# An Effective Defense Mechanism Against Network Attacks

Abhijit S. Pande

Dept. of Computer Technology
RGCER, Nagpur, India
abhijitpande@ymail.com

Rahul Pitale

Dept. of Computer Engineering
PCCOE, Pune, India
rahulpitale3@gmail.com

**Abstract**

In the past few years there is tremendous increase in the use of internet. With the development of large open networks, security threats have increased significantly in the past 20 years. Network attacks results in consumption of network resources and degrading network performance. As networks and information systems become complex, the security problems faced by such systems have evolved. Network attacks are still evolving and there is an utmost need to develop mechanisms which can be effective against them as network Security is a fundamental component of every network design. In this project we have developed a defense mechanism against network attack such as TCP, TCP-SYN flood and UDP attack. Rate limiting mechanism is used to provide defense against TCP-SYN attack and Ingress filter mechanism to defend against TCP and UDP attack. The defense mechanism is deployed on practical network having client-server architecture.

**Index Terms**— TCP, TCP-SYN Flood, UDP, client-server architecture, Ingress filter

## I. INTRODUCTION

Security is a fundamental component of every network design. Hackers have discovered more network vulnerabilities, and because you can now download applications that require little knowledge to implement, applications intended for troubleshooting and maintaining and optimizing networks can be used maliciously and pose severe threats. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies. The easiest way to protect a network from an outside attack is to close it off completely from the outside world. However, internal threats still exist. The different network attacks include passive attack, active attack, insider attack, close-in attack, phishing attack, spoof attack, buffer overflow attack, DoS and DDoS Attack. The network attack results in consumption of network resources and degrading system performance. So proper defense mechanism is required to improve the degraded system performance.

In this paper we have developed a defense mechanism against network attack which consists of attack classification and defense against those attack and is explained in further chapters. We have used signature based approach for attack detection in which various fields of incoming packets are checked. Assuming the attack has been detected, the algorithms begins by checking internal details of each packets. Proposed defense mechanism provide defense against TCP, TCP-SYN flood and UDP attack. Rate limiting mechanism[4] is used to provide defense against TCP-SYN attack and Ingress filter mechanism[1] to defend against TCP and UDP attack.

## II. TYPES OF NETWORK ATTACKS

In computer networks, attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network. In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. A buffer overflow attack is when the attacker sends

more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell. Denial of Service attack is designed to cause an interruption or suspension of services of a specific host/server by flooding it with large quantities of useless traffic or external communication requests.

## III. PROPOSED WORK

In this paper we are presenting a defense mechanism against network attack. It consist of 1) Attack classification and 2) Defense against those attack. We have used signature based approach for attack detection in which various fields of incoming packets are checked. Assuming the attack has been detected, the algorithms begins by checking internal details of each packets which include following fields.

**TCP Packet**

- Source Port and Destination Port :If any of the above mentioned port is blank or 0 then it will treated it as attack packets.
- Checksum: If the checksum field of incoming packets is empty or contains invalid value then that packet will be treated as attack.
- Time To Live: TTL is an 8-bit field so its value ranges from 0 to 255. If TTL field of incoming packets contains value outside the range then that packet will be treated as attack packet.
- Flags:

  *Combination of RST and FIN flag:*

  FIN is an orderly close of an existing connection in one direction, after all pending data is sent. RST is is an *error condition* that says there is no such connection. It is not possible to use both at the same time. If such condition occurs then it will treated it as attack.

  *Combination of SYN and FIN:*

  Both the SYN and FIN control flags are not normally set in the same TCP segment header. The SYN flag synchronizes sequence numbers to initiate a TCP connection. The FIN flag indicates the end of data transmission to finish a TCP connection. Their purposes are mutually exclusive. Hence combination of both the flags in a single packet results in an attack.
- URG flag: If urgent pointer contains null value even after URG flag is set then it can be classified as attack.
- Total Length:Total length defines the entire packet (fragment) size, including header and data, in bytes. So header length must be lass than that of total length.

**TCP SYN flood**

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. We have used rate limiting mechanism for classifying attack as a TCP-SYN flood attack.If number of packets that have being received from a particular IP and Port numberwith its SYN flag set, crosses the threshold value then we classify those packets as SYN floodattacking packets. The threshold value is set by the user.

**UDP Packet**

For classifying an incoming UDP packet as an attacking packet various details of every packet is been checked. To classify as an attacking UDP packet we have checked the following fields-

- Source or destination Port number – If the source ordestination port number of incoming packet is invalid (0) then packet is classified as attack packet.
- Checksum – If any of the incoming UDP packets is having blank checksum valuethen it is classified as attacking packet.

After detecing and classifying packets as attack packets the defense mechanism is applied so that to prevent victim from further attack. Once the IP is classified as attacker IP, we have block that IP using appropriate firewall rule. Firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. A firewall has two default rules, one for inbound traffic and one for outbound.

*Inbound rules* explicitly allow, or explicitly block, inbound network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly allow traffic secured by IPsec for Remote Desktop through the firewall, but block the same traffic if it is not secured by Ipsec.

*Outbound rules* explicitly allow, or explicitly block, network traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a computer (by IP address) through the firewall, but allow the same traffic for other computers.

We have created inbound rule for blocking attack packets. This rule are created automatically when the number of attack packets from the particulat IP crosses the the\reshold set by the user.

## IV. IMPLEMENTATION

We have used C#.net platform for GUI to captures packets and check various fields of packets. User have to first select an appropriate network interface from all of the available interface on which he has to capture packets. Once an network interace is selected then it will displays all the network traffic between client and server systems. Figure 1 shows initial GUI for selecting network interface. Figure 2 shows TCP, UDP and flooding attack originating from different client systems. Figure 3 shows option to save content of network traffic into a file which can be used for analysis of network traffic.

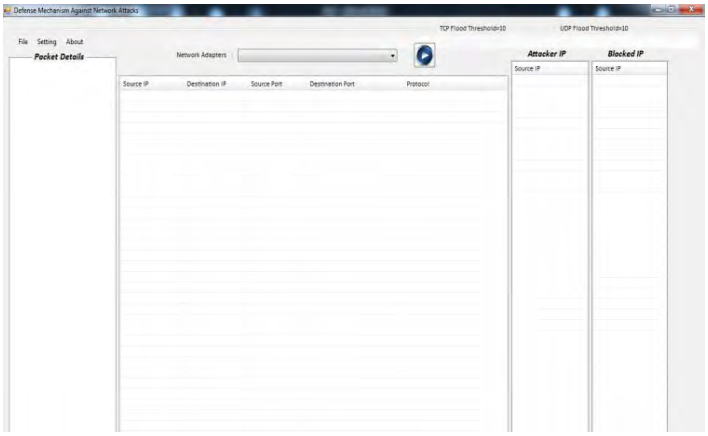

Figure 1: Initial GUI

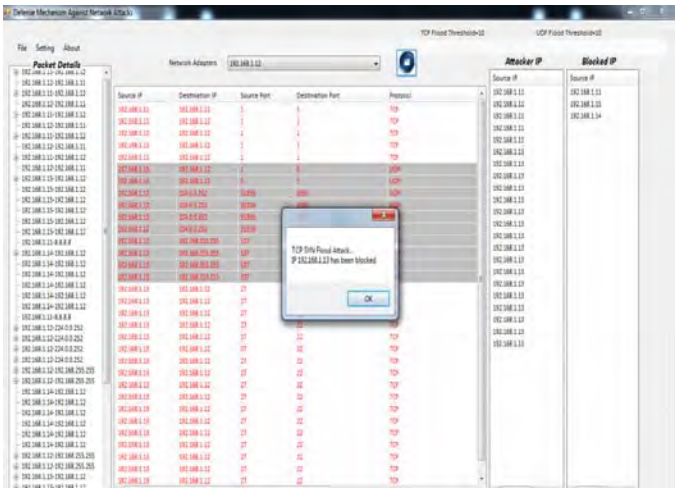

Figure 2: Defending TCP, UDP and TCP-SYN Flood Attack

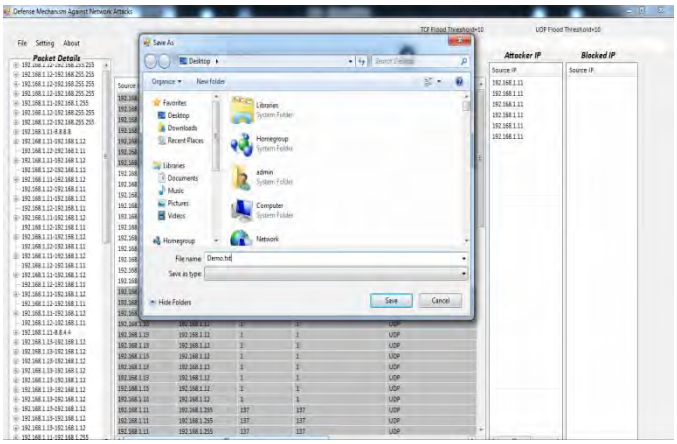

Figure 3: Saving captured network traffic into file

## V. CONCLUSION

Designed defense mechanism uses rate limiting mechanism and Ingress filtering mechanism for providing defense against attack originating from multiple systems simultaneously. It helps to improve system performance in case of network attack. It also helps to reduce bandwidth utilization in case of flooding attack. The performance of our defense mechanism is evaluated using CPU utilization, Memory utilization, Bandwidth utilization of system in case of low, normal and heavy attack traffic.

## VI. FUTURE WORK

Evaluation of our defense mechanism will be based on different parameters as False positive,False negative ,and system performance which includes CPU utilization, bandwidth utilization, memory Utilization in case of low, normal and heavy attack traffic.

## REFERENCES

[1] Danai Chasaki, Tilman Wolf, "Attacks and Defenses in the Data Plane of Networks", IEEE Transactions on dependable and secure computing, Vol. 9 , No. 6, November/December 2012
[2] Jan Stanek, Lukas Kencl," SIP Protector: Defense Architecture Mitigating DDoS Flood Attacks Against SIP servers", First IEEE International Workshop on Security and Forensics in Communication Systems, 2012, Page(s): 6733 – 6738
[3] Fei Wang, Xiaofeng Hu, Jinshu Su," Mutual-aid Team: Protect Poor Clients in Rate-limiting-based DDoS Defense", 2012
[4] Rachana Yogesh Patil, Lata Ragha, "A Rate Limiting Mechanism for Defending Against Flooding Based Distributed Denial of Service Attack",2011 World Congress on Information and Communication Technologies (WICT) ,Page(s): 182 - 186
[5] Biplab Sikdar, Joe H. Chow, "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks", IEEE Transaction on Smart Grid, Vol. 2, No. 4, December 2011
[6] Usman Tariq, Yasir Malik, Bessam Abdul razak and ManPyo Hong, "Collaborative Peer to Peer Defense Mechanism for DDoS Attacks", The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), Procedia Computer Science 5 (2011) 157–164
[7] Pin-Yu Chen, Kwang-Cheng Chen," Intentional Attack and Fusion-based Defense Strategy in Complex Networks", Global Telecommunications Conference (GLOBECOM), IEEE 2011,Page(s): 1 – 5
[8] Anh Le, Athina Markopoulou, "TESLA-Based Defense AgainstPollution Attacks in P2P Systems with Network Coding", International Symposium on network coding ,2011, Page(s): 1 - 7
[9] Mehran S. Fallah,"A Puzzle-Based Defense Strategy against Flooding Attacks Using Game Theory", IEEE Transactions on dependable and secure computing, Vol. 7, No.1, January-March 2010
[10] Wan Xiao-Yu, Zhang Li , Fan Zi-Fu," A SIP DoS Flooding Attack Defense Mechanism based on Priority Class Queue", IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS),2010, Page(s): 428 - 431
[11] Jerry Chi-Yuan Chou, Bill Lin, Subhabrata Sen, Oliver Spatscheck," Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks",IEEE/ACM Transaction on Networking, Vol. 17, No 6, December 2009
[12] Katerina Argyraki, David R. Cheriton, "Scalable Network-Layer Defense Against Internet Bandwidth-Flooding Attacks", IEEE/ACM Transaction on Networking, Vol. 17, No. 4, August 2009
[13] Yonghua You, Mohammad Zulkernine, Anwar Haque," A Distributed Defense Framework for Flooding-Based DDoS Attacks", The Third International Conference on Availability, Reliability and Security,2008
[14] Mihui Kim, Inshil Dohand, Kijoon Chae, "Defense Mechanism using Overlay against DDoS Attacks on Converged Networks",Feb.12-14, 2007,ICACT2007
[15] Abraham Yaar, Adrian Perrig, Dawn Song," StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 10, October 2006