http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 5 (3): 489-493, 2006
ISSN 1812-5638

Network Topology Against Distributed Denial of Service Attacks

[1]S. Behin Sam, [1]S. Sujatha, [2]A. Kannan and [1]P. Vivekanandan
[1]Department of Mathematics, Anna University, Chennai, India
[2]Department of Computer Science and Engineering, Anna University, Chennai, India

Abstract: Distributed Denial of Service (DDOS) attacks have emerged as a prevalent way to shut an organization off from the internet and has resulted in financial losses to the same. In the case of DDOS attack, an adversary attempts to disconnect network elements by disabling the communication links or nodes. The effectiveness of DDOS defenses depends on factors such as the specific attack scenario and various characteristics of the network routers. However, little research has focused on the nature of the network's topology that can also be an effective DDOS defense. This study focuses on the adversaries who try to disable the communication links. It stresses the need for either a strong connectivity or m-connectivity among the nodes (routers). This approach will discourage the adversary from attempting to disable the network, as the cost for causing the damage will increase. Validation of this approach was performed using a network simulator and the results are shown.

Key words: Computer networks, denial of service, undirected graph, edge connectivity

INTRODUCTION

Computer-based attacks on critical infrastructure have become a great concern to many organizations as they have become increasingly reliant on the network to exchange information among various systems. There currently exist multiple threats and vulnerabilities in the security of computer systems and networks against attacks. The possible types of computer attacks include:

- Attacks that deny access to some services or resources that a system provides.
- Attacks that allow an intruder to operate on a system with unauthorized privileges.
- Attempts to probe a system to find potential weaknesses
- Physical attack against computer hardware
- Attacks by worms or viruses

All these and other attacks have been gaining in sophistication and power to cause harm. Attacks are increasingly automated, so now the attack tools may initiate new attack cycles by themselves with no person involved. Distributed attack tools are capable of coordinating use of numerous attack platforms and scripts spread out in the network, thus launching truly devastating Distributed Denial of Service (DDOS) attacks.

Many defenses have been discussed to control the on-going attack traffic (Douligeris and Mitrokosta, 2003). Recent advances in encryption, public key exchange, digital signatures, and the development of related standards have set a foundation for strong security. However, security on a network goes way beyond encryption of data. It must include the security of computer systems and networks, at all levels, top to bottom. It is imperative to arm the network systems and elements with well designed, comprehensive, and integrated attack defeating policies and devices. However, foolproof prevention of attacks is challenging, because at best the defensive system and application software may also contain unknown weaknesses and bugs.

Researchers across the world have concentrated on factors such as the specific attack scenario and various aspects of the network routers for developing DDOS defenses. Little importance has been given to the networks topology, which can be an active DDOS defense. This paper focuses on designing the network to be strongly connected or m-connected. By designing the network in such a way will discourage the intruder from any future attempts to disable the network, as the cost for disabling the network will be high. Thus designing strong and reliable network is required in order to prime the execution of countermeasures.

Perspectives on intrusion: victims and attackers: From a victim's perspective, intrusions are characterized by their manifestations which might or might not include damage. The attackers intent has a bearing on the cost of

Corresponding Author: Behin Sam, Department of Mathematics, Anna University, Chennai-600 025, India

causing the attack and risk of exposure. A victim's view of an attack usually focuses on the manifestations:

- What happened?
- What is affected and how?
- Who is the intruder?
- How to rectify the damage?
- How to stop such attacks in future?

The attacker has a quite different view

- What is my objective?
- What vulnerabilities exist in the target system?
- To what extent the attack will cause the damage?
- Cost for causing the damage?
- What attack tools are available?
- What is the risk of exposure?

DEFINITIONS

We model the communication network as an undirected graph. A graph G is defined by the 2-tuple <V, E >, where V is a non-empty set of nodes (vertices) and E is a set of edges (or arcs). A key component in the networking criteria is the concept of graph connectedness. A graph G is connected if there is at least one path between every pair of nodes in G. The edge connectivity of a graph is also an important measure of graph connectedness.

A graph G' = <V', E'> is a sub graph of graph G =< V, E >, if V'⊂ V and E' ⊂ E. In an attack, some nodes and links are disabled. Our model of the network assumes the use of adaptive routing algorithms. As long as there is at least one good route from the source to a node, the service is available. The service is denied when the last connection from the source fails.

PROBLEM DESCRIPTION

A denial of service attack is considered to take place only when access to a computer network resource is intentionally blocked or degraded as a result of malicious actions taken by another user. These attacks do not necessarily damage data directly, or permanently, but they intentionally compromise the availability of the resource (Howard, 1997). A distributed denial of service attack is usually launched from multiple hosts on the network to saturate the bandwidth of the victim's connections. In a DDOS attack, an attacker could trigger tens of thousands of concurrent attacks on either one or a set of targets by using different nodes in the network to coordinate these attacks (CERT/CC., 1999).

A number of defenses against DDOS attacks have been proposed. These are reviewed in next section. Generally DDOS defenses are deployed at nodes (routers) that are central nodes that control the flow of information through the network topology (Freeman and Borgatti, 1991). Foolproof prevention of attacks is challenging, because at best the adversary can break any defense. This research focuses on designing the network topology in such a way that, even when the adversary is able to disable one or few connections the network is still connected. And also as the DDOS defense at the node will learn about the attacker with every attempt, it will make it harder for the attacker to break the connection with ease. And as the attacker has to spend certain cost for disabling the connection, a cost model is presented that grows exponentially discouraging the attacker from any future attempts in breaking the network.

PREVIOUS DDOS DEFENSES

Reaction points to attack could be network-based or host based. Network-based methods are deployed on the points were packets are routed through network connections, such as routers or proxy servers (Bellovin, 2000; Burch, 2000; Ferguson and Senie, 1998; Ioannidis and Bellovin, 2002). Host-based defenses are deployed on the machines that are potential targets of attacks (Spatscheck and Peterson, 1999; Yan and Early, 2000). These methods could increase the victim's ability to tolerate attacks but not stop them.

A few defenses are designed to actively respond to the attack traffic while the majority is designed to passively trace/log attack traffic. Tracing back to the real sources of attacks has been established, a part of DDOS defense studies (Bellovin, 2000; Burch and Cheswick, 2000). In contrast other defenses are designed to actively reduce the amount of on-going attack traffic (Ioannidis and Bellovin, 2002; Mahajan and Bellovin, 2002; Mirkovic and Reiher, 2005).

Since examining every packet that goes through a router may impose an enormous storage or computational power requirement, some defenses sample network packets probabilistically to reduce the number of packets to be examined/logged (Huang and Pullen, 2001).

Some defenses need to be turned on all the time in order to detect the suspicious packets. Egress (SANS, 2000) and Ingress filtering (Ferguson and Senie, 1998) are deployed at local edge routers to examine all incoming and outgoing packers. A few defenses trigger attack response based on the congestion level of network links (Huang and Pullen, 2001; Ioannidis and Bellovin, 2002; Mahajan and Bellovin, 2002; Xiong and Liu, 2001).

It is hard to distinguish attack packets from normal packets especially when both types of packets are sent to the same destination. Most intrusion detection systems detect attacks based on anomaly pattern matching or statistical measures of attack signatures (Debar and Dacier, 1999). The pushback method treats traffic aggregates as attack flows (Ioannidis and Bellovin, 2002; Mahajan and Bellovin, 2002). TCP SYN packet flood can be identified by a state machine (Schuba and Krsul, 1997). Attack packets with spoofed source IP addresses can be identified given knowledge of the network topology (Park and Lee, 2001).

QUANTITATIVE ANALYSIS OF COST OF BREAKING NODES FOR DIFFERENT NETWORK TOPOLOGIES

According to Andrew, (1998) there are different router interconnection topologies. They are ring, strongly connected, m-connected, bus and star topologies. A study has been done by disconnecting the connections for breaking or isolating the nodes. The cost involved in breaking the connections for various topologies has been shown in Fig. 1 For this quantitative analysis, assumptions has been made that there are no filters installed and the cost for transporting a unit of traffic is 10 units and the capacity of each link/connection is 100 units and also a 11 node strongly connected network and 5-connected network is considered.

By the above Fig. 1 it can be clearly seen that for breaking a single node in distributed denial of service attack, the cost of strongly connected network and the m-connected network is high. So from the network designer point of view its clear that the two topologies will be preferred over all other topologies against distributed denial of service attack.

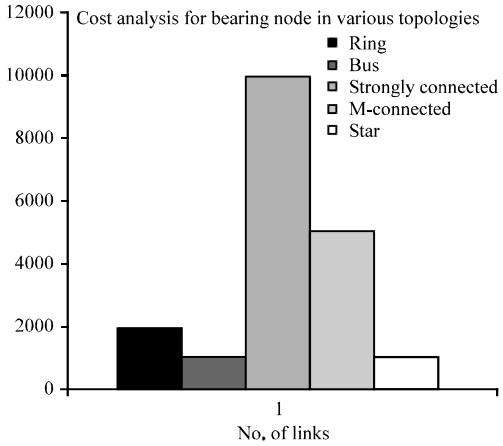

Fig. 1: Cost analysis for breaking nodes in various topologies

According to Ralph (2002), we have a theorem that says "The edge connectivity of a graph G cannot exceed the degree of the vertex with the smallest degree in G". This clearly shows that the network can be disconnected by just removing the d (v) edges incident on vertex v. So higher the connectivity, the more reliable the network will be against attacks. Designing a network with strong survivability is explained here.

DESIGNING THE NETWORK

Case 1: Strongly connected network: A graph G is strongly connected if for all x, y $\subset$V, there is an edge. The degree of each vertex is d (v) = n-1, where n is the number of nodes.

Case 2: m-Connected network: The least number of edges that an m-connected graph on n vertices can have is m, with the assumption that m<n. The degree of each vertex is d (v) = m. Depending on the value of m there are two sub cases, they are

Case 2.1: m is even: Let m = 2r. Then G<n, 2r> is constructed as follows. It should have vertices 0, 1, 2..., n-1 and two vertices i and j are joined if i-r = j = i+r (where addition is taken modulo n).

Case 2.2: m is odd: Let m = 2r+1. Then G<n, 2r+1> is constructed by first drawing G<n, 2r> and then adding edges joining vertex i to vertex i + (n/2) for 1 = i = n/2.

EXAMPLE NETWORK

Case 1: In the case of strongly connected network with eight nodes, twenty eight links are shown as given in Fig. 2.

Case 2: In the case of m-connected network, we have two sub cases

Case 2.1: m is even. Here there are eight numbers of nodes and sixteen numbers of links. The network is shown in Fig. 3.

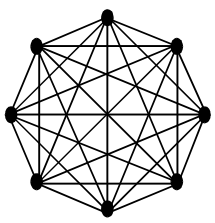

Fig. 2: G (7,8) network

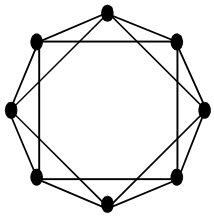

Fig. 3: G (4, 8) network

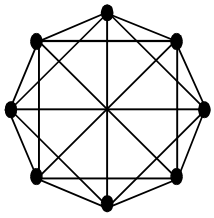

Fig. 4: G(5,8) Network

Case 2.2: m is odd. Here there are eight numbers of nodes and twenty numbers of links. The network is shown in Fig. 4.

COST MODEL

Both the normal traffic and the attack traffic impose cost on the normal user and the attacker, respectively. In this section, a cost model quantifies the costs during an attack for an attacker. Measuring cost will make it possible to the attacker to reexamine his strategy for attacking the network. Attack sources of an attack are usually nodes that generate attack packets and send it to the path which it wants to break. However, these attack packets could be defended to an extent, by deploying filter software with learning mechanism at nodes (routers).

NOTATIONS

$A(t)$	The attack traffic generated at time t.
$T_A(t)$	The total attack traffic at time t.
$e^{-\partial(t)}$	It denotes the exponential filtering rate, where $\partial(t)$ learning rate of filter and also $0<\partial(t)<1$.
$A_{TA}(t)$	The total attack traffic that is allowed to pass through the filter node at time t.
B	The capacity of the victim link.
A_{TR}	The attack traffic required to break the link.
C_T	The transport cost of a unit of traffic.
T_{CB}	The Total cost for breaking a link

Equation 1 quantifies the total attack traffic that is generated at time t.

$$T_A(t) = \sum_{i=1}^{n} A_i(t) \quad (1)$$

Where, i is the set of all distributed attack nodes.

Equation 2 quantifies the total attack traffic that is allowed to pass through the filter node at time t.

$$A_{TA}(t) = T_A(t) * e^{-\partial(t)} \quad (2)$$

Equation 3 quantifies the total attack traffic required to break the link.

$$A_{TR} = B * e^{\partial(t)} \quad (3)$$

Equation 4 quantifies the total cost for breaking a link.

$$T_{CB} = A_{TR} * C_T \quad (4)$$

SIMULATION RESULTS

In this section we use simulation to study the survivability of our newly proposed network against attacks. We use NS2 (Network Simulator 2) for our study. In order to design the network more reliable against denial of service attack we use the new design method given in the previous sections this paper. When we run the simulation in Fig. 5 how well the data is flowing without disruption.

When the intruder tries to disrupt the flow of data he has to break the connections and for this he has to spend certain cost. As the nodes in the network can filter certain amount of attack traffic because of learning facility, the cost involved in causing the damage to the networks in terms of different learning rate for ten links is shown in Fig. 6.

Table 1 gives the value of learning rate $\partial(t)$ in terms of percentage.

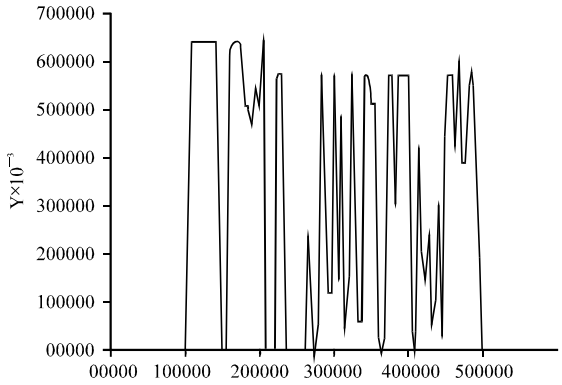

Fig. 5: Data flow analysis

Table 1: Value of ∂(t) in terms of %

∂(t)	(%)
0.0	0
0.1	10
0.2	29
0.3	30
0.4	40
0.5	50
0.6	60
0.7	70
0.8	80
0.9	90
1.0	100

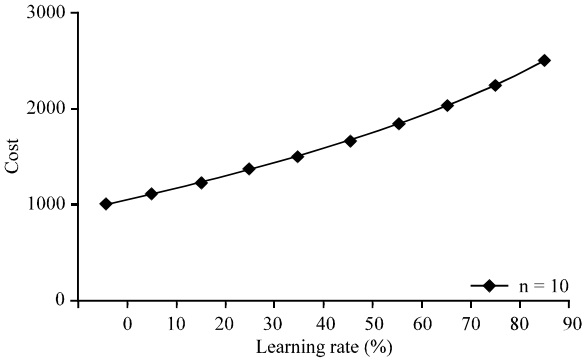

Fig. 6: Cost involved to cause damages for different learning rates

When the attacker examines his strategy by seeing the above cost analysis Fig. 6, must reconsider its decision for attacking the network.

CONCLUSIONS

This study gives importance to the networks topology, which can act as an active DDOS defense. Quantitative analyses on various topologies have been done and it has been found out that designing the network to be strongly connected or m-connected will be better defense against DDOS. A Cost model has been developed for the attacker about how much he will have to spend on breaking the links. By designing the network to be strongly connected or m-connected, an intruder is discouraged from any future attempts to disable the network, as the cost for disabling the network will be high.

REFERENCES

Andrew, S.T., 1998. Computer Networks, PHI, 3rd Edn.

Bellovin, S.M., 2000. ICMP traceback message, Internet Draft: draft-bellovin-itrace-00.txt.

Burch, H. and B. Cheswick, 2000. Tracing anonymous packets to their approximate source, In Proceedings of LISA 2000, New Orleans, LA.

CERT/CC, 1999. Results of the distributed-systems intruder tools workshop., Pittsburgh, Pennsylvania, USA, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University.

Douligeris, C. and A. Mitrokotsa, 2003. DDoSattacks and defense mechanisms: A classification. In Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology.

Debar, H. and M. Dacier *et al*., 1999. Towards a taxonomy of intrusion detection systems. Computer Networks, 31: 805-822.

Ferguson, P. and D. Senie, 1998. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. IETF RFC2267.

Freeman, L.C. and S.P. Borgatti, 1991. Centrality in valued graphs: A measure of betweeness based on network flow. Social Networks, 13: 141-154.

Howard, J.D., 1997. An analysis of security incidents on the internet. Department of Engineering and Public Policy, Pittsburgh, PA, Carnegie Mellon University.

Huang, Y. and J.M. Pullen, 2001. Countering denial-of-service attacks using congestion triggered packet sampling and filtering. In Proceedings of International Conference on Computer Communications and Networks, www.ieeexplore.ieee.org.

Ioannidis, J. and S.M. Bellovin, 2002. Implementing pushback: Router defense against DDoS attacks. In Proceedings of Network and Distributed System Security System Symposium, www.rpa.ajou.ac.kr.

Mahajan, R. and S.M. Bellovin, 2002. Controlling high bandwidth aggregate in the network. In ACM STGCOMM Computer Communication Review, www.portal.acm.org.

Mirkovic, J. and P. Reiher, 2005. D-WARD: A Source-End Defense against Flooding Denial-of-Service Attacks. IEEE Transactions on Dependable and Secure Computing, 2: 216-232.

Park, K. and H. Lee, 2001. On the effectiveness of route-based packet filtering distributed DoS attack prevention in power-law Internet. ACM SIGCOMM'01, San Diego, CA, Department of Computer Science, Purdue University.

Ralph, P.G., 2002. Discrete and combinatorial mathematics. Pearson Education Asia, Fourth Edition.

SANS, 2000. Egress filtering v 0.2., SANS Institute, www.sans. Org/y2k/egress.htm.

Schuba, C.L. and I.V. Krsul, 1997. Analysis of a denial of service attack on TCP. IEEE Computer Society Symposium on RES Security and Privacy, www.doi.ieeecs.org.

Spatscheck, O. and L.L. Peterson, 1999. Defending against denial of service in scout. In Proceedings of OSDI, www.usenix.org.

Xiong, Y. and S. Liu *et al*., 2001. On the defense of the distributed denial of service attacks: An on-off feedback control approach. IEEE Transaction on Systems, Man and Cybernetics-Part A: Systems and humans, 31: 282-293.

Yan, J.S. and S. Early, 2000. The XenoService-A distributed defeat for distributed denial of service. In Proceedings of Information Survivability Workshop, www.sunsite.redirisies.