随机公平队列对UDP洪流的抑制效果分析

于 明
(大连理工大学电子与信息工程学院 大连 116024)

摘 要 随机公平队列(Stochastic Fairness Queueing,SFQ)是一种典型的公平队列调度算法。UDP洪流是实施DDoS攻击的一种主要攻击手段。研究了SFQ调度和网络中广泛应用的先到先服务(First Come First Server,FCFS)队列调度策略对UDP洪流攻击的抑制效果。基于多协议网络模拟平台NS2的仿真结果表明,FCFS调度难以对UDP洪流攻击产生有效的抑制作用,而SFQ调度却能在一定程度上抑制该攻击。

关键词 UDP洪流,队列调度,DDoS,SFQ,攻击抑制
中图法分类号 TP393.08 **文献标识码** A

Analysis of Mitigating UDP Flooding by Stochastic Fairness Queueing

YU Ming
(School of Electronic and Information Engineering, Dalian University of Technology, Dalian 116024, China)

Abstract Stochastic Fairness Queueing (SFQ) is a typical implementation of Fair Queueing (FQ). UDP flooding is a common way to launch a DDoS attack. In this paper, a comparative study was made between the widely used FCFS (First Come First Served) and SFQ on their efficacy in mitigating UDP flooding. Simulation results based on Network Simulator 2 show that FCFS has little effect on UDP flooding mitigation while SFQ is more effective.

Keywords UDP flooding, Queue scheduling, DDoS, SFQ, Attack mitigation

UDP洪流攻击是DDoS攻击的一种主要攻击形式,是基于UDP协议而发起的。UDP协议是一种无连接协议,它在传送数据时无需进行连接建立操作。当攻击者实施UDP洪流攻击时,会利用伪造的IP地址向某个或某些随机选择的或特定的目标机器端口发送大量的UDP报文。目标机器收到UDP报文后会将其交给相应端口的进程处理。若该端口没有处于监听状态的进程,目标机器就会向报文的源地址发送一个ICMP报文,指明"目的端口不可达"。大量发送到目标机器封闭端口的UDP报文连同返回的ICMP报文不仅会使目标机器发生宕机现象,而且会大量占用其所在网段的带宽,从而影响到目标主机所在网络的正常运行。

随机公平队列(Stochastic Fairness Queueing,SFQ)[1]是一种典型的公平队列调度方式,它只需要很小的计算量即可实现较高的公平度。SFQ调度的核心是"流"(针对UDP数据)或"连接"(针对TCP数据)。数据流量被分配到多个先进先出(First In First Out,FIFO)队列中,每个FIFO队列对应一个流或一个连接,数据按照简单轮转的方式发送,每个流或连接都按顺序得到发送机会。这种调度方式保证了每一个流或连接都不会被其它流量所淹没。SFQ的"随机性"主要表现为它并不是真的为每一个流或连接创建一个队列,而是使用一个散列算法,把所有的流或连接映射到有限的几个队列中去。因为使用了散列,所以可能会有多个流或连接被分配到同一个队列里,从而使得这些流或连接需要共享分组发送的机会,也就是共享带宽。

本文将SFQ与UDP洪流抑制联系到一起,主要是基于这样一种认识,即UDP洪流(以及其它类型的洪流攻击,如SYN洪流等)实质上是对网络资源的一种滥用,而对网络资源的竞争性使用进行管理恰恰是实施队列调度策略的主要目的之一[2]。因此,在DDoS防御中选择适当的队列调度策略,有可能会对UDP洪流等DDoS攻击实现某种程度的抑制。事实上,Felix Lau等人已在仿真中发现[3],基于类的队列(Class-Based Queuing,CBQ)调度在目标系统遭受UDP洪流攻击时能够为某些正常用户保留一定的可用带宽,从而削弱UDP洪流的破坏性。相比而言,本文立意的新颖性在于没有将网络流量进行分类或分级,而是着眼于在计算机和通信网中广泛使用的公平队列调度策略,假设攻击流和正常用户流均具有相同的链路使用权限,重点研究了具有公平、无类别特征的SFQ调度对UDP洪流攻击的抑制效果。本文立意的合理性在于:

(1)在实际应用中,服务器常常会为不同的应用确定不同的服务优先级,但对同一应用中的不同用户流量却很少进行区分。

(2)DDoS攻击往往都是针对某一种应用而发起的,因而攻击源可视作同一应用中的不同用户。

(3)对于同时针对多种应用发起的DDoS攻击来说,其资源耗尽的效果相当于针对每一种应用进行攻击的资源耗尽效果之和。

为了说明SFQ调度抑制UDP洪流攻击的有效性,本文

到稿日期:2008-10-28 返修日期:2009-01-07 本文受国家"863"计划课题(2005AA123910)资助。
于 明(1975-),男,博士,讲师,主要研究方向为网络对抗与信息安全,E-mail:yu_ming1111@hotmail.com。

同时考察了当前网络中广泛应用的先到先服务(First Come First Server,FCFS)调度策略对 UDP 洪流攻击的抑制效果,并将二者进行了对比。

1 研究方案设计

本文选择了多协议网络模拟平台 Network Simulator 2(NS2)[4]作为主要仿真工具,利用 NS2 中基于 UDP 协议的固定速率分组流实现了对 UDP 攻击流的仿真。攻击仿真的基本步骤如图 1 所示。其中最重要的就是 Otcl 脚本的编写,它完成的任务主要是:(i)配置仿真环境中的网络拓扑结构并设置相关链路的基本特性,如延迟、带宽和调度策略等;(ii)建立协议代理,包括端设备的协议绑定和通信业务量模型的建立;(iii)配置业务量模型的参数;(iv)设置 Trace 对象,以便把仿真过程中发生的特定类型的时间记录在 Trace 文件中(NS2 通过 Trace 文件来保存整个仿真过程,仿真完成后,用户可以对 Trace 文件进行分析研究);(v)设置其他辅助过程及仿真结束时间。

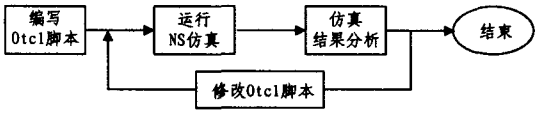

图 1 利用 NS2 进行攻击仿真的基本步骤

仿真环境中的网络拓扑结构如图 2 所示。其中,正常用户节点有 10 个,分别标记为 N1～N10;攻击节点有 6 个,分别标记为 N11～N16;正常用户节点和攻击节点分布于 7 个源端网络中,相应的源端网络接入路由器标记为 R_2～R_8;中间的广域传输网络等效为路由节点 R_1,被攻击网络等效为路由节点 R_9,二者之间的链路为仿真过程中的瓶颈链路。

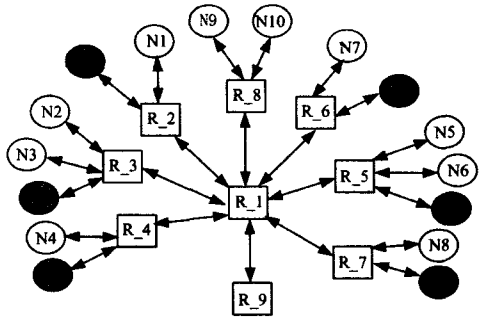

图 2 仿真环境的网络拓扑

据统计,因特网上 95%的字节以及 90%的数据包都是使用 TCP 协议进行传输的[5],因此本文将仿真环境中正常用户的流量均设置为 TCP 流。仿真环境中的其他参数设置如下:(i)用户链路的带宽为 1Mbps,时延为 5ms,用户分组大小为 1kB,链路缓存容量为 50 个分组,各用户在 0～5s 内随机发起连接;(ii)路由节点间的链路带宽为 2Mbps,时延为 20 毫秒,链路缓存容量为 50 个分组;(iii)瓶颈链路的缓存容量为 60 个分组;(iv)攻击流分组的大小为 1kB;(v)攻击源采用匀速发送的方式产生攻击流,并在 2～3s 内随机发起攻击。

本文衡量 UDP 攻击流是否被有效抑制的主要指标是瓶颈链路中所有正常用户的吞吐率总和。判断 UDP 攻击流被抑制的依据是:瓶颈链路中正常用户的总吞吐率越高,低吞吐率持续的时间越短,说明攻击流被抑制的效果越好。图 3 给出了对仿真结果进行处理的程序流程框图。

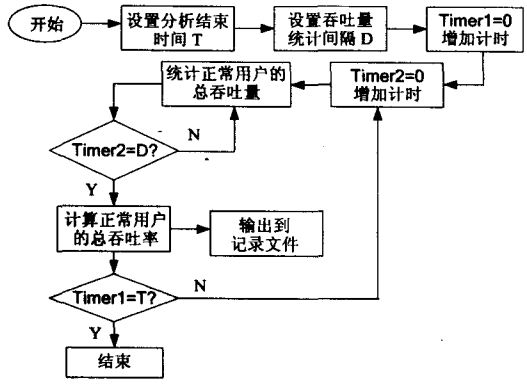

图 3 计算瓶颈链路中正常用户总吞吐率的程序流程框图

2 攻击流抑制效果分析

2.1 SFQ 抑制攻击流的有效性分析

将攻击流的发送速率设置为 0.4Mbps。FCFS 和 SFQ 均采用 NS2 中默认的参数设置,即在 FCFS 调度中,队列分组缓冲容量为 50;在 SFQ 调度中,"散列队列数目"(NS2 中用变量 buckets 表示该参数)设置为 16。仿真结果如图 4 所示。

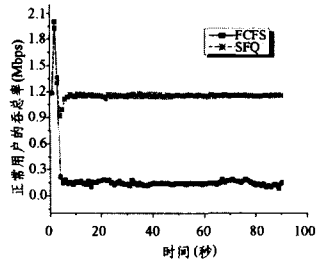

图 4 攻击速率为 0.4Mbps 时正常用户的总吞吐率

从仿真结果来看,SFQ 调度对攻击流具有更好的抑制效果。为了避免参数设置的差异对处理结果的影响,需要改变两种调度方式的配置参数并对相同设置下的攻击流重新进行仿真。在 NS2 的算法实现中,FCFS 调度的关键参数是队列的分组缓冲容量,SFQ 调度的关键参数是反映分组流映射队列数目的 buckets 变量。仿真试验结果表明,改变 FCFS 调度的队列缓冲容量对用户的总吞吐率没有明显的改善,FCFS 对攻击流的抑制效果与图 4 中的结果类似。但是,改变 SFQ 调度中的 buckets 参数,却极大地影响到 SFQ 对攻击流的抑制效果。图 5 分别给出了在攻击源数目为 6、buckets 变量分别设置为 4,8 和 16 时的仿真试验结果。

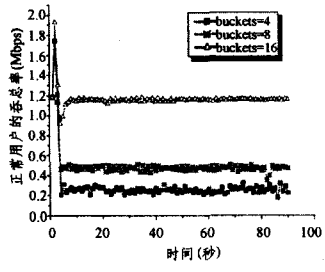

图 5 改变 buckets 参数后正常用户的总吞吐率

上述仿真结果表明:

(1)在非优先级、无类别的网络流量管理环境中,FCFS 调度难以对攻击流产生有效的抑制作用,而具有公平性特征的 SFQ 调度却能在一定程度上抑制攻击。由于 FCFS 调度

不能保证对网络业务流的公平性，而正常业务流在发生分组丢失后又会主动降低发送速率，从而使攻击流能够占据目标网络大部分甚至全部的带宽资源。与之相反，SFQ 调度能够保证网络业务流对带宽占用的公平性，因而使攻击流受到了很大的抑制。在本文仿真中，正常业务流和攻击流的数量之比为 10:6，按照公平性原则，正常业务流的吞吐率应占据瓶颈链路总吞吐率的 62.5%，即 1.25Mbps，这与图 4 的结果是相吻合的。

(2)SFQ 调度对攻击流的抑制作用与其分组流映射队列参数(即变量 buckets)有关。由图 5 可以看出，改变 buckets 参数会对 SFQ 抑制攻击流的效果产生很大的影响：当 buckets 的数值小于实际网络数据流的总量时，buckets 越小，SFQ 调度对攻击流的抑制作用就越弱。所以，当目标网络所服务的正常用户较多时，提高 buckets 的取值可以对 UDP 洪流类 DDoS 攻击产生抑制效果。

2.2 SFQ 抑制攻击流的稳健性分析

提高攻击流的发送速率是攻击者用于增强攻击流破坏性的一种常用手段。由 4.1 节的讨论结果可知，FCFS 调度对攻击流难以产生有效的抑制作用，因而其对攻击者提高攻击流发送速率以增强攻击破坏性的行为也无抑制能力。那么，此时 SFQ 调度对攻击流的抑制是否会受到影响。2.1 节的仿真结果表明，在 SFQ 调度下，SFQ 对 UDP 洪流的抑制效果取决于网络数据流总数与 buckets 变量的取值，因此可以设想，当实际网络数据流总数小于 buckets 的取值时，SFQ 调度依然能够对提高发送速率后的攻击流产生有效的抑制作用。只有当攻击流数目大于 buckets 的取值时，SFQ 的抑制作用才有可能被削弱。图 6 给出了对于上述结论的仿真试验结果。

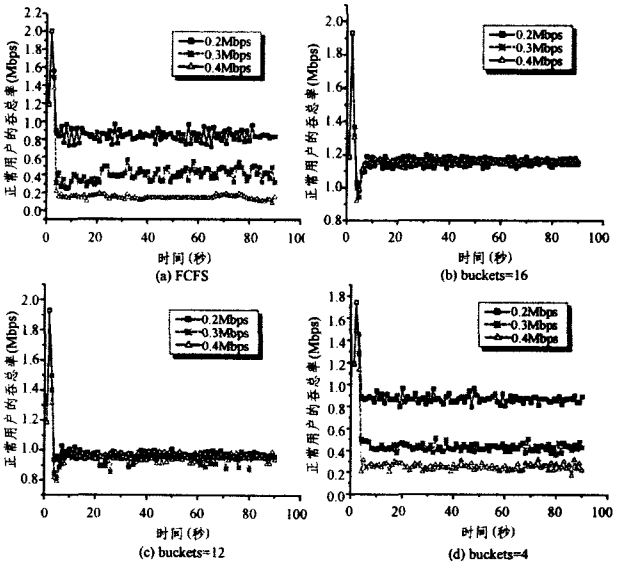

图 6 攻击源总数一定、不同的攻击流发送速率下正常用户的总吞吐率

降低攻击流的发送速率是攻击者躲避防御方检测的一种手段。在攻击源数目一定的情况下，降低攻击流发送速率可能会削弱攻击流的破坏性。因此，攻击方往往通过增加攻击源的数目来保证一定的攻击流破坏性。图 7 分别给出了攻击仿真环境中 FCFS 和 SFQ 对不同的攻击源数目及不同的攻击流发送速率下攻击流的抑制效果。图中，(0.2,6,1.2)表示攻击源的发送速率为 0.2Mbps，攻击源数目为 6，攻击流在目标网络处的汇聚速率为 1.2Mbps。其他表示与此类似。从图 7 中可以看出：

(1)在降低攻击流发送速率的同时增加攻击源的数目，可以获得与高速攻击流情况下相同的破坏效果。

(2)在增加攻击源数目的同时也削弱了 SFQ 调度对攻击流的抑制效果。

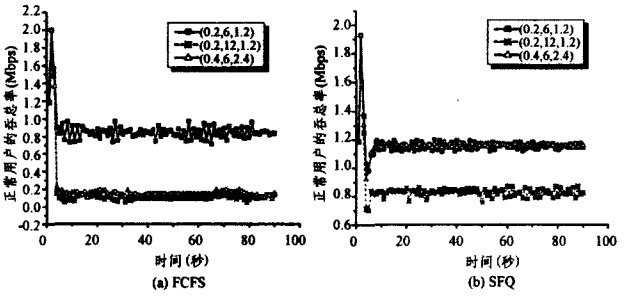

图 7 不同的攻击源数目及攻击流发送速率下正常用户的总吞吐率

结束语 DDoS 攻击是当前威胁因特网安全运行的“顽疾”之一。如何有效地实现对 DDoS 攻击的检测、追踪和抑制，一直是网络安全领域研究的热点。本文分别从有效性和稳健性两个方面研究了具有公平、无类别特征的 SFQ 调度对 UDP 洪流攻击的抑制效果，并对比研究了当前网络中广泛应用的 FCFS 调度策略对 UDP 洪流攻击的抑制效果。仿真结果表明，(i)FCFS 调度难以对攻击流产生有效的抑制作用；(ii)SFQ 调度能够在一定程度上抑制攻击；(iii)攻击方必须保证有足够数目且同时处于攻击状态的攻击源时才能够对抗目标方所采取的类似于 SFQ 之类的公平调度方式。这说明，防御方通过合理地选择调度策略可以对 DDoS 攻击流产生一定的抑制效果。在 DDoS 防御日趋艰难的今天，希望本文能够起到抛砖引玉的作用，使利用队列调度策略抑制 DDoS 攻击流的思想能够得到更多研究者的关注，为 DDoS 攻击抑制提供更加有效、更加完善的解决方案。

参 考 文 献

[1] McKenney PE. Stochastic fairness queueing[J]. Internetworking: Research and Experience, 1991(2): 113-131

[2] 林闯，单志广，任丰原. 计算机网络的服务质量(QoS)[M]. 北京：清华大学出版社，2004：170-173

[3] Lau F, Rubin S H, Smith M H, et al. Distributed denial of service attacks[C]// Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics (Vol. 3). 2000: 2275-2280

[4] 徐雷鸣，庞博，赵耀. NS 与网络模拟[M]. 北京：人民邮电出版社，2003

[5] http://www.isi.edu/nsnam/ns/

[6] Moore D, Voelker G, Savage S. Inferring internet denial of service activity[J]. ACM Transactions on Computer Systems, 2006, 24(2): 115-139