

一种基于 Haar 小波变换的 低速率拒绝服务攻击检测方法

蔡晓丽¹, 陈舜青¹, 宁 慧²

(1 常州工学院 计算机信息工程学院, 江苏 常州 213002;

2 哈尔滨工程大学 计算机科学与技术学院, 黑龙江 哈尔滨 150001)

摘 要: 依据 LDoS 攻击周期性脉冲突发的特点, 提出一种基于 Haar 小波特征提取的低速率拒绝服务攻击检测方法. 该方法采用信号处理技术来分析网络流量提取特征指标, 通过小波多尺度分析对网络流量综合诊断, 较好地缓解了合法用户背景流量对攻击特征提取的干扰. NS-2 仿真实验结果表明, 该方法检测率高, 消耗计算资源少, 具有良好的理论研究和实用价值.

关键词: 低速率拒绝服务攻击; 流量特征; 异常检测

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)11-0102-04

A Low-Rate Denial-of-Service Attack Detection Method Based on Haar Wavelet Analysis

CAI Xiao-li¹, CHEN Shun-qing¹, NING Hui²

(1 School of Information & Engineering, Changzhou Institute of Technology, Changzhou 213002, China;

2 College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract: The traditional statistical testing based methods have the shortcomings of low efficiency and high false positives. To solve this problem, according to the characteristic of periodicity and short burst in LDoS flows, a detection method against LDoS attacks has been designed and implemented based on feature extraction using wavelet transform. The proposed method extracts five feature indices of LDoS flows through wavelet multi-scale analysis of network traffic. Experiment results show that the method, capable of detecting the LDoS attack, achieves high detection rate with low computation cost, and hence has good practical value.

Key words: low-rate denial-of-service attacks (LDoS); traffic character; abnormal detection

1 引言

低速率拒绝服务攻击(low-rate denial-of-service, LDoS), 属于一种新型的资源消耗型攻击^[1]. LDoS 利用系统适应性机制或网络协议中的安全漏洞, 通过向目标发送周期性脉冲攻击流, 导致受害端服务性能降低. LDoS 攻击者具有间歇性的攻击特点, 它在大部分时间内并不活跃, 只有在短暂

的活动时间段内才发送高强度脉冲流, 这使得攻击流的平均数据率与合法用户并无太大区别. 面对分布式 LDoS 攻击, 传统检测方法面临着检测效率低、误报率高的严峻考验^[2].

针对这一问题, 文中分析了 LDoS 攻击流与正常 Internet 数据流的差异, 结合 LDoS 的攻击规律, 提出了一种 LDoS 检测方法 DSWA(detection system based on wavelet analysis). DSWA 方法基于小

收稿日期: 2011-02-23; **修回日期:** 2011-03-30

基金项目: 国家自然科学基金项目(60975071); 国家“八六三”计划项目(2009AA04Z215); 常州工学院教学科研基金项目(J080513, J080102)

波特征提取,分析对象是到达检测路由器的数据包数目.它利用信号处理技术分析网络流量,通过小波工具能够很好地缓解正常用户背景流量对攻击特征提取的干扰,健壮性、可移植性较强,消耗的计算资源少;其综合诊断器采用小波多尺度分析防范实现,能够准确地检测出标准的 LDoS 攻击,而且对 LDoS 的变种攻击也有很好的效果.另外,它还可以定位攻击数据包的到达时刻,为追踪攻击数据源提供较准确的线索^[3-6].

2 LDoS 检测方法技术原理

LDoS 攻击主要是利用端系统或网络中常见的自适应机制所存在的安全漏洞.其核心思想在于攻击瓶颈链路或者是路由器,在瞬间产生拥塞,导致大量 TCP 报文丢失,迫使网络发出拥塞信号(丢包,对端重传的 ACK),使得源端的 TCP 拥塞控制机制启用,进行自适应的调整发送窗口大小,尝试恢复到稳定状态.周期性的进行攻击,就会造成 TCP 性能的震荡,严重降低 TCP 的吞吐量.

LDoS 攻击利用系统的暂态性能比较低的特征,通过周期性发起一定强度的攻击流,使系统不断在失效和稳定两个状态切换,即总是处于低效暂态,从而降低系统的整体性能.

Shrew 攻击是目前受到普遍关注的一种 LDoS 攻击方式,它针对 TCP 拥塞控制机制.在 TCP 协议中,慢启动(slow start)以及和增积减(additive increase/multiplicative decrease, AIMD)的本质均是不断地测试网络所能承受的最大传输极限.如果发现数据包丢失,就立刻减小拥塞窗口,降低发送速率. Shrew 攻击利用此机制,在特定时刻发送脉冲式攻击流,造成大量的网络数据包丢失,使得 TCP 发送方误认为网络始终存在拥塞.根据 TCP 协议,数据发送速率一直很低,传输效率急剧减小,该过程如图 1 所示.

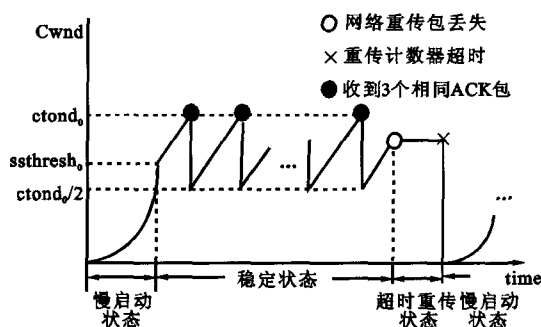


图 1 LDoS 攻击示意图

3 基于 Haar 小波变换的 LDoS 攻击特征提取

LDoS 攻击在传统的 DDoS 基础上改进很大,它设计精巧、降低了攻击流的平均数据率,但通过对网络流量的包过程分析得知, LDoS 攻击在时频两域仍然有着比较明显的特征.因此,通过提取这些特征,可以检测网络中是否存在 LDoS 攻击.

小波变换是一种信号分析工具,它的时-频窗面积固定、形状可自适应调整,它可以将信号分解到不同频带上,高频段上可以反映信号的瞬时变化情况,在低频段上则可以反映信号的缓慢变化.小波变换在时、频局部化方面优势独特,特别适合于检测异常信号.阿尔弗雷德哈尔最先提出了小波变换, Haar 小波变换是最简单的小波变换的变换.小波分解的主要思路是把非平稳时间序列分解成一种更加稳定的时间序列,然后再分别对各个序列进行研究. Mallat 算法基于多分辨率分析,是二进离散小波变换的快速算法,它利用构造的两个滤波器对样本划分各个频带,小波重构和分解中经常使用该算法.文中将把 Haar 小波变换应用于包过程的处理.

小波空间和尺度空间构成了多分辨率分析中的两个函数空间.假设 $x(t)$ 是一个时间序列,在每一个时间尺度内,采用一系列的尺度函数(即对基本尺度函数的位移与伸缩)和小波函数(即基本小波函数的位移与伸缩)作为逼近信号和细节信号部分,在逼近信号部分重复这个分解过程,直至达到要求的分辨率.这里用一系列尺度系数 $a_{j,k}$ 表示逼近信号,小波系数序列 $d_{j,k}$ 表示细节信号.假设 N 是时间序列长度,那么 $x(t)$ 可以表示为:

$$x(t) = \sum_{k \in \mathbb{Z}} \alpha_{p,k} \phi_{p,k}(t) + \sum_{0 \leq j \leq p} \sum_{k \in \mathbb{Z}} d_{j,k} \psi_{j,k}(t) \quad (1)$$

$$p \leq \log N$$

简单地说,小波函数的作用就是在小波分析中构建坐标系,当一个信号用小波函数来表示时,在实现过程中需要一个频域的底座和平台,因为信号是被映射在了时频平面内的,从平台起到底座的函数就是尺度函数.在滤波实现中低频滤波就相当于尺度函数的作用,高频滤波器的效果则类似小波函数的功能.

文中采用与文献[6]相同的无抽取的离散小波变换的 à trous 算法,该算法是一个冗余变换,对长度为 N 的时间序列,在每一个时间尺度上的分解序列长度仍是 N .因此在每一个时间尺度的相同时间

点就可以建立直接联系,并且具有时移不变性. 这样虽然会多占用一些存储空间,但现在存储空间已经不是问题,对性能影响不大. 可以用离散低通滤波器 h 得到尺度系数(设输入时间序列为 $x(t)$):

$$c_0(t) = x(t)$$

$$c_{j+1} = \sum_{l=-\infty}^{\infty} h(l)c_j(2^j l + t) \quad (2)$$

根据 $\hat{a}$ trous 小波变换的性质,可通过尺度系数来表示各尺度下的细节系数,即:

$$d_{j+1}(t) = c_j(t) - c_{j+1}(t) \quad (3)$$

则集合 $\{d_1, d_2, \dots, d_p, c_p\}$ 为原时间序列直到分辨率 p 的小波变换,其中逼近信号是 c_p ,各尺度下的细节信号是 $d_j (j = 1, 2, \dots, p)$. 原时间序列可以由逼近信号和细节信号进行重构:

$$x(t) = c_p(t) + \sum_{j=1}^p d_j(t) \quad (4)$$

无抽取 Haar 小波变换是在 $\hat{a}$ trous 小波变换算法的基础上,根据公式(2)(3),以 $h = (1/2, 1/2)$ 作为低通滤波器,尺度系数和小波系数的计算方法为:

$$c_{j+1}(t) = 0.5(c_j(t - 2^j) + c_j(t))$$

$$d_{j+1}(t) = c_j(t) - c_{j+1}(t) \quad (5)$$

上面的这个变换称为无抽取 Haar 小波变换. 若设 N 为时间序列的长度,使用金字塔算法,在每一个时间尺度上无抽取 Haar 小波变换的计算时间复杂度可以提高到 $O(N)$. 同时,对每一个时间点 t ,都不需要使用 t 之后的数据计算尺度系数和小波系数,即随着所获取数据的增加,不需要重新计算前面的系数. 无抽取 Haar 小波变换的这两项特点使其运算速度极高,适合在多种场合下应用. 通过利用针对 Haar 小波频率计算,低频段变化信息的攻击流子带 $Xa(t)$ 可以通过选取 3、4、5 层的小波系数重构来体现,网络流量整体趋势的背景流子带 $Xb(t)$ 则通过分解系数重构反映. 这样,各流量子带的频率成分更加单纯,便于针对 LDoS 攻击提取特征指标.

4 LDoS 攻击检测框架

基于以上攻击流特征子带提取方法,文中设计了一种 LDoS 检测框架 DSWA,其结构如图 2 所示. 网络流量采集模块负责采集网络数据包,它从检测路由器按一定频率采样,得到流量信息,并建立包过程,按照到达时刻顺序记录数据包的包头信息; Haar 小波分析模块负责对包过程进行小波分解,它在观察窗口内计算各尺度的小波系数,根据频率的不同选取特定尺度的分解系数重构背景流子带和攻

击流子带; LDoS 攻击特征提取模块负责计算特征指标并存入特征库;一旦判断网络中出现 LDoS 攻击,那么攻击脉冲定位器将分析特征尺度上的小波系数,在时间轴上定位攻击脉冲的到达时刻,并结合此时记录的包头信息,将报警信号与攻击包信息记入报告模块和攻击信息中.

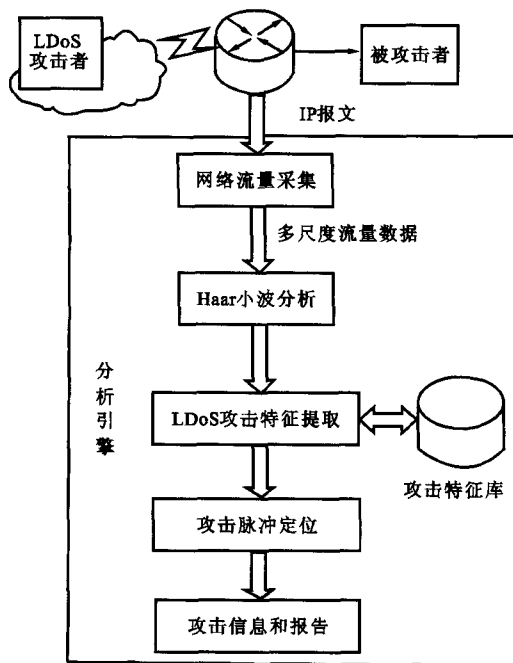


图2 LDoS攻击检测框架 DSWA

DSWA 框架中的攻击脉冲定位器的功能是用来确定检测窗口内攻击数据包的到达时刻. 当攻击者发起 LDoS 攻击后,其发送的脉冲数据足以占据瓶颈链路带宽,合法流量受到严重抑制,整个包过程基本上可以看成是低幅度的平稳背景信号和周期脉冲信号的叠加^[4]. 在检测窗口中,要确定攻击数据包的到达时刻,从而获得攻击者的信息,关键就是从混合信号中确定周期脉冲信号的突变点. 因此,在观察窗口内,只要查找由脉冲信号产生的局部模极大点,就能排除背景信号模极大的干扰,准确地定位具体的攻击源地址.

5 实验数据与分析结果

文中通过 NS-2 网络模拟实验,对检测系统进行检验,从而评测 DSWA 检测方法的有效性. 当中用 GT-ITM 工具包生成了网络拓扑结构以提高模拟实验的仿真度. 具体的仿真平台如图 3 所示. 图 3 中:0、2 和 4 号节点为正常的 TCP 流,而 1 号和 3 号模拟攻击的 UDP 数据流,5 号节点为路由器,用来采集数据,6 号节点是目标服务器.

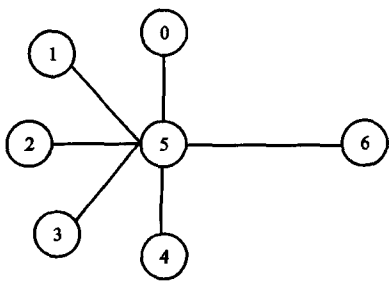


图3 NS-2 仿真拓扑

该图中,网络瓶颈在 5 号及 6 号链路上,各节点间的链路带宽为 40Mbps. 在该网络拓扑结构中,共产生了 452 条数据流,平均每个节点有 700 多条数据流,其中包括 333 条 UDP 流,489 条 TCP 连接. 各 TCP 连接的往返时延 RTT 在 90ms~200ms 之间. LDoS 攻击脉冲是采用 UDP 发送的,使攻击流与背景数据流混合. LDoS 攻击周期 T 的变化范围为 0.5s~5s,脉冲强度的变化范围为 15Mbps~40Mbps,脉冲持续时间的变化范围为 100ms~270ms.

图 4 顶部是原始流量图,即未产生 LDoS 攻击的时候,可以看出 TCP 流量是平稳的,且趋于平缓. 底部是对原始流量过滤后,做小波分解计算出 wavelet variance 的图像,从图中可以清楚地看到在 22:15 出现了异常情况.

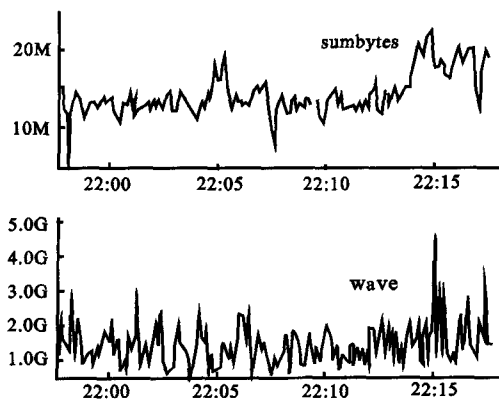


图4 利用小波变换发现异常

此时总共发送了 1200 个数据包,每个数据包的大小是 1000B,因此可以计算得到 TCP 平均流量是 $1200 \times 1000 \times 8 / 10 = 0.96 \text{ Mbit/s}$;在链路 0 号、2 号和 4 号上的 3 条正常数据流总流量是 2.88Mbit/s,约等于瓶颈链路最大吞吐量 3Mbit/s.

另外,在 wavelet variance 的图像中并没有反映出 22:05 原始流量出现的一次突发. 原因在于,这次突发是那些在缓存中的长时流引起的,因而这部分突发流量被滤掉了. 在攻击发生时,因为大量的新流产生(DDoS 攻击通常用随机 IP 作为源 IP,以防

止被跟踪定位),这些新流大量地涌入缓存中,将本来位于缓存中的长时流挤了出来,引起了 wavelet variance 异常变化.

6 结束语

文中针对低速率拒绝服务攻击比传统的 DDoS 攻击更具隐蔽性和欺骗性,依据其周期性脉冲突发特点,设计实现了一种基于 Haar 小波特征提取的 LDoS 检测方法. 该方法通过小波多尺度分析对网络流量综合诊断. 一旦检测出 LDoS 攻击,系统定位攻击脉冲数据的到达时刻以获得攻击者的相关信息. 实验结果表明,该方法具有高检测率,消耗计算资源少,从整体上提高了大流量网络环境下 LDoS 攻击检测和防御的可行性,具有良好的理论研究和工程实用价值.

参考文献:

- [1] Kuzmanovic A, Knightly EW. Low-Rate TCP-targeted denial of service attacks—the shrew vs. the mice and elephants[C] // Proc. Of the ACM SIGCOMM 2003. New York: ACM Press, 2003: 75–86.
- [2] 李刚,华蓓,杨兴良. 自适应分布式拒绝服务攻击的防御机制研究[J]. 计算机仿真, 2006, 23(11): 125–129.
- [3] Sun H, Lui J C S, Yau D K Y. Defending against low-rate TCP attacks: dynamic detection and protection[C] // Proc. of the 12th IEEE Int'l Conf. on Network Protocols (ICNP 2004). New York: IEEE Press, 2004: 196–205.
- [4] 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): 1137–1151.
- [5] 徐晨,赵瑞珍,甘小冰. 小波分析·应用算法[M]. 北京: 科学出版社, 2004: 81–117.
- [6] Shensa M J. The discrete wavelet transform: wedding the à trous and mallat algorithms[J]. IEEE Transactions on Signal Processing, 1992, 40(10): 2464–2482.

作者简介:

蔡晓丽 女, (1981—), 硕士研究生, 讲师. 研究方向为网络安全、数据挖掘技术.

陈舜青 女, (1964—), 副教授. 研究方向为信息管理与数据挖掘.

宁 慧 女, (1964—), 副教授, 硕士生导师. 研究方向为人工智能、计算机网络、数据挖掘技术.