计算机应用 2007 27 (08): 1884-1887 ISSN: 1001-9081 CN: 51-1307/TP

网络与信息安全

基于Multi-stream Combined隐马尔柯夫模型源端检测DDoS攻击

康健[1];李强[1];张原[1]

吉林大学计算机科学与技术学院[1]

收稿日期 2007-2-13 修回日期 网络版发布日期 2007-8-27 接受日期

摘要 提出了一种新颖的综合考虑多维观测特征的DDoS攻击源端检测方法。该方法引入S-D-P特征概念，并抽取TCP/IP包头中的标志位和ID字段构成多维观测特征，采用Multi-stream Combined隐马尔可夫模型（MC-HMM）在源端网络检测DDoS攻击。大量实验表明,MC-HMM方法克服了基于一维观测特征的检测算法信息量过小的固有缺陷，能够有效降低检测的误报率和漏报率，提高DDoS攻击源端检测精度。

Abstract A new approach for DDoS attacks detection was proposed in source-end network. This approach used Multi-stream Combined Hidden Markov Model (MC HMM) for integrating multi-features simultaneously. The multi-features included the S-D-P feature, TCP header control flags, and IP header ID field. Experiments show that the approach effectively reduces false positive rate and false negative rate, and detection precision of MC-HMM based on multiple detection features is clearly higher than that of the algorithms based on single-feature.

关键词 分布式拒绝服务攻击 隐马尔柯夫模型 源端检测

Key words DDoS attacks;Hidden Markov Model (HMM);source-end detection

分类号

DOI:

通讯作者:
康健 kj885788@gmail.com; kangjian@jlu.edu.cn

作者个人主页: 康健 李强 张原