OPTIMAL FILTER ASSIGNMENT POLICY AGAINST DISTRIBUTED DENIAL-OF-SERVICE ATTACK

A.BALARAM[1], DASARI MANITEJA[2], BALE VIGNESH[3], GOURARAM VAMSHI[4]

ASSOCIATE PROFESSOR[1], UG SCHOLAR[2,3&4]

DEPARTMENT OF CSE, CMR INSTITUTE OF TECHNOLOGY, KANDLAKOYA VILLAGE, MEDCHAL RD, HYDERABAD, TELANGANA 501401

ABSTRACT— A distributed denial-of-service (DDoS) attack is a cyber-attack in which attackers from different locations send out many requests to exhaust the capacity of a server. Current DDoS attack protection services filter out the DDoS attack packets in the middle of the path from the attacker to the servers. Some of the DDoS protection systems filter them out at the victim server. As a result, unnecessary attack traffic congests the network and wastes bandwidth. This can be minimized if we block them as early as possible. In this paper, we propose a DDoS attack protection system by using the filter router. The victim needs to wisely select and send filters to a subset of filter routers to minimize attack traffic and blockage of legitimate users (LUs). Many filters can easily minimize the attack traffic and blockage of LUs, but it is costly to the victim. So, we formulate two problems with different settings for selecting filter routers given a constraint on the number of filters. We propose dynamic programming solutions for both problems. Both problems consider the blockage of all attack traffic before it reaches the victim. We conduct extensive simulation to support our solutions.

Index Terms——botnet, DDoS defense, DDoS, flooding attack, filter router, network security, filter assignment.

I. INTRODUCTION A denial-of-service attack (DoS attack) is a cyber-attack in which the attacker seeks to make a machine (e.g., web server) or network resource temporarily unavailable to its users. DoS attacks are considered a federal crime under the Computer Fraud and Abuse Act with penalties that include years of imprisonment [1]. The Computer Crime and Intellectual Property Section of the US Department of Justice handles cases of DoS attacks. Therefore, detecting DoS attacks and identifying attackers have been important issues in Network Forensics. Moreover, DoS attacks are increasing day by day in both number and size; CloudFlare [2] recently reported a 400 Gbps massive DoS attack that took place in their servers. There are several types of DoS attacks such as SYN Floods, Malformed Packets, UDP Floods, Amplification Attacks, and Distributed Attacks [3]. In a SYN Flood attack, the perpetrator sends many SYN messages to set up TCP connection. The server replies ACK and waits for the client's ACK, but the attacker does not reply ACK and the connection remains half-open till timeout. The objective of a SYN flood is to simply fill up the limited slots that the target system has available for half-open connections. In some cases, it's easy to detect a SYN Flood attack if a lot of SYN requests come from an address in short interval. Detection is harder, however, when the attacker spoofs IP address, SYNs come from multiple addresses, and arrival time varies. In a UDP Flood attack, the purpose would likely be to consume all available network bandwidth. Attackers send a large amount of spoofed requests with large useless payloads. The application wastes CPU cycles trying to determine the meaning of the garbage. The objective of the DDoS attack is to generate a lot of packets from different locations to exhaust the incoming/outgoing bandwidth of the victim (e.g., web server). A coordinator would send commands to workers, who continue to send requests to the target. The workers are known as bots and the network of workers is known as botnet. As users also send requests through the NAT, it is difficult for the victim to differentiate between the bot requests and user requests. Fig. 1(a) shows the DDoS attack model by a botnet. The existing works which are based on DDoS detection at the router level increase router computation overhead. The works which are based on filtering at the victim increase the network overhead. The routers that detect DDoS traffic based on some generalized characteristics cannot detect DDoS traffic better than the victim. Besides, the characteristics of DDoS traffic are different for different victims. An effective method of preventing DDoS attacks is to use filter routers (FRs) in the network infrastructure. FRs are special types of routers that are capable of packet marking and receiving filter tasks. Marking a packet means appending the FR's IP address to the packets it forwards. A FR does not mark all the packet it forwards, rather it probabilistically selects some packets to mark. The task of receiving filter refers to receiving a filter from a web server. A web server can block all or part of the traffic destined to it.

II. LITERATURE SURVEY

1. Optimal Filter Assignment Policy Against Distributed Denial-of-Service Attack

Rajorshi Biswas, Jie Wu Published in IEEE Transactions on… 1 January 2022

A distributed denial-of-service (DDoS) attack is a cyber-attack in which attackers from different locations send out many requests to exhaust the capacity of a server. Current DDoS attack protection services filter out the DDoS attack packets in the middle of the path from the attacker to the servers. Some of the DDoS protection systems filter them out at the victim server. As a result, unnecessary attack traffic congests the network and wastes bandwidth. This can be minimized if we block them as early as possible. In this paper, we propose a DDoS attack protection system by using the filter router. The victim needs to wisely select and send filters to a subset of filter routers to minimize attack traffic and blockage of legitimate users (LUs). Many filters can easily minimize the attack traffic and blockage of LUs, but it is costly to the victim. So, we formulate two problems with different settings for selecting filter routers given a constraint on the number of filters. We propose dynamic programming solutions for both problems. Both problems consider the blockage of all attack traffic before it reaches the victim. We conduct extensive simulation to support our solutions.

2. Profit-oriented cooperative caching algorithm for hierarchical content centric networking

Meiyi Yang, Mingchuan Zhang, +3 authors I. Wassell Published in IET Communications 3 February 2020

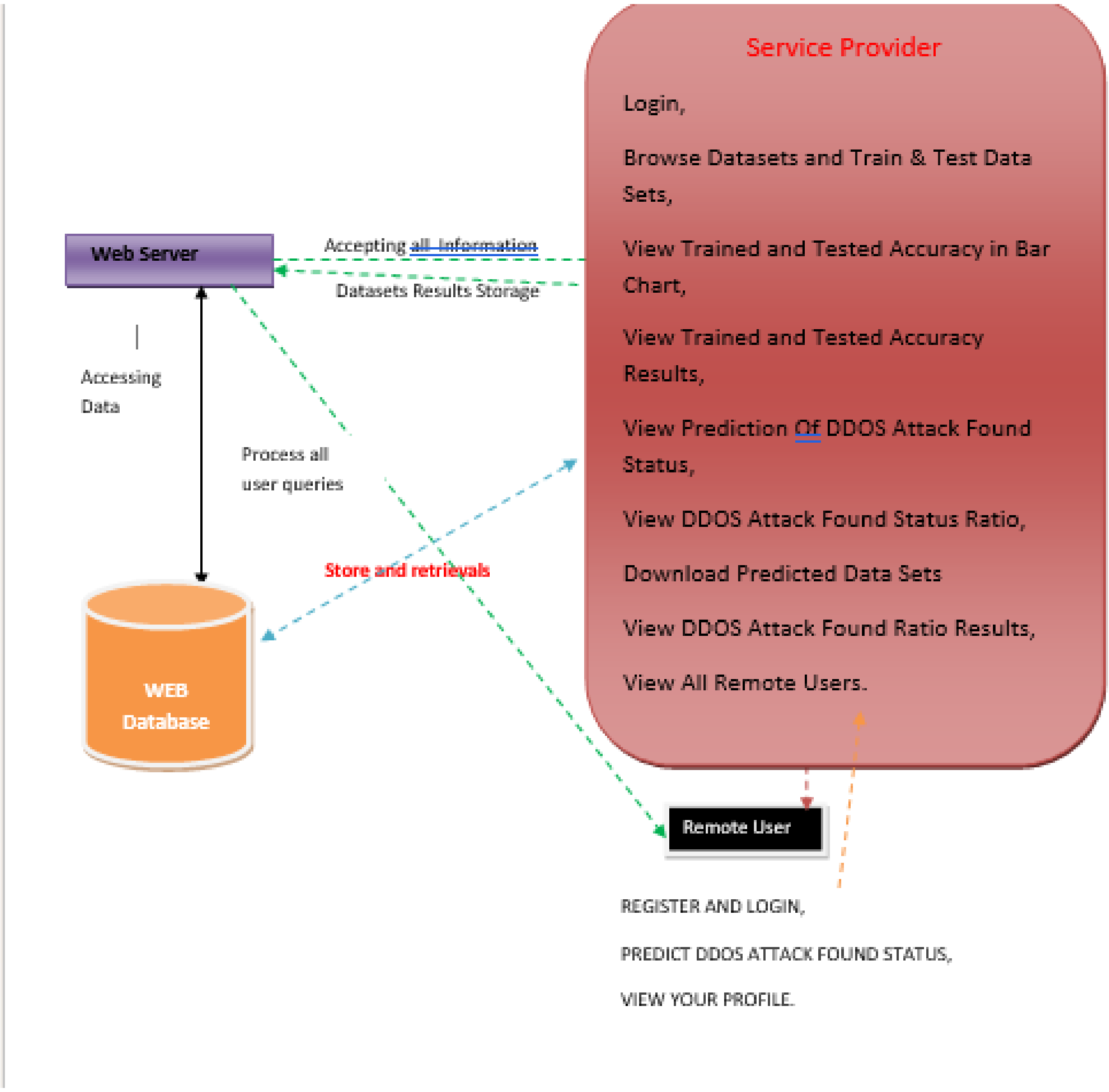
Cooperative caching among nodes is a hot topic in Content Centric Networking (CCN). However, the cooperative caching mechanisms are performed in an arbitrary graph topology, leading to the complex cooperative operation. For this reason, hierarchical CCN has received widespread attention, which provides simple cooperative operation due to the explicit affiliation between nodes. In this study, the authors propose a heuristic cooperative caching algorithm for maximising the average provider earned profit under the two-level CCN topology. This algorithm divides the cache space of control nodes into two fractions for caching contents which are downloaded from different sources. One fraction caches duplicated contents and the other caches unique contents. The optimal value of the split factor can be obtained by maximising the earned profit. Furthermore, they also propose a replacement policy to support the proposed caching algorithm. Finally, simulation results show that the proposed caching algorithm can perform better than some traditional caching strategies.

3. Network anomaly detection: A survey and comparative analysis of stochastic and deterministic methods

Jing Wang, Daniel Rossell, +1 author I. Paschalidis Published in IEEE Conference on Decision… 18 September 2013

We present five methods to the problem of network anomaly detection. These methods cover most of the common techniques in the anomaly detection field, including Statistical Hypothesis Tests (SHT), Support Vector Machines (SVM) and clustering analysis. We evaluate all methods in a simulated network that consists of nominal data, three flow-level anomalies and one packet-level attack. Through analyzing the results, we point out the advantages and disadvantages of each method and conclude that combining the results of the individual methods can yield improved anomaly detection results..

III. PROPOSED SYSTEM


Service Provider
Login,
Browse Datasets and Train & Test Data Sets,
View Trained and Tested Accuracy in Bar Chart,
View Trained and Tested Accuracy Results,
View Prediction Of DDOS Attack Found Status,
View DDOS Attack Found Status Ratio,
Download Predicted Data Sets
View DDOS Attack Found Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT DDOS ATTACK FOUND STATUS,
VIEW YOUR PROFILE.

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View All Antifraud Model for Internet Loan Prediction, Find Internet Loan Prediction Type Ratio, View Primary Stage Diabetic Prediction Ratio Results, Download Predicted Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT PRIMARY STAGE DIABETIC STATUS, VIEW YOUR PROFILE.

CONCLUSION

The DDoS attack is the most powerful attack that makes a service unavailable to users. It is not possible to protect any server from DDoS attacks without the help of the network equipment. As the most important component in a network, routers can be upgraded to filter routers easily. Besides, the filter router can work in a network with legacy routers. In the four-phase DDoS protection system, the filter routers block the attack traffic according to the victim's instruction. Although the blocking control of an Internet service provider (ISP) is at the victim's hand, who may not belong to the ISP but it will help the ISP minimize traffic congestion. Therefore, both parties are benefited. In this work, we present three filter assignment policies for two different settings. We observe the performances of the proposed policies in synthetic and real topologies. Both the source-based and destination-based filters have some advantages and limitations. In the future, we may formulate another problem for finding an optimal assignment using the filter type most fitted to a filter router.

REFERENCES

[1] United States Code: Title 18,1030, “Fraud and related activity in connection with computers — Government Printing Office,” http: //www.gpo.gov, 2014.

[2] “CloudFlare,” https://blog.cloudflare.com/.

[3] B. B. Gupta and O. P. Badve, “Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment,” Neural Computing and Applications, vol. 28, no. 12, Dec 2017.

[4] J. Wang and I. C. Paschalidis, “Statistical Traffic Anomaly Detection in Time-Varying Communication Networks,” IEEE Transactions on Control of Network Systems, vol. 2, no. 2, Jun 2015.

[5] W. Wei, F. Chen, Y. Xia, and G. Jin, “A Rank Correlation Based Detection against Distributed Reflection DoS Attacks,” IEEE Communications Letters, vol. 17, no. 1, Jan 2013.

[6] A. Kulkarni and S. Bush, “Detecting Distributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics,” J. Netw. Syst. Manage., vol. 14, no. 1, Mar. 2006.

[7] T. A. Ahanger, “An effective approach of detecting DDoS using Artificial Neural Networks,” in 2017 International Conference on Wireless Communications, Signal Processing and Networking, Mar 2017.

[8] D. Almomani, M. Alauthman, F. Albalas, O. Dorgham, and A. Obeidat, “An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms,” International Journal of Cloud Applications and Computing, vol. 8, 04 2018.

[9] B. B. Gupta, Computer and cyber security: principles, algorithm, applications, and perspectives. CRC Press, 2018.

[10] K. Bhushan and B. B. Gupta, “Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment,” Journal of Ambient Intelligence and Humanized Computing, vol. 10, Apr 2018.

[11] X. Ma and Y. Chen, “DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy,” IEEE Communications Letters, vol. 18, no. 1, Jan 2014.

[12] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, Feb 2014.

[13] P. Ning and S. Jajodia, “Intrusion Detection Techniques,” 2004.

[14] N. Ye, S. Emran, Q. Chen, and S. Vilbert, “Multivariate statistical analysis of audit trails for host-based intrusion detection,” IEEE Transactions on Computers, vol. 51, no. 7, Jul 2002.

[15] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, “Advance DDOS detection and mitigation technique for securing cloud,” International Journal of Computational Science and Engineering, vol. 16, no. 3, 2018.

[16] B. K. Joshi, N. Joshi, and M. C. Joshi, “Early Detection of Distributed Denial of Service Attack in Era of Software-Defined Network,” in 2018 Eleventh International Conference on Contemporary Computing, Aug 2018.

[17] A. Procopiou, N. Komninos, and C. Douligeris, “ForChaos: Real Time Application DDoS Detection Using Forecasting and Chaos Theory in Smart Home IoT Network,” Wireless Communications and Mobile Computing, vol. 2019, 2019.

[18] V. Matta, M. D. Mauro, and M. Longo, “DDoS Attacks With Randomized Traffic Innovation: Botnet Identification Challenges and Strategies,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, Aug 2017.

[19] H. Luo, Z. Chen, J. Li, and A. V. Vasilakos, “Preventing Distributed Denial-of-Service Flooding Attacks With Dynamic Path Identifiers,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, Aug 2017.

[20] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Y. Yau, and J. Wu, “Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, Jul 2018