计算机工程　2007 33 (16): 139-141　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于流连接信息熵的DDoS攻击检测算法

赵继俊，胡志刚，张 健

(中南大学信息科学与工程学院，长沙 410083)

收稿日期　修回日期　网络版发布日期 2007-8-15　接受日期

摘要　分析了分布式拒绝服务(DDoS)攻击的特点，提出了流连接信息熵的定义，并通过对流连接信息熵时间序列的分析，采用非参数CUSUM算法进行DDoS攻击检测。该检测方法对固定IP、端口号随机变化的DDOS攻击有比较好的检测效果。实验结果证明，该方法能够以较高的精确度及时地检测出DDoS 攻击行为。

关键词　分布式拒绝服务攻击；相关数据包；流连接信息熵；非参数CUSUM算法

分类号　TP393

DOI:

对应的英文版文章：071651

通讯作者:

作者个人主页:

赵继俊;胡志刚;张 健