Abstract

A Distributed Denial of Service (DDoS) attack is an explicit attempt by an attacker to disrupt an online server or make it unavailable by overwhelming it with unsolicited traffic from multiple sources, thereby consuming the entire bandwidth of the target. The target could be a wide variety of important resources, from banks to news websites etc. and thus present a major threat to the service 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 co-ordinated, large-scale attack against one or more targets. For networks, DDoS attacks can cause bandwidth saturation or even inundate network infrastructure, causing widespread outages to customers on the entire network. Also, there is the problem of flash crowds, which are legitimate flows but have very similar properties to that of DDoS attack, in terms of internet traffic, thus making DDoS attack detection more challenging. In this work, we empirically evaluate F-divergence measures, namely Kullback-Leibler divergence, Hellinger distance, Total Variation Distance and Alpha divergence between the probability distribution of traffic samples in their ability to detect DDoS flooding attacks. We evaluated the method on number of intrusion benchmark datasets to illustrate the efficiency and effectiveness of each measure for DDoS attack detection.

Keywords: Distributed Denial of Service (DDoS), probability distribution, F-divergence.