# TDFA: Traceback-Based Defense against DDoS Flooding Attacks



| | |
|---|---|
| Title | TDFA: Traceback-Based Defense against DDoS Flooding Attacks |
| Publication Type | Conference Paper |
| Year of Publication | 2014 |
| Authors | Foroushani, V.A., Zincir-Heywood, A.N. |
| Conference Name | Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on |
| Date Published | May |
| Keywords | attack packets, attacking traffic, Bandwidth, Computer crime, computer network security, DDoS Attack, DDoS flooding attacks, detection component, Deterministic Flow Marking, distributed denial of service attack, Filtering, Image edge detection, Internet, IP networks, IP Traceback, network security problems, packet filtering, packet forwarding rate, Protocols, quality of service, spoofed IP addresses, TDFA, telecommunication traffic, trace back component , traceback-based defense, Traffic Control, traffic control component |

Abstract

Distributed Denial of Service (DDoS) attacks are one of the challenging network security problems to address. The existing defense mechanisms against DDoS attacks usually filter the attack traffic at the victim side. The problem is exacerbated when there are spoofed IP addresses in the attack packets. In this case, even if the attacking traffic can be filtered by the victim, the attacker may reach the goal of blocking the access to the victim by consuming the computing resources or by consuming a big portion of the bandwidth to the victim. This paper proposes a Trace back-based Defense against DDoS Flooding Attacks (TDFA) approach to counter this problem. TDFA consists of three main components: Detection, Trace back, and Traffic Control. In this approach, the goal is to place the packet filtering as close to the attack source as possible. In doing so, the traffic control component at the victim side aims to set up a limit on the packet forwarding rate to the victim. This mechanism effectively reduces the rate of forwarding the attack packets and therefore improves the throughput of the legitimate traffic. Our results based on real world data sets show that TDFA is effective to reduce the attack traffic and to defend the quality of service for the legitimate traffic.

URL https://ieeexplore.ieee.org/document/6838719
DOI 10.1109/AINA.2014.73
Citation Key 6838719

attack packets attacking traffic Bandwidth Computer crime computer network security DDoS Attack DDoS flooding attacks detection component Deterministic Flow Marking distributed denial of service attack Filtering Image edge detection internet IP networks IP Traceback network security problems packet filtering packet forwarding rate Protocols quality of service spoofed IP addresses TDFA telecommunication traffic trace back component traceback-based defense traffic control traffic control component