软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(3):591−605 [doi: 10.13328/j.cnki.jos.004520]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

低速率拒绝服务攻击研究与进展综述*

文 坤[1,2], 杨家海[1,2], 张 宾[1,2]

[1](清华大学 网络科学与网络空间研究院,北京 100084)

[2](清华信息科学与技术国家实验室(筹)(清华大学),北京 100084)

通讯作者: 杨家海, E-mail: yang@cernet.edu.cn

摘 要: 低速率拒绝服务攻击是新型的拒绝服务攻击,对 Internet 的安全造成严重的潜在威胁,引起众多研究者的兴趣和重视,成为网络安全领域的重要研究课题之一.自 2003 年以来,研究者先后刻画了 Shrew 攻击、降质攻击、脉冲拒绝服务攻击和分布式拒绝服务攻击等多种低速率拒绝服务攻击方式,并提出了相应的检测防范方法.从不同角度对这种新型攻击的基本机理和攻击方法进行了深入的研究;对 TCP 拥塞控制机制进行了安全性分析,探讨了引起安全问题的原因;对现有的各种各样的 LDoS 攻击防范和检测方案,从多个方面进行了分类总结和分析评价;最后总结了当前研究中出现的问题,并展望了未来研究发展的趋势,希望能为该领域的研究者提供一些有益的启示.

关键词: 网络安全;低速率拒绝服务攻击;异常检测;TCP 拥塞控制;主动队列管理

中图法分类号: TP309 **文献标识码**: A

中文引用格式: 文坤,杨家海,张宾.低速率拒绝服务攻击研究与进展综述.软件学报,2014,25(3):591−605. http://www.jos.org.cn/1000-9825/4520.htm

英文引用格式: Wen K, Yang JH, Zhang B. Survey on research and progress of low-rate denial of service attacks. Ruan Jian Xue Bao/Journal of Software, 2014,25(3):591−605 (in Chinese). http://www.jos.org.cn/1000-9825/4520.htm

Survey on Research and Progress of Low-Rate Denial of Service Attacks

WEN Kun[1,2], YANG Jia-Hai[1,2], ZHANG Bin[1,2]

[1](Institute for the Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China)

[2](Tsinghua National Laboratory for Information Science and Technology (Tsinghua University), Beijing 100084, China)

Corresponding author: YANG Jia-Hai, E-mail: yang@cernet.edu.cn

Abstract: Low-Rate denial of service (LDoS) attack is a new category of denial of service attacks which may become a serious threat to Internet. It has attracted many researchers' interest and is becoming an important research topic in network security area. Since 2003, researchers have revealed several kinds of low-rate denial of service attacks, such as the shrew attack, the reduction of quality (RoQ) attack, the pulsing denial-of-service (PDoS) attack and the distributed low-rate denial of service attacks (DLDoS). They also proposed some corresponding defense and detection methods. This paper thoroughly reviews the state-of-the-art of LDoS attack and prevention research, and also analyzes the basic mechanism and attack methods of different LDoS attacks. Especially, it analyzes the security of TCP congestion avoidance mechanism, and illustrates the cause of potential security issue of such mechanism. In addition, the paper also reviews and evaluates the current LDoS attack prevention and detection approaches. Finally, the paper identifies some open research issues and points out possible future research directions in LDoS attack research area.

Key words: network security; low-rate DoS (LDoS) attacks; anomaly detection; TCP congestion control; AQM

拒绝服务(denial of service,简称 DoS)攻击的方式有很多种,从广义上来说,任何可以通过合法的方式使服

* 基金项目: 国家重点基础研究发展计划(973)(2009CB320505); 国家自然科学基金(61170211, 61202356); 教育部博士学科点专项基金(20110002110056)

收稿时间: 2012-07-17; 定稿时间: 2013-11-11; jos 在线出版时间: 2013-11-28

CNKI 网络优先出版: 2013-11-28 14:41, http://www.cnki.net/kcms/detail/11.2560.TP.20131128.1441.003.html

务器不能提供正常服务的攻击手段都属于 DoS 攻击的范畴,攻击的对象可以是任何联网计算机、路由器或整个网络[1].尽管检测和防范技术越来越多[2,3],但由于 Internet 的开放式设计,使网络上缺少限制这种恶意攻击数据包的措施,网络中,任意数据包都可以发往目的地址端,加上网络上已有现成的工具[4]可被利用,因此 DoS 攻击相对容易发生,已经发展成为 Internet 严重的威胁之一.从 Arbor 公司最新的调查报告[5]显示,DoS 攻击在各种网络攻击中发生率最高、攻击流量最大,且其规模和频率还在加速增加.精心构造的攻击甚至能够达到 24Gbps 或更大的攻击流量,足以充斥任意服务器的接入带宽.许多大公司的网络都遭受到攻击,只不过它们中的大多数都没有被报道[6].

随着攻击方式的不断演变,出现了许许多多 DoS 攻击的变种[7,8].2001 年,美国的 Asta Networks 公司在 Internet2 Abilene 骨干网上监控到一种新型的 DoS 攻击.Rice 大学的 Kuzmanovic 和 Knightly 在 2003 年的 SIGCOMM 会议上,首次对该攻击的基本原理进行了描述和定义[9],称其为 Shrew 攻击,他们认为,这是一种针对 TCP 协议的 DoS 攻击,能够明显降低和限制 TCP 流量,且很容易逃避现有的 DoS 检测机制.随后,国际上其他研究者也对该攻击给出了相似的理解和定义,比如:Boston 大学的 Guirguis 等人称这种攻击为降质(reduction of quality attacks,简称 RoQ)攻击[10],香港理工大学的 Luo 等人称这种攻击为脉冲拒绝服务(pulsing denial-of-service,简称 PDoS)攻击[11],武汉大学的何炎祥、刘陶、曹强等人在文献[12]中对该攻击的基本原理和攻击方法做了很好的阐释和总结.总的看来,不管如何称呼,也不管利用的是哪种网络协议和网络服务,对其攻击原理已经达成共识,也就是:该攻击不需要维持持续的高速攻击流,它是利用网络协议或应用服务协议的自适应机制中存在的安全漏洞,通过周期性地发送高速脉冲攻击数据包,达到降低受害端的服务性能的目的.与传统的 DoS 攻击相比,该攻击有 3 个显著的特点:

- 攻击目标是各种自适应机制,攻击引起的反应和调整是合法的,这会使得受害端受到长期攻击而毫无察觉;
- 攻击流量与许多真实的数据流特征类似,因此,该攻击隐蔽性非常好;
- 攻击成本低,一个单一的攻击源就可以发动一次攻击,需要发送的数据远小于洪泛式 DoS 攻击.

因此,这种攻击不但能达到预期的效果,而且很容易逃避检测,防范难度很大.目前,Kuzmanovic[9],Sarat 和 Terzis[13],Sun[14],Chen[15]和 Wei[16]等学者都先后提出了不同的检测和防御方法.国防科学技术大学的张长旺等人、浙江大学的魏蔚等人和中国民航大学的吴志军等人分别在文献[17−19]中提出了各自的检测方法,这些检测和防御方法将在本文第 3 节详细分析和总结.迄今为止,尽管提出了不少的方法,却仍没有成熟的解决方案.不难看出,LDoS 攻击具有很强的隐蔽性和攻击性,已经对 Internet 的安全形成了严重的潜在威胁,对其进行深入的研究已是刻不容缓.

在下文中,根据国际通用的称呼,把低速率拒绝服务(low-rate denial of service)攻击简称为 LDoS 攻击,把分布式的低速率拒绝服务(distributed low-rate denial of service)攻击简称为 DLDoS 攻击.另外,当前研究的 LDoS 攻击都是针对 TCP 拥塞控制机制的攻击,因此,本文也基于此展开研究分析.

1 TCP 拥塞控制及安全分析

为防止网络的拥塞现象,提出了一系列的拥塞控制机制.Van Jacobson 首次给出的拥塞控制算法,由慢启动(slow start)和拥塞避免(congestion avoidance)两部分算法组成;1990 年出现的 TCP Reno(RFC2001)版本中,又有针对性地加入了快速重传(fast retransmit)和快速恢复(fast recovery)算法[20],避免了网络拥塞不严重时慢启动所造成的发送窗口过多降低的问题,至今已经普遍应用.近几年中,一些新的 TCP 改进版本如 New Reno (RFC2582),SACK(RFC2018),Vegas 等[21,22]也引入了新的拥塞控制机制,并被集成到 Linux 等操作系统的内核之中.

1.1 基本原理

TCP 拥塞控制的自适应原理是,发送端会根据当前的链路拥塞情况动态地调整发送报文的速率.LDoS 攻击正是利用了 TCP 拥塞控制算法中的 RTO(retransmission time out)和 AIMD(additive increase multiplicative

decrease)两种自适应机制,故意制造网络拥塞状况,使拥塞控制一直处于调整状态.尽管 TCP 拥塞控制考虑到了避免崩溃的安全问题,即设置了 RTO 的最小值和最大值,但由于这两种自适应机制调整的值大小差异明显,因此在低速率拒绝服务攻击发生时,发送端的发送速率会迅速变小,导致受害端的服务性能显著降低.

(1) RTO 机制

发送端为发送的每个报文设置一个定时器,如果在收到该报文的确认之前定时器超时,则启动慢启动算法,根据指数退避算法将 RTO 值成倍数增加,将发送端的阈值(ssthresh)设置为当前拥塞窗口(cwnd)的一半,将 *cwnd* 值设为 1,并重新发送此报文,然后等待应答报文,直到重传成功或放弃重传.其拥塞控制的状态调整如图 1 所示.

(2) AIMD 机制

当拥塞控制进入拥塞避免阶段,启动 AIMD 算法调整拥塞窗口大小,如果发送端收到 3 个重复的 ACK 报文时,*cwnd* 减半,并立即重传此报文.其拥塞控制的状态调整如图 2 所示.

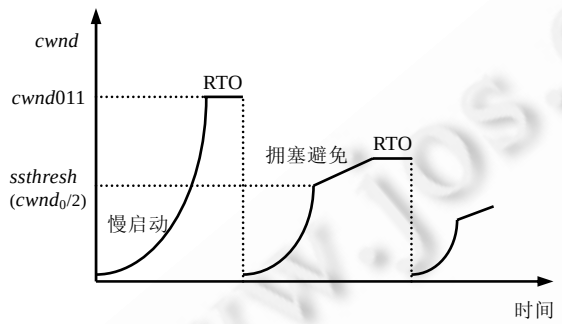

Fig.1 Adjustment of RTO mechanism

图 1 RTO 机制的状态调整

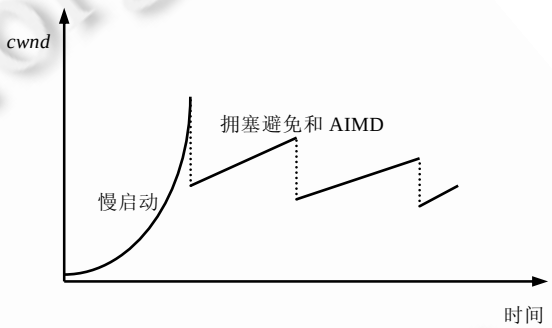

Fig.2 Adjustment of AIMD mechanism

图 2 AIMD 机制的状态调整

1.2 安全性分析

在 TCP 拥塞控制协议中,发送方仅仅通过丢包状况来判断网络是否拥塞,然后调整自身流量输出.但是,网络中除了有 TCP 协议外,还同时使用 UDP 协议等进行数据传输.那么,当网络发生拥塞时,不同的协议由于其调整的方法不同,导致协议间对网络资源的争夺失去公平性原则,进一步会引起一系列安全性问题.

1.2.1 公平性

公平性是在发生拥塞时,各源端仍能平等地共享同一网络资源(如带宽、缓存等).文献[23]中解释了产生公平性的根本原因:当发生拥塞时,必然导致数据包丢失,而数据包丢失会导致各数据流之间为争抢有限的网络资源发生竞争,争抢能力弱的数据流将受到更多损害.

传输层上的公平性问题,主要是因为面向连接的 TCP 和无连接的 UDP 在拥塞发生时对拥塞有着不同的反应和处理,进而导致对网络资源的不公平使用问题.在拥塞发生时,有拥塞控制反应机制的 TCP 数据流会按拥塞控制步骤进入拥塞避免阶段,从而主动减小发送入网络的数据量;但对无连接的数据报 UDP,由于没有端到端的拥塞控制机制,即使网络发出了拥塞指示(如数据包丢失、收到重复 ACK 等),UDP 也不会像 TCP 那样减少向网络发送的数据量.结果,遵守拥塞控制的 TCP 数据流得到的网络资源越来越少,没有拥塞控制的 UDP 则会得到越来越多的网络资源,这就导致了网络资源在各源端的分配出现严重不公平.

网络资源分配的不公平,会导致两种严重的网络安全后果:一是拥塞崩溃;二是网络中数据严重失衡,争夺能力弱(比如基于 TCP 的连接)的数据将越来越少,从而使 TCP 拥塞控制机制失去其应有的作用.后者正是产生 LDoS 攻击问题的根源.攻击者可以利用这个安全漏洞“欺骗”发送方,使发送方认为网络正在发生拥塞而抑制输出流量,这样就达到了 DoS 攻击的效果.因为,只要攻击者周期性地将攻击包注入网络而使网络发生周期性拥塞,则经过该网络的所有 TCP 连接都会周期性地丢包,就会周期性地进行拥塞控制,那么 TCP 发送方的输出流量就会明显降低.

1.2.2 效 率

从控制理论的角度,TCP 拥塞控制算法属于闭环的拥塞控制[24],经历 3 个阶段:检测网络中拥塞的发生;将拥塞信息报告到拥塞控制点;拥塞控制点根据拥塞信息进行调整以消除拥塞.这种闭环的拥塞控制可以动态地适应网络的变化,但它的缺陷是算法性能受到反馈延迟的影响,算法性能也因此可能严重下降,资源的使用效率将会大幅度降低.

TCP 拥塞控制协议使用了两种大小有明显差异的时间尺度来调整源端的发送速率,RFC2581 中进行了详细的描述:一个是往返时间(RTT),这是一个比较短的时间,一般为 10ms~100mx.在链路轻度拥塞的情况下,表现为发送端重复收到 3 个相同的确认报文,此时就进行 RTT 时间尺度控制,主要是采用 AIMD 策略实现拥塞控制,使各发送端以一个相对合理的速率发送报文;而当网络重度拥塞的时候,表现为在超时重传时间内没有收到确认,此时使用 RTO 的时间尺度,RFC2988 中最小 RTO 值缺省为 1s.在网络发生拥塞时,不管是采用 RTT 值,还是采用 RTO 值进行控制,网络的使用效率都会减小.LDoS 攻击正是利用了这点,就是当网络在遭受攻击后,拥塞控制机制不断使用 AIMD 和 RTO 机制进行调整,如果链路的拥塞状况一直得不到改善,资源使用效率会不断减小,特别是使用 RTO 时间尺度机制调整时,效率更会急剧下降.

简单地说,由于公平性原因,在遭受 LDoS 攻击时,相对 UDP 数据流量而言,TCP 流量明显减少,与此同时,TCP 自身拥塞控制机制加剧了使用效率进一步恶化.如果出现这种情况,TCP 协议将面临一个非常尴尬的局面.

2 LDoS 攻击基本模型及方法

2.1 攻击数据流基本模型

2.1.1 单源攻击

LDoS 攻击利用上述两种自适应机制,发动周期性的脉冲攻击,其攻击波形如图 3 所示,其中,T 代表攻击周期,R 代表攻击速率,L 代表单个攻击脉冲持续时间.当攻击强度($R\times L$)足够大时,就可以造成足够多的报文丢失,从而引发上述 RTO 或 AIMD 机制,造成持续频繁的自适应调整,从而达到攻击的效果.

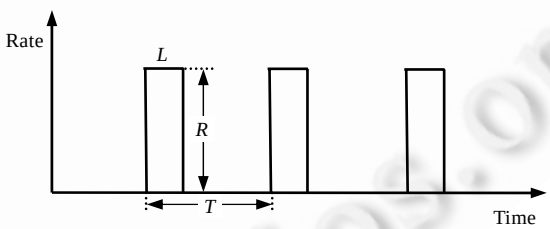

Fig.3 Pulse of LDoS attack

图 3 低速率拒绝服务攻击流示意图

2.1.2 分布式攻击

DLDoS 攻击由多个攻击源协同攻击,因此攻击强度更大,且攻击特征更加不明显.主要有两种方式:一种是图 4 所示,攻击源(假设 n 个)在每个攻击周期内同时产生一定强度的攻击脉冲($r\geq R/n$),这些脉冲在受害者端聚成高强度脉冲($\approx R$).这种方式对攻击源之间的同步要求较高,实现难度较大;另一种方式是图 5 所示,攻击源分周期发送攻击脉冲,即各源端攻击周期为 nT,脉冲强度为 R,最后在受害者端形成攻击周期为 T、脉冲强度为 R 的完整攻击.与图 4 相比,这种攻击方式对同步的精度要求较低,因为 LDoS 攻击周期一般为 1s~5s,而链路往返延迟 RTT 一般小于 0.1s,轻度延迟误差对攻击整体效果影响不大.

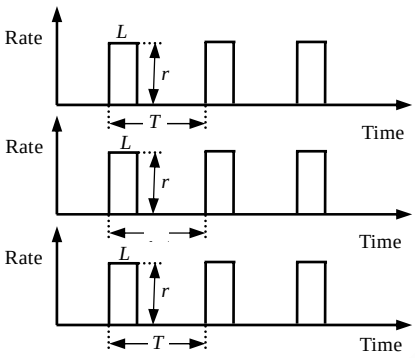

Fig.4 Synchronous DLDoS attack

图 4 同步的 DLDoS 攻击

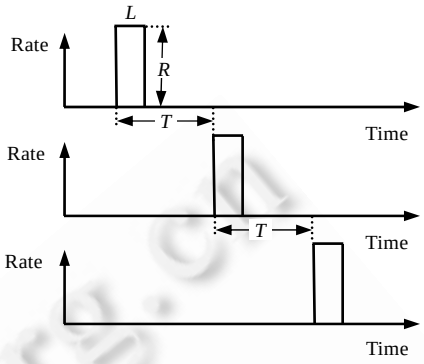

Fig.5 Asynchronous DLDoS attack

图 5 异步的 DLDoS 攻击

2.2 基于RTO机制的攻击

理论上讲,如果攻击者能够精确知道 TCP 发送端每次发送报文时的 RTO 值,就可以在其每次重传数据包的时候发动攻击脉冲,使得每次重传都超时,*cwnd* 始终保持为 1,达到最大化攻击效果.而实际上,根据 TCP 协议 RFC2988,RTO 值是一个动态值,需要根据往返时间 RTT 更新 RTO 值.RTO 的核心算法见公式(1):

$$RTO=\min\{RTO_{\max},\max\{RTO_{\min},SRTT+\max(G,4\times VRTT)\}\} \tag{1}$$

其中,G 是时间尺度,SRTT 和 VRTT 分别表示平滑后的往返时延和往返时延的变化.

实际上,由于该值跟发送端每次收到的 RTT 值有关,所以是动态的,根本无法精确预测.一般正常链路状态中 RTT 较小,因此 $SRTT+\max(G,4\times VRTT)$值也较小,$RTO_{\min}>SRTT+\max(G,4\times VRTT)$.根据公式(1),RTO 取 $RTO_{\min}$,通常设为 1s.

当一个攻击脉冲发出后,TCP 发送端进入超时重传状态,此时,需要延长较短的时间 T_{lag} 发送下一个脉冲,使得发送端能够在 T_{lag} 时间段内成功地重传并发送一些数据包,这样可以让发送端从超时重传中恢复过来,从而使 RTO 值能够通过公式(1)的计算重新回到 $RTO_{\min}$,保证了攻击周期保持不变.一般情况下,可以将 T_{lag} 设为 2~3*RTT*,那么,攻击周期为 $RTO_{\min}+T_{lag}$,攻击效果如图 6 所示.

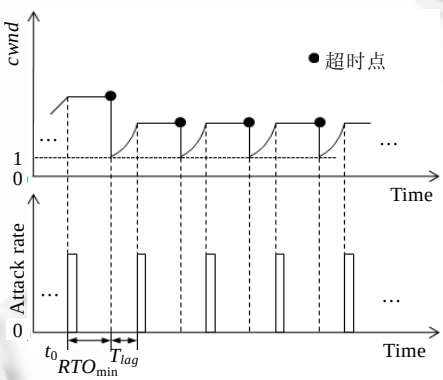

Fig.6 LDoS attack based on RTO mechanism

图 6 基于 *RTO* 重传机制的攻击

Knightly 提出的 Shrew 攻击[9]就属于这类攻击,其攻击模型如图 6 所示[12].它使 TCP 发送方在每个周期内自动地采取超时重传拥塞控制.这种攻击方法效果不错,但是有一个缺陷,就是如果要使 TCP 发送方采取超时重传,就要让瓶颈路由器发生严重的拥塞来丢弃大部分包,因此,攻击者需要注入网络的数据包数量太多,容易被

检测出来.不过,快速重传/恢复具有同样的问题,只不过如果要使 TCP 发送方不断采取快速重传/恢复,那么攻击者所需注入的数据包个数就要少很多.

2.3 基于AIMD机制的攻击

理论上,这种攻击每次都使 *cwnd* 减半,最终,*cwnd* 会减少到 2.与基于 RTO 的重传机制不同,AIMD 机制用于轻度拥塞情况下的控制,TCP 发送方所收到的拥塞信号是 3 个重复的 ACK 报文,而不是重传计时器超时.所以,基于 AIMD 机制的攻击需要的攻击脉冲强度相对弱一些,AIMD 算法的核心可以用公式(2)表示:

$$\begin{cases} I: W_{t+R} \leftarrow W_t + \alpha,\ \alpha > 0 \\ D: W_{t+R} \leftarrow \beta \times W_t,\ 0 < \beta < 1 \end{cases} \tag{2}$$

其中,I 表示增加算法,在一个 RTT 内接收到 ACK 确认包时使用;W_t 是 t 时刻 *cwnd* 的值;R 代表 RTT;W_{t+R} 代表又过了一个 RTT 后的 *cwnd* 值;α是参数值;D 表示乘性减小算法;β是参数值.通常,α,β分别为 1 和 0.5.

基于 AIMD 机制的 LDoS 攻击需要的攻击周期比较短,持续的脉冲攻击使窗口的收敛值越来越小,攻击效果如图 7 所示.RoQ 攻击的一个特例即是对 AIMD 攻击[10],可以使用持续时间更短、周期更小的脉冲针对 TCP 拥塞控制中 AIMD 机制进行有效攻击.

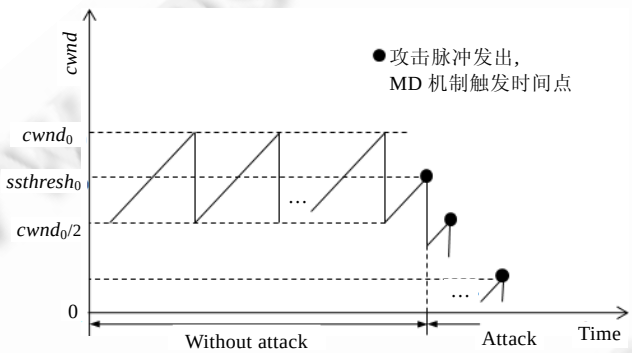

Fig.7 LDoS attack based on AIMD mechanism

图 7 基于 AIMD 机制的攻击

在实际 Internet 中,由于 TCP 发送方的拥塞窗口是同时受 RTO 和 AIMD 两种机制控制的,因此,实际攻击效果很可能是基于 RTO 和 AIMD 两种情况交替出现,即某一时刻攻击产生超时重传效果,而另一时刻则可能产生 AIMD 的效果,这取决于攻击强度以及当时网络中的拥塞状况.

3 LDoS 攻击的检测和防御

一般传统的 DoS 攻击检测方法是针对网络数据流和服务器负荷激增等特征进行检测的,而 LDoS 攻击表现出来许多不同的特征,比如攻击数据流平均速率较低、服务器负荷不升反降等.因此,传统的检测方法很难适用于检测 LDoS 攻击.在这里,根据是否需要提前建立攻击模式特征库,可以将大多数检测方法分为两类:特征检测和异常检测.特征检测针对具有明确攻击特征的已知攻击,要先建立了一个特征库,如果检测到数据与特征库中的特征参数匹配,则判定为有攻击发生.异常检测针对尚无明确攻击特征的未知攻击,需要用统计的网络数据建立一个正常的网络流量模型,如果检测到的数据使得流量模型出现异常,则判定为有攻击发生.除此之外,研究者还提出了一些其他的方法,比如改进网络协议和服务协议的防御方法、基于终端服务器的检测和防御等.

3.1 特征检测及防御

自提出 LDoS 攻击以来,研究者对其攻击特征进行了不少的分析和总结.尽管其平均速率低、隐蔽性很强,但其脉冲强度、持续时间和攻击周期等特征也很明显,特别是结合其周期性特征和短时高速脉冲特征,能够很好检测到攻击.当识别到正遭受 LDoS 攻击时,最常见的防御策略就是改进路由器的主动队列管理(active queue

management,简称 AQM)技术.其目的一是丢弃符合设定攻击特征的数据流的数据包;二是重新进行带宽分配,尽量保护 TCP 数据流,抑制 LDoS 攻击流.

AQM 技术是 IETF 为了解决 Internet 拥塞控制问题而提出的一种路由器缓存管理技术.它具有主动防御的特性:根据队列的实时情况自动地进行拥塞控制.AQM 会根据各种网络特性进行,计算一定的概率来提前丢包,从而达到减少和避免网络拥塞,提高服务质量.在现有的主动队列管理机制方案中,判断拥塞的度量有队列长度、输入速率、缓冲溢出或空白等网络特性.

文献[30−32]讨论了在网络发生拥塞时,如何通过丢包来管理队列长度.AQM 的目的就是将队列长度稳定在一个较小的值,使得最小化数据传输延迟,最大化此路由器的吞吐量.改变路由器的队列管理机制,可以减弱低速拒绝服务攻击的效果.

最早提出的 AQM 算法 RED[31]采用平均队列长度这个度量计算丢包概率,以这个概率来丢包.这个概率是队列长度和空闲时间的线性函数.BLUE[33,36]会监测链路的空闲状态、丢包事件.BLUE 的主要思想是通过链路空闲和缓冲溢出的状况来调整报文标记丢失概率.如果缓冲溢出,就增大概率;如果线路空闲,就减小概率.BLUE 的稳定性较好,但会造成缓冲频繁溢出.AVQ[34]利用线性微分方程在线调节虚拟容量,对利用率因子进行调整,对两个性质进行恰当的折衷:高利用率和低时延.但是 AVQ 的性能还不甚完善,因为 AQM 没有对队列长度的显式控制.还有 REM[30]机制,REM 探测和控制网络的拥塞状态是利用了网络优化理论中价格的概念来进行的.计算丢弃分组概率的依据是依赖于价格的特性,丢弃概率与“价格”呈指数关系.

在 LDoS 攻击时,RED 路由器使系统一直交替地处于过载(over-load)和欠载(under-load)的状态,队列长度始终无法稳定,从而严重影响路由器的性能,增长数据传输延迟时间,减小路由器吞吐量[35,37].另外,RED 机制还会直接影响端系统的数据传输控制,因为端系统的拥塞控制反馈信号全都来自于队列管理情况(丢包或标记).所以当路由器受到攻击时,其会向端系统传输控制机制发送大量噪声反馈信号,端系统会根据这些反馈信号调整自己的发送速率,而以新的速率发送的包又会导致队列抖动更为严重,有时队列甚至为空,网络链路利用率急剧下降.

基于 LDoS 攻击数据流量的周期性特征,Sun 在文献[14,45]中提出了一种采用动态时间封装(dynamic time warping,简称 DTW)的方法进行攻击识别.他对 LDoS 攻击的数学模型进行定义,用一个五元组(T,L,R,S,N)描述攻击的特征,其中,T 表示攻击的周期,L 表示一个突发攻击流持续的时间,R 表示突发攻击流量的峰值速率,S 表示计时开始到第一个突发攻击流量开始之间的时间差,N 表示背景流量的等级;并提出:在路由器上使用差额循环(deficit round robin,简称 DRR)调度算法对带宽进行分配,以保护 TCP 数据流的资源.这种方法可以识别攻击周期和脉冲长度变化的基于 RTO 或 AIMD 机制的 LDoS 攻击.但是,DTW 方法检验的误报率很高,而且需要链路中的背景流量在一个较低的范围内,且其中所采用的 DRR 算法并没实现对 LDoS 攻击流的过滤作用.

基于 LDoS 攻击数据流短时高速脉冲特征,Kuzmanovic 在文献[9]、Sarat 和 Terzis 在文献[13]、Lija Mohan 在文献[38]中都提出了利用 AQM 机制来防御 LDoS 攻击的方法.这些方法都监测变化剧烈的数据流量,能够有效过滤基于 RTO 机制的攻击流.然而,现有路由器 AQM 机制(如 SRED[35]等)对持续较长时间的高速数据流的调整效果更为明显,如果更改 AQM 机制使其对短时高速率流也起到过滤作用,则可能导致大量合法 TCP 数据流一并被识别成非法数据流一起过滤掉.

针对这种情况,Kwok 在文献[39]中提出了一种新的路由器队列管理方法 HAWK,其在传统 AQM 算法的基础上又加入了一种数据流检测算法,主要利用 LDoS 攻击的脉冲强度、持续时间和发送周期等特征,分别对数据流短时间间隔内峰值速率以及长时间间隔峰值速率设定门限值,如果检测到符合设定的数据流,则判定其为 LDoS 攻击,丢弃此数据流的所有数据包.Luo 在文献[40]中建立了一个称为 Vanguard 的检测系统,可以使用更多的攻击特征和流量变化特征实现更大范围的检测,不仅包括 LDoS 攻击,也可以检测传统的拒绝服务攻击.

在构造 LDoS 攻击的防御方法时,绝大多数研究者会在路由器上选用一种 AQM 机制,并对 AQM 算法做相应的修改,使之适应 LDoS 攻击所造成的拥塞模式.当路由器在收到攻击数据流的时候会感觉到拥塞,于是会主动丢弃攻击流中的包,降低攻击的效果.这种特征检测及防御方法的优点是容易实现,对基于 RTO 和 AIMD 机制

的 LDoS 攻击都有很好的防御效果;其缺点是误报率较高,且需要一定的存储空间来存放攻击流特征信息.

3.2 异常检测及防御

特征检测需要有明确的攻击特征,通过特征匹配来检测攻击行为,但是对于层出不穷的新类型攻击而言,攻击特征并不完全明确,特征检测方法误报率会很高;同时,特征检测方法很容易将 Internet 上正常的数据流误报为攻击流量,比如流媒体点播 RTSP 协议、VoIP 等业务所产生的瞬时突发流量等.因此,为解决上述问题,有些研究者采用了异常检测的方法.迄今为止,研究者已将小波变换分析[50]、频谱分析、统计分析和信息度量分析等技术引入到异常检测中来提高检测效果.

(1) 小波变换分析

小波变换能够同时在时域和频域突出信号的局部特性,几乎所有的信号都能根据从原始数据提取出来的某些特征来表现信号[51,52].

在 Luo 提出的 PDoS 攻击检测方法中,使用了一种基于小波分析的两阶段检测方法[11],实现高精度的检测:

首先,使用离散小波变换(discrete wavelet transform,简称 DWT)分析路由器中到来的流量与发送的 TCP ACK 流量的变化.DWT 由度量函数$\varphi_{j,k}(t)$和小波函数$\psi_{j,k}(t)$组成.小波函数的表现与使用窄时间窗口计算信号差异的高通滤波器类似,可以检测到来数据流量的变化;而度量函数可以起到低通滤波器的作用.度量函数与小波函数的结合可以检测发送的 TCP ACK 流量的变化.为了实现在线检测,使用了滑动窗口进行连续 G 组取样,对于到来数据流量的第 n 个取样信号强度的度量,使用了基于统计的方法;

在第 2 阶段,使用累积和(cumulative SUM,简称 CUSUM)算法,根据 ACK 数据包变化的规律检测攻击的发生,将第 1 步骤得到的两个值 $E_H(n)$和 $E_L(n)$转换成随机序列:$Z_H(n)=E_H(n)-\beta_H$;$Z_L(n)=\beta_L-E_L(n)$.其中,β_H取 $E_H(n)$序列的上界,$\beta_L=\overline{E_L(n)}-P_{tolerance}\times[\Delta(E_L(n))]$,$\Delta(E_L(n))$是 $E_L(n)$序列的标准差.累积和算法用于检测偏移,通过累积误差来检测待检对象与目标之间的偏移.其使用持续时间更短、周期更小的 UDP 脉冲攻击 TCP 的拥塞避免过程,通过两阶段的检测算法,在路由器上检测攻击流量.该算法更多的是针对 RTO 攻击的特征,对于其他类型攻击的检测效果一般.

(2) 频谱分析

在 LDoS 攻击过程中,正常的 TCP 流和异常的攻击流在传输中呈现周期性,而周期信号和非周期信号在频率域呈现不同的特性,因此,可以利用傅立叶转换在频谱域中检测这些差异.

Chen 团队在文献[15,25,44]中用时域和频域变换方法实现低速率攻击的检测,魏蔚[18]和吴志军[19]也提出相似的频谱特征检测方法.这种方法存在的一个重要缺点是:频域变换造成计算复杂度增加,检测速度慢,不适合高速网络.为了解决这个问题,在文献[45]中,Chen 等人提出了一个 FPGA(field programmable gate array)的嵌入式加速器,它具有强大的计算能力和类似软件的灵活性.虽然增加了硬件成本,但是新的方法可以在几秒钟之内就迅速地检测到 LDoS 攻击.这种方法不仅可以检测出 Shrew 攻击和传统洪泛式 DoS 攻击,而且还可以检测出各种周期变化的基于 RTO 或 AIMD 机制的 LDoS 攻击.

(3) 统计分析

统计分析需要先建立一个统计模型,比如马尔科夫模型等.如果建立的统计模型与真实数据的实际分布相符合,则异常检测的准确率是很高的.但是在实际的应用当中,特别是以高维数据或者数据流为处理对象时,很难建立非常准确的统计模型.

Xie 在文献[46]中研究了针对 HTTP 服务的 LDoS 攻击,文中提出了使用通过 Web 服务器上可以获得的文件关注度,用矩阵作为关注度的度量,通过多元化统计分析检测针对 HTTP 协议的 LDoS 攻击.他认为:尽管用户关注的内容不同,文章的关注度在高负荷的 Web 网站上仍具有一定的稳定性,可以作为检测的信号.同时,针对仅仅使用文档关注度作为检测时误报率比较高的问题,作者采用扩展隐性马尔可夫模型的方法,用来观察文件关注度矩阵的变化以及监视针对 HTTP 协议的 LDoS 攻击.在文献[53,54]中,都是通过对 TCP 流量变化情况进行统计分析,根据攻击前后 TCP 流量的明显变化,从而判断是否有攻击发生.这类检测算法检测速度快,但误报率很高.

(4) 信息度量分析

信息熵(entropy)用于判断网络系统的离散和无序程度,文献[55–58]中对其应用在网络安全领域的检测效果都进行了验证,其检测实时性好,检测精度高.

Xiang 等人[26]利用广义熵和信息距离在分离度上优于传统的香农熵和 KL 距离的原理,提出了一种新的信息度量对低速率分布式拒绝攻击进行检测和回溯,基于这两种新的信息量度的检测算法,可通过调整参数值来调节检测精度,以满足不同的检测要求.另外,文章提出的回溯算法可以跟踪到攻击者所在的子网,切断攻击流量,并作出标记.该方法的优点是检测的实时性好、精度高,缺点是需要在每个路由器部署监测点,成本高.

(5) 小信号检测分析

吴志军[49]利用小信号检测理论,提出一种基于小信号模型的 LDoS 攻击检测的方法.该方法通过构造特征值估算矩阵,对 30s 时间内(3 000 个采样点)到达的数据包个数进行统计,则通过特征值估算矩阵,可较精确地检测并计算出 LDoS 攻击的周期值.在 NS-2 环境中的仿真实验结果表明,本方法具有较高的检测率.

相对而言,异常检测的方法可以对时间序列变化信息进行更全面细致的分析,因此检测精度比较高.但是现有的异常检测方法在检测 LDoS 攻击时,只是从整体上分析信息变化情况,却都没有考虑基于 RTO 和 AIMD 机制的攻击之间的差别,因而不能更准确地区分攻击方法.如果要检测这两种不同的攻击方式,需要利用时频分析的方法在局部进行更多的分析:一方面,在频率变化上要划分更多层进行分析;另一方面,在时间上要进行信息变化的周期性分析.

3.3 基于终端应用服务器的检测和防御

Gabriel 等人对基于应用服务器端的 LDoS 攻击建立了一个数学模型[41],这种模型允许在动态网络中,通过配置攻击参数实现对相关性能的评估.通过将性能结果与仿真结果比较,证明该数学模型是有效的.但其在建模中忽略了攻击时的有序的、动态的进程.基于此,Xu 等人针对应用层协议提出了一种针对应用服务器的低速率拒绝服务攻击(low-rate denial of service attacks against application servers,简称 LoRDAS)[42].从一个全局的观点进行观察和研究,提出了一种攻击进程的队列模型,把攻击作为一个单独的进程,通过改变场景和协同不同攻击策略,精确地表示动态的行为.通过计算概率分布,评估了攻击带给不同网络流量的影响程度.通过实验分析,证明了该模型能精确地描述攻击行为.

Chang 等人提出了一种简单的保护机制 SAP(shrew attack protection),用来抵御 shrew 攻击[43].不需要试图跟踪和分离 shrew 攻击者,SAP 通过监视端口丢包率进行辨别 TCP 受害者,优先使来自于受害者丢包率高的数据包送入输出队列.这样,确保 TCP 对话可以带宽共享.仿真证明:在 shrew 攻击下,SAP 可以防止 TCP 对话关闭,有效地使 TCP 流量保持一个高吞吐量.SAP 是一个基于端口的终端机制,只需要少量计数器就可以找到潜在的受害者,这使得 SAP 很容易在现有的路由器机制的顶端实现.

3.4 改进网络协议和服务协议

LDoS 攻击的对象是各种自适应机制的网络协议和服务协议,对它们进行修改、填补漏洞才能彻底避免遭受 LDoS 攻击.除了针对 TCP 协议的分析,还有 BGP 协议[47,48]和 HTTP 协议[46]的分析,但主要还是针对基于 RTO 机制的 LDoS 攻击,最早也最具有代表性的是针对 Shrew 攻击随机化 $RTO_{\min}$ 方法.在这种方法中,用 $\rho(T)$ 表示攻击的效果,TCP 的发送端在 $[a,b]$ 范围内随机化其自身的 $RTO_{\min}$.当 $T\geqslant b$ 时,$\rho(T)=\dfrac{T-\dfrac{a+b}{2}}{T}$,当 $T\in[a,b)$ 时,令 $k=\dfrac{b}{T}$,则有,

$$\rho(T)=\frac{T-a}{b-a}\frac{T-\dfrac{T+a}{2}}{T}+\sum_{i=1}^{k-1}\frac{T}{b-a}\frac{T/2}{(i+1)T}+\frac{b-kT}{b-a}\frac{(k+1)T-\dfrac{kT+b}{2}}{(k+1)T};$$

当 $T<a$ 时,可以近似地认为

$$\rho(T)=\begin{cases}\dfrac{\dfrac{a}{T}T-\dfrac{a+b}{2}}{\dfrac{a}{T}T}, & k=1\\ \dfrac{\dfrac{a}{T}T-a}{b-a}\dfrac{\dfrac{a}{T}T-\dfrac{\dfrac{a}{T}T+a}{2}}{T}+\sum_{i=1}^{k-1}\dfrac{T}{b-a}\dfrac{T/2}{(i+1)T}+\dfrac{b-kT}{b-a}\dfrac{(k+1)T-\dfrac{kT+b}{2}}{(k+1)T}, & k\geqslant 2\end{cases}.$$

该方法通过随机化 $RTO_{\min}$ 破坏了 RTO 的周期性规律,这使得攻击者无法准确预测 TCP 端下一次发送数据的时间,也就无法在准确的时刻发送攻击数据流,从而能够有效防御 LDoS 攻击.Yang[27]也提出了相似的观点,并通过模拟实验对其进行了进一步验证.Efstathopoulos[28]通过对一个实际系统(Linux)的研究,证明了这种利用 RTO 随机化方法实现低速率拒绝服务攻击防御的有效性.

这种方法虽然在一定程度上能够减轻攻击的影响,但同时会带来许多的负面影响,比如在没有 LDoS 攻击的时候会降低 TCP 的性能.另外,这种方法始终无法判断是否存在 LDoS 攻击.更加麻烦的是,Internet 上许多重要的网络协议和服务协议已经广泛实现和应用,要对其进行修改和更换,涉及几乎所有合法用户程序,成本太高,因此,该方法不太可行.

3.5 LDoS攻击的检测和防御方法比较

根据近 10 年的研究情况来看,LDoS 攻击的检测和防御方法五花八门,为清晰起见,分别将检测和防御进行列表分析比较.表 1 从检测技术、检测到的攻击类型、识别率、误报率、实时性、其他开销和部署位置等方面显示了各种检测方法之间的差异.表 2 列出了几种防御方法各自的策略,并对各自优缺点进行了比较.

Table 1 Comparison table of detecting methods

表 1 LDoS 攻击检测方法比较表

检测类型		检测技术	能检测到的攻击类型	识别率	误报率	实时性	其他开销	部署位置
特征检测	周期性特征	DTW	LDoS	低	高	好		受害端 路由器
	高速脉冲特征	AQM 识别	LdoS, DoS	低	高	好		受害端 路由器
	多种特征混合	HAWK	LDoS	低	低	好	计算、存储	受害端
		Vanguard	LdoS, DoS	高	低	一般		路由器
异常检测		DWT(离散小波变换)	LdoS, DoS	高	低	一般		受害端 路由器
		频谱分析	LDoS	高	低	一般	计算量大, 需要硬件支持	受害端 路由器
		统计分析	LDoS	低	低	一般		受害端 服务器
		信息度量	LdoS, DoS, DDoS	高	低	好	多点部署、 成本高	整个网络 路由器
		小信号检测分析	LDoS	高	低	一般		受害端 路由器

Table 2 Comparison table of defending methods

表 2 LDoS 攻击的防御方法比较表

防御方法	部署位置	防御策略	优点	不足
改进 TCP 协议	整个网络	随机化 $RTO_{\min}$	有效抵御 Shrew 攻击	成本太高, 实现困难
改进 AQM 算法	受害端 路由器	提高攻击包丢弃概率	容易实现	误报率高, 防御效果一般
		带宽分配,保护正常流	能减缓攻击效果	
增强受害端服务器功能	受害端 服务器	SAP(Shrew Attack Protection)	有效识别和抵御 Shrew 攻击	不能应对 其他攻击

4 研究展望

LDoS 攻击已经引起了部分国内外研究者的关注,相关文献也在增多.研究者对其基本攻击原理已经形成共识,根据目前的研究,本文认为,应特别关注 LDoS 攻击以下几个重要特征:

(1) 隐蔽性

LDoS 攻击的特征不明显,每次攻击流量持续时间都很短,与很多基于 UDP 的正常应用如流媒体点播 RTSP 协议、VoIP 等业务所产生的瞬时突发流量非常类似.另外,LDoS 攻击利用的是自适应机制中的动态调整过程,攻击时,服务器系统流量不升反降,这会使得网络长期受到攻击而没有察觉.因此,现有的入侵检测机制难以检测到 LDoS 攻击.

(2) 多样性

现有的攻击方法非常少,也比较单一,基本上都是针对 TCP 拥塞控制协议的攻击.攻击的目标要么是路由器,要么就是单个服务器,攻击的变种也只是形式上的简单变化.实际上,从广义上来讲,任何使用较小的成本就能使服务器不能提供正常服务的攻击手段都属于 LDoS 攻击的范畴,被攻击的对象可以是联网主机、路由器或者是整个网络,利用的安全漏洞可以包括所有具有自适应机制的任何网络协议或系统.

(3) 分布式

分布式的攻击将会使攻击的特征更加不明显,检测和防范的难度更大,攻击效率却更高.不难预料,DLDoS 必将成为未来网络安全的巨大威胁,是一个重要的研究领域.同样,LdoS 的最佳防范方法也应采用分布式体系结构.然而不论是在传统的 DoS 防范上,还是在 LDoS 防范中,分布式的方法存在着诸多困难,如在异构网络环境下消息的传递方式、知识的共享与理解、检测点的部署问题、防范系统本身的安全性和鲁棒性等,这些都是需要进行广泛研究的问题.

总的来讲,当前大多数对 LDoS 攻击的研究是在一种比较理想的状态下进行的,研究中还存在许多不明确的或未知的问题,研究还处于起步阶段.下面,重点从 3 个方面分析当前研究存在的不足,并指出未来研究需要关注的问题:

(1) 攻击原理和攻击方法的研究

文献[9−11]等对攻击基本原理和攻击方法都进行了深入的探讨,但是绝大多数有关 LDoS 攻击方法都是针对 TCP 协议的拥塞控制机制的.事实上,Internet 上应用的大量具有自适应机制的网络协议和服务协议都可能成为攻击的对象[46,47].因此,研究者应该多关注其他自适应机制的协议和服务的工作原理,拓展研究的范围.另外,攻击者为达到自己的攻击效果,会不断有新的变种、新的攻击方式诞生,防范的难度也随之增大,这需要在未来的研究中格外关注.

(2) 攻击检测和防御方法的研究

传统 DoS 攻击的检测和防御一直是一个难以解决的问题,而与传统 DoS 攻击相比,低速率 DoS 攻击的检测和防范更加困难.迄今为止,研究者提出了许多不同的检测和防范方案.比如:根据 LDoS 攻击的周期性和短时高速脉冲等显著特征,文献[9,11,13,14,38,39]等分别提出了不同的特征检测方法,并通过改进路由器的 AQM 算法,丢弃识别到的攻击流,有效地防御了 LDoS 攻击;为了提高对新型或未知攻击类型的检测精度,文献[18,19,26,27,52]等提出了不同的异常检测方法;另外,文献[41−43]提出了基于终端应用服务器的检测和防御方法,也有很好的防御效果.尽管这样,目前还没有成熟的检测和防御方法.对于这种新型的攻击类型,本文认为未来应特别重视以下 3 方面问题的研究.

- 建立完善的网络流量统计模型.

要统计的网络流量,是指网络层主机到主机的数据流和传输层端口到端口的数据流.一个网络流由一组属性唯一识别:源 IP 地址、目的 IP 地址、源端口、目的端口、协议类型、服务类型、路由器输入接口等.为提高检测的精确性,统计常常同时选取多个属性统一研究.

网络流量统计为检测提供基础研究数据,依据 LDoS 攻击的特点,网络流量数据统计主要包括统计包特征和流特征在时间轴上的分布、网络总体流量统计、包尺寸分布统计、协议使用和分布统计、地址分布统计等.

- 建立合适的异常检测模型.

每种攻击类型都有其自身特征,只有选定合适的数学分析模型,才能建立有效的异常检测方法.在第 3 节已经提到了许多异常检测技术,未来的研究除了要灵活应用已经提到的各种技术,还应关注已经在网络安全领域有不错表现的其他技术.比如基于分类的异常检测技术、基于最近邻居的异常检测技术和基于聚类的异常检测技术等.

异常检测只检测网络流量中的一个或几个特征向量,而且选取的特征向量和攻击特征并不一一对应,因而异常报警时只能判定异常,而无法提取和描述具体的攻击特征.为实现精确检测并及时判定攻击类型,常常需要运用 Internet 安全测量等技术配合异常检测方法[59,60].

- 加强 DLDoS 攻击的检测研究.

尽管国防科学技术大学的张长旺[17]和 Xiang[27]等人提出了一些 DLDoS 攻击的检测过滤方法,但这还远远不够.分布式网络攻击是该攻击的演变方向,因此,攻击防范要能实现对分布式网络攻击的检测.该攻击隐蔽性强,攻击特征不明显,分布式的攻击将会使攻击的特征更加不明显,检测和防范的难度更大,攻击效率却更高.不难预料,DLDoS 必将成为未来网络安全的巨大威胁.

此外,新的检测与防范方法要注重其实时性和兼容性.如果受害者具有巨大的经济、军事意义,那么较高的检测时延会带来巨大的损失.因此,要求能够快速检测到 LDoS 攻击并及时响应.进一步讲,如果能将针对 LDoS 攻击的检测模块有效地整合到现有的入侵检测系统中,这样既可以检测 LDoS 攻击,又可以检测其他类型的攻击,从而设计出更完善、更有效的检测和防范方案.

(3) 实验验证问题

当前的实验环境都是自己建立的模拟仿真环境,攻击的效果和检测的方法等也都是在模拟的或者简单的网络环境下得出的,这种没有充分考虑复杂网络的各种实际情况而得到的数据分析结果是无法让人信服的,提出的解决方案都会因理想化而无法得到验证.

因此,在利用仿真实验环境对上述理论模型进行初步验证的基础上,要从理论到实践,对上述理论模型要在真实复杂的网络环境中验证,在验证的基础上,进一步调整特征指标体系,优化模型.

5 结 论

本文首先介绍了LDoS攻击发展历程和不同研究者对它的独到见解,并针对TCP拥塞控制机制进行了安全性分析,找到了其安全漏洞的根源;接着,分类描述了攻击的基本模型和现有攻击方式的基本原理;对于现有的各种各样的 LDoS 攻击检测和防御方案,从多个方面进行了分类总结和分析;本文最后对当前研究中出现的问题和未来的研究趋势提出了一些理解和建议.LDoS 攻击是一种新兴的网络攻击手段,由于其行为隐蔽性强、危害性大等特点,需要我们进一步研究这种最新的网络攻击形式.通过分析和挖掘这类攻击的原理和基本规律,掌握在这类攻击发生情况下的流量特性和流量分布特性的变化规律,从而提出新的有效的检测和防御技术,防止其危害进一步扩大.

致谢 感谢安长青和王会老师的耐心指导;感谢实验室王子玉博士、李福亮博士和其他同学在写作过程中给予的无私支持和帮助.

References:

[1] Chang RKC. Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Communications Magazine, 2002,40(10):42−51. [doi: 10.1109/MCOM.2002.1039856]

[2] Hussain A, Heidemann J, Papadopoulos C. A framework for classifying denial of service attacks. In: Proc. of the ACM SIGCOMM 2003. Karlsruhe: ACM Press, 2003. 99−110. [doi: 10.1145/863955.863968]

[3] Hao S. Research on intrusion detection to denial of service attacks [MS. Thesis]. Beijing: Tsinghua University, 2005 (in Chinese with English).

[4] Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 2013,15(4):2046−2069. [doi: 10.1109/SURV.2013.031413.00127]

[5] Worldwide infrastructure security report. Volume Ó. Arbor Networks, 2011. http://www.arbornetworks.com/report

[6] Sun CH, Liu B. Survey on new solutions against distributed denial of service attacks. Acta Electronica Sinica, 2009,37(7): 1562−1571 (in Chinese with English abstract).

[7] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review, 2004,34(2):39−53. [doi: 10.1145/997150.997156]

[8] Xu QH. A core technique of DDoS attack prevention [MS. Thesis]. Shanghai: Shanghai Jiao Tong University, 2007 (in Chinese with English abstract).

[9] Kuzmanovic A, Knightly EW. Low-Rate TCP-targeted denial of service attacks: The shrew vs. the mice and elephants. In: Proc. of the ACM SIGCOMM 2003. Karlsruhe: ACM Press, 2003. 75−86. [doi: 10.1145/863955.863966]

[10] Guirguis M, Bestavros A, Matta I, Zhang Y. Reduction of quality (RoQ) attacks on Internet end systems. In: Proc. of the 24th IEEE INFOCOM. Miami: IEEE, 2005. 1362−1372. [doi: 10.1109/INFCOM.2005.1498361]

[11] Luo XP, Chang RKC. On a new class of pulsing denial-of-service attacks and the defense. In: Proc. of the Network and Distributed System Security Symp. San Diego: The Internet Society, 2005.

[12] He YX, Liu T, Cao Q, Xiong Q, Han Y. A survey of Low-rate denial-of-service attacks. Journal of Frontiers of Computer Science and Technology, 2008,2(1):1−19 (in Chinese with English abstract). [doi: 10.1299/jcst.2.1]

[13] Sarat S, Terzis A. On the effect of router buffer sizes on low-rate denial of service attacks. In: Proc. of the 14th Int'l Conf. on Computer Communications and Networks (ICCCN 2005). San Diego: IEEE Press, 2005. 281−286. [doi: 10.1109/ICCCN.2005.1523867]

[14] Sun HB, Lui JCS, Yau DKY. Defending against low-rate TCP attacks: Dynamic detection and protection. In: Proc. of the 12th IEEE Int'l Conf. on Network Protocols (ICNP 2004). Berlin: IEEE COMPUTER SOC, 2004. 196−205. [doi: 10.1109/ICNP.2004.1348110]

[15] Chen Y, Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. Journal of Parallel and Distributed Computing, 2006,66(9):1137−1151. [doi: 10.1016/j.jpdc.2006.04.007]

[16] Wei W, Dong YB, Lu DM, Jin G, Lao HL. A novel mechanism to defend against low-rate denial-of-service attacks. Journal of Computer Science, 2006,3975:261−271. [doi: 10.1007/11760146_23]

[17] Zhang CW, Yin JP, Cai ZP, Zhu E, Cheng JR. An approach of detecting distributed low-rate DoS attack based on the congestion participation rate. Computer Engineering & Science, 2010,32(7):49−54 (in Chinese with English abstract).

[18] Wei W, Dong Y, Lu DM, Jin G. Detection and response of low-rate TCP-targeted denial of service attacks. Journal of Zhejiang University, 2008,42(5):757−765 (in Chinese with English abstract).

[19] Wu ZJ, Zeng HL, Yue M. Approach of detecting LDoS attack based on time window statistic. Journal on Communications, 2010, 31(12):55−63 (in Chinese with English abstract).

[20] Stevens W. RFC2581: TCP congestion control. Internet RFCs, 1999. http://rfc.net/rfc2581.html

[21] Paxson V, Allman M. RFC 2988: Computing TCP's retransmission timer. Internet RFCs, 2000. http://rfc.net/rfc2988.html

[22] Mathis M, Mahdavi J. RFC 2018: TCP selective acknowledgment options. Internet RFCs, 1996.

[23] Cui T, Andrew LLH, Zukerman M, Tan LS. Improving the fairness of FAST TCP to new flows. Communications Letters, IEEE, 2006,10(5):414−416. [doi: 10.1109/LCOMM.2006.1633341]

[24] Luo WM, Lin C, Yan BP. A survey of congest ion control in the Internet. Chinese Journal of Computers, 2001,24(1):1−18.

[25] Chen Y, Hwang K, Kwok YK. Collaborative defense against periodic shrew DDoS attacks in frequency domain. Journal of ACM Trans. on Information and System Security, 2005. 1−30.

[26] Xiang Y, Li K, Zhou WL. Low-Rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans. on Information Forensics and Security, 2011,6(2):2011:426−438. [doi: 10.1109/TIFS.2011.2107320]

[27] Yang G, Gerla M, Sanadidi MY. Defense against low-rate TCP-targeted denial-of-service attacks. In: Proc. of the 9th Int'l Symp. on Computers and Communications (ISCC 2004). Washington: IEEE, 2004. 345−350.

[28] Efstathopoulos P. Practical study of a defense against low-rate TCP-targeted DoS attack. In: Proc. of the Int'l Conf. on Internet Technology and Secured Trans. (ICITST 2009). London, 2009. 1−6.

[29] Floyd S, Jacobson V. Random early detection gateways for congestion avoidance. IEEE/ACM Trans. on Networking, 1993,1(4): 397−413. [doi: 10.1109/90.251892]

[30] Athuraliya S, Low SH, Li VH, Yin QH. REM: Active queue management. IEEE Network, 2001,15(3):48−53. [doi: 10.1109/65.923940]

[31] Christiansen M, Jeffay K, Ott D, Smith FD. Tuning RED for Web traffic. ACM Computer Communication Review, 2000,30(4): 139−150. [doi: 10.1145/347057.347418]

[32] Feng W, Kandlur DD, Saha D. The blue active queue management algorithms. IEEE/ACM Trans. on Networking, 2002,10(4): 513−528. [doi: 10.1109/TNET.2002.801399]

[33] Kunniyur S, Srikant R. Analysis and design of an adaptive virtual queue algorithm for active queue management. In: Proc. of the ACM SIGCOMM 2001. New York: ACM Press, 2001. 123−134. [doi: 10.1145/383059.383069]

[34] Feng WC, Kandlur DD, Saha D, Shin KG. A self-configuring RED gateway. In: Proc. of the IEEE INFOCOM. New York: IEEE Communications Society, 1999. 1320−1328. [doi: 10.1109/INFCOM.1999.752150]

[35] Ott TJ, Lakshman TV, Wong LH. SRED: Stabilized RED. In: Proc. of the IEEE INFOCOM. New York: IEEE Communications Society, 1999. 1346−1355. [doi: 10.1109/INFCOM.1999.752153]

[36] Feng WC, Kandlur DD, Saha D, Shin KG. Blue: A new class of active queue management algorithms. Technical Report, CSE-TR-387-99, University of Michigan, 1999. http://www.eecs.umich.edu/~wuchang/blue/

[37] Hollot CV, Misra V, Towsley D, Gong WB. On designing improved controllers for AQM routers supporting TCP flows. In: Proc. of the IEEE INFOCOM. Anchorage: IEEE Communications Society, 2001. 1726−1734. [doi: 10.1109/INFCOM.2001.916670]

[38] Mohan L, Bijesh MG, John JK. Survey of low rate denial of service (LDoS) attack on RED and its counter strategies. In: Proc. of the 2012 IEEE Int'l Conf. on Computational Intelligence and Computing Research (ICCIC). 2012. 1−7. [doi: 10.1109/ICCIC.2012.6510186]

[39] Kwok YK, Tripathi R, Chen Y, Hwang K. HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks. In: Proc. of the Networking and Mobile Computing. Zhangjiajie: Computer Science, 2005. 423−432. [doi: 10.1007/11534310_46]

[40] Lou XP, Chan EWW, Chang RKC. Vanguard: A new detection scheme for a class of TCP-targeted denial-of-service attacks. In: Proc. of the Network Operations and Management Symp. (NOMS 2006). Vancouver, 2006. 507−518.

[41] Maciá-Fernández G, Diaz-Verdejo JE, Garcia-Teodoro P. Mathematical model for low-rate DoS attacks against application servers. Journal of IEEE Trans. on Information Forensics and Security, 2009,4(3):519−530. [doi: 10.1109/TIFS.2009.2024719]

[42] Xu XD, Guo X, Zhu SR. A queuing analysis for low-rate DoS attacks against application servers. In: Proc. of the IEEE Int'l Conf. on Wireless Communications Networking and Information Security (WCNIS). 2010. 500−504.

[43] Chang CW, Lee S, Lin B, Wang J. The taming of the shrew: Mitigating low-rate TCP-targeted attack. In: Proc. of the 29th IEEE Int'l Conf. on Distributed Computing Systems. Montreal, 2009. 137−145.

[44] Chen Y, Hwang K. Spectral analysis of TCP flows for defense against reduction-of-quality attacks. In: Proc. of the IEEE Int'l Conf. on Communications 2007. Glasgow, 2007. 24−28.

[45] Chen H, Chen Y. A novel embedded accelerator for online detection of shrew DDoS attacks. In: Proc. of the Int'l Conf. on Networking, Architecture, and Storage. Chongqing, 2008. 365−372. [doi: 10.1109/NAS.2008.13]

[46] Xie Y, Yu SZ. Detecting shrew HTTP flood attacks for flash crowds. In: Proc. of the Int'l Conf. on Computational Science (1). 2007. 640−647. [doi: 10.1007/978-3-540-72584-8_85]

[47] Zhang Y, Mao ZM, Wang J. Low-Rate TCP-targeted DoS attack disrupts Internet routing. In: Proc. of the Network and Distributed System Security Symp. (NDSS 2007). 2007.

[48] Liu XM, Li Q, Liu XG. A novel pattern of distributed low-rate denial of service attack disrupts Internet routing. In: Proc. of the 8th Int'l Conf. on Computing Technology and Information Management (ICCM). 2012. 119−123.

[49] Wu ZJ, Pei BS. The detection of LDoS attack based on the model of small signal. Acta Electronica Sinica, 2011,39(6):1456−1461 (in Chinese with English abstract).

[50] Mallat S. A Wavelet Tour of Signal Processing. 2nd ed., New York: Academic Press, 1999.

[51] Li L, Lee G. DDoS attack detection and wavelets. IEEE Trans. on Information Theory, 2003,(3):421−427. [doi: 10.1109/ICCCN.2003.1284203]

[52] Chaovalit P, Gangopadhyay A, Karabatis G, Chen Z. Discrete wavelet transform-based time series analysis and mining. ACM Computing Surveys, 2011,43(2):1−37. [doi: 10.1145/1883612.1883613]

[53] Chen K, Liu HY, Chen XS. EBDTA-Method for detecting LDoS attack. In: Proc. of the IEEE Int'l Conf. on Information and Automation. 2012. 911−916.

[54] Barbhuiya FA, Gupta V, Biswas S, Nandi S. Detection and mitigation of induced low rate TCP-targeted denial of service attack. In: Proc. of the 2012 IEEE 6th Int'l Conf. on Software Security and Reliability. 2012. 291−300. [doi: 10.1109/SERE.2012.27]

[55] Lakhina A, Crovella M, Diot C. Mining anomalies using traffic feature distributions. In: Proc. of the ACM SIGCOMM. 2005. [doi: 10.1145/1090191.1080118]

[56] Wagner A, Plattner B. Entropy based worm and anomaly detection in fast IP networks. In: Proc. of the 14th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise. 2005. 172−177. [doi: 10.1109/WETICE.2005.35]

[57] Brauckhoff D, Tellenbach B, Wagner A, May M, Lakhina A. Impact of packet sampling on anomaly detection metrics. In: Proc. of the ACM SIGCOMM Conf. on Internet Measurement. Rio de Janeriro, 2006. 159−164. [doi: 10.1145/1177080.1177101]

[58] Lall A, Sekar V, Ogihara M, Xu J, Zhang H. Data streaming algorithms for estimating entropy of network traffic. In: Proc. of the ACM SIGMETRICS Performance Evaluation Review. 2006. 145−156. [doi: 10.1145/1140277.1140295]

[59] Yang JH, Wu JP, An CQ. Internet Measurement Theory and Application. Beijing: The People's Posts and Telecommunications Press, 2009 (in Chinese).

[60] Zhang B, Yang JH, Wu JP. MBST: Detecting packet-level traffic anomalies by feature stability. The Computer Journal, 2012. [doi: 10.1093/comjnl/bxr134]

附中文参考文献:

[3] 郝双.对拒绝服务攻击的检测方法研究[硕士学位论文].北京:清华大学,2006.

[6] 孙长华,刘斌.分布式拒绝服务攻击研究新进展综述.电子学报,2009,37(7):1562−1571.

[8] 胥秋华.DDoS 攻击防御关键技术的研究[硕士学位论文].上海:上海交通大学,2007.

[12] 何炎祥,刘陶,曹强,熊琪,韩奕.低速率拒绝服务攻击综述.计算机科学与探索,2008,2(1):1−19. [doi: 10.1299/jcst.2.1]

[17] 张长旺,殷建平,蔡志平,祝恩,程杰仁.基于拥塞参与度的分布式低速率 DoS 攻击检测过滤方法.计算机工程与科学,2010,32(7):49−54.

[18] 魏蔚,董亚波,鲁东明,金光.低速率 TCP 拒绝服务攻击的检测响应机制.浙江大学学报,2008,42(5):757−765.

[24] 罗万明,林闯,阎保平.TCP/IP 拥塞控制研究.计算机学报,2001,24(1):1−18.

[49] 吴志军,裴宝崧.基于小信号检测模型的 LDoS 攻击检测方法的研究.电子学报,2011,39(6):1456−1461.

[59] 杨家海,吴建平,安常青.互联网络测量理论与应用.北京:人民邮电出版社,2009.

文坤(1976－),男,河南方城人,博士生,主要研究领域为网络测量,入侵检测.
E-mail: wenkun.c@gmail.com

张宾(1976－),男,博士生,主要研究领域为网络流量特征及建模,网络测量,异常检测.
E-mail: zhang_bin163@163.com

杨家海(1966－),男,博士,教授,博士生导师,主要研究领域为计算机网络,网络管理与测量,网络安全,云计算及安全.
E-mail: yang@cernet.edu.cn