Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks 5 (2007) 613–625
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Analysis of area-congestion-based DDoS attacks in ad hoc networks

Qijun Gu [a], Peng Liu [b,*], Chao-Hsien Chu [b]

[a] Department of Computer Science, Texas State University, San Marcos, TX 78666, United States
[b] School of Information Sciences and Technology, Pennsylvania State University, 313G IST Building, University Park, Pennsylvania, PA 16802, United States

Received 8 September 2004; received in revised form 28 September 2005; accepted 11 April 2006
Available online 15 May 2006

Abstract

Increased instances of distributed denial of service (DDoS) attacks on the Internet have raised questions on whether and how ad hoc networks are vulnerable to such attacks. This paper studies the special properties of such attacks in ad hoc networks. We examine two types of area-congestion-based DDoS attacks – remote and local attacks – and present in-depth analysis on various factors and attack constraints that an attacker may use and face. We find that (1) there are two types of congestion – self congestion and cross congestion – that need to be carefully monitored; (2) the normal traffic itself causes significant packet loss in addition to the attack impacts in both remote and local attacks; (3) the number of flooding nodes has major impacts on remote attacks while, the load of normal traffic and the position of flooding nodes are critical to local attacks; and (4) given the same number of flooding nodes and attack loads, a remote DDoS attack can cause more damage to the network than a local DDoS attack.

Keywords: Ad hoc network; Security; Congestion; Distributed denial of service; Denial of service

1. Introduction

DDoS attacks present a serious threat to network computing and have recently attracted much attention [1–6]. When a DDoS attack is launched, a large number of hosts controlled by the attackers flood a target with a high volume of packets to significantly degrade the target's service performance or render it unable to deliver any service. Ad hoc networks differ from the Internet in several critical ways that make them especially vulnerable to DDoS attacks. First, ad hoc nodes are peers. Because of this, once an attacker compromises a node, they can attack the network from inside. Second, every node in an ad hoc network is not only a host but also a router. Thus, it is harder to determine whether a suspicious packet is from an attacker or relayed from a legitimate node. These features indicate that there may be "easier" ways to cause denial of service (DoS) in ad hoc networks than in the Internet, and that existing Internet DDoS defense mechanisms may not be enough to counter DDoS attacks in ad hoc networks.

* Corresponding author. Tel.: +1 814 863 0641.
E-mail address: pliu@ist.psu.edu (Q. Gu).

1570-8705/$ - see front matter
doi:10.1016/j.adhoc.2006.04.002

Although congestion was recognized as a simple and effective DoS attack approach in ad hoc networks, previous studies mainly focused on individual attackers and the attack impacts on individual nodes and traffic flows. In an ad hoc network, it is easy for attackers to attack simultaneously from distributed locations; however, it is not clear how damaging the attacks can be and what are the unique characteristics of the attacks. Due to the relative newness of these concerns, more research on the properties and methods of DDoS attacks in ad hoc networks is needed.

Motivated by these observations, we explore the possible DDoS attacks and their impacts on ad hoc networks. In particular, we investigate how attackers flood legitimate routes with junk packets. Because wireless bandwidth is limited, the junk packets can easily cause severe wireless channel contention among nearby nodes on the legitimate routes. Therefore, the attack creates network-wide congestion instead of congestion surrounding only the destination as in conventional Internet DDoS attacks. In this paper, we explore and discuss two types of congestion – self and cross congestions – that may be caused by attacks. We analyze the important factors that may affect the attacks. We also review the existing defense mechanisms against these DDoS attacks. This research lays the necessary foundation for developing more effective defense strategies against DDoS attacks in ad hoc networks.

2. Background

In this section, we present background information on DDoS and DoS attacks and review related works.

2.1. DDoS attacks

In the Internet, attackers can launch a DDoS attack from a huge number of hosts to conquer a few target servers. Many attacking approaches have been identified. For example, attackers can send a flood of SYN packets to block one of the server's TCP ports [7], flood the targets with misformed ICMP echo packets [8], or bruteforcely flood them with UDP packets [9]. Since most flooding packets in DDoS attacks are sent out with spoofed source addresses, much research on defense has focused on identifying the true flooding sources, tracing back to those sources, and filtering out the flooding packets. Aura et al. [10] proposed letting the server ask the client to respond to a cookie or solve a puzzle when the client requests connection to the server. If the client is spoofed, no reply will come from a spoofed machine, or the real attacker will be overwhelmed by the server's response requests. Ferguson et al. [1] proposed the ingress filtering technology to filter packets with a spoofed address outside the attacker's network. Mirkovic et al. [4] proposed D-WARD to set a rate limit for a suspicious flow that does not match its normal model. With the help of routers that embed trace information in a number of normal packets, the victim can figure out the real attack sources based on trace back [2,11]. Pi [5] lets the victim identify the flooding source by putting unique path identifiers in packets. Push back [3,12] identifies attack aggregates in congested routers. SAVE [13] requires routers to verify the source address of incoming packets. In SIFF [6], routers manipulate the marking fields in packets so that an end-host can selectively stop individual flows from reaching its network. A comprehensive overview and classification of DDoS attacks and defense approaches can be found in [14].

A major characteristic of DDoS attacks in the Internet is that the attacking sources are end hosts that connect to the Internet from their access networks and are remote to the victim. To take over the target, the flooding packets travel through the Internet from the flooding sources to the target. In an ad hoc network, this kind of attack approach is not the only choice for attackers. Since ad hoc nodes are inside the network, the attackers are closer to the target and can directly congest it. The attackers can also redirect and forward traffic to the target instead of generating junk packets by themselves. In addition, because mobile nodes are no longer the end hosts in an ad hoc network, attackers can bypass the defending nodes. Hence, it is important to clearly understand the possible new features of such attacks and how DDoS attacks can be prevented in an ad hoc network.

2.2. DoS attacks in ad hoc networks

There are many approaches to launching DoS attacks in an ad hoc network. In the physical layer, jamming can be used to disrupt and suppress normal transmission [15]. In the MAC layer, the attackers can exploit defects of MAC protocol messages and procedures. For instance, in the 802.11 MAC protocol, the attackers can provide bogus duration infor-