ABSTRACT

A flooding attack is an attempt to make an online service unavailable by 'flooding' it with unsolicited traffic from multiple sources, thereby leading to denial of service. The target could be a wide variety of important resources, like government websites or business and news websites, etc., and thus present a major threat to the services provided by the internet. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies, also called "botnets". Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. Such an attempt of flooding attack is also called distributed denial of service attack or DDoS attack. For a website under flooding attack, it means that the site will not be available leading the customers from making any purchases, view content, or log into accounts. For networks, such attacks can cause bandwidth saturation or even incapacitate network infrastructure. Also there is the problem of flash crowds, which are legitimate flows but have very similar properties to that of flooding attack, in terms of internet traffic, which makes flooding attack detection more challenging. In our approach to combat flooding attack, we are employing the concept of information theory. We try to quantify the difference between malicious traffic and legitimate traffic based on probability distributions. Here our focus is on the target-end of the network. We illustrate the use of Renyi's entropy metric and also α-divergence measure between the probability densities of traffic samples, along with the average http request response time, thereby differentiating the traffic behavior. Our simulations using datasets like those of CAIDA and UCLA packet traces show that our approach is competent to handle such flooding attacks.

Keywords: Distributed Denial of Service (DDoS), probability distribution, Renyi's entropy, α-divergence.