Heterogeneous Tracers against DDoS Attacks

王俊鑫,張大鈞
Computer Science & Information Engineering
Computer Science and Informatics
chwang@chu.edu.tw

Abstract

To solve the DoS/DDoS problems efficiently, the first things is to locate the attack origins and then cooperate the filter(s) nearby for dropping abnormal packets in time. The original routers can't provide these functions such as tracking, filtering, and etc. They have to be enhanced with additional functions to defend DoS/DDoS attacks. We refer the enhanced routers as tracers. According to the characteristic, cost and necessity of tracers, three kinds of heterogeneous tracers are selected, namely tunneling-enabled tracers, marking-enabled tracers and filteringenabled tracers. The tunneling-enabled tracers with the lowest cost can alter the path of the passing packets to destination easily. In this paper, we study how to use tunneling-enabled tracers efficiently to forward packets to the best marking-enabled or filtering-enabled tracer for locating attack origins and filtering abnormal packets in time. Four methods are proposed and compared with the optimal solution. The fourth method with the assistance of marking-enabled tracers has the best performance of protecting network bandwidth by simulation result.

Keyword：DDoS, Tracers