DMZ: A trusted honeypot for secure transmission

[1,]M.Buvaneswari , [2,]M.P. Loganathan
Postal Address:6/16 Mohan Street, East Tambaram, Chennai-600059

ABSTRACT:
In general, denial of service is nothing but flooding of unrelated information over the network. This causes, overload of network and higher bandwidth consumption. Therefore particular service requested by authorized user cannot receive at particular time. Thus causes larger security threat in network. When these system get distributed (distributed network), the mitigation becomes very complex. In existing technique the DoS has been mitigated using many filtering technique. In order to reduce the effect of DDoS attack we had introduced the concept of ihoneycol[1], which includes the collaboration of firecol(intrusion prevention system) these forms a virtual mitigation shield around the destination and safe guard from the source and honey pot(intrusion detection system). To improve these security, we are going to introduce "trusted honey pot". These can be done using honey token and honey sign.

KEYWORDS: *Denial of service, ihoneycol, honey pot, honey token, honey sign.*

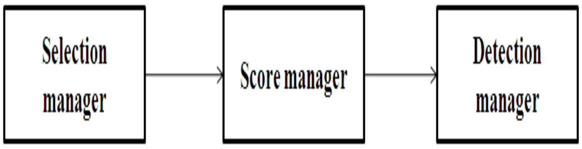
I. INTRODUCTION:

Denial of service or otherwise generally known as packet flooding over the network. This leads to exploitation of OS and causes major security threats[2]. Worms and viruses are also poses security issues which are not related to denial of service attack.Denial of Service detection algorithm are located near the vulnerability and victim vicinity around them. Here the detection of threat is made as flexible as possible. The major trade off is that, the local response is made ineffective and the bandwidth occupies the upstream path.The most coupling problem is that "IP ttraceback"[3] and "IP pushback"[4]. These aim to identify the attack and move on to counter measures which lies near the source of threat. To deal with this problem "Fire Collaborator" has been introduced which deals with the problem at ISP level. It takes the advantage of various IPS rules[5]. It is detection and alert information sharing system that makes the IPS rules that mitigate the effect of denial of service attack which is far from the victim destination. Honeypot is a trap set to detect unauthorized traffic pattern for detection.

II. RELATED WORKS:

Firecol" is either a hardware of software helps in reducing the effect of denial of service using many IPS rules. Initially all the customer in the network register at ISP level. Each customer receives an UID(unique identity) number. When more than one nodes use the same UID number then it is detected as a malicious or unauthorized node. Firecol contains various IPS rules according to the detection of various traffic each rules will be activated.

Fig 1.Firecol functions.



As we already seen that firecol contains many rules and these rules will be activated in the following manner. The selection manager will determine the rules according to the attack and absorb the various malicious traffic over the network. The score manager assigns the scores according to the belief traffic and the rules designed. These scores can be exchanged as a token of trust within the neighbors in the network. The detection manager reads and detect the various traffic among the authorized and unauthorized traffic from the clients.
The following are existing solution for denial of service attack:

[1] Attack prevention and pre-emption:
The attacks are prevented at the client side itself and the mode of mitigation done from far clients. Pre-emption is done when the authorized clients itself wanted to send the malicious data. To achieve this they swap with neighbor network devices.

[2] Attack detection and filtering:
Here the attack is detected and filtered according to various network traffic monitored by the detection system. These traffic are registered as patterns. These filtering technique can be integrated in to firewall. It can be either software or hardware.

[3] Attack source and identification:
Once the attack is identified the main source of attack is detected and its IP address has been moved to blacklist and stored in honeypot server.

Traditionally denial of service mitigation takes place in two major phases:
1.deployment phase: Here the deployment of many compromised nodes take place in network.
2. Attack phase: Here the attack mitigation and prevention takes place.

Reduction of Denial of Service include techniques like spoofing, prevention technique(Ingress and RPF filtering[6]). The other includes manually employed countermeasures (firewall filtering, rate limiting or route black holes[7]).Various abrupt traffic patterns are absorbed in multiple network domains[8]. These leads to very accurate detections and communication overheads. Group testing is performed to identify the denial of service at backend server[9]. Here various malicious traffic are distinguished.Denial of service also distinguish various network traffic and quantify network[10]. This reduces false alarm rate over the network. In order to achieve effective result, this honeypot should be integrated with any IPS system like firewall hardware or softwares[11].

III. PROPOSED WORK:

In general, the client system will be arranged in form of network. The trusted transmission occur among them using authentication and authorization procedures. The client forward the information via firecol routers. These routers are made up of set of IPS rules(intrusion prevention system). They check the traffic according to the rules embedded in it. Later the data get forwarded to load balancer in network. Here we use "Non-cooperative scheme with communication" for attaining higher performance.The traffic here are classified accordingly normal and abrupt traffic. Normal traffic are forwarded to original server or the destination. Abnormal traffic patterns are detected and monitored by set of honeypot system called honeycomb.

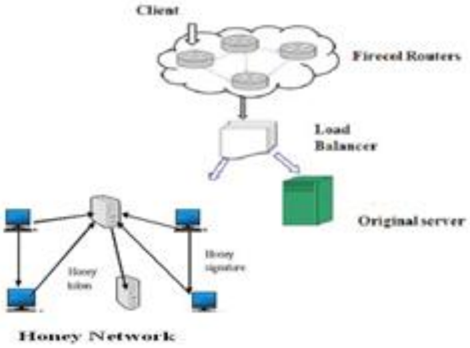


Fig 1.2 Proposed Network

Honeycomb is defined as set of interconnected mesh network. They are multiprocessor system. The group of honeypot performs similar task known as honeycomb.

IV. HYBRID LOAD BALANCER:

Load balancing in general used to attain higher performance in transmission. Initially all the node get registered with the server using their own IP address and load status of an individual node in network. According to load(also trace the historical pattern and sends the maximum load it can take) the load balancer allots a specific weights to all nodes. If the weight crosses the threshold value then that node is called as high weight node, other called as light weight node. These weights are assigned within the fuzzy value interval of [0,1]. The transmission takes place using all the light weight node irrespective of shortest path to attain higher performance. Since we are taking the calculation of individual node we call it as "Non-cooperative scheme with communication".

V. TRUSTED HONEYCOMB:

Honeycomb contains the set of interconnecting mesh network computers. Each honeycomb contains set of honeypot systems and honey servers. Honeypot are computer system whose values can be lied and can be easily compromised. Each honeypot will be exchanging the trusted note by passing honey signatures. Honey signatures are unique signature generated by each system and get stored in honey server. Each honey servers can be recognized using honey token which was made initially while forming the network. Honeytokens are trusted token exchanged among the various honey servers during regular interval of time dynamically.This honey comb environment separately forms an de-militarized zone where it is invisible for authorized users.

VI. CONCLUSION:

By considering the above technique as an effective way we can solve many network security threats. In future I have planned to apply this for four various threat. The usage of signatures and tokens can be extended to original servers using various algorithms.

REFERENCES

[1]. C.Siaterlis,B.Maglaris."Detecting DDoS attacks with passive measurement based heuristics",IEEE conference publication 2004.

[2] S.Savage, D.Wetherall, A.Karlin, T.Anderson.
Practical network support for IP traceback", proceedings of 2000ACM SIGCOMM conference.

[3]. J.Ioannidis and M.Bellovin. "Implementing pushback,router based defense against DDoS attack", proceeding of NDSS,Feb2002.The internet society.

[4]. J.Francois,Adel,E.Atawy,E.Al-Shaee, R.Boutaba,"A collaborative approach for proactive detection of DDoS attack",IEEE transaction 2012.

[5]. CISCO.Remote triggered blackhole filtering.ftp//ftp_eng.cisco.com/cons/isp/
security/.

[6] Kai Hwang and Wei-Shinn Ku," A collaborative detection of DDoS attack over multiple domain", IEEE journal 2007.

[7]. Yin Xuan, Incheol Shin, My T.Thai,Taieb Znati, "Detecting application Denial of Service attack: A group testing based approach", IEEE publication 2009.

[8]. Yan Xiang,Ke LI,Wanlei Zhou,"Low rate DDoS attackdetection and traceback by using new information metrics",IEEE publication 2011.

[9]. Nathalie Weiler,"Honeypots for DDoS attack",IEEE conference publication 2002.

[10] Satish.P and A.T.Chronopoulos, "Dynamic multi user load balancing in distributed system", IEEE publication 2007.

[11] Christian K and Jon Crowcroft "Honeycomb- creating intrusion detection signature using honeypot" http://nms.lcs.mit.edu/HotNets-II/papers/honeycomb.pdf.