Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 1 (2016) 21-23. Submitted 23/01/2016. Published 2/02/2016

MODERN CRACKING ALGORITHM BASED DETECTION AND PREVENTION OF DDOS ATTACK

Varalakshmi.S, Department of Computer Science and Engineering,
Mrs. A.Umamaheswari, Assistant Professor, Department of Computer Science and Engineering,
Mahendra engineering college, Namakkal.

Abstract:

One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Lastly, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

Keywords- OLSR, Victim, DOS.

1. INTRODUCTION

These algorithms differ from the standard routing used in classic networks due to frequent topology changes. Portability is one aspect of mobile computing. It is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information. When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line. People who use mobile devices while driving are often distracted from driving and are thus assumed more likely to be involved in traffic accidents. While this may seem obvious, there is considerable discussion about whether banning mobile device use while driving reduces accidents or not. Cell phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health have been raised.

2. PROPOSED SYSTEM

Most of these protocols assume a trusted and cooperative environment.The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. The special network characteristics, such as limited battery power and mobility, make the prevention techniques based on cryptographic primitives ineffective to cope with such attack.Rather, a more proactive alternative is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails,some economic-based approaches can be adopted to alleviate theattack consequences by motivating the nodes cooperation.

3. DATA COMMUNICATION

Some enterprise deployments combine networks from multiple cellular networks or use a mix of cellular, Wi-Fi and satellite.[16] When using a mix of networks, a mobile virtual private network (mobile VPN)

not only handles the security concerns, but also performs the multiple network logins automatically and keeps the application connections alive to prevent crashes or data loss during network transitions or coverage loss. Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from Unix-like hosts (the -t flag on Windows systems is much less capable of overwhelming a target, also the -l (size) flag does not allow sent packet size greater than 65500 in Windows). However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server can make, keeping it from responding to legitimate requests until after the attack ends.

4. PROACTIVE PROTOCOLS

As the name suggests, it uses the link-state scheme in an optimized manner to diffuse topology information. In a classic link-state algorithm, link-state information is flooded throughout the network. OLSR uses this approach as well, but since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. The attackers sent many ICMP ping packets using a botnet to each of the servers.

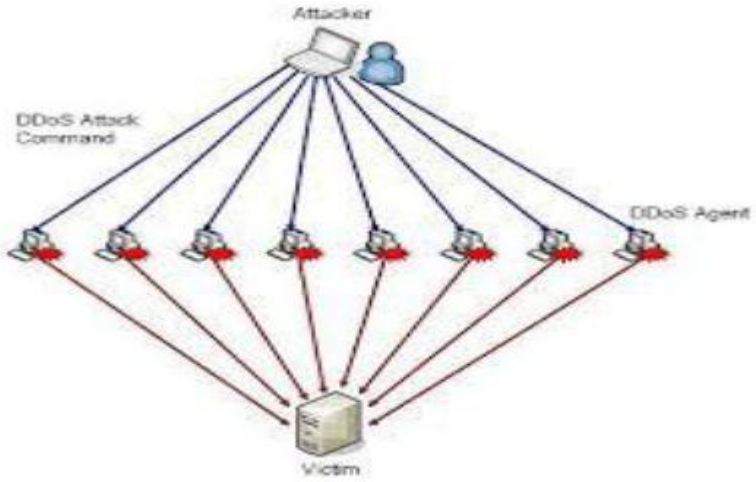

Fig.1 . DDOS Attack

However, because the servers were protected by packet filters which were configured to block all incoming ICMP ping packets, they did not sustain much damage and there was little to no impact on Internet users. At least two of the root servers (G-ROOT and L-ROOT) reportedly "suffered badly" while two others (F-ROOT and M-ROOT) "experienced heavy traffic". The latter two servers largely contained the damage by distributing requests to other root server instances wit Distributed denial of service attack usually occurs in MANETS or in wireless networks. It is an attack where numerous systems comprise together and target a single system causing a DDos.

5. RESULT ANALYSIS

Denial of service attack consumes a large amount of network bandwidth or occupies network equipment resources by flooding them with packets from the machines distributed all over the world. Now my objective is to study various detection and prevention techniques of DDOS attack. Detection

mechanism such as profile based detection, specification based detection, and flow based detection. And prevention technique include new cracking technique. The DDos attack is the most popular attack in network and internet. This kind of attack consumes a large amount of network bandwidth and occupies network equipment resources by flooding them with packet from the machines distributed all over the earth. DDos attack has been regular in the works attacks that badly intimidate the stability of the internet.There are mainly three categories of DDos attacks: protocol attack, logical attack and flood attack.

CONCLUSION

Distributed denial of services attack usually occurs in MANETS or in wireless networks. It is an attack where numerous systems comprise together and target a single system causing a denial of service. A denial of service is an attack with a purpose of preventing legitimate users from using a specified network resource such as web service, website or computer system. A DDos attack is distributed a large scale attempt by malicious users to flood the victim network with an enormous numbers of packets. More Network Overhead occurs due to the usage of numerous acknowledgement packets in each nodes of the network, Fragmentary packet transmission is rather possible in the network.

REFERENCES

[1] C. E. Perkins and P. Bhagwat, ―Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers,‖ in Proceedings of the Conference on Communications Architectures, Protocols and Applications, ser. SIGCOMM ’94. New York, NY, USA: ACM, 1994, pp. 234–244. [Online]. Available: http: //doi.acm.org/10.1145/190314.190336

[2] C. Perkins and E. Royer, ―Ad-hoc on-demand distance vector routing,‖ in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA ’99. Second IEEE Workshop on, Feb 1999, pp. 90–100.

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, ―Optimized link state routing protocol for ad hoc networks,‖in Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, 2001, pp. 62–68.

[4] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, ―Securing the olsr protocol,‖ in Proceedings of Med-Hoc-Net, 2003, pp. 25–27.

[5] T. Clausen and P. Jacquet, ―RFC 3626 - Optimized Link State Routing Protocol (OLSR),‖ p. 75, 2003. [Online]. Available: http: //www.ietf.org/rfc/rfc3626.txt

[6] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, ―An advanced signature system for olsr,‖ in Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc.