**Exposys Data Labs**

**Abstract**

Denial of service (DoS) attacks have become a major threat to current computer networks. To have a better understanding on DoS attacks, this article provides an overview on existing DoS attacks and major defence technologies in the Internet and wireless networks. In particular, we describe network based and host based DoS attack techniques to illustrate attack principles. DoS attacks are classified according to their major attack characteristics. Current counterattack technologies are also reviewed, including major defence products in deployment and representative defence approaches in research. Finally, DoS attacks and defences in 802.11 based wireless networks are explored at physical, MAC and network layers.

Table of Contents:

| NAME | PAGE NO: |
| --- | --- |
| Introduction | 2 |
| Existing Method | 2 |
| Proposed method with Architecture | 2-3 |
| Methodology | 3 |
| Implementation | 3-4 |
| Conclusion | 5 |

**Introduction**

Denial of Service (DoS) attack is executed to determine a specific category of information warfare where a malicious user blocks legitimate users from accessing network services by exhausting the resources of the victim system. Without hacking the password files or stealing sensitive data, a DoS attacker creates network congestion by generating a large volume of traffic in the area of the targeting system. The size of the caused overload is enough to prevent any packet from reaching its destination. Normally, a TCP connection is established through a three-way handshake. A client initiates a connection by sending a SYN packet to the server. The server acknowledges the request by sending a SYN ACK packet back to the client and allocating space for the connection in a buffer.

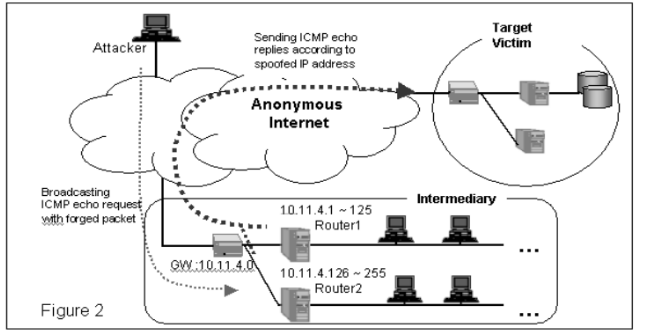
**Existing Methods**

Inferring of Internet Denial-of-Service Activity is extremely difficult for even system administrators because the current Internet protocol does not require a mechanism for the current packets to be pre-verified before leaving from a source network, during traversing through inter-networks and finally to be authenticated after arriving at any machines of the destination network. This anonymity is the most beautiful of the Internet in spite of leaving unfavourable security issues.

**Proposed System with Architecture**

Establishing a defence mechanism which provides a powerful security against resource consumption attacks namely denial of service attacks. Before the successful attack the attacker’s traffic consumes much network resources which lead to congestion over the network. This mechanism is a hybrid model consisting of a pushback mechanism with client puzzles. With this mechanism the attack causing traffic pattern can be easily identified and defence against the attack will be done successfully.

The intelligent router over the ISP network identifies the attacker hosts and pushes back the host addresses to the upstream router. The upstream router upon receiving the pushback request with the suspected host addresses gives a puzzle to the suspected host, the suspected host has to solve the puzzle and send back the puzzle answer to the router issued puzzle. Normally resource consumption attacks are not made by human requests, it makes resource consumption attacks, and attackers write a program to continuously keep on requesting the server. So if it is an attacker host it can’t solve the puzzle, then it is confirmed as an attacker host. The router issued the puzzle conforms the suspected hosts as attackers and asks the edge router to block all the traffic from attacker hosts.



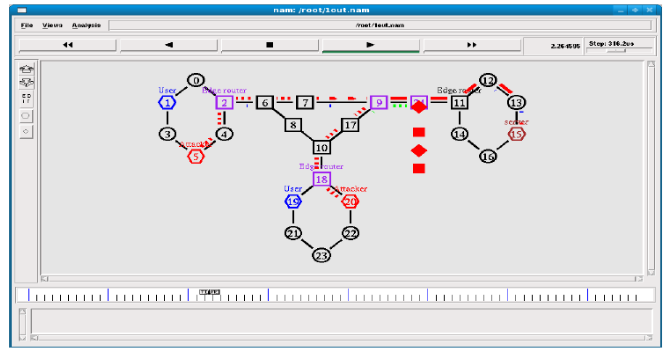
**Methodology**

The proposed work is a hybrid model for providing the defence against DoS/DDoS attacks. A router based client puzzle to suppress the attack traffic at the edge router itself is introduced. Intelligent routers have the responsibility of authenticating the host requests and allocating the network resources. This router based model is integrated with the pushback method. With this a very powerful defence against both the DoS/DDoS attacks can be provided.

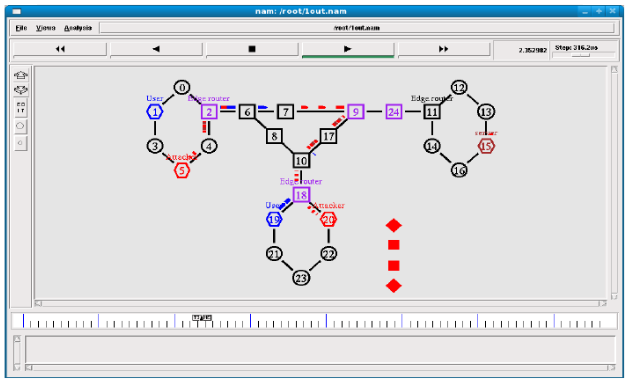
**Implementation**

To simulate the proposed system, we have to create the network. This network consists of LAN’s connected with ISP’s. This Network layout was created in Network Simulator. Figure 4 shows the network layout structure .In the below figure L1, L2 and L3 represents LANS Connected with ISP’s. In the network simulator all the nodes will have the same functionality and capabilities, to implement the proposed system in the above network; separate functionality in the nodes is implemented. Nodes with square shape have the router functionality; nodes with the hexagonal shape are the active hosts on the network. Node-1 and Node-19 are used as legitimate users, Node-5 and Node-20 are used as attacker hosts, Node-24 is the intelligent router that has the capabilities to check the traffic pattern and identify the attack causing events.

1. Attack Traffic Generation Phase



1. Pushback Mechanism Phase



**Conclusion**

This proposed method provides a strong defence against the malicious hosts in the network, and it easily identifies the attacker hosts by their traffic nature and blocks all the traffic from the attacker hosts. Client puzzles give the advantage to validate the suspected hosts in order to confirm whether the suspected hosts are from an attacker or from a legitimate user. Pushback helps to outsource the client puzzle workload to the upstream router, which helps to decrease the processing workload on intelligent routers. Using the proposed work, the attacker traffic is effectively blocked at the edge routers and hence the denial of service causing attacks can be identified in advance and offended successfully.