DDoS 攻击下 Ad hoc 网络队列管理算法研究与仿真

冯 永, 姚龙海
(解放军电子工程学院 网络系, 合肥 230037)

摘 要: 针对分布式拒绝服务攻击(DDoS)对于 Ad hoc 网络性能的影响进行了研究。在介绍三种经典网络队列管理算法——Drop-Tail、RED 和 REM 的基础上,利用网络仿真软件 NS2,分析比较了 Ad hoc 网络在遭受 DDoS 攻击时三种队列管理算法的防御能力。仿真表明,在中、轻度 DDoS 攻击下,主动式队列管理算法 REM 和 RED 较被动式队列管理算法 Drop-Tail 具有更强的防御能力,但在重度 DDoS 攻击下,三种队列管理算法性能均大幅下降。为有效提高 Ad hoc 网络对于 DDoS 攻击的防御能力,除采用主动式队列管理算法之外,应结合网络检测等其他防御机制。

关键词: 分布式拒绝服务攻击; 无线自组织网络; 队列管理算法; 网络仿真软件; 防御策略
中图分类号: TP393.08;TP391.7 **文献标志码**: A **文章编号**: 1001-3695(2012)12-4648-03
doi:10.3969/j.issn.1001-3695.2012.12.062

Research and simulation of three queue management algorithms in Ad hoc network under DDoS attack

FENG Yong, YAO Long-hai
(*Dept. of Network, Electronic Engineering Institute of PLA, Heifei* 230037, *China*)

Abstract: Concentrating on the influence of DDoS imposed on Ad hoc network, this paper introduced three classic queue management algorithms: Drop-Tail, RED and REM. Applying in Ad hoc network, it analysed and compared these algorithms with NS2 under DDoS attack. The result shows that the active queue management algorithms, like REM and RED, exhibit a stronger defense ability than the passive queue management algorithm like Drop-Tail under medium and small scale DDoS attack. But under large scale DDoS attack, all three algorithms don't show enough ability against this attack. It means that other defense scheme like network detection must be integrated into security sheme to defeat DDoS attack.

Key words: distributed denial of service(DDoS); Ad hoc network; queue management algorithm; network simulation software; defense scheme

0 引言

近年来,DDoS 攻击(分布式拒绝服务攻击)已成为网络中比较盛行且很难检测的一类攻击。由于其攻击方式隐秘且简单有效,DDoS 攻击被公认是网络服务所面临的最主要的威胁之一[1,2]。队列管理算法是在网络发生拥塞时提供资源公平分配方案和服务质量 QoS 的重要保证,是网络面对 DDoS 攻击时的第一道防线,其算法设计好坏,直接关系到网络能否提供正常的带宽分配、时延、发包率等基本服务[3]。本文研究分析了常见的三种队列管理算法:Drop-Tail、RED、REM,并基于 Ad hoc 网络环境,利用网络仿真软件 NS2 对各队列管理算法在 DDoS 攻击下的性能进行了仿真比较,并得出了最终的结论。

1 Ad hoc 网络和 DDoS 攻击

如图 1 所示,Ad hoc 网络是一种分布式的无线自组织网络,组成网络的节点既是通信终端,又具有路由器功能。数据以多跳的方式传送,无须固定基础设施的支持,从而具有很强的抗毁性,因此被认为是数字化战场的首选网络技术[2]。但由于其基于开放式的无线通信方式、信道带宽较窄、计算能力有限且靠电池供电,因此布署具体的 Ad hoc 网络时常常要在资源利用效率和安全方案复杂度之间作出相应的权衡[4]。与固定的有线网络相比,Ad hoc 网络面临更多的安全威胁,其中尤以分布式拒绝服务攻击 DDoS 较为常见。

DDoS 攻击是在传统的拒绝服务 DoS 攻击基础之上产生的一类攻击方式,其基本特点是利用网络与受害节点之间的巨大的资源不对称性,实现对资源的大量耗费,从而达到攻击的目的,这种资源的耗费表现形式通常是网络的带宽耗费或是如主机内存或者 CPU 等服务器资源的耗费[5]。

DDoS 攻击,特别是地址欺骗 DDoS 攻击往往会产生海量的攻击数据流,它们会产生巨大的空间开销,使网络性能出现急剧地下降[2]。以 Ad hoc 网络为例,由于各节点采用分布式的无线网络连接,敌手很有可能采取替换或操控网络中的若干节点(如图 2 中的 1、2 节点),赋予其大量资源,利用原有的网络地址作为掩护,在一定时间段内不断地向邻近节点发送无用的网络数据包,占据有限的无线网络带宽,使得 Ad hoc 中的各种网络服务不可用。

收稿日期: 2012-04-06; **修回日期**: 2012-06-20

作者简介:冯永(1986-),男,江西南昌人,硕士研究生,主要研究方向为嵌入式技术、Ad hoc 网络(superferras@163.com);姚龙海(1964-),男,安徽和县人,教授,主要研究方向为嵌入式技术、Ad hoc 网络.

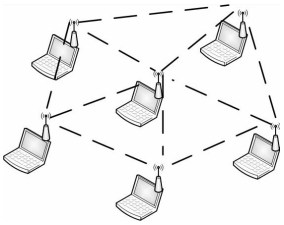

图1　Ad hoc网络构成

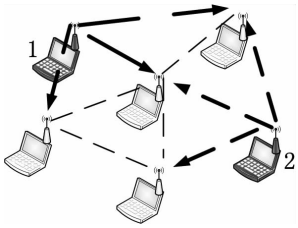

图2　DDoS攻击下的Ad hoc网络

2　队列管理算法

网络主要是基于存储转发和统计复用技术而组成的,由于数据本质上是突发的,因此网络允许传输突发的数据包非常必要。而路由器中队列的重要作用就是吸收突发的数据包,较大的队列能够吸收更多的突发数据,提高吞吐量,但另一方面又增加了数据包的排除延迟。因此需要路由器对队列进行管理,维持较小的队列长度,由此产生了一系列的队列管理算法[6]。

目前的队列管理算法可以分为被动式队列管理(PQM)算法和主动式队列管理(AQM)算法两大类。

2.1　被动式队列管理算法

被动式队列管理算法,即管理队列长度的传统方法,是对每个队列设置一个最大值(以包为单位),然后接收数据包进入队列直到队列长度达到极限,随后到达的数据包就要被拒绝进入队列直到队列长度下降,这种技术也就是传统的去尾(Drop-Tail)算法,由于此算法是在队列满后被迫丢包,因此称为被动式队列管理[6]。Drop-Tail 队列管理机制仍是目前网络中使用最为广泛的分组排队和丢弃方式。

2.2　主动式队列管理算法

相对于被动式队列管理算法,主动式队列管理算法在队列满之前就开始把数据包丢弃,这样可以对原来具有拥塞控制的传输端作为流量速度管制,以避免满队列状态所带来的较长的端到端延迟时间或利用率降低等负面效应。常见的主动式队列管理算法有随机早期探测算法(RED)和随机指数标记算法(REM)。

2.2.1　RED 队列管理算法

RED[6,7]队列管理算法是使用平均队列长度来预测即将发生的网络拥塞,并采用随机选择的方式对数据包进行丢弃,使得在拥塞尚未发生之前就向具有拥塞控制的传输端提示要进行流量速度管制,以避免拥塞的发生。

RED 采用平均指数加权的方式计算平均队列长度,其计算式为

$$\text{avg} = (1 - w_q) \times \text{avg} + w_q \times q$$

其中:avg 是平均队列长度;q 为目前实际的队列长度;w_q 为目前实际的队列加权系数,其值需要满足 $0 < w_q < 1$。通常来说,w_q 的值都设得很小,这样可使计算平均队列长度变化很慢,不会因为突发流量的到来而使得平均队列长度增大很快,造成大量的数据包丢弃。当平均队列长度介于最短队列长度 $\min_{\text{th}}$ 和最长队列长度 $\max_{\text{th}}$ 之间时,则根据下面的概率式来丢弃数据包:

$$P_b = \max_p \times (\text{avg} - \min_{\text{th}}) / (\max_{\text{th}} - \min_{\text{th}})$$

其中:$\max_p$ 为预先设置的丢弃概率值,P_b 为目前数据包丢弃的计算值。

2.2.2　REM 队列管理算法

REM 管理机制,即随机指数标记算法,是从最优化流控制理论得到的[8]。REM 算法利用 Kelly 提出的网络流量优化理论中价格的概念来探测和控制网络的拥塞状态。价格的变化由两方面的因素决定:一方面是实际队列长度和期望队列长度之差;另一方面是聚合流的输入速率与端口输出速率之差。在价格的深化算法中,REM 使用了简单的比例关系。单节点上概率与链路上价格的总和呈现出近似的比例关系。REM 将输入速率稳定在链路容量附近,并将队列长度在一个小的目标区间内,而不管有多少个连接共享链路,因为 REM 算法是梯度寻优的解。基于负载的 REM 算法,其核心特征有两点[9]:

a)比较速率清空缓冲。计算报文到达速率,将速率差值用队列差值近似。链路的价格按下式计算:

$$p_l(t+1) = [p_l(t) + \gamma(q_l(t+1) - (1 - \alpha_l)q_l(t) - \alpha_l \times q_l^*)]^+$$

其中:$\gamma > 0, \alpha_l > 0, [z]^+ = \max\{0, z\}$($z$ 为任意表达式或值),$q_l(t)$ 为链路 l 的队列在时刻 t 的瞬时队列长度,q_l^* 为目标队列长度。

b)计算总价。链路 l 的队列在 t 时刻的标记速率为

$$m_l(t) = 1 - \varphi^{-p_l(t)}$$

其中:φ 为常数,且 $\varphi > 1$。报文端的标记概率为

$$1 - \varphi^{-\sum_l p_l(t)}$$

从上面的分析可以看出,与基于队列的算法不同,REM 算法主要测量链路的负载情况,并由此计算出丢包率[10]。

3　攻击效果仿真及分析

本文基于 Ad hoc 网络,在 Ubuntu 环境下利用网络仿真软件 NS2(版本为 2.35),按表 1 给定的参数[11],对 DDoS 攻击下分别采用 Drop-Tail、RED、REM 三种队列管理算法的 Ad hoc 网络在发包率和平均端到端延时两项指标上进行了比较(所有节点处于静止状态),其仿真结果如图 3、4 所示。

表 1　NS2 仿真参数设置

仿真参数	值	仿真参数	值
场景/m^2	300 × 300	路由协议	AODV
节点数/个	100	业务流	CBR
时间/s	100	包大小/Byte	512
MAC 协议	802.11	最大连接数	10

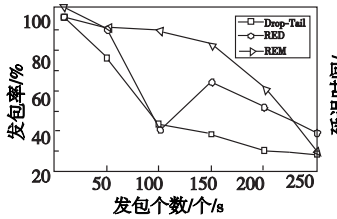

图3　DDoS攻击下Ad hoc网络发包率

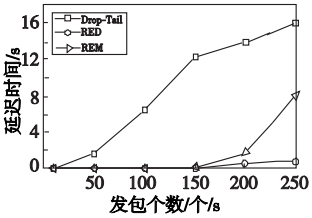

图4　DDoS攻击下Ad hoc网络平均端到端延时

由图 3 和 4 可以看出,在相同发包速率的情况下,Drop-Tail 性能最差,RED 次之,REM 性能最好。但当发包速率不断增加时,三种算法的性能都有明显的下降。仿真表明,作为网络应对突发流量的第一道防线,传统的主动式和被动式队列管

理算法对于 DDoS 攻击的防御能力非常有限。

4 防御 DDoS 攻击的主要策略

在低发包率的条件下,主动式队列管理算法对于 DDoS 攻击的防御能力较强。但在较高发包率的情况下,主动式和被动式队列管理算法均无法有效防范 DDoS 攻击,所以 Ad hoc 网络若要有效防范 DDoS 攻击,需要结合其他机制,综合运用各种防御策略。

由于传统 DDoS 攻击是利用底层协议的安全隐患或是系统设计问题进行攻击的,因此针对这种攻击类型的大部分研究主要是依靠分析网络数据包的分组特征、流特征、请求速率等方面的内容来检测攻击,由此提出的防御方案主要可以分为基于攻击源进行检测和基于受攻击节点进行检测两种类型[12]。

文献[13]是一种典型的基于攻击源的检测方案。该方案基于反馈机制建立了一种简单的数据过滤模型。该过滤模型采用统计概率的方法,根据当前网络数据流量、延时以及过滤节点的处理能力确定丢弃该包的概率。

而作为基于受攻击节点的检测方案,文献[12]设计了一种基于决策树机制的 DDoS 检测系统,该系统在检测到攻击后,利用数据流模型匹配机制追踪攻击者的位置及攻击路径。仿真表明,该系统能够检测出 DDoS 攻击者的漏报率为 1.2% ~ 2.4%,误报率仅为 2% ~10%,发现攻击路径的漏报率和误报率分别为 8% ~12% 和 12% ~14%。

5 结束语

本文介绍了三种传统的网络队列管理算法:Drop-Tail、RED 和 REM,并在 Ad hoc 网络环境中,利用网络仿真软件 NS2 对三种算法在 DDoS 攻击下的发包率和平均端到端延时进行了仿真比较。结果表明:在轻、中度 DDoS 攻击下,主动式队列管理算法(如 RED、REM 等)与被动式队列管理算法(Drop-Tail)相比性能较优;然而在重度 DDoS 攻击下,无论是主动式队列管理算法还是被动式队列管理算法,其性能均有明显下降。由于队列管理算法的先天不足,在实际应用中,一般都将队列管理算法与其他防范 DDoS 攻击的策略(如 DDoS 攻击检测)相结合以提高对 DDoS 攻击的防御能力。另一方面,在确保网络服务质量 QoS 的前提下,如何对原有的主动式队列管理算法作出相应修改,使其能够有效应对 DDoS 攻击,则是本文下一步的研究重点。

参考文献:

[1] 金舒原,云晓春,方滨兴. DDoS 攻击检测的挑战[J]. 信息技术快报,2008,6(5):25-35.

[2] 张长旺,殷建平,蔡志平,等. 抗 DDoS 攻击的主动队列管理算法[J]. 软件学报,2011,22(9):2182-2192.

[3] 王建新,荣亮,肖雪峰. 几种主动队列管理算法的仿真及性能评估[J]. 计算机工程,2007,33(3):128-130.

[4] 韦蓉. Ad hoc 网络关键技术研究[D]. 北京:邮电大学,2008.

[5] PENG T, LECKIE C, RAMAMOHANARAO K. Survey of network-based defense mechanisms countering the DoS and DDoS problems [J]. ACM Computing Surveys,2007,39(1):1-42.

[6] 方路平,刘世化,陈盼,等. NS-2 网络模拟基础与应用[M]. 北京:国防工业出版社,2008:156-166.

[7] ZHANG Wei, TAN Liang-sheng, PENG Gang. Dynamic queue level control of TCP/RED systems in AQM routers[J]. Computers and Electrical Engineering,2009,35(1):59-70.

[8] 刘明,张鹤颖,窦文华. 随机指数标记算法的性能分析与控制模型[J]. 计算机工程与科学,2005,27(9):66-68.

[9] ATHURALIYA S, LOW S H, LI V H, *et al*. REM : active queue management[J]. IEEE Network,2001,15(3):48-53.

[10] 吴春明,姜明,朱淼良. 几种主动式队列管理算法的比较研究[J]. 电子学报,2004,32(3):429-434.

[11] 柯志亨,程荣祥,邓德隽. NS-2 仿真实验——多媒体和无线网络通信[M]. 北京:电子工业出版社,2009:315-331.

[12] WU Y C, TSENG H R, YANG W, *et al*. DDoS detection and trace-back with decision tree and grey relational analysis[J]. Ad hoc and Ubiquitous Computing,2011,7(2):121-136.

[13] TAN H X, SEAH W K G. Framework for statistical filtering against DDoS attacks in MANETs[C]//Proc of the 2nd International Conference on Embedded Software and Systems. Berlin: Springer-Verlag, 2006:456-465.

(上接第 4638 页)的有效性及可靠性。实验结果表明本文提出的算法适合图像的加密传输,以及在数字水印等隐蔽传输中的置乱预处理,有很好的实用价值和应用前景。下一步的工作主要包括:如何选择合适的工作密钥使置乱算法达到最优,该算法在数字水印等技术中的应用以及在其他领域应用的研究。

参考文献:

[1] 谭永杰,张文娟,崔海花. 图像置乱技术综述[J]. 周口师范学院学报,2010,27(5):98-102.

[2] 练芝飞,徐荣聪. 幻方变换加密分形图[J]. 福建电脑,2009(12):111-112.

[3] 柏森,曹长修,柏林. 基于仿射变换的数字图像置乱技术[J]. 计算机工程与应用,2002,38(10):74-75,78.

[4] 李用江,葛建华,李昌利,等. 一种新的 n 维广义 Arnold 矩阵构造方法及其在图像置乱中的应用[J]. 北京科技大学学报,2010,32(12):1630-1636.

[5] 万里红,孙燮华,林旭亮. 分形 Hilbert 曲线混合 Gray 码的图像加密算法研究[J]. 计算机工程与应用,2010,46(34):184-186,194.

[6] 丁玮,闫伟齐,齐东旭. 基于生命游戏的数字图像置乱与数字水印技术[J]. 北方工业大学学报,2000,12(1):1-5.

[7] 关可,王建新,亓淑敏. 信息论与编码技术[M]. 北京:清华大学出版社,2009:210-211.

[8] 马苗,谭永杰. 基于相邻像素间位异或的图像置乱算法[J]. 计算机工程与应用,2008,44(9):187-189.

[9] 李志伟,陈燕梅,张胜元. 基于 SNR 的数字图像置乱程度评价方法[J]. 厦门大学学报:自然科学版,2006,45(4):484-487.

[10] 赵红,温文雅. 数字图像置乱技术综述[J]. 福建电脑,2007(12):10-12.

[11] QI Dong-xu, ZOU Jian-cheng, HAN Xiao-you. A new class of scrambling transformation and its application in the image information covering[J]. Science in China:Series E,2000,43(3):304-312.

[12] 熊玮. 一种基于位置变换和灰度变换相结合的数字图像置乱方法[J]. 软件导航,2011,10(11):159-161.

[13] 林雪辉,蔡利栋. 基于 Hilbert 曲线的数字图像置乱方法研究[J]. 中国体视学与图像分析,2004,9(4):224-227.