通过流量和数据包综合估计内网感染蠕虫概率的研究

http://www.firstlight.cn 2010-01-01

提出了一种分析内网感染蠕虫可能性大小的方法。对通过内网交换机上的数据包使用蠕虫行为进行分析，得到行为异常的数据包数量，然后使用AR模型分析异常数据包的数量得到异常数据包的增长率；对内网异常流量和异常数据包增长率加权，并对它们综合估计得到内网中感染蠕虫概率的大小。实验表明该方法有效可行。

存档文本