Proceedings of the National Conference; INDIACom-2007
Computing for Nation Development, February 23 – 24, 2007
Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

Mitigating Attacks in Routing Protocol

Prof. M.N. Hoda, Mrs. Umang
BVICAM, New Delhi
Email: mca@bvicam.ac.in, singh.umang@rediffmail.com

ABSTRACT
Any information and network security issue, combating Does is primarily an exercise in risk management. Guarding against attacks is a critical component of any security system. In DoS attacks, illegitimate packets are indistinguishable from legitimate packets, making detection difficult; typical "signature" pattern matching, performed by IDSs, do not work. The goal of this paper is to highlight recent trends in the deployment of DoS and DDoS attacks. New enhancements in routing and security technologies enable them to protect their last mile users from compromising malware. By utilizing approaches, the impact of an attack can be limited to the victim, and the attack can quickly be mitigated. This paper has also discussed several approaches to mitigate the effects of DoS and DDoS attacks.

KEYWORDS
Attacks, DoS, DDoS, MANET, AODV, ICMP, Network Intrusion Detection System, Selective Bin Verification.

INTRODUCTION
A "denial-of-service" (DoS) [1-5] is an attack with the purpose of preventing legitimate users from using a specified network resource for which they have authorization. A Distributed Denial of Service (DDoS) attack, is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The DoS and DDoS attacks in combination with malicious codes implantations are easily launched but difficult to completely stop. Attacks on ad

hoc network routing protocols generally fall into one of two categories:

1. Routing-disruption attacks. The attacker attempts to cause legitimate data packets to be routed in dysfunctional ways.
2. Resource-consumption attacks. The attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth or to consume node resources such as memory (storage) or computation power.From an application-layer perspective, both attacks are instances of a denial-of-service (DoS) attack.

Classification of DoS Attacks: In a denial of service attack, a malicious user exploits the connectivity of the Internet to cripple the services offered by a service provider, often simply by *flooding* with many requests. Software exploit attacks [6] exploit specific software bugs in the operating system or an application, and can potentially disable the victim machine with a single or a few packets. A well known example is the *ping of death* that causes the operating system to crash by sending a single large Internet control message protocol (ICMP) echo packet. A DoS attack can be either a *single-source* attack, originating at only one host, or a *multi-source*, where multiple hosts coordinate to flood the victim with a barrage of attack packets. The later is called a distributed denial of service (DDoS) attack. Sophisticated attack tools that automate the procedure of compromising hosts and launching attacks are readily available on the Internet, and detailed instructions allow even an amateur to use them effectively. Figure 1 presents the classification of DoS attacks based on volume of packets and number of attackers.

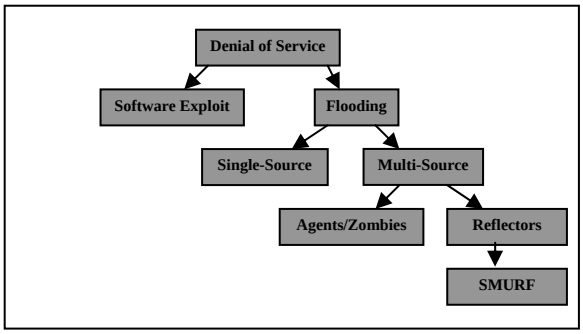

Fig: Classification of DoS Attacks

Differences in DoS and DDoS Attack: DoS attacks are a class of attacks initiated by individual or group of individuals exploiting aspects of the Internet Protocol to deny other users from legitimate access to systems and information. In the past, DoS flooding attacks has been associated to SMURF attacks (**"SMURF"** attack [7] is one example of DoS attack, which exploits the router incapability to limit or prevent the router from performing IP broadcast and becoming an amplifier), which were targeted at routers. If an attacker can force a router to stop forwarding packets, then all hosts behind the router are effectively disconnected. Nowadays many other forms of attacks are crafted to attack web servers, mail servers and other services [8].

1. **Destructive** – Attacks which destroy the ability of the device to function, such as deleting or changing configuration information or power interruptions.
2. **Resource consumption** – Attacks which degrade the ability of the device to function, such as opening many simultaneous connections to the single device.
3. **Bandwidth consumption**: Attacks which attempt to overwhelm the bandwidth capacity of the network device. Network with small bandwidth may suffer from high bandwidth consumption instantaneously, if it becomes target. Response rate will depend on cooperation from service providers, for example in applying filters at upstream routers.

DDoS on the other hand is a combination of DoS attacks staged or carried out in concert with various hosts to penalize the target host from further serving its function.
DDoS term is coined when the source of the attack is not coming from a single source, but multiple source. DDoS cannot be eliminated with merely filtering the source internet protocols since it is often launched from multiple points installed with agents.

Recent trends in the deployment of DoS and DDoS attacks: Nowadays, DoS and DDoS attacks are carried out by organized criminals targeting financial institutions, e-commerce, and gambling sites. Such sites are taken down by bandwidth or server extortion caused by the traffic thrown at the target. DDoS attacks range from small and targeted attacks to large scale versions launched from thousands of bots, affecting not only the target victim, but also the infrastructure of the service provider. This in turn impacts other customers' services and if the network stability is affected even voice and other public services may be impacted. As hacking has turned to a tool used by organized criminals, we witness a higher degree of sophistication and the magnitude of the attacks has also increased dramatically. Service providers have a unique role to play to combat DDoS attacks.

Large organizations like Amazon, eBay; Yahoo and Microsoft have been affected by large DDoS attacks. Lately, we witness an increase of targets in financial institutions and other organizations that keep financial records. Auction, e-commerce and gambling sites are blackmailed before major events are due, e.g. in August 2005 the Hamburg-based gambling site www.jaxx.de was blackmailed to pay 40,000 euros to stop an ongoing DDoS attack.
Security flaws and attacks on routing protocol in Ad hoc On Demand Distance Vector : In AODV protocol when a node (source) needs to communicate with another node (destination) but the source does not have the route, it broadcasts RREQ(Route REQuest) to its neighbors. The process continues until an intermediate node having the fresh route to the destination is found (or the destination itself is found). To prevent unnecessary processing of same RREQ packet from different neighbors, each node processes the RREQ packet that first arrives, thereby ignoring other copies. A direct (tunneling) link (wired/wireless) is faster than general hop-by hop propagation. Usually it involves two attackers; one near the source and another near the destination. When a source broadcasts an RREQ packet the first attacker records it and transmits directly through a tunnel to the second attacker (who is near the destination). Any neighbor of destination receives the RREQ from the attacker it normally processes. In the meantime the original RREQ comes to it using hop-by-hop propagation; it simply discards it, as already it has received the packet. Thus can cause DoS attack. Further it bounds the source and destination to use the attacker nodes.
Known attacks on AODV are as follows [9][10]:

i. Traffic redirection by modification
ii. Replay attacks
iii. Loop formation by spoofing
iv. False Route Error

New enhancements in routing and security approaches enable them to protect their broadband users from compromising malware that turn PCs into zombies or botnets.
Securing routing protocol [11] in ad hoc network is a daunting task. The solution has been carried out based on AODV protocol as follows, although it is well suited for any standard routing protocol in adhoc networks, as well.

(1) The use of two different metrics (trust level and workload) for routing selection is a probabilistic approach to enhance security of the discovered path.
(2) To remove a node from a route it uses the mechanism to detect malicious node which does not depend on global clock synchronization but on its local timing only.
(3) In order to prevent replay attacks it employs session- key for data transfer. Even if it is stolen or hijacked its consequence is limited to only the concern session as it expires after a certain period.

By utilizing technologies at hand and designing the networks using best practices, the impact of an attack can be limited to the victim, and the attack can quickly be mitigated.
Instead, attacks are carried out in a more targeted fashion, and the level of sophistication increases.

Now Our Objective is how to mitigate such DoS and DDoS attack: The following two approaches are being discussed to mitigate attacks from real world scenario:

1. **Network Intrusion Detection Systems [NIDS]:** NIDS [12] are effective at detecting certain types of DoS attacks. However, approaches that rely on

signature or anomaly detection make the assumption that the attack packets are distinguishable from the legitimate traffic. While this may be true for certain attacks (e.g., "smurf" attacks [13]), other DoS techniques merely inundate a service with requests that appear valid.

2. **Selective bin verification [SBV]:** SBV provides the ability to protect authenticated broadcast from AODV. It is also an efficient technique to protect point to point protocols. An important advantage of selective bin verification is that it reduces the effects of a DoS attack even in the case where one fails to detect the attack. It is a software-based approach and requires no hardware modifications.

Currently, the technique requires communication overhead even in the absence of an ongoing attack. Thus, an appropriate extension incorporates intrusion detection. For Example, selective bin verification could be deactivated in the steady state and automatically enabled during an attack. Evaluating best protocols in selective bin verification is another useful future research area.We can also make combined approach of selective bin verification and network Intrusion detection system for future defense against DoS and DDoS attacks.

Conclusion and Future work: The impact of an attack can be limited to the victim, and the attack can quickly be mitigated by using Network Intrusion detection System and Selective Bin Verification technique. Where one, our future work will try to simulate AODV routing protocol with these discussed techniques and evaluate the results.

REFERENCES

[1] Udaya Kiran Tupakula Vijay Varadharajan, "A Practical Method to Counteract Denial of Service Attacks", Information and Networked System Security Research, 2003, Australian Computer Society, Inc.

[2] Computer Emergency Response Team. "CERT Advisory CA-2000-01 Denial- Of-Service developments". http://www.cert.org/advisories/CA-2000-01.html, Jan.2000.

[3] Computer Emergency Response Team. "CERT Advisory CA-1999-17Denial-of-Service Tools". http://www.cert.org/advisories/CA-1999-17.html.

[4] D.Dittrich: "The stacheldraht" distributed denial of service attack tool". http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt, Dec.1999.

[5] D.Dittrich: "The Tribe Flood Network distributed denial of service attack tool". http://staff.washington.edu/dittrich/misc/tfn.analysis,Oct.1999.

[6] Alefiya Hussain, John Heidemann,,and Christos Papadopoulos, "A Framework for Classifying Denial of Service Attacks",ISITR2003569 @2003

[7] Huegen, Craig A. "The Latest in Denial of Service Attacks: "Smurfing" Description And Information to Minimize Effects". 8 February 2000. http://www.pentics.net/denial-of-service/white-papers/smurf.cgi(4 Jan.2002)

[8] Mandia, Kevin & Prosise, Chris. "Incident Response: Investigating Computer Crime". Berkeley: Osborne/McGraw-Hill, 2001. 360-361.

[9] J. Zhen and Sampalli Srinivas. Preventing Replay Attacks for Secure Routing in Ad Hoc Network. ADHOC-NOW 2003, LNCS 2865, pp. 140-150, 2003

[10] K. Sanzgiri, B.Dahill, B.N.Levine,C.Shields and E. M.Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. *Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02)* 2002

[11] Abu Raihan Mostofa Kamal, "Adaptive Secure Routing in Ad Hoc Mobile Network", SecLab, Department of Computer and Systems, Science (DSV).Stockholm, Sweden, 2004

[12] V. Paxson. Bro: a system for detecting network intruders in real- time. Computer Networks (Amsterdam, Netherlands: 1999), 31(23–24):2435–2463, 1999.

[13] CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks, Jan. 1998.