DDoS攻击与IP拥塞控制研究

吴国纲

(成都西科微波通讯有限公司 成都 610091)

【摘要】IP网络的流量控制是在网络正常工作时采取的一系列措施，通过避免出现发生网络拥塞所需的条件，来进行拥塞控制。该文讨论了现有的主流方法，并对其应用于DDoS攻击防护的性能进行了分析和比较。结果表明，其中的任何一种方法都需要在改进后，才能有效地应用于控制DDoS攻击所造成的网络拥塞。

关 键 词 拥塞控制； DDoS攻击； 性能
中图分类号 TP393 文献标识码 A

Research on DDoS Attack and IP Congestion Control

WU Guo-gang

(Chengdu Seekon Microwave Communicaition Co. Ltd. Chengdu 610091)

Abstract Traffic control based on IP network is normally used to realize congestion control through avoiding conditions of congestion. This paper discusses primary methods of congestion control in existence. The analysis and comparison of these methods when they are used to defend attacks from the distributed denial of serve(DDoS). The results show that these methods could be used to control DDoS attacks after improved.

Key words congestion control; DDoS attack; performance

1 DDoS攻击防护机制

随着分布式拒绝服务(Distributed Denial of Serve，DDoS)攻击的日益增多，其攻击手段已引起各国的高度重视，并被认为是Internet所面临的最大威胁之一。根据DDoS攻击的方法和特性，目前普遍认为，在独立站点上实现对DDoS攻击的有效防护是不可能的，应通过不断的研究，提出一些可行的解决办法。图1所示是一些常用的DDoS攻击防护机制和方法。其中包括[1]：通过修改配置和协议预防攻击、反向查找攻击源头、攻击检测和过滤、分布式攻击检测和过滤(主机端/路由器端)等。

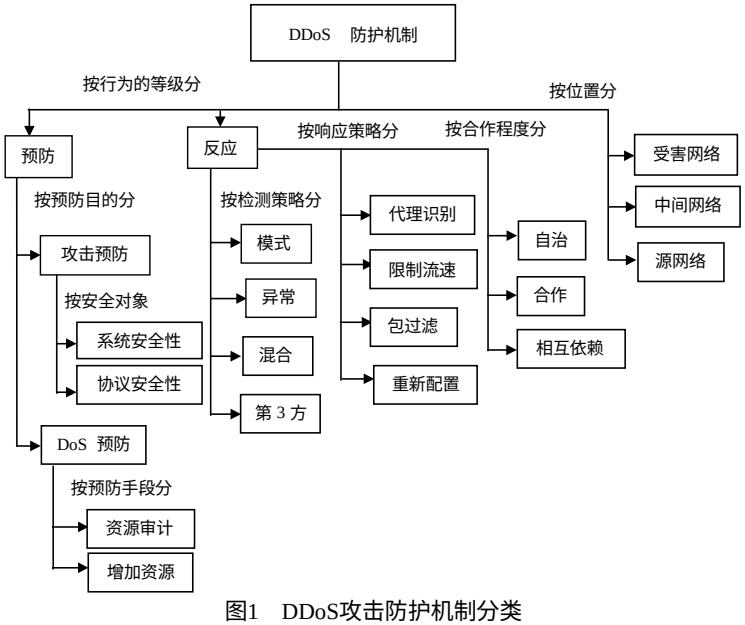

图1 DDoS攻击防护机制分类

收稿日期：2005 – 09 – 12
作者简介：吴国纲(1972 –)，男，硕士，主要从事计算机应用和数字通信方面的研究.

从DDoS攻击的过程和效果来看，当攻击发生时，攻击者通过控制傀儡机向目标发送大量的请求，导致系统资源耗尽或网络拥塞，从而使目标系统或网络不能响应正常用户的请求。虽然DDoS攻击的类型很多，但对于绝大部分攻击而言，防护重点可集中于缓解攻击所造成的网络拥塞和防止被攻击主机的资源耗尽两个方面。TCP基于窗口的端到端拥塞控制机制，对于Internet的稳定性起到了关键作用，也是当前互联网上拥塞控制的主要措施之一[2]。然而DDoS攻击引起的网络拥塞，是由恶意主机控制大量傀儡机所造成的，并非传统意义上的端到端拥塞，所以只能在路由器上进行控制。本文所讨论的DDoS攻击防护就是基于IP拥塞控制来进行的。

2　DDoS攻击与网络拥塞

网络产生拥塞的根本原因在于用户提供给网络的负载超过了网络的存储和处理能力，表现为无效数据包增加、报文时延增加与丢失、服务质量降低等。如果不能采取有效的检测和控制手段，就会导致拥塞逐渐加重，甚至造成系统崩溃。文献[3]分析了在一般情况下形成网络拥塞的三个直接原因。

(1) 路由器存储空间不足。几个输入数据流需要同一个输出端口，如果入口速率之和大于出口速率，就会在这个端口上建立队列。如果没有足够的存储空间，数据包就会被丢弃，对突发数据流更是如此。增加存储空间从表面上看似乎能解决这个矛盾，但根据文献[4]的研究，如果路由器有无限存储量时，拥塞只会变得更坏。

(2) 带宽容量相对不足。直观地说，当数据总的输入带宽大于输出带宽时，在网络的低速链路处就会形成带宽瓶颈，网络就会发生拥塞(相关证明可参考香农信息理论)。

(3) 处理器处理能力较弱。如果路由器的CPU在执行排队缓存、更新路由表等操作时，处理速度跟不上高速链路，也会产生拥塞。同理，低速链路对高速处理器也会产生拥塞。

以上是早期Internet网络发生拥塞的三个主要原因。对此，TCP拥塞控制给出了较好的解决方案。在实际应用中，如果所有的端用户均遵守或兼容TCP拥塞控制机制，网络的拥塞就能得到很好地控制。但是，当DDoS攻击造成网络拥塞时，TCP基于窗口的拥塞控制机制对此无法加以解决，原因是攻击带来的拥塞是由大量恶意主机发送数据所造成的，这些主机不但不会完成TCP拥塞控制机制所规定的配合工作，甚至本身就可能包含伪造源地址、加大数据发送量、增加连接数等攻击方式。在此情况下，对DDoS攻击所造成的网络拥塞就必须在路由器上进行处理，这只能基于IP拥塞控制来实现。

需要注意的是，DDoS攻击所造成的网络拥塞不同于上面所分析的普通情况，它们之间存在着本质差异。相比之下，DDoS攻击所造成的拥塞，其攻击数据常常在分组大小、到达时间、协议类型等诸多方面具有一定相关性，这是由分布式拒绝服务自身的特点所决定的。而普通情况下的网络拥塞，其数据并非由多个受控攻击者发送，因而不具有类似的相关性。对攻击所造成的拥塞进行防护，就应首先找到这个相关性，在此基础上引入传统拥塞控制机制并加以完善，才能进行高效、准确的检测和控制工作。本文研究一般情况下和攻击发生时所造成的网络拥塞的差异。

3　IP拥塞控制研究进展

关于IP拥塞控制的研究和应用，目前有两个方面需要加以重视。一方面是近年来IPv6所取得的进展，另一方面是SG13(国际电信联盟ITU中，负责网络总体设计的研究组)的有关研究工作。可以预见，随着对Ipv6的深入研究和该协议在下一代互联网(Next Generation Internet，NGI)中的广泛应用，该协议中的拥塞控制策略将发挥较大作用，而DdoS攻击的防护手段也将得到更大的完善和丰富。

IP网络的流量控制是在网络正常工作时采取一系列措施，通过避免出现发生网络拥塞所需的条件，来进行拥塞控制，这些措施包括：网络资源管理、接入允许控制、流量参数控制、非一致性IP数据包的标记和IP数据包的有计划分流等。这些措施可使网络拥塞的强度、持续时间和扩散的影响减至最小。目前，关于IP网络流量控制和拥塞控制标准化的工作还处于起步阶段。

下面研究近年来IP拥塞控制的有关策略[5-6]，并对它们应用于DDoS攻击时的防护能力进行简要评价。根据DDoS攻击的原理和机制，本文对各种机制的防护能力给出以下评价标准：(1) 是否能按一定规则进行特征设定；(2) 是否能根据一定规则对流经的数据加以区分；(3) 是否能针对不同类型的数据包提供不同优先级的服务。如果一个拥塞控制机制满足了以上三条标准，就基本具备了防护DDoS攻击的能力。下面按此标准条件进行逐一分析。

(1) 先进先出(First In First Out，FIFO)。传统的

先进先出策略是目前Internet上使用最广泛的一种服务模型。它的最大优点是便于实施，但由于FIFO本质上是一种“去尾”(Drop-tail)的算法，所以当突发性数据到达时容易出现包丢失现象，其公平性较差，对上层的TCP快速恢复的效率也较低。对照评价标准，该算法没有满足任何一个条件。过于简单且缺乏智能性，完全不能用于DDoS攻击防护。

(2) 随机早期检测(Random Early Detection，RED)算法。RED算法按一定概率丢弃进入路由器的数据包。RED的早期设计思路是避免丢弃属于同一连接的连续数据包，从而提高连接的吞吐量。通过分摊包丢失率，RED可以在各连接之间获得较好的公平性，对突发业务的适应性较强。RED算法的处理过程中，包丢失率P为平均排队长度Q_e的函数，Q_{min}、Q_{max}和P_{max}为可配置的RED参数；Q_e为排队长度的统计平均。RED也存在一些不足，例如可能会引起网络的不稳定，而且选择合适的配置参数也不是一件容易的事，如图2所示。近年来，研究者提出了许多RED的改进算法[7]，这些算法都在一定程度上从不同方面改善了RED的性能。对照评价标准，该方法对DDoS攻击的防护作用不大，由于其设计思路是分摊包丢失率，对正常业务和攻击数据“过分公平”，不能做到有所区分，从而使得大量正常业务在攻击发生时无法得到服务。

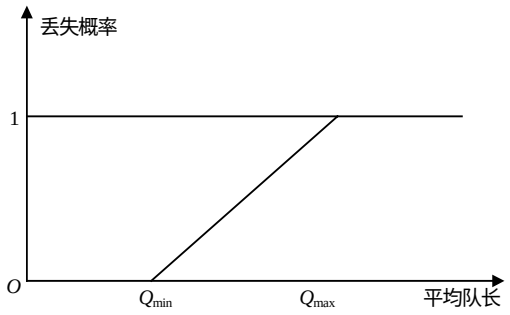

图2 随机早期检测算法RED示意图

(3) 显示拥塞指示(Explicit Congestion Notification，ECN)算法。前面两种拥塞控制算法都是通过包丢失来告诉端系统，网络已经发生拥塞。而显示拥塞指示算法通过明确的拥塞提示(RFC2481)来实现拥塞控制，对一次性大批量数据传输的效果比较理想，但对时延有一定要求。

该算法在源端数据包中嵌入ECN，由路由器根据网络情况设置CE(Congestion Experienced)比特位。源端接收到从网络中反馈回来的这种CE置位数据包后，将随后发出的数据包标记为可丢弃的数据包。ECN的优势在于不需要超时重传，也不依赖于粗粒度的TCP定时，所以在对时延有一定要求的应用场合性能较好。还有另一种提出的改进算法，通过调整拥塞窗口CWND的大小，纠正有长时间RTT的TCP连接的偏差，来改进共享瓶颈处带宽的公平性。对照评价标准可知，ECN算法对防护DDoS攻击效果不大，原因在于无攻击特征识别和区分功能，在攻击发生时智能性较差。

(4) 公平排队(Fair Queuing，FQ)算法。在FQ算法中，路由器对每个输出线路都建有一个排队队列。当一条线路空闲时，路由器来回扫描所有队列，依次将每队的第一个包发出。FQ的带宽分配独立于数据包大小，各种服务在队列中几乎同时开始。因此在没有牺牲统计复用的情况下提供了另外的公平性，与端到端的拥塞控制机制可以较好地协同。但缺点在于实现起来很复杂，需要每个数据流的排队处理、每个流的状态统计、数据包的分类以及包调度的额外开销等。对照评价标准可知，该算法对防护DDoS攻击效果不大，原因同ECN算法。

(5) 加权公平排队(Weighted Fair Queuing，WFQ)算法。WFQ算法是FQ的改进算法，根据不同数据流的不同带宽要求，对每个排队队列采用加权方法分配缓存资源，从而增加FQ对不同应用的适应性，该算法还有其它一些改进算法[8]。对照评价标准可知，该方法改进后可用于防护DDoS攻击，设计思路是首先对攻击进行检测和分类，然后将入口数据按攻击数据、正常数据、可疑数据三种类型分别排队处理，对攻击数据直接丢弃，通过对可疑和正常数据赋予一定权值，来提供不同质量的服务。在路由器性能良好、处理能力强的情况下，甚至可以采取更复杂、智能的处理策略，例如多优先级队列。

(6) 加权随机先期检测(Weighted Random Early Detection，WRED)。WRED将随机先期检测与优先级排队结合起来，为高优先级分组提供优先通信服务能力。当某个接口开始出现拥塞时，它有选择地丢弃优先级较低的分组，而不是简单地随机丢弃分组。对照评价标准可知，该方法通过改进后可用于防护DDoS攻击，设计思路与WFQ类似，它们都符合评价标准条件(3)，改进应从增加条件(1)和条件(2)着手。

(下转第655页)

估，从而使得评估结果更具科学性与合理性。同时需指出的是，模糊集理论不仅可用来解决具有模糊性质的现实问题，也可应用于解决某些本身具有精确性质的现实问题。

参 考 文 献

[1] CAVANO J P, McCall J A. A framework for the measurement of software quality[C]//Proc. ACM Software Quality Assurance Workshop NewYork: ACM, 1987, 133-139.

[2] ISO/ IEC JTC1/ SC7/ WG6, ISO/ IEC 9126- 1: Information technology-software quality characteristics and metrics-Part 1: Quality model[S]. 2001.

[3] ISO/ IEC JTC1/ SC7/ WG6, ISO/ IEC 14598 Part1-Part6: 2001. Information technology-evaluation of software product[S]. 2001.

[4] PEDRYCZ W. Fuzzy set technology in knowledge discovery[J]. Fuzzy sets syst., 2001, 98: 279-290.

[5] KLIR G J, YUAN B. Fuzzy sets and fuzzy logic: Theory and application[M]. Upper Saddle River: Prentice Hall, 1995.

[6] LI H X, YEN V C. Fuzzy sets and fuzzy decision-making[M]. Boca Raton: CRC Press, 1995.

[7] HAN J, KAMBER M. Data mining: Concepts and techniques [M]. America: Morgan Kaufmann Publishers, Inc., 2001.

编　辑　熊思亮

(上接第616页)

(7) 定制排队。定制排队是为允许具有不同最低带宽和延迟要求的应用程序共享网络而设计的。定制排队为不同协议分配不同的队列空间，并以循环方式处理队列，当特定协议的数据流被分配了较大的队列空间，也就获得了较优先的服务。定制排队比优先级队列更为公平，可以保证每一个特定的通信类型得到固定的可用带宽，同时在链路紧张的情况下，避免数据流企图超出预分配量限制的可能。对照评价标准可知，该方法改进后可用于防护DDoS攻击，在资源分配和使用时为不同业务提供优先级加权，改进思路与WFQ和WRED类似。

以上简略分析了当前的一些主流IP拥塞控制算法，并对其防护DDoS攻击的可行性进行了评价。可以看出，这些算法的防护能力存在着较大差异，其中的任何一种都需要改进，才能有效地应用于控制DDoS攻击所造成的网络拥塞。

4 结 束 语

针对防护DDoS攻击所进行的研究工作，应从网络拥塞和主机资源耗尽两个方面来着手开展，本文对前一个问题进行了系统的研究。在分析传统IP拥塞控制算法思想的同时，对其应用于DDoS攻击防护的能力进行了评价，为进一步研究DDoS防护提供了依据和基础。

参 考 文 献

[1] MIRKOVIC P R J, PRIER G. Attacking ddos at the source[C]// In Proc.: 10th IEEE international conference on network protocols. Paris: [s. n.], 2002.

[2] VICISANO L, RIZZO L, Crowcroft J. TCP-like congestion control for layered multicast data transfer[C]//In Proc.: IEEE INFOCOM’98. San Francisco: [s.n.], 1998.

[3] 罗万明, 林　闯, 阎保平. TCP/IP拥塞控制研究[J]. 计算机学报, 2001, 24(1): 1-18.

[4] NAGEL J. On packet switches with infinite storage[J]. IEEE Trans. on Commun., 1987, 35: 435-438.

[5] PAREKH A K, GALLAGER R G. A generalized processor sharing approach to flow control in integrated services networks: The single-node[J]. IEEE/ACM Trans. Networking, 1993, 1(3): 344-357.

[6] FLOYD S. TCP and explicit congestion notification[J]. ACM Computer Communication Review, 1994, 24(5): 8-23.

[7] ATHURALIYA S, LOW S, LAPSLEY D. Random early marking. in proceedings of the first International workshop on quality of future internet services[C]//QofIS'2000.Berlin: [s.n.] , 2000.

[8] DEMERS A, KESHAV S, SHENKER S. Analysis and simulation of a fair queueing algorithm[C]//Proc. ACM SIGCOMM’89. Austin: ACM Press, 1989.

编　辑　熊思亮