计算机工程与应用 2009 45 (27): 88-91 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种面向DDoS攻击的网络安全态势评估方法

李 珂[1，3]，连一峰[1，2，3]

1.中国科学院 研究生院 信息安全国家重点实验室，北京 100049
2.中国科学院 软件研究所，北京 100190
3.中国科学院 研究生院，北京 100190

收稿日期 2008-11-3 修回日期 2009-2-26 网络版发布日期 2009-9-28 接受日期

摘要 从网络拥塞对应用服务器及网络结构造成的影响出发，引入图论的相关算法，提出一种面向DDoS攻击的网络安全态势评估方法，根据拥塞链路与服务器的距离以及拥塞链路是否处于网络映射图的最小边割集内，计算攻击行为对网络安全态势的影响值，以此进行态势的量化分析。最后使用网络仿真工具验证了该方法的适用性。

关键词 安全态势 态势评估 DDoS攻击 图论 链路拥塞度

分类号 TP393.08

Method of network security situation assessment under DDoS attacks

LI Ke[1，3]，LIAN Yi-feng[1，2，3]

1.State Key Laboratory of Information Security，Graduate University，Chinese Academy of Sciences，Beijing 100049，China
2.Institute of Software，Chinese Academy of Sciences，Beijing 100190，China
3.Graduate University，Chinese Academy of Sciences，Beijing 100190，China

Abstract

This paper analyzes the impacts that all congested links cause on application servers and network architecture，introduces graph algorithms and presents a new method to assess the network security situation under DDoS attacks，which computes the influence value that attacks cause on network security situation according to the distance between the congested link and application server and whether the link is in the min-cut set，and this value is used for quantitative situation assessment.The applicability of this method is verified by simulated experiments with the network simulation tool.

Key words security situation situational assessment DDoS attack graph theory link-congestion degree

DOI: 10.3778/j.issn.1002-8331.2009.27.027

通讯作者 李 珂 like@is.iscas.ac.cn