INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1999 – 2003
RECEIVED: 15-03-2017. PUBLISHED: 04-04-2017.

April 04, 2017

MITIGATING DENIAL OF SERVICE ATTACKS IN OLSR PROTOCOL USING FICTITIOUS NODES

[1]Kalavathy.D, [2]A Gowthami,
[1]PG Scholar, Dept Of CSE, Salem college of engineering and technology,
[2]Asst Prof, Dept Of CSE, Salem college of engineering and technology.

ABSTRACT

With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Over the years, emphasis has also been placed on improving the security of these networks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. 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. Through extensive experimentation, we demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable. Last, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

Keyword: Distributed denial-of-service (DDoS), Denial Contradictions with Fictitious Node Mechanism (DCFM), Optimized Link State Routing protocol (OLSR)

1. INTRODUCTION

Mobile computing is human computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. It is taking a computer and all necessary files and software out into the field. It is being able to use a computing device even when being mobile and therefore changing location.

2. DISTRIBUTED ATTACK

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. A botnet

is a network of zombie computers programmed to receive commands without the owners' knowledge. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hard coding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent, or the Trojan may contain one. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents. In some cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback, organized by the group Anonymous. These attacks can use different types of internet packets such as: TCP, UDP, ICMP etc.

Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DoS. These flood attacks do not require completion of the TCP three way handshakes and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a denial-of-service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack.

3. DDOS

Distributed denial-of-service attacks on root name servers are Internet events in which distributed denial-of-service attacks target one or more of the thirteen Domain Name System root name server clusters. The root name servers are critical infrastructure components of the Internet, mapping domain

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1999 – 2003
RECEIVED: 15-03-2017. PUBLISHED: 04-04-2017.
April 04, 2017

names to IP addresses and other resource record (RR) data. Attacks against the root name servers could, in theory, impact operation of the entire global Domain Name System, and thus all Internet services that use the global DNS, rather than just specific websites. However, in practice, the root name server infrastructure is highly resilient and distributed, using both the inherent features of DNS (result caching, retries, and multiple servers for the same zone with fallback if one or more fail), and, in recent years, a combination of any cast and load balancer techniques used to implement most of the thirteen nominal individual root servers as globally distributed clusters of servers in multiple data centers.

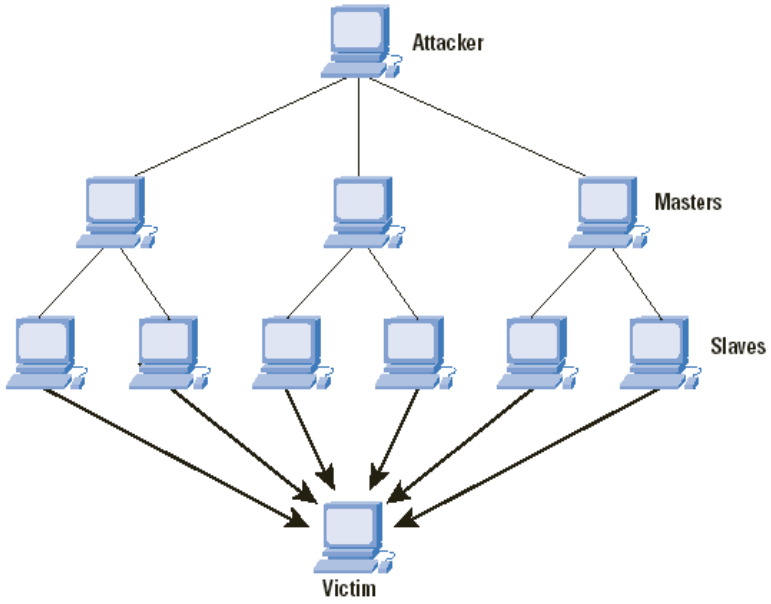

Fig..1. DDOS ATTACK

In particular, the caching and redundancy features of DNS mean that it would require a sustained outage of all the major root servers for many days before any serious problems were created for most Internet users, and even then there are still numerous ways in which ISPs could set their systems up during that period to mitigate even a total loss of all root servers for an extended period of time: for example by installing their own copies of the global DNS root zone data on name servers within their network, and redirecting traffic to the root server IP addresses to those servers. Nevertheless, DDoS attacks on the root zone are taken seriously as a risk by the operators of the root name servers, and they continue to upgrade the capacity and DDoS mitigation capabilities of their infrastructure to resist any future attacks.

4. PROPOSED WORK

Our solution called Denial Contradictions with Fictitious Node Mechanism (DCFM) relies on the internal knowledge acquired by each node during routine routing, and augmentation of virtual (fictitious) nodes. Moreover, DCFM utilizes the same techniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as network size increases, which is consistent with general claim that OLSR functions best on large networks.

DCFM is unique in that all the information used to protect the MANET stems from the victim's internal knowledge, without the need to rely on a trusted third party. In addition, the same technique used for the attack is exploited in order to provide protection. By learning local topology and advertising fictitious nodes, a node is able to deduce suspect nodes and refrain from nominating them as a sole MPR, thus, sidestepping the essential element of the attack

Advantages:

- DCFM successfully prevents the attack, specifically in the realistic scenario in which all nodes in the network are mobile.
- it was discovered that as node population increases in density and size, the closer DCFM overhead is to OLSR.
- OLSR functions best in dense large networks, DCFM can function without real additional cost.

5. Implementation

Node Creation

This module is developed to node creation and more than 50 nodes placed particular distance. Mobile nodes placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

Zone Partition

It features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. It uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner.

Data Routing

After the hierarchical zone partition process, the source and destination claimed to be in different zones. The source node sends the data to destination through the intermediate relay nodes. The user data gram protocol is used to transfer the data routing from one relay node to next relay node.

OLSR Working Process

The main objective of the OLSR Protocol is to provide a security to the MANET by means of trust extended authentication mechanism. The proposed setup a temporary destination TD and informs to all mobile nodes in the network, so that the attacker concentrates only on TD to hack the data. By means of diverting the attacker's concentration the data from source is delivered to original destination in secure manner.

Key Server Management

The extended technique or proposed technique of this project is key server management. In this mechanism doesn't suitable for heavier traffic condition since OLSR is a light weight trusting mechanism. So in order to overcome this issue key server management technique is proposed. Through KSM (key server management) technique provides a more authentication and secure transmission than new mechanism through data encryption and decryption technique.

CONCLUSION

DCFM is unique in that all the information used to protect the MANET stems from the victim's internal knowledge, without the need to rely on a trusted third party. In addition, the same technique used for the attack is exploited in order to provide protection. By learning local topology and advertising fictitious nodes, a node is able to deduce suspect nodes and refrain from nominating them as a sole MPR, thus, side-stepping the essential element of the attack. Simulation shows that DCFM successfully prevents the attack, specifically in the realistic scenario in which all nodes in the network are mobile. In addition, it was discovered that as node population increases in density and size, the closer DCFM overhead is to OLSR. Given that OLSR functions best in dense large networks, DCFM can function without real additional cost.

REFERENCE

[1] C. E. Perkins and P. Bhagwat, "Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers," in Proc. Conf. Commun. Archit., Protocols Appl., 1994, pp. 234–244.

[2] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in Proc. IEEE Int. Multi Topic Conf. Technol., 2001, pp. 62–68.

[3] 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

[4] D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," Dynamic Source Routing Protocol (DSR) Mobile Ad Hoc Netw. IPV4, 2007. [Online]. Available: http://tools.ietf.org/html/rfc4728

[5] C. Perkins and E. Royer "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., Feb. 1999, pp. 90–100.

[6] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in Proc. 32nd IEEE Conf. Local Comput. Netw., Oct. 2007, pp. 1043–1052.

[8] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proc. Med-Hoc-Net, 2003, pp. 25–27.