Abstract

Distributed denial of service (DDoS) attack is an ever challenging problem with the increasing number of tools and advanced techniques. Most DDoS attacks are carried out using sophisticated tools and botnets maintaining a varied packet transmission rate and packet types in order to overcome detection techniques. In this dissertation we propose a DDoS detection mechanism based on packet arrival pattern regardless of attack methods and packet types. Since DDoS attacks are carried out using existing tools and botnets they inherits some repeatable patterns which are different from the characteristic of a normal traffic . Based on this we proposed a detection method using coefficient of variation on the packet arrival rate to distinguish probable patterns during attack followed by refined analysis for confirmation. Our extensive experiments with existing benchmark datasets confirmed the theoretical analysis and establish effectiveness of the proposed method in near real time scenario.

Keywords: DDoS attacks, Coefficient of Variation, Least Square Method, Pearson Correlation Coefficient, Traffic patterns