International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 6 3614 - 3617

DDoS Attack Detection Using Cooperative Overlay Networks and Gossip Protocol

Shreya Bhattacharya #1, Sabah H Qazi *2, Surekha J S *3, Shruthi J G *4, Sanjeetha R #5
Department of Computer Science & Engineering,
M.S. Ramaiah Institute of Technology,

Abstract:- DDoS attacks have major impact on the affected networks viz. packet transmission delays, network outage, website sabotage, financial losses, legitimate-user blockage and reputation damage. Existing DDoS detection techniques are either implemented at the victim node (but the damage is already done) or at many intermediate routers which run DDoS detection algorithms, that adds additional delay and more processing.

We aim to detect DDoS attacks by using a new technique of cooperative overlay networks which overcomes the above problems by implementing the DDoS detection algorithm at one hop distance nodes (called defense nodes) from the victim.

Keywords: *cooperative overlay networks, gossip protocol, defense nodes, victim node*

*****

I. INTRODUCTION

Flooding based DDoS (Distributed denial of service) attacks are malicious attempts to make a server or network resource unavailable to the legitimate users, using globally distributed internet connections to flood targeted machine with unwanted packets. These DDoS attacks are more frequent in today's networks. It results in packet transmission delays, network outage, website sabotage, financial losses, legitimate-user blockage and reputation damage.

The cost of DDoS attacks can continue to impact the victim even long after the event has been dealt with and current solutions are still unable to withstand large scale DDoS attacks.

II. EXISTING SOLUTIONS

This method uses a cooperative approach that uses the Intrusion Detection Message Exchange Format (IDMEF) that can detect coordinated attack scenarios through alert correlation of distributed IDSs (Intrusion Detection Systems). In this paper intrusion detection is used as a barrier to counter these distributed attacks. For the detection, scenarios of alerts are constructed corresponding to the scenarios of actions executed by the attacker. To do this, the set of actions available for the attacker and a set of intrusion objectives are modelled using the LAMBDA (Language to Model a Database for Detection of Attacks) language [9].

Another method examines a front-end software object named "bouncer" written in Java that analyzes packets and places them in a priority queue based on their frequency of requests and their originating source[12].

This method paper firstly pre-process network traffic by cumulatively averaging it with a time range, and using the simple linear AR model, and then generate the prediction of network traffic. Second assuming the prediction error behaves chaotically, chaos theory is used to analyze it and then a novel Network Anomaly Detection Algorithm (NADA) is proposed to detect the abnormal traffic. With this abnormal traffic, a neural network is trained to detect DDoS attacks. The preliminary experiments and analyses indicate that the proposed DDoS detection algorithm can accurately and effectively detect DDoS attacks.[13]

III. PROPOSED METHODOLOGY

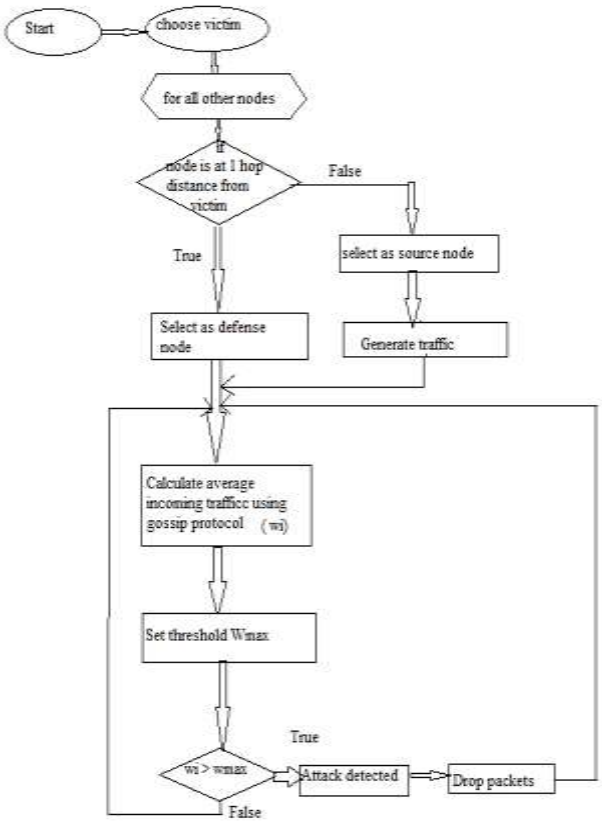
In our paper, we consider a network with a single victim and nodes surrounding this victim at one hop distance *d* are identified as defense nodes and are used to form a overlay network.

DDOS detection algorithm:

i. After receiving the packets, the defense nodes calculate the average incoming traffic and communicate this value to its neighboring defense nodes.
   Using gossip protocol between 2 neighboring nodes, the average of the two incoming traffic values ω_i are calculated and stored for each of the defense nodes.
ii. The threshold value of the network traffic for the victim ω_{max} is set to twice the average incoming regular traffic at the defense nodes.
iii. If the average incoming traffic calculated for 50% of the defense nodes exceeds the set threshold value i.e $\omega_i > \omega_{max}$. DDoS attack is detected.
iv. Once the attack is detected, the packets are dropped at the defense nodes.

 ISSN: 2321-8169
3614 - 3617

Flowchart :



IV. SIMULATION TOPOLOGY

NS2 is used to simulate our topology that consists of 23 nodes. One node is considered as a victim node. 10 nodes surrounding the victim is considered as defense nodes. The remaining are source nodes which generate different types of traffic. We simulate 3 types of application traffics viz., CBR, FTP and TELNET. The simulation is run for 30 minutes, the first 10 minutes of which is used to send normal traffic and determine threshold values. The next 10 minutes are simulated with attack traffic by increasing the number of packets sent by CBR traffic. Last 10 minutes again depicts normal traffic scenario.

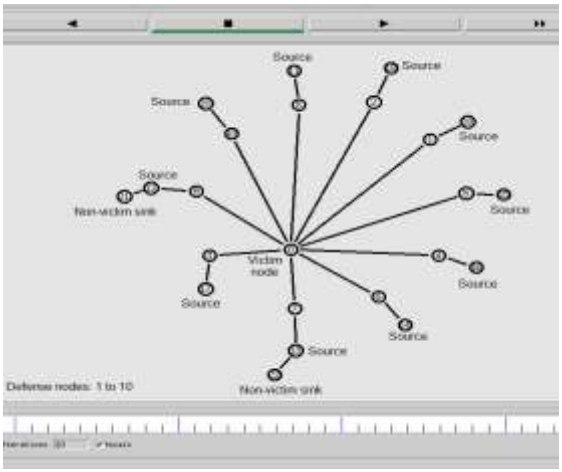


Fig 1:Simulation topology

IV. EXPERIMENTAL RESULTS

The following results were observed for the above mentioned simulation scenario:

We first evaluate the effectiveness of the traffic estimation technique. We simulate to plot and obtain a graph of the overall traffic sent in the network for the entire simulation which runs for 30 minutes.

The graphs are plotted with time(sec) on the x-axis and traffic(MB) on y-axis. The total traffic in the network in depicted in Fig2 where the high growth in number of packets during attack interval is seen.

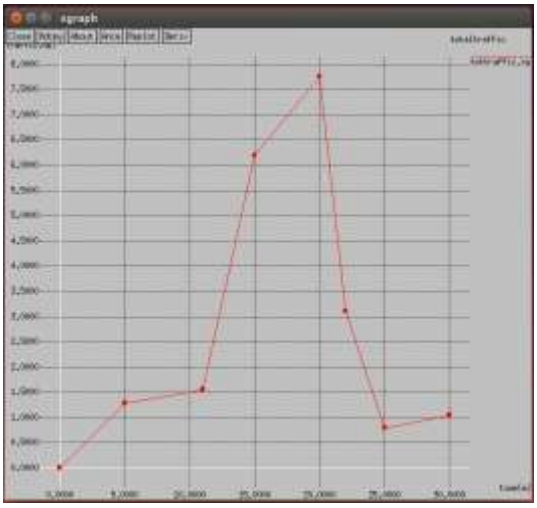


Fig 2:Total traffic in the network

The user datagram packet and transmission control packet traffic is compared in Fig 3. There is high growth in the UDP packets which is simulated to be the attack traffic.

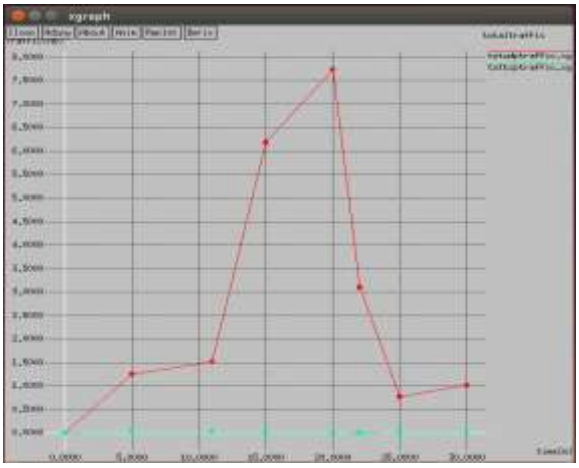


Fig 3: Comparing TCP and UDP traffic during UDP attack traffic

 ISSN: 2321-8169
3614 - 3617

Fig 4 shows the comparision of number of packets received by the victim node in the presence and absence of defense nodes. The traffic at victim is reduced by approximately 45% when our algorithm is implemented using defense nodes.

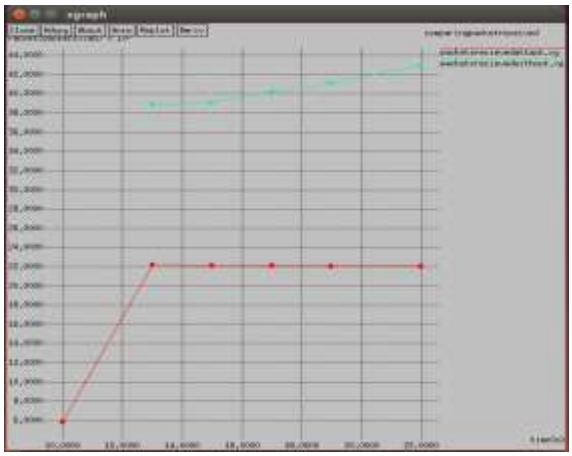


Fig 4: packets received by victim during DDoS attack in presence and absence of defense nodes.

Fig 5 shows the overall traffic load on victim in presence and absence of defense nodes.

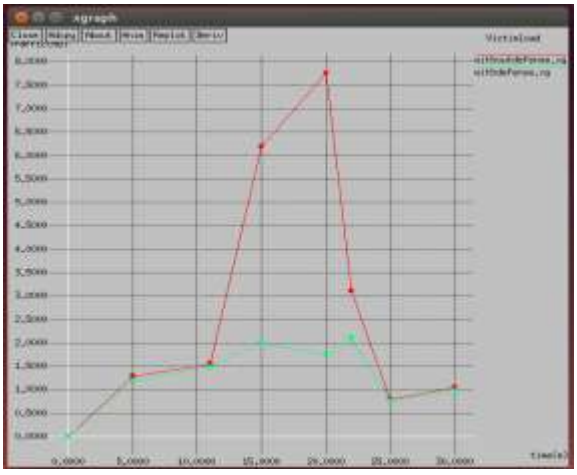


Fig 5: Overall traffic load on victim in presence and absence of defense nodes

IV. CONCLUSION & FUTURE SCOPE

The DDoS inflicted failure-rate on the victim is significantly reduced due to effective detection at the defense nodes. The unnecessary attack load on the victim is minimized resulting in better services to the genuine clients. Efficient and minimal processing at the overlay network reflects in the improved reliability of entire network.

Our project is a purpose-built architecture that includes the ability to specifically detect and defeat increasingly sophisticated, complex, and deceptive flooding-based DDoS attacks. It holds the potential to be an effective alternate to the existing network devices and traditional perimeter security technologies such as firewalls and intrusion detection systems (IDSs) which do not by themselves provide comprehensive DDoS protection.

We can enhance our project to dynamically change the victim and the defense nodes to detect DDoS attack much more efficiently.

We can also extend the project to identify the source of the DDoS attack

V. ACKNOWLEDGEMENTS

We acknowledge the support and help provided by Staff, HOD, Department of Computer Science & Engineering, Principal and Management of M.S. Ramaiah Institute of Technology, Bengaluru.

REFERENCES

[1] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[2] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, IEEE INFOCOM'06, 2006.

[3] R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer J. IEEE Commun. Magazine, Vol. 40, no. 10, pp. 42-51, 2002.

[4] R. Puri, Bots and Botnet – an overview, Aug. 08, 2003,

[5] B. Todd, Distributed Denial of Service Attacks, Feb. 18, 2000, [online] http://www.linuxsecurity.com/resource files/intrusion detection/ddos–whitepaper.html

[6] X. Geng, Y. Huang, and A. B. Whinston, Defending wireless infrastructure against the challenge of DDoS attacks, Mobile Networks and Applications, vol. 7, no. 3, pp. 213-223, 2002.

[7] A. D. Wood, and J. A. Stankovic, A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004 (invited chapter).

[8] S. T. Zargar, M. B. H. Weiss, C. E. Caicedo, and J. B. D. Joshi, Security in Dynamic Spectrum Access Systems: A Survey, in Telecommunications Policy Research Conference, Arlington VA, 2009.

[9] T. Velauthapillai, A. Harwood and S Karunasekara, Global detection of Flooding-Based DDoS Attacks Using a Cooperative Overlay Network, in 2010 Fourth International Conference on Network and System Security .

[10] V. Santhi, A M Natarajan, NEWQUE with Per-flow Scheduling: Performance Improvement of the Active Queue Management Algorithm.

[11] Yacine Bouzida, Frederic Cuppens and Sylvain Gombault, Detecting and Reacting against Distributed Denial of Service Attacks.
[12] Gregory Safko, Defending against Denial of Service Attacks Using a Modified Priority Queue: Bouncer.
[13] Cisco guard mitigation appliances (2004). http://www.cisco.com/en/US/products/ps5894
[14] Yinghong Fan, Hossam Hassanein and Pat Martin ,Proactively Defeating Distributed Denial of Service Attacks.
[15] W. Shi, Y. Xiang and W. Zhou, Distributed Defense Against Distributed Denial-of-Service Attacks.