DOI:10.13245/j.hust.2010.09.028
第38卷 第9期 华中科技大学学报(自然科学版) Vol.38 No.9
2010年 9月 J. Huazhong Univ. of Sci. & Tech.(Natural Science Edition) Sep. 2010

针对 RED 的 LDoS 攻击模型

吴黎兵[a,b] 徐 翱[a,b] 何炎祥[a] 王 超[a]
(武汉大学 a 计算机学院; b 空天信息安全与可信计算教育部重点实验室, 武汉 430072)

摘要: 针对随机早期检测(RED)算法的低速率拒绝服务攻击(LDoS)会导致路由器的缓冲队列长度出现严重震荡、使网络服务质量急剧下降的问题, 分析了针对 RED 的 LDoS 攻击模型, 并推理了高速率攻击脉冲使路由器缓冲队列迅速增加的过程, 提出了攻击脉冲长度 l 和脉冲速率 R 的理论计算方法. 对于一个示例场景, 当采用大于瓶颈链路带宽的攻击脉冲时, 400 ms 左右的脉冲能够对网络性能造成很大影响. 在 NS2 中的模拟实验证明了实验结果与理论预期的一致性, 针对 RED 的 LDoS 攻击流能够使网络服务质量大幅度下降, 并且攻击流具有较好的隐蔽性.

关 键 词: 网络安全; 网络性能; 拥塞控制; 低速率攻击; 拒绝服务; 随机早期检测
中图分类号: TP393.0 文献标志码: A 文章编号: 1671-4512(2010)09-0050-05

The model for low-rate denial-of-service attack on RED

Wu Libing[a,b] *Xu Ao*[a,b] *He Yanxiang*[a] *Wang Chao*[a]
(a School of Computer; b Aerospace Information Security and Trusted Computing Key Laboratory of Ministry of Education, Wuhan University, Wuhan 430072, China)

Abstract: The LDoS (low-rate DoS) attack on RED (random early detection) algorithm reduced the quality of network service by delivering periodic attack pulses that caused the router queue jitter seriously. The model of LDoS attack on RED was analyzed, and the process how the attack pulse make the queue length to increase rapidly was inferred. On the basis of theoretical analysis, a method to compute the pulse length l and pulse rate R is proposed. For a sample scenario, if the pulse rate is larger than the bandwidth of bottleneck link, it is calculated by the formula that an attack with pulse length about 400 ms could cause a great impact on network performance. Finally, through simulation experiments in NS2 platform, it is found that the results of the experiment coincide with the theoretical expectations. From the theoretical calculation and experimental, it is demonstrated that the LDoS attack stream targeting RED could cause significant decline of network service of quality and possessed excellent stealth capabilities.

Key words: network security; network performance; congestion control; low-rate attack; denial of servic; random early detecton (RED)

拒绝服务攻击(DoS)一直是网络面临的最为严峻的威胁之一. 分布式拒绝服务攻击(DDoS)的攻击虽然破坏性很大, 但是需要攻击者采取一种压力方式向被攻击者发送大量攻击包, 即要求攻击者维持一个高频率、高速率的攻击流. 正是这种特征, 各种传统 DoS 攻击与正常网络流量相比都具有一种异常统计特性, 因此对其进行检测相对简单. 新型的低速率拒绝服务(LDoS)攻击不需要维持高速率攻击流以耗尽受害者所有可用资源, 而是利用网络协议或应用服务中常见的自适应机

收稿日期: 2009-12-25.
作者简介: 吴黎兵(1972-), 男, 副教授, E-mail: cswlb@126.com.
基金项目: 国家自然科学基金资助项目(60773008; 60642006); 空天信息安全与可信计算教育部重点实验室开放基金资助项目.

制(如 TCP 的拥塞控制机制)所存在的安全漏洞，通过在一个特定的短暂时间间隔内突发性地发送大量攻击数据包，从而降低被攻击端的服务性能. LDoS 攻击只是在特定时间间隔内发送数据，而在其他时间沉默，攻击流的平均速率比较低，与合法用户的数据流区别不大，不再具有上述异常统计特性，使得很难用已有的方法对其进行防范. Shrew 攻击[1] 是最早的一种 LDoS 攻击.

自 Kuzmanovic 提出了针对 TCP 的 LDoS 攻击后，引起了很多学者的关注[2~8]. 与此同时，国内学者在此领域的研究也取得了一些成果[9~14]. 本课题组对 LDoS 攻击方式进行了分类描述和建模[15]，在此基础上研究了 Ad-hoc 场景下的 LDoS 攻击[16]，并提出了分布式协同检测方法[17] 和基于小波特征提取的检测方法[18].

通过发送脉冲攻击流能够使 RED 的平均队列长度不断地处于剧烈波动中而使网络服务质量大幅度下降. 由于 Shrew 攻击是利用 TCP 传输的 2 个时间尺度 RTT(往返时延)和 RTO(超时重传时间)的差异来确定攻击脉冲，因此脉冲长度 l 和脉冲周期 T 很容易确定，而针对 RED 的攻击则是使平均队列发生波动以达到攻击效果，攻击参数不易确定. 本文针对 RED 的 LDoS 攻击原理，通过 NS2 中的模拟实验分析了在脉冲攻击下 RED 的缓存溢出情况以及平均队列长度变化规律，得出如何合理控制攻击参数以达到较理想攻击效果.

1　攻击原理及模型

当前网络中广泛应用的 TCP/RED 拥塞控制系统依靠其自适应机制使之维持在一个较稳定的运行状态，即初始时或环境发生变化时，系统可以通过自适应机制逐渐调整或重新回到一个稳定状态. 为了使系统达到最优性能，系统或网络协议往往假设系统大部分时间都是处于稳定状态，并全力保证系统稳定状态的性能，但却忽略了系统的暂态性能，即系统不稳定及从不稳定到稳定状态转换过程中的性能. 针对 RED 的 LDoS 攻击就是利用这一缺陷发起周期性的攻击脉冲，使系统不断在失效和有效 2 个状态间切换，即总是处于低效状态，从而降低系统的整体性能.

1.1　RED

RED[19] 是为了解决网络拥塞控制问题而提出的一种路由器缓存管理技术，它的基本思想是路由器通过监控队列的平均长度来探测拥塞，一旦发现拥塞逼近，就随机地选择源端来通知拥塞，使它们在队列溢出之前降低发送数据速率，以缓解网络拥塞. RED 算法主要包括 2 步：首先计算平均队列长度；然后计算丢弃包的概率. RED 采用下式计算平均队列长度，

$$x = (1-\alpha)x + \alpha x_c, \qquad (1)$$

式中：α 为权值；x_c 为采样测量时实际队列长度. 权值 α 决定了路由器对输入流量变化的反应程度. 计算平均队列长度的目的就是为了反映拥塞程度并据此来计算丢包概率. 路由器在 t 时刻的包丢弃概率

$$p(t) = \begin{cases} 0 & (0 \leqslant x < x_{\min}); \\ \dfrac{x - x_{\min}}{x_{\max} - x_{\min}} p_{\max} & (x_{\min} \leqslant x \leqslant x_{\max}); \\ 1 & (x > x_{\max}), \end{cases}$$

式中：$x_{\max}$ 和 $x_{\min}$ 是队列长度的最大和最小阈值；$p_{\max}$ 为最大丢弃概率.

1.2　攻击原理

针对 RED 的 LDoS 攻击主要通过发送周期性的攻击脉冲使得目标路由器上的队列长度无法稳定，尽量将路由器的数据包丢弃概率维持在一个较高值，经过此路由器的大多数数据包都会被丢弃，从而严重影响目标路由器及 TCP 链接终端用户的传输性能. 可以用一种自适应的反馈机制[20] 来描述这个过程，如图 1 所示.

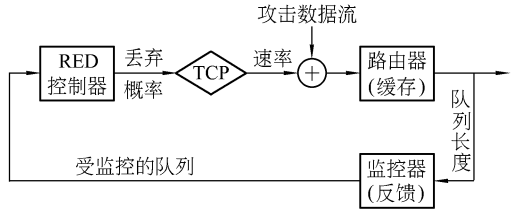


图 1　针对 TCP/RED 机制的 LDoS 攻击

攻击开始时，攻击脉冲强度较大，目标路由器的平均队列长度会迅速增加，由于路由器 RED 机制的控制，路由器的丢弃概率会因为前一时刻平均队列长度过长而变大，大量合法 TCP 数据包会被丢弃. 此外，由于 TCP 拥塞控制的作用，大部分合法 TCP 链路终端用户进入超时等待状态并停止发送数据包. 以上 2 个原因，直接导致合法 TCP 的吞吐量迅速减小. 攻击沉默时，虽然瞬时队列长度很小，但是平均队列长度的减小相对滞后. RED 机制的丢弃概率是一个平滑减小的过程，同时 TCP 用户也刚从超时重传中恢复过来进入慢启动阶段，二者使得路由器缓冲队列平均长度的恢复缓慢. 当队列长度进入稳定状态(恢复到正常值)时，攻击方又会立即发起下一次攻击脉冲. 由此可得，LDoS 攻击下，目标路由器一直处

于一种低效不稳定状态,其与相应 TCP 链接终端用户的传输效能都受到严重影响.

1.3 攻击模型

考虑如下情况:在一条带宽为 C 的瓶颈链路上共有 N 个 TCP 链接和 1 个 UDP 链接,且 UDP 链接上的CBR(constants bit rate)服务代表 LDoS 攻击者. LDoS 攻击周期为 T,脉冲长度为 l,脉冲速率为 R,假设攻击发动前路由器处于稳定状态,可以认为此时的瞬时队列长度和平均队列长度保持稳定.

一轮攻击流的攻击目标是在脉冲长度 l 内使队列平均长度 x 达到或超出正常波动范围,然后攻击沉默,待网络恢复到一定程度发动下一轮攻击,这样路由器平均队列长度将会发生较大的震荡.攻击过程分为 2 个阶段:第 1 阶段脉冲长度为 l_1,攻击流将在极短时间内填满路由器缓存区,使队列瞬时长度达到最大值;第 2 阶段脉冲长度为 l_2,瞬时队列长度维持在最大值 B,使平均队列长度不断增加直到$(x_{max}+x_{min})/2$. $l=l_1+l_2$,并且需要攻击强度满足 $R(1-p_{max})\gg C$ (C 为链路传输能力).

考虑一条带宽为 16 Mbit/s(2 000 包/s)的 RED 链路,路由器缓冲区大小为 250 包,RED 参数中,最小和最大阈值分别为 50 和 120 包,平均队列权值为 0.000 2,最大丢弃概率为 0.1.若这条链路被 19 条 RTT 为80~120 ms 的 TCP 用户分享,则当路由器缓冲队列稳定时,平均队列长度在 70 包左右波动,这时加入一条 R 为 18 Mbit/s 的 LDoS 攻击流.假设第 1 阶段能够在 1 个 RTT 内完成,那么合法流还来不及减小发送窗口,这时它们的流量和应该约等于链路传输能力,即

$$l_1 < B/R \approx 110\ \text{ms}, \qquad (2)$$

计算结果基本符合假设.

在第 2 阶段,瞬时队列长度维持为 B,则 x 按式(1)规律变化,其变化率为 $\mathrm{d}x/\mathrm{d}t=V\alpha(B-x)$,式中 V 为数据包的到达速率,可以认它刚好等于链路传输能力 C.近似地认为第 2 阶段开始时队列平均长度仍然为 x_0(这是保守估计,不会弱化攻击效果),得到微分方程

$$\mathrm{d}x/\mathrm{d}t = C\alpha(B-x) \quad (t=0\text{ 时 }x=x_0),$$

解之可得

$$-\ln(B-x)=\alpha Ct-\ln(B-x_0),$$

代入 $x=(x_{max}+x_{min})/2=0.75x_{max}$, $x_{max}=2x_{min}$,得到

$$l_2 = [\,1/(\alpha C)]\ln[\,(B-x_0)/(B-0.75x_{max})\,].$$

在上述实例中,若取稳定时平均队列长度为 70 包,则得 l_2=294 ms.由 l_1 和 l_2 计算结果可知 400 ms 的脉冲(即脉冲强度为 ms 级)就足以达到攻击目的,然后等待链路恢复后发动下一轮攻击,这通常需要较长时间(s 级,具体视网络状况而定),这样就达到了低速率的攻击目的.

2 模拟实验

为了更加深入地对 LDoS 攻击进行分析,在 NS2 平台上构造网络拓扑结构(如图 2 所示)进行模拟实验,并对实验所得结果进行了分析.实验环境配置为:瓶颈链路带宽 16 Mbit/s,其他链路带宽 100 Mbit/s,路由器缓冲区大小 2 Mbyte,TCP 数据流 20 条,攻击数据流 1 条,链路传播时延为 15~25 ms (这样可以满足各 TCP 流的 RTT 为 90~150 ms).路由器平均队列长度的上下阈值分别为 50 和 120 个数据包(1 个数据包为 1 Kbyte),p_{max}=0.1.

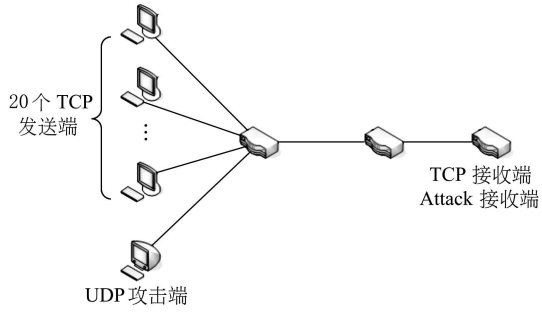
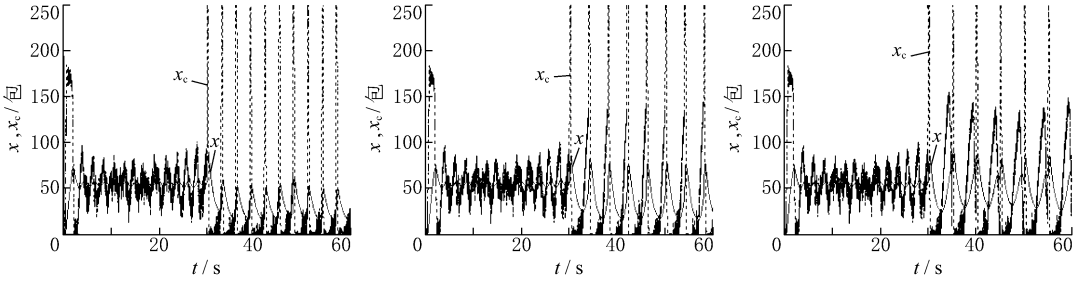


图 2 LDoS 攻击网络拓扑结构

2.1 攻击对队列的影响

现在构造脉冲强度为 18 Mbit/s,脉冲长度为 200 ms,脉冲周期为 T 的 LDoS 攻击流,t= 30 s 时发动攻击直到t=60 s 时实验结束,得到队列变化情况如图 3 所示.从图 3(a)中可以看到,攻击发生前,平均队列长度稳定在 70 包左右,当攻击发动后,瞬时队列迅速达到最大值 250 包,然后维持在此水平,平均队列长度开始快速增加.当一个脉冲停止时,平均队列长度开始一个较缓的减小过程,直到网络状况开始恢复,这时新的一轮攻击开始了.通过比较攻击前后平均队列长度波动状况,发现 LDoS 攻击对路由器的服务性能产生了巨大的危害.

比较图3(a),(b)和(c),发现 T= 3 s 时,攻击周期偏小,第一波攻击过后,还没等到网络恢复到稳定程度,后续攻击波就开始了,这样队列平均长度就会在一个较低水平波动,取更小的攻击周期会对网络性能造成更大的伤害,但是它要耗费更大的攻击代价;T=4s时,刚好网络当恢复到稳



（a）T= 3 s　　（b）T= 4 s　　（c）T= 5 s

图 3　队列变化图

定状态时，下一波攻击开始，每次都能使平均队列长度趋近最大值，造成更大的丢弃概率，从而有较高的攻击性价比；T=5 s 时，攻击周期偏大，每波攻击过后，网络在稳定一段时间后才迎来下一波攻击，这样攻击性能就不佳了．所以攻击者可以根据自己的攻击效果期望和拥有的资源来选择合适的攻击周期．

2.2　攻击结果分析

首先考察 LDoS 攻击对路由器丢包情况的影响，通过分析上述实验的结果，统计出攻击前 30 s 和攻击后 30 s 合法 TCP 流在路由器的丢包情况（见表 1）．由于 LDoS 攻击对 TCP/RED 系统的影响，合法 TCP 流发送端的发送速率发生了约 40%的下降，而在路由节点上包的丢弃数却增加了数倍，由此可见 LDoS 攻击对网络性能产生了显著的影响．同时，通过比较不同周期的攻击效果还可以发现，攻击周期选得过短或者过长都会减弱攻击效果，在不能精确确定攻击周期的情况下，可以让攻击周期偏小，若周期偏大则会极大地减弱攻击效果．

表 1　路由器丢包统计

类型		接收的 TCP 包	丢弃的 TCP 包	丢包率/ %
无攻击		57 375	262	0.46
有攻击	T= 3 s	33 137	1 308	3.95
	T= 4 s	32 598	1 743	5.35
	T= 5 s	45 022	713	1.58

在试验条件不变的情况下，比较无攻击和t= 10 s 时发出的脉冲强度为 18 Mbit/s，脉冲长度为 200 ms，脉冲周期为 4 s 的攻击 2 种情况下合法 TCP 流的吞吐率（β）情况，如图 4 所示．结果表明，低速率的攻击流使合法流的吞吐率下降了 35%左右，此外，虽然 LDoS 攻击是周期性的攻击流，但是它对合法流的吞吐率的影响却比较显著且是持续的．

分析整个实验，以 T= 4 s 的实验为例，可以计算出 LDoS 流的平均速率只有 Rl/T= 1.35

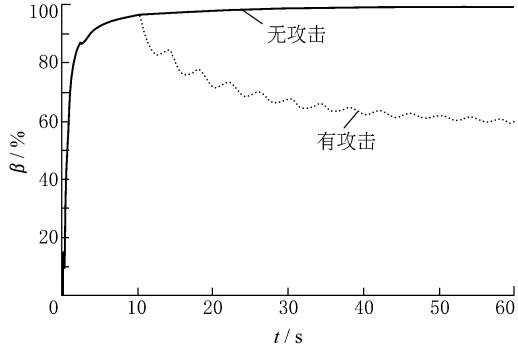


图 4　吞吐率变化

Mbit/s，但是它对网络造成的影响却是不可低估的，它的低速率特性使得系统很难用常规流量特性将攻击检测出来．此外，攻击不必以路由器为攻击目的地，只需攻击端与目的主机间的 IP 数据包经过被攻击路由器即可，这也使得检测攻击存在的难度变大．

相较于针对 TCP 的攻击而言，针对 RED 的 LDoS 攻击效果略差，但是其攻击周期更长，使得攻击的开销更小，其防范难点主要体现在：**a**．因 LDoS 攻击源端大部分时间内都保持沉默，只是周期性地在短时间间隔内发送攻击流，平均速率较低，很难将其与正常数据流区别开来；**b**．攻击所导致的系统不稳定现象与正常情况下的系统状态转换并无很大区别，除非攻击持续很长时间以后，发现系统不稳定现象一直没有消除，才可能引起检测机制的怀疑；**c**．攻击目标为网络中某一路由器，攻击数据包的源地址和目的地址都可不同，只需要它们在传输过程中都经过攻击目标即可，因此传统的以源地址、目的地址作为攻击包识别主要特征的方法在此就毫无用处了；**d**．攻击者还可能采用分布式方式来实施攻击，形成分布式低速率拒绝服务攻击（Distributed LDoS），即由多个攻击源端同时或分时地发送数据流最后在攻击目的端才汇聚成完整的攻击流，这样来自每个源端的攻击流特征将更加不明显甚至与正常数据流毫无差别，攻击检测和防范工作难度将进一步加深．

参 考 文 献

[1] Kuzmanovic A, Knightly E W. Low-rate TCP-targeted denial of service attacks and counter strategies [J]. IEEE/ACM Transactions on Networking, 2006, 14(4): 683-696.

[2] Guirguis M, Bestavros A, Matta I. Exploiting the transients of adaptation for RoQ attacks on internet resources[C] //Proceedings of the 12th IEEE International Conference on Network Protocols. Berlin: IEEE Computer Society, 2004: 184-195.

[3] Guirguis M, Bestavros A, Matta I, et al. Reduction of quality (RoQ) attacks on internet end-systems [C] //Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Miami: IEEE Computer Society, 2005: 1 362-1 372.

[4] Luo X, Chang R. On a new class of pulsing denial-of-service attacks and the defense[C] //Proceedings of Network and Distributed System Security Symposium. San Diego: Internet Society, 2005: 67-85.

[5] Zhang Ying, Mao Z M, Wang Jia. Low-rate TCP-targeted DoS attack disrupts internet routing[C] // Proceedings of Network and Distributed System Security Symposium. San Diego: Internet Society, 2007: 135-146.

[6] Sun H, Lui J, Yau D. Defending against low-rate TCP attacks: dynamic detection and protection[C] // Proceedings of the 12th IEEE International Conference on Network Protocols. Berlin: IEEE Computer Society, 2004: 196-205.

[7] Chen Y, Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis [J]. Journal of Parallel and Distributed Computing, 2006. 66(9): 1 137-1 151.

[8] Kwok Y K, Tripathi R, Chen Yu. Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks[C] //Proceedings of Networking and Mobile Computing. Zhangjiajie: Lecture Notes in Computer Science, 2005: 423-432.

[9] 吴志军, 岳 猛. 低速率拒绝服务 LDoS 攻击性能的研究[J]. 通信学报, 2008, 29(6): 87-93.

[10] 吴志军, 张 东. 低速率 DDoS 攻击的仿真和特征提取[J]. 通信学报, 2008, 29(1): 71-76.

[11] 吴志军, 岳 猛. 基于卡尔曼滤波的 LDDoS 攻击检测方法[J]. 电子学报, 2008, 36(8): 1 590-1 594.

[12] Dong K, Yang S B, Wang S L. Analysis of low-rate TCP DoS attack against FAST TCP[C] //Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications. Jinan: IEEE Computer Society, 2006: 86-91.

[13] Wei Wei, Dong Yabo, Lu Dongming, et al. A novel mechanism to defend against low-rate denial-of-service attacks[C] //Proceedings of Intelligence and Security Informatics. San Diego: Lecture Notes in Computer Science, 2006: 261-271.

[14] 魏 蔚, 董亚波, 鲁东明, 等. 低速率 TCP 拒绝服务攻击的检测响应机制[J]. 浙江大学学报: 工学版, 2008, 42(5): 757-762.

[15] 何炎祥, 刘 陶, 曹 强, 等, 低速率拒绝服务攻击研究综述[J]. 计算机科学与探索, 2008, 2(1): 1-19.

[16] Yanxiang He, Yi Han, Qiang Cao, et al. LDoS attack in Ad-hoc network[C] //Proceedings of International Conference on Wireless On-demand Network Systems and Services, Snowbird: IEEE Computer Society, 2009: 251-257.

[17] 何炎祥, 刘 陶, 韩 奕, 等. 一种针对 LDoS 攻击的分布式协同检测方法[J]. 小型微型计算机, 2009, 30(3): 13-16.

[18] 何炎祥, 曹 强, 刘 陶, 等. 一种基于小波特征提取的低速率 DoS 检测方法[J]. 软件学报, 2009, 20(4): 930-941.

[19] Floyd S, Jacobson V. Random early detection gateways for congestion avoidance [J]. IEEE/ACM Transactions on Networking. 1993, 1(4): 397-413.

[20] Guirguis M. Reduction-of-quality attacks on adaptation mechanisms[D]. Boston: Graduate School of Arts and Science, Boston University, 2007.