

网络、通信、安全

防TTL值欺骗的数据包标记算法研究

刘渊^{1,2}, 李秀珍², 朱晓键²

1.南京理工大学 计算机学院, 南京 210094

2.江南大学 信息工程学院, 江苏 无锡 214122

收稿日期 2007-10-17 修回日期 2008-1-11 网络版发布日期 2008-8-5 接受日期

摘要 分布式拒绝服务攻击是目前最难处理的网络难题之一, 针对分布式拒绝服务攻击提出了多种应对方案, 这些方案都各有优缺点, 但其中自适应概率包标记受到了广泛地重视和运用。针对攻击者对TTL初始值的伪造提出了一种自适应策略, 有利于防止TTL值的伪造, 减少路由器处理器的负担, 节省了IP包头的空间。

关键词 [分布式拒绝服务](#) [包标记](#) [自适应概率包标记](#) [IP回溯](#)

分类号

Research on packet marking algorithm resisted spoofed TTL value

LIU Yuan^{1,2}, LI Xiu-zhen², ZHU Xiao-jian²

1.School of Computer, Nanjing University of Science & Technology, Nanjing 210094, China

2.College of Information Engineering of Southern Yangtze University, Wuxi, Jiangsu 214122, China

Abstract

Distributed Denial of Service (DDoS) attack is among the hardest network problems. To reply it, many kinds of schemes of countermeasures are proposed, these schemes all respectively have the good and bad points. But among these, an Adaptive Probabilistic Packet Making (APPM) is promising and using. In this paper, based on the spoofed initial TTL value by the attacker, an adaptive marking scheme is improved, which is advantageous to resist spoofed TTL value, to reduce the router burden and save the IP packet's space.

Key words [Distributed Denial of Service \(DDoS\)](#) [packet marking](#) [Adaptive Probabilistic Packet Making \(APPM\)](#) [IP traceback](#)

DOI: 10.3778/j.issn.1002-8331.2008.23.039

通讯作者 刘渊 mblxz@yahoo.com.cn

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(556KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [复制索引](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ 本刊中 包含“分布式拒绝服务”的 [相关文章](#)

▶ 本文作者相关文章

· [刘渊](#)

·

· [李秀珍](#)

·

· [朱晓键](#)