Abstract

Distributed Denial of Service (DDoS) attacks continue to harm servers using intense wars against popular ecommerce and content websites. The short term and long term types of popular DDoS attacks can be detected, prevented and mitigated using the proposed novel Qualified Vector Match and Merge Algorithm (QVMMA) in real time. 14 feature components are used to generate an attack signature in real time and stored in dynamically updated DDoS Captured Attack Pattern (DCAP) database. It is effective in detecting new and old attacks. Persistent DDoS attacks cause financial damage or reputation loss by loss of the company's valuable clients. The server's availability is heavily compromised.
Popular websites Github and BBC UK faced DDoS attacks in 2015. Long term DDoS attack directed on Github continued for over 118 hours. Short term DDoS attack experienced by BBC website caused its patchy response. The main crux of the problem is the absence of a way to differentiate between attack records and legitimate records while the attack is occurring in real time. Several methods are listed in brief in the paper. Post mortem solutions are not applicable in real time. Available real time solutions are slow. QVMMA is an ideal faster real time solution to prevent DDoS attacks using Statistical Feature Vector Generation. Matlab is used for DDoS real time simulation where the topologies (bus, star, abilene network) are created using OMNET++. QVMMA generates and uses Statistical Feature Vector for Attack Signature Generation, Matching and Identification only for qualifier satisfied records. The web server’s log files used as input to QVMMA are according to W3C log format standard. Experimentation is completed with exhaustive 336 cases. Four networks are tested with 5, 8, 10, 13 nodes. Performance evaluation of QVMMA concludes EER is 11.8% when threshold is 1.6. Using model of FAR and FAR, the trendline provides threshold at 1 with EER at 10%. Abilene network achieves best result. As the number of attackers, nodes and intermediate routers increase, detection time increases. If threshold is increased, the accuracy reduces. If the number of nodes increases, accuracy increases. Thus it is concluded that QVMMA can be used for effective layer 3 DDoS Prevention and Mitigation in real time based on results generated in Matlab simulation. Extended results are provided. A model is provided in this paper to predict the detection time for any number of attackers. Other models are provided based on data collected through experimentation to formulate a relation between detection time, accuracy, Actual Attack Traffic Passed Rate (A_ATPR) with respect to the number of attackers. The corresponding correlation coefficient and regression coefficient are calculated to identify and conclude the strong relationships. This paper focuses on results and discussion on studying the effects and trend observed based on increasing the number of attackers during a DDoS attack. Thus QVMMA is fast enough to be used in real time to detect and mitigate short term or long term layer 3 Denial of Service (DoS) and more complex DDoS attacks.

References

- Arun Kumar, Sai Ashritha. Analysis of various IP traceback techniques- A Survey. IJCA(0975-8887), September 2013; Volume 77-No. 13, pp. 13-16.
QVMMA: A Short Term and Long Term Layer 3 DDoS Detector and Mitigator

- Wei Xiong, Naixue Xiong, Laurence T. Yang, Jong Hyuk Park, Hanping Hu, Qian Wang. An anomaly-based detection in ubiquitous network using the equilibrium state of the catastrophe theory. Published online: Springer Science Business Media, LLC 5 July 2011.
computerverworld-nsl@idgindia.net
One in five DDoS attacks last for days even weeks. Deccan Chronicle, April 29, 2015, 15. 55pm IST. Available from URL: www.deccanchronicle.com/150429/technology-latest/one-five-ddos-attacks-last-days-or-even-weeks/.
Method and system for protecting against denial of service attacks using trust, quality of service, personalization and hide port messages. US 20070266426 A1
Detecting Application Layer DDoS Attacks. China Patent CN102638474B.
QVMMA: A Short Term and Long Term Layer 3 DDoS Detector and Mitigator

Index Terms

Computer Science

Information Sciences

Keywords

Ddos  Dos  qvmma  Matlab  Omnet++