst_dropping mechanisms in terms of decreasing burst (data packages) loss_rate. [6]

The author has presented an analysis of various routing approaches which are existing in Optical Burst Switching networks. The author initiate with a proper explanation of various routing methods and then follow the discussion through a detailed taxonomy of various routing procedures in Optical Burst Switching networks. After that, author talk over communal Optical Burst Switching network loss_models, which are commonly utilized in routing_optimization. As instances of such type of application, author demonstrate a linear as well as a non-linear formulation of a multi-path routing optimization issue with an indication on convenient_resolution approaches. The presented procedures are suitable for proactive_load_balancing_routing as well as aim at the upgrading of network-wide burst loss performance. To match performance results of proposed system, both methods are evaluated by simulation in a set of unified network scenarios. [7]

Amit Kumar Garga, and R.S. Kaler have proposed a burst flexible and enhancing bandwidth utilization burst dropping technique for contention resolution in optical burst switched networks. When contention occurs, any part of a contending burst could possibly be dropped/misplaced, rather than only the head or else tail of specific bursts. The proposed dropping approach makes utilization of bandwidth much more flexible and efficient. The simulation results show that the proposed dropping scheme performs better than existing burst dropping schemes. [8]

P. Siva Subramanian has identified the burst duplication attack since some core nodes can be compromised to replicate the specific control_signal that might results in theft of data_burst. The author has found two different ways to alleviate the burst_stealing_attack, likedigital signature technique along with trusted node technique. Then author deliberated about both types of methods individually. The authors simulated the results through NS2 simulator by using the modified optical burst switching patch. [9]

Mmoloki Mangwala and O.O. Ekabua have presented concepts of optical burst switching and burst assembly algorithms. It is apparent that the use of traffic statistics to predict oncoming traffic is very important. Research shows that burst assembly algorithms where parameters i.e. time or length thresholds are selected based on traffic statistics perform better than the traditional ones. [10]

Alan Saied, Richard E. Overill, and Tomasz Radzik have presented concept of using Artificial Neural Network so as to detect and mitigate the known and unknown DDoS attacks. They detected TCP, UDP and ICMP attacks based on characteristic pattern that allow the genuine traffic to pass through it while restricting the abnormal traffic. Their approach managed to detect known and unknown attack, but could not detect all the unknown attacks. [11]

Same authors have presented concept of using Artificial Neural Network so as to detect and mitigate the known and unknown DDoS attacks. They detected TCP, UDP and ICMP attacks based on characteristic pattern that allow the genuine traffic to pass through it while restricting the abnormal traffic. They identified the patterns most popular among DDoS attackers to launch the attack. Their approach managed to detect known and unknown attack, but could not detect all the unknown attacks in a physical environment rather than simulations. [12]

3. CONCLUSION

DDoS attacks are one of the major threats to almost all the emerging technologies. There is a need of various identification techniques, a lot of security measures so as to withstand such attacks in future. This paper serves as a brief survey on DDoS attacks, its types and various approaches to mitigate the DDoS attacks that are being used so far. This survey confers various DDoS attacks detection, prevention and tolerance techniques. From the survey, it is evident that the DDoS attacks do threaten the internet community and emerging distributed computing technologies significantly.

In order to make the services more reliable and transpaent IT industries are trying to transfer their services to cloud. The effects of DDoS attacks in the Cloud environment have been identified. Of various attacks in cloud environment a significant percentage is contributed by DDoS attacks.

The future work is to design a secured infrastructure capable of mitigating the attacks identified and to withstand the future attacks. One can think of employing effective technique like artificial neural networks to design such a secured infrastructure.

4. REFERENCES

[1] Bo Wen, Nilesh M. Bhide, Ramakrishna K. Shenai, and Krishna M. Sivalingam, “Optical Wavelength Division Multiplexing Network Simulator: Architecture and Performance Studies” SPIE Optical Networks Magazine, Vol.2, no.5, pp.16-26, 2001.

[2] Craig CAMERON, Andrew Zalesky, and Moshe Zukerman, “Prioritized deflection routing in optical burst switching networks." IEICE transactions on communications Vol.88, no.5, pp. 1861-1867, 2005

[3] Byung-Chul Kim, You-Ze Cho, Jong-Hyup Lee, Young-Soo Choi, and Doug Montgomery, “Performance of Optical Burst Switching Techniques in Multi-Hop Networks” in Global Telecommunications Conference, IEEE, Vol. 3, no., pp.2772-2776, 2002.

[4] S.Selvakani, and R.S. Rajesh, “Genetic Algorithm for framing rules for Intrusion Detection”, IJCSNS International Journal of Computer Science and Network Security, Vol.7, No.11, pp. 285-290, 2007.

[5] Amit KumarGarga, and R.S.Kaler, “An efficient scheme for optimizing channel utilization in OBS networks” Optik - International Journal for Light and Electron Optics Vol. 121, No. 9, pp. 793–799, 2010.

[6] Amit Kumar Garga, and R.S. Kaler, “Burst dropping policies in optical burst switched network” Optik - International Journal for Light and Electron Optic, Vol. 121, No. 15, pp.1355–1362, 2010.

[7] Mirosław Klinkowski, João Pedro, Davide Careglio, Michał Pióro, João Pires, Paulo Monteiro, and JosepSolé-Pareta, “An overview of routing methods in optical burst switching networks” Optical Switching and Networking, Vol. 7, No. 2, pp. 41–53, 2010.

[8] Amit Kumar Garga, and R.S. Kaler, “A new flexible and enhancing bandwidth utilization burst dropping technique for an OBS network” Optik - International Journal for Light and Electron Optics Vol. 122, No. 3, pp. 225–227, 2011.

[9] P. Siva Subramanian, K. Muthuraj, “Threats in Optical Burst Switched Network” Vol. 2, pp. 510-514, 2011.

[10] Mmoloki Mangwala and O.O. Ekabua, “A Survey of Burst Assembly Algorithms for Optical Burst Switching (OBS)” International Journal of Engineering and Technology Research, Vol. 1, No. 7, pp. 107 – 115, 2013.

[11] Alan Saied, Richard E. Overill, and Tomasz Radzik, “Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept” PAAMS 2014 Workshops, CCIS 430, Springer International Publishing, pp. 309–320, 2014.

[12] Alan Saied, Richard E. Overill, and Tomasz Radzik, “Detection of Known and Unknown DDoS using Artificial Neural Networks in the Detection”, Elsevier pp. 385–393, 2015.

[13] R. Kaizaki, K. Cho, O. Nakamura, "Detection Denial of Service Attacks Using AGURI", International Conference Telecommunications, Beijing China, June 2002.

[14] T. Peng, C. Leckie and R. Kotagiri. "Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring", In Proceedings of the Third International IFIP-TC6 Networking Conference (Networking 2004), Athens, Greece, 2004.

[15] R. Bazek, H. Kim, B. Rozovskii, and A. Tartakovsky, "A novel approach to detection of enial-of-service attacks via adaptive sequential and batch-sequential change-point methods", IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2001.

[16] Sanguk Noh , Cheolho Lee ,Gihyun Jung, Kyunghee Choi, “Detection of Distributed Denial of Service Attacks Through Inductive Learning ”, International Conference on Advances in Infrastructure for Electronic Business, Education, Science, Medicine and Mobile Technologies on the Internet, 2003.

[17] L. Ming Li, "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition", Computers & Security, Vol. 23, no. 7, Elsevier, ISSN 0167-4048, April 2004.

[18] A. Hussain, J. Heidemann, and C. Papadopoulos. "A Framework for Classifying Denial of Service Attacks". In Proceedings of the ACM SIGCOMM Conference, Karlsruhe, Germany, pp. 99-110, 2003.