软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(5):1549−1562 [doi: 10.13328/j.cnki.jos.005658]

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

基于小波能谱熵和隐半马尔可夫模型的 LDoS 攻击检测*

吴志军, 李红军, 刘 亮, 张景安, 岳 猛, 雷 缙

(中国民航大学 电子信息与自动化学院,天津 300300)

通讯作者: 吴志军, E-mail: zhijun-wu@163.com

摘 要: 低速率拒绝服务(low-rate denial of service,简称 LDoS)攻击采用周期性发送短脉冲数据包的方式攻击云计算平台和大数据中心,导致连接用户的路由器丢包和数据链路传输性能下降.LDoS 攻击流量平均速率很低,具有极强的隐蔽性,很难被检测到.在分析 LDoS 攻击流量的基础上,通过小波变换得到网络流量的小波能谱熵,并以此作为隐半马尔可夫模型(HSMM)的输入,设计采用 HSMM 网络模型的 LDoS 攻击判决分类器,提出了基于小波能谱熵和隐半马尔可夫模型的 LDoS 攻击检测方法.该检测方法在 NS-2 和 Test-bed 环境中分别进行了测试.实验结果表明,该方法具有较好的检测性能,通过假设检验得出检测率为 96.81%.

关键词: 低速率拒绝服务;网络测量;小波分析;隐半马尔可夫模型;异常检测

中图法分类号: TP309

中文引用格式: 吴志军,李红军,刘亮,张景安,岳猛,雷缙.基于小波能谱熵和隐半马尔可夫模型的 LDoS 攻击检测.软件学报, 2020,31(5):1549−1562. http://www.jos.org.cn/1000-9825/5658.htm

英文引用格式: Wu ZJ, Li HJ, Liu L, Zhang JA, Yue M, Lei J. Detection of LDoS attacks based on wavelet energy entropy and hidden semi-Markov models. Ruan Jian Xue Bao/Journal of Software, 2020,31(5):1549−1562 (in Chinese). http://www.jos.org.cn/1000-9825/5658.htm

Detection of LDoS Attacks Based on Wavelet Energy Entropy and Hidden Semi-Markov Models

WU Zhi-Jun, LI Hong-JUN, LIU Liang, ZHANG Jing-An, YUE Meng, LEI Jin

(College of Electronic Information and Automation, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Low-rate denial of service (LDoS) attack can cause the packets loss of the legitimate users and reduce the transmission performance of the transport system by sending short bursts of packets periodically. The LDoS attack flows always mix with the legitimate traffic, hence, it is hard to be detected. This study designs an LDoS attack classifier based on network model, which uses hidden semi-Markov model (HSMM), and deploys a decision indicator to detect LDoS attacks. In this method, wavelet transform is exploited to compute the network traffic's wavelet energy spectrum entropy, which is used as the input of the HSMM. The proposed detection method has been evaluated in NS-2 and Test-bed, and experimental results show that it achieves a better performance with detection rate of 96.81%.

Key words: low-rate denial of service; network measurement; wavelet analysis; hidden semi-Markov model; anomaly detection

低速率拒绝服务(low-rate denial of service,简称 LDoS)攻击是一种降质服务攻击[1],它能以很小的速率占用正常的 TCP 连接带宽,降低合法用户的服务质量.LDoS 攻击只需要周期性地发送窄脉冲,就能达到很好的攻击效果.LDoS 攻击流混合在合法的 TCP 流中,具有很好的隐蔽性.由于网络数据传输中的流量有 80%以上是 TCP 协议的数据[2],这就使得 LDoS 攻击具有巨大的破坏力.为了提高网络的安全性,保证正常用户能够取得高质量

* 基金项目: 国家自然科学基金委员会与中国民航局联合基金(U1933108); 天津市教委科研项目(2019KJ117)

Foundation item: Joint Foundation of National Natural Science Foundation of China and Civil Aviation Adminstration of China (U1933108); Scientific Research Project of Tianjin Municipal Education Commission (2019KJ117)

收稿时间: 2018-01-26; 修改时间: 2018-05-17; 采用时间: 2018-08-15

的服务,对 LDoS 攻击的防御措施进行研究具有重大意义.

本文从网络测量的角度出发,研究 LDoS 攻击的机制及其主要特征,然后分别提取正常网络和有 LDoS 攻击时网络数据包的特征进行定量分析,提出基于网络测量的 LDoS 攻击检测方法.该方法通过小波变换对包过程进行分解重构,得到网络流量的小波能谱熵,并以此作为隐半马尔可夫模型(hidden semi-Markov model,简称 HSMM)的输入.设计采用 HSMM 网络模型的 LDoS 攻击判决分类器,设置决策指标,从而进行 LDoS 攻击检测.

本文第 1 节是相关工作,主要介绍现有的研究成果,并对它们进行对比分析.第 2 节从网络流量的角度对 LDoS 攻击的特点进行分析,得到网络流量的小波能谱熵.第 3 节介绍利用 HSMM 模型建立的 LDoS 攻击检测分类器.第 4 节是实验验证,分别在 NS-2 和 Test-bed 网络环境下对提出的方法进行测试,并对实验结果进行比较分析.第 5 节对全文工作进行总结,并指出本文研究中的不足之处和今后的研究思路.

1 相关工作

美国 Rice 大学的 Knightly 教授领导的研究团队在 2003 年的 SIGCOMM 会议上第一次提出了针对 TCP 协议的低速率拒绝服务攻击[3].此后,针对 LDoS 攻击检测的研究一直都是网络安全方向的一个热点.根据是否建立关于攻击模式的特征数据库,将 LDoS 攻击的检测方式分为两类:特征检测和异常检测[4].近些年也有研究人员从改进网络和服务协议角度着手,提出基于网络协议的检测和防御方法等.

(1) 特征检测及防御方法

虽然 LDoS 攻击具有平均速率低、隐蔽性强的特点,但是其脉冲强度、持续时间和攻击周期等特征也非常突出.根据 LDoS 攻击的周期性和短时高速脉冲的特征,可以比较准确地检测 LDoS 攻击[4].当网络中有 LDoS 攻击时,可以导致链路带宽的使用率变低,同时,队列抖动变大,丢包率增加,网络的拥塞情况可以通过路由器队列的变化反映出来.因此,很多学者研究了基于路由器队列的 LDoS 攻击检测方法.香港大学的 Kwok 教授[5]改进了路由器队列管理算法来检测 LDoS 攻击,称为加权窒息中断异常法.国防科技大学的张静等人[6]提出了基于平局队列长度的检测方法.中国船舶重工集团公司第七一三研究所的吴娜等人[7]对基于数据流量势能特征的分布式拒绝服务(distributed DoS,简称 DDoS)攻击中的隐蔽流量运用了支持向量机的方法来实现分类和检测.电子科技大学的 Luo 和北京科技大学的 Yang[8]根据 TCP 协议对低速率 DoS 攻击进行研究.

(2) 异常检测及防御方法

网络中正常的流媒体点播以及 VoIP 等业务也会产生突发的数据流,这些正常的数据流很容易被特征检测误报为攻击流量,利用特征检测的方法就会产生较高的误报率.采用异常检测的方法进行检测就可以避免上述问题.目前常用的异常检测方法分为基于统计学分析和基于数字信号处理的时频变换等等.南加州大学洛杉矶分校的 Hwang[9]教授领导的团队通过研究攻击数据流与合法数据流的时域和频域特征.根据其归一化功率谱密度分布的差异来检测 LDoS 攻击.华中科技大学的陈凯等人[10]提出运用加权指数移动平均算法来检测 LDoS 攻击.中国民航大学吴志军教授的研究团队[11]通过对网络中流量的多重分形特性进行分析,根据网络中 LDoS 攻击流量的多重分形特征来检测 LDoS 攻击.

此外,还有一些专家根据网络协议研究 LDoS 攻击.Chang 等人[12]就反馈控制网络对 LDoS 攻击的脆弱性进行了研究.杨义先教授等人[13]研究了针对路由器协议的 LDDoS 攻击策略.

本文首先研究 LDoS 攻击的机制及其主要特征,然后分别提取正常网络和有 LDoS 攻击时网络数据包的不同特征并进行定量分析,提出基于网络测量的 LDoS 攻击检测方法.该方法首先利用小波能谱熵表征 TCP 流量和 LDoS 攻击流量,再将其作为 HSMM 的输入特征向量.利用 HSMM 的网络流量状态分类器判断当前网络所处的状态.

2 面向 LDoS 攻击检测的网络流量测量与分析

本节对到达路由器节点的数据包的数量进行测量分析,根据包过程[9,14,15]对其进行描述.

2.1 网络流量分析

本研究中作为背景流量的正常流量采用 TCP 协议,LDoS 攻击流量采用 UDP 协议.在下面的实验中,TCP 流量数据由 Linux TCP 核源码产生,LDoS 攻击流量由软件工具产生[3].LDoS 攻击模型的原理如图 1 所示.

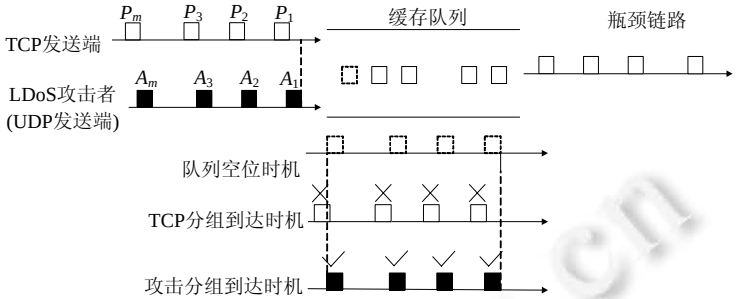


Fig.1 LDoS attack through UDP

图 1 基于 UDP 的 LDoS 攻击

LDoS 攻击通过周期性发送 UDP 分组来占据路由器缓存队列.当缓存队列被占满后,TCP 分组无法进入缓存队列,从而导致合法用户的 TCP 协议分组被队列丢弃.由于 TCP 提供可靠的服务,当发生分组丢失时,TCP 链接会降低发送速率,最终导致服务质量的下降.在 NS-2 仿真环境下,以 1ms 的采样间隔对网络中的正常流量、攻击流量和混合流量数据包个数进行统计,结果如图 2 所示.当网络中存在 LDoS 攻击时,正常的 TCP 流量下降明显,网络流量的平均值也降低.

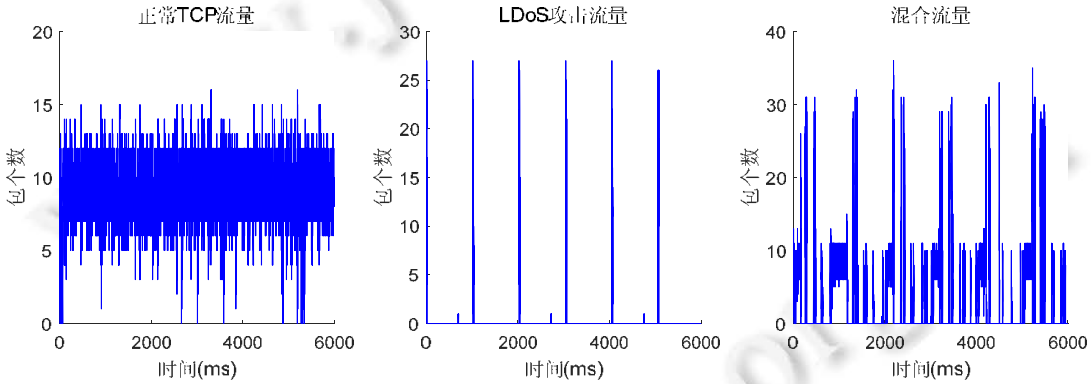


Fig.2 Packets number of traffic

图 2 流量的包个数

2.2 基于小波变换的网络流量特征提取

本节的检测方法从网络流量的包过程出发,用小波变换的方法重构网络正常状态和异常状态的数据流并计算其能谱熵,利用小波变换理论定义归一化小波能谱熵来提取 LDoS 的攻击特征,分析网络数据流在正常状态和有攻击状态时不同的分布情况.图 3 是用 NS-2 软件模拟的 LDoS 攻击的包过程,其中,前 100s 网络处于正常状态,100s~150s 网络受到 LDoS 攻击.

定义随机过程$\{X(t),t=n\Delta t,n\in\mathbf{Z}^+\}$为包过程[16],$\Delta t$ 表示采样时间的间隔,$X(t)$为在$(t-\Delta t,t]$的时间段内通过路由器的数据包数量.小波变换是一种时-频窗面积固定、形状可自适应调整的信号分析工具,在时域和频域局部化方面具有独特优势,非常适合于信号的异常检测[17,18].

首先,通过小波函数$\psi_{j,k}(t)$和尺度函数$\varphi_{j,k}(t)$,将包过程$\{X(t)\}$作 J 层分解[17]:

$$X(t)=\sum_k c_{J,k}\varphi_{J,k}(t)+\sum_k\sum_{j=1}^{J} d_{j,k}\psi_{j,k}(t) \tag{1}$$

其中,$C_{j,k}$为近似系数,表示尺度 J 上的逼近信息;$d_{j,k}$为小波系数,表示尺度 j 上的细节信息.公式(1)中的小波分解是可逆的,根据近似系数和细节系数可以重构原信号 $X(t)$.在小波分解下,不同的尺度大小会使信号具有不同的时间和频率分辨率,选择特定尺度上的小波系数和近似系数重构信号可以分离出相应的频率成分[17].这里采用 Db4 小波对网络流量的包过程$\{X(n)\}$进行 5 层小波分解.提取波形趋势,结果如图 4 所示.

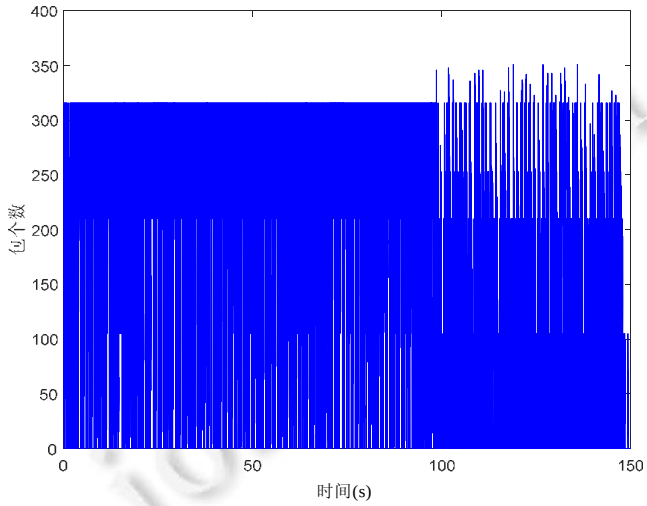


Fig.3 Packets process of LDoS attack simulated by NS-2

图 3 NS-2 模拟 LDoS 攻击的包过程

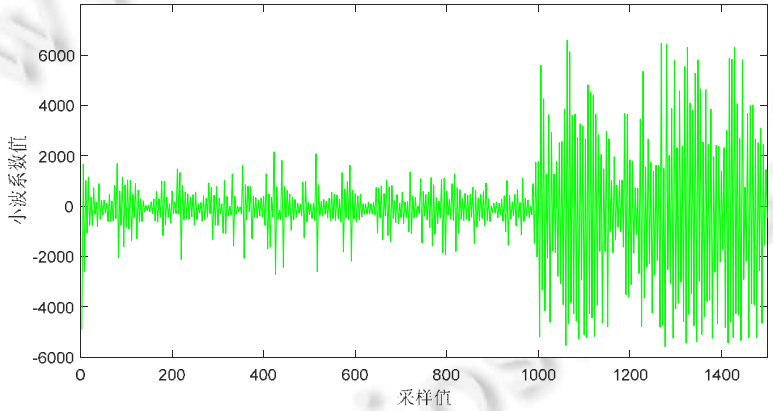


Fig.4 Wavelet coefficients of process of network traffic packets

图 4 网络流量包过程的小波系数

经过小波变换分解后,可以看到网络流量在攻击前后波动性差异.根据网络数据包的小波系数在 LDoS 攻击前后的这种波动性,从能量变化的角度,可以求出其小波能量在攻击前后的变化.$E=(E_1,E_2,\ldots,E_n)$是信号 $X(t)$在尺度 j 上的小波能谱.设 $p_k=E_k/E$,其中,E 为信号的总功率.定义小波能谱熵 W_{EE}[19]为

$$W_{EE}=-\sum_k p_k \log p_k \tag{2}$$

正常的网络中,能量集中在高频部分,低频部分的能量很小,其对应的小波能量值就会相对集中.当正常的网络受到 LDoS 攻击后,其高频分量因为受到攻击的抑制而减少,低频部分的能量增加,其对应的小波能量值就

会相对分散.小波能谱熵可以反映信号在每个小波尺度值上的分布是否均匀:熵值小,表示能谱分布相对集中;熵值大,则表示能谱分布相对分散.所以,处于正常状态的网络流量的小波能谱熵较小.反之,当受到 LDoS 攻击时,网络流量的小波能谱熵就会增大.因此,小波能谱熵能较好地表征 LDoS 攻击的存在.对网络流量的数据包数量进行采样,并设置一个滑动窗口,窗口长度 W 设置为 2 500,滑动大小 δ=10.按照前面的介绍的方法对网络在正常状态和有 LDoS 攻击时的包个数进行统计,并计算 25 组小波能谱熵值,其分布情况如图 5 所示.从图 5 可以看出,网络处于正常状态时的小波能谱熵值较小,而当网络中有 LDoS 攻击时,小波能谱熵值较大.

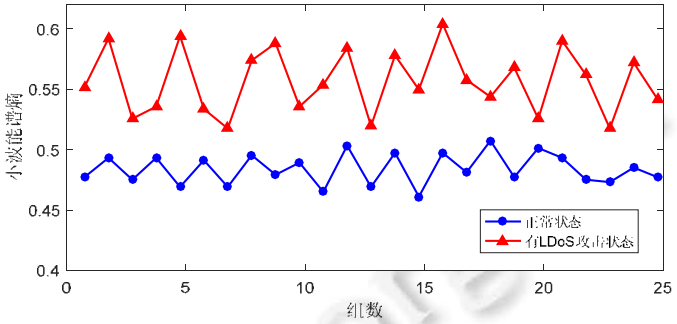


Fig.5 Changes in wavelet energy spectrum entropy under normal network conditions and in the presence of LDoS attacks

图 5 网络正常状态和有 LDoS 攻击时的小波能谱熵变化情况

3 基于 HSMM 模型 LDoS 攻击检测方法

HSMM 是隐马尔可夫模型(hidden Markov model,简称 HMM)的扩展形式,其在 HMM 模型的基础上增加了状态的驻留时间参数.通过这个驻留时间参数,能够更准确地描述 HMM 中的状态转移关系.所以,HSMM 模型可以更客观地描述网络状态.

3.1 HSMM模型的定义

一个典型的 HSMM 模型可以由四元组 $\lambda=(\pi,A,B,P_i(d))$来表示,其中,π是初始状态,A 是各个状态间的状态转移矩阵,B 是输出概率矩阵,$P_i(d)$是状态驻留参数.图 6 为 HSMM 的示意图[19].

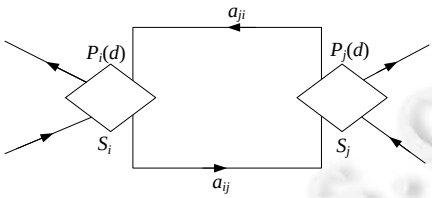


Fig.6 Schematic diagram of HSMM

图 6 HSMM 模型示意图

HSMM 各个参数的最大似然参数估计公式如下.

$$\overline{\pi}=\gamma_1(i) \tag{3}$$

$$\overline{a}_{ij}=\frac{\sum_{t=1}^{T-1}\zeta_t(i,j)}{\sum_{t=1}^{T}\gamma_t(i)}(1\leqslant i\leqslant N,1\leqslant j\leqslant N) \tag{4}$$

$$\bar{b}_j(k)=\frac{\sum_{t=1,s.t.O_t=v_k}^{T}\gamma_t(j)}{\sum_{t=1}^{T}\gamma_t(j)}(1\leqslant j\leqslant N,1\leqslant k\leqslant M) \tag{5}$$

$$\bar{p}_i(d)=\frac{\sum_{t=1}^{T}\omega_{t,d}(i)}{\sum_{\tau=1}^{D}\sum_{t=1}^{T}\omega_{t,\tau}(i)} \tag{6}$$

其中,$\gamma_t(i)$是在给定模型参数λ和状态观测序列$O=\{O_1,O_2,\ldots,O_t\}$情况下,在时刻t的状态是S_i的概率;$\xi_t(i,j)$表示在给定模型参数λ和状态观测序列O情况下,在时刻t的状态是S_i,而在$t+1$时刻的状态为S_j的概率;$\omega_{t,\tau}(i)$表示给定模型λ和观测序列O情况下,在当前时刻$t(1\leqslant t\leqslant T)$系统处于状态$S_i(1\leqslant S_i\leqslant N)$且系统还将在$S_i$上驻留$\tau(0\leqslant\tau\leqslant D)$个时间单位时的概率.

3.2 HSMM模型训练

用已知正常行为的小波能谱熵训练确定HSMM的参数$\lambda=(\pi,A,B,P_i(d))$,建立正常主机行为的HSMM模型,训练过程如图7所示.

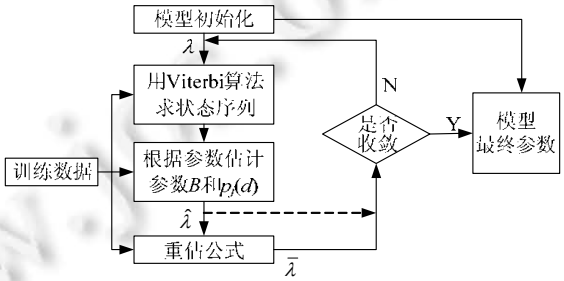


Fig.7 Training process of HSMM

图7 HSMM模型的训练过程

HSMM模型的状态数N取2分别表示正常状态和受到LDoS攻击状态,观测序列长度T取26.训练时,把状态转移概率矩阵初始值设定为$\pi=\{1,0\}$.当训练迭代的次数等于25时训练停止.网络状态的训练曲线如图8所示,纵轴为输出似然概率的对数值.当训练步数达到15步时,模型就开始收敛.

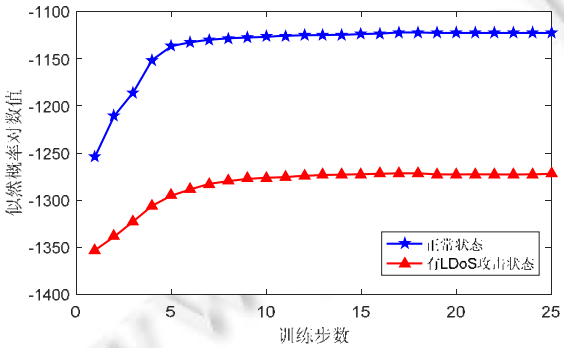


Fig.8 Training state curve

图8 训练状态曲线

3.3 HSMM模型的LDoS攻击检测方法

HSMM网络状态判别模型含有两个状态:正常状态和异常状态.首先对提取的网络流量信息进行处理采样,

然后把采样的数据通过小波分解与重构得到小波能谱向量,将提取的特征向量作为 HSMM 的网络流量状态分类器的输入.最后提取经过预处理的数据的特征作为观测向量,利用已经训练好的网络状态模型来判别网络状态的情况.即把观测向量输入到训练好网络状态的分类器,利用 Viterbi 算法求出各个观测向量在不同模型下的似然概率,似然概率值最大的状态就是当前网络所处的状态.基本的流程图如图 9 所示.

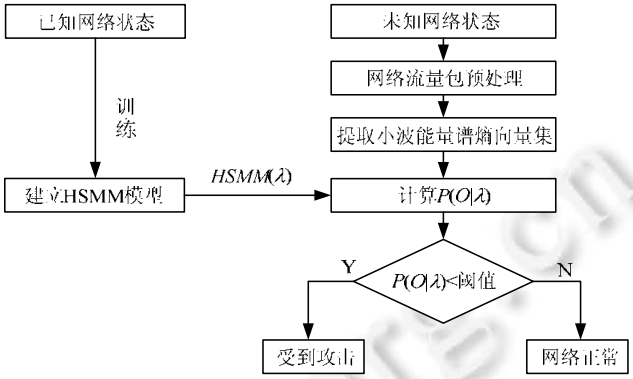


Fig.9 Flow chart of LDoS attack detection by HSMM

图 9 HSMM 检测 LDoS 攻击流程图

HSMM 定义 $P(O|\lambda)\times P_i(d)$为时间状态乘积,时间状态乘积是这个观测值序列对于 HSMM 的偏离度.因为在正常网络状态的基础上构建的 HSMM 模型,所以偏离度越大就表示网络中遭到 LDoS 攻击的几率越大[19].定义变量 $a_T(j)$和 $b_j(O_i)$,其中,$a_T(j)=P\{O_1,O_2,\ldots,O_t,S_j|\lambda\}(1\leqslant j\leqslant N,1\leqslant t\leqslant T)$,$N$ 是隐藏的状态数目.$a_T(j)$表示 HSMM 参数为λ并且 t 时刻的观测值序列为 O 时,HSMM 的隐藏状态为 S_j 的概率;$b_j(O_i)$表示在隐藏状态为 S_j 时,观察值为 O_i 的概率.对 $P(O|\lambda)$的求解利用前向算法[20],其具体的过程如下.

$$p(O\mid\lambda)=\sum_{j=1}^{N}a_T(j)=a_T(1)+a_T(2)=a_T(1) \tag{7}$$

其中,$a_T(1)=b_1(O_T)b_1(O_{T-1})\ldots b_1(O_3)b_1(O_2)b_1(O_1)$.公式(7)可以化简得到:

$$P(O\mid\lambda)=\prod_{i=1}^{T}b_1(O_i)=[P(V_1\mid S_1)]^a[P(V_2\mid S_1)]^{T-a}=[1-P(V_2\mid S_1)]^a[P(V_2\mid S_1)]^{T-a} \tag{8}$$

其中,T 表示整个观测序列中观测值的总个数,a 表示在观测序列中正常状态的观测值数目,$P(V_2|S_1)$表示虚警率.使用小波能谱熵的检测方法对网络状态进行初检测,将虚警率记作 r_{fp}.为了方便,用ξ表示观测值序列对于 HSMM 的偏离度,可得:

$$\xi=P(O|\lambda)\times P_i(d)=(1-r_{fp})^a(r_{fp})^{T-a}\cdot P_i(d)(0\leqslant a\leqslant T) \tag{9}$$

由公式(9)可知,ξ主要由 r_{fp} 的值决定.由以往实验分析可知,$(1-r_{fp})$的值比 r_{fp} 要大,所以在 T 个观测值中,正常状态的观测值个数 a 越多,ξ的值就越大,表示网络状态为正常的几率也就越大.

4 实验及结果分析

为了验证本文方法的有效性,通过搭建 NS-2 和 Test-bed 实验平台,模拟仿真 LDoS 攻击的网络环境,对本文所提出的基于网络测量的 LDoS 攻击检测方法进行验证.通过在 NS-2 和 Test-bed 平台中采集网络数据,利用 HSMM 网络模型完成 LDoS 攻击的检测,并将实验结果与现有方法的结果进行了比较分析.

4.1 NS-2仿真实验及其结果分析

根据 Rice 大学的 NS-2 仿真实验环境[3],对网络的参数进行设置,建立如图 10 所示的网络拓扑进行仿真实验来验证本文方法的性能.

在图 10 的网络拓扑中,0 号和 1 号节点表示路由器,2 号节点表示的是 FTP 服务器,3 号节点表示 UDP 服务

器,4 号~6 号节点表示合法的用户,7 号节点表示 LDoS 的攻击端.其中加入 3 条 UDP 背景流.合法用户和路由器间的带宽设置成 100Mb/s,LDoS 的攻击端和路由器间的带宽也设置成 100Mb/s,单向的时间延迟成 10ms.瓶颈链路的带宽设置成 10Mb/s,单向延时 10ms;1 号与 2 号节点带宽设为 100Mb/s,单向延时 10ms.节点 7 是攻击端,其攻击速率为 12Mb/s,略大于瓶颈带宽 10Mb/s,攻击周期为 1 150ms,攻击脉宽为 200ms.4 号~6 号从 0s 开始传输正常流量到 200s 时结束,攻击端从 100s 开始发送攻击数据包到 200s 停止.

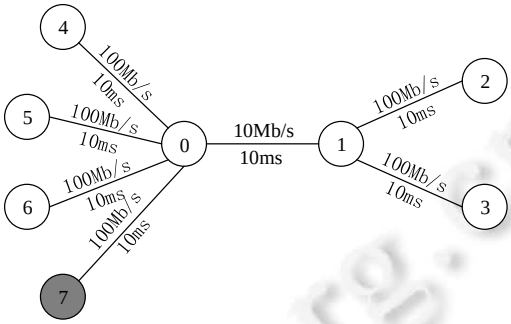


Fig.10 Network topology in NS-2

图 10 NS-2 中网络拓扑结构

对网络中数据包的采样值,设定一个滑动窗口 W,大小为 3s,即每 3s 采样的值做一次小波能谱熵,得到一个检测结果.窗口 W 的滑动步长设为 1s,共移动 200s.对网络流量的小波能谱熵向量值的统计结果如图 11 所示.

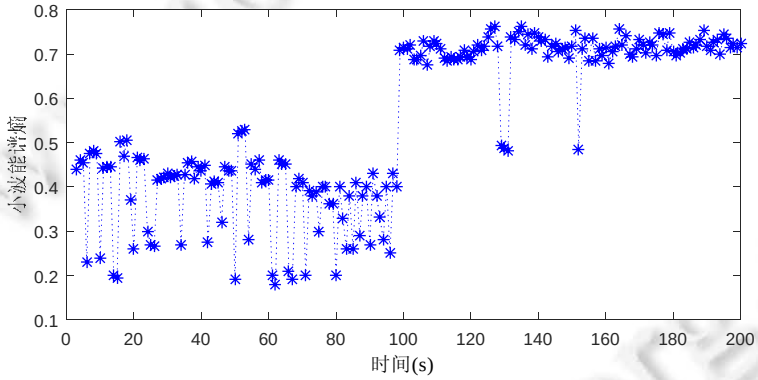


Fig.11 Vector values of wavelet energy spectrum entropy

图 11 小波能谱熵向量值

由图 11 可知,小波能谱熵值在前 100s 内在较小的值附近波动,到 100s 有 LDoS 攻击时发生了很大的变化.通过对未攻击时的小波能谱熵和受到攻击时的小波能谱熵结果进行一维拟合并取加权平均,把小波能谱熵的判决门限λ设置成 0.5.对上述情况的小波能谱熵值的检测结果进行统计分析(为了和 HSMM 结果比较分析,同时减轻突发变化的影响,舍弃了未攻击时判决前两个结果和有攻击时判决的前 5 个结果),得出小波能谱熵的检测结果见表 1.

Table 1 Wavelet energy spectrum entropy decision results

表 1 小波能谱熵判决结果

未攻击时的判决次数/有攻击时的判决次数	正确判决次数	漏警次数	虚警次数
100/100	95	5	6

由表 1 可计算出此时使用小波能谱熵的方法来检测 LDoS 攻击的检测率是 95%,漏警率是 5%,虚警率是 6%.为了得到更好的检测效果,把上面小波能谱熵检测的结果当作观察值.每间隔 1s 滑动一次,3 个一组作为观测值

序列集合,观测值序列集合 $O=\{O_1,O_2,O_3\}$,则由公式(9)可以得到 HSMM 模型下网络状态的判决依据ξ值,其值分布如图 12 所示.

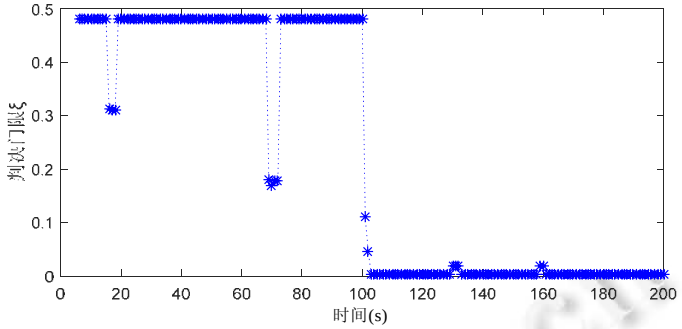


Fig.12 Simulation value of decision threshold ξ

图 12 判决门限ξ仿真值

由图 12 可知,在没有攻击的前 100s 内,正常的网络状态的判决门限较高;在第 100s 后,网络遭受 LDoS 攻击,判决门限较低.对此实验条件下的 HSMM 模型的检测结果进行统计,结果见表 2.

Table 2 Judgment result of HSMM

表 2 HSMM 判决结果

未攻击时的判决次数/有攻击时的判决次数	检测门限	正确判决次数	漏警次数	虚警次数
100/100	0.1	96	4	0
100/100	0.2	98	2	4
100/100	0.3	95	5	7

表 1 与表 2 的统计结果对比分析可知,在判决次数一定的情况下,如果选择合适的检测门限,则 HSMM 模型的检测方法比小波能谱熵的方法更加稳定,检测率略有提高,虚警次数明显下降.

4.2 Test-bed实验及结果分析

为了验证 HSMM 方法在真实网络环境中的检测效果,采用研究 LDoS 攻击的通用平台 Test-bed 进行重复实验.该平台及其参数的设置参考 Rice 大学在 NS-2 中搭建的实验环境[3,21]设计的 Test-bed 实验平台,结构如图 13 所示.

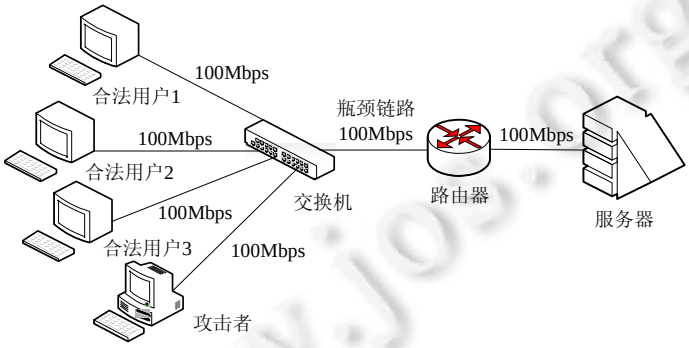


Fig.13 Test-bed experimental topology graph

图 13 Test-bed 实验拓扑图

3 个合法用户从 FTP 服务器下载资源,一台主机作为攻击者发起攻击.交换机选用的是 CISCO WS-C3750X,路由器采用的是 CISCO 2911.瓶颈链路带宽设为 10Mb/s,其他客户端到交换机以及服务器到路由器的带宽也是 10Mb/s.其中,实验计算机均使用 Redhat9.0 系统.为了保证实验的合理性,在林肯实验室的 DARPA 数据集中加入 2000 年某一周某大型网站的正常数据作为背景流量.利用 ShrewAttack 攻击软件[3]发送 LDoS 攻击包,受害端为

ftp 服务器.仍然是从 100s 开始发起 LDoS 攻击.攻击的周期为 1 150ms,攻击的脉冲长度设成 200ms,攻击的速率是 10Mb/s.

在实际的网络环境中,采用 tcpstat 软件工具以 0.5s 的采样间隔来统计网络中的数据包.同样设定了大小是 3s 的滑动窗口,把每 3s 采样的值做一次小波能谱熵,得到一个检测结果.窗口 W 的滑动步长为 1s.网络流量的小波能谱熵的统计结果如图 14 所示.

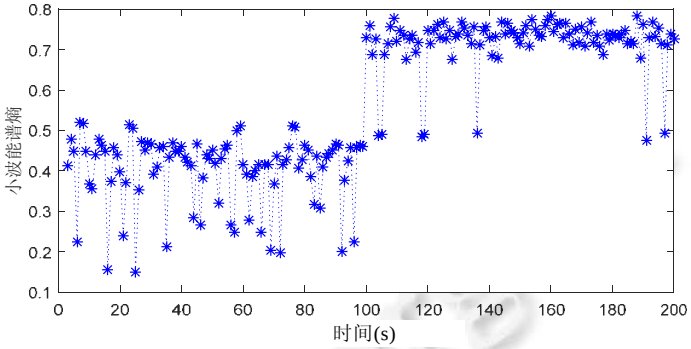


Fig.14 Value of wavelet energy spectrum entropy of network traffic

图 14 网络流量的小波能谱熵值

如图 14 所示,Test-bed 平台数据的小波能谱熵值同样在 100s 时出现了跳变.同样使用判决门限λ=0.5,对此时的小波能谱熵值的检测结果进行统计分析,得出小波能谱熵的检测结果,见表 3.

Table 3 Decision results of wavelet energy spectrum entropy

表 3 小波能谱熵判决结果

未攻击时的判决次数/有攻击时的判决次数	正确判决次数	漏警次数	虚警次数
100/100	92	8	8

由表 3 可知,在 Test-bed 平台采集的实际网络数据通过计算后,使用小波能谱熵方法检测 LDoS 攻击的检测率是 92%,漏警率是 8%,虚警率是 8%.与 NS-2 平台的模拟数据相比,虽然检测性能有所下降,但仍有较好的检测效果.对实验数据做与 NS-2 平台下相同的处理,得到 HSMM 下网络状态的判决依据ξ值的分布如图 15 所示.

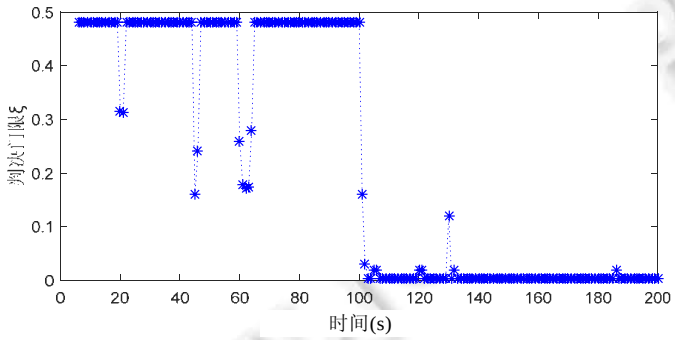


Fig.15 Simulation value of HSMM decision threshold ξ (Testbed)

图 15 HSMM 的判决门限ξ仿真值

Test-bed 实验数据与 NS-2 仿真数据相比,在正常或受到 LDoS 状态下都具有更大的波动性,从而造成了小波能谱熵的相对不稳定.这主要有以下原因.

1) NS-2 仿真时,各个 TCP 节点的网络流量较为平均,提取的各个特征较为平稳.而实际的网络环境中,各个用户之间存在竞争关系,随机突发增多,这造成了网络流量变化的不稳定性.

2) 实际的网络环境中,FTP 服务器存在一定的防御机制,使得 LDoS 攻击效果并不如 NS-2 仿真环境中的理想.

观察图 15 可知,在没有 LDoS 攻击的前 100s 内的判决门限较高,而在 100s 后,网络中有 LDoS 攻击发生,相应的判决门限降低,与之前不同的网络状态对应不同判决门限ξ值的结论一致.对 Test-bed 平台数据经过 HSMM 检测后进行统计分析后,得到的 HSMM 的判决结果见表 4.

Table 4 Judgment results of HSMM

表 4 HSMM 判决结果

未攻击时的判决次数/有攻击时的判决次数	检测门限	正确判决次数	漏警次数	虚警次数
100/100	0.1	94	6	0
100/100	0.2	95	5	5
100/100	0.3	95	5	8

HSMM 的检测方法利用状态转移关系和驻留时间参数,以后验概率来判断是否有 LDoS 攻击发生,比单一利用小波能谱熵判定 LDoS 攻击更具有稳定性和抗干扰性.在引入 HSMM 后,ξ在正常状态和异常状态下的分布与小波能谱熵值相对松散的分布相比更加集中.因此,两种情况下的分类更加精确.同时,ξ在两种状态下均值变化更大,即两种情况下的区分度更高,降低了误判的概率.所以在引入 HSMM 后,能够实现更加准确的分类检测.与 NS-2 仿真平台中的实验结果相比,即使在真实实验平台 Test-bed 下有随机突发等外界因素的干扰,HSMM 算法在检测率上也基本没有下降,说明 HSMM 检测方法适用于 LDoS 攻击的检测,且有较好的检测效果.

4.3 算法的检测性能分析

由中心极限定理的知识可知,很多随机变量都近似是正态分布.定义参数:H_0表示网络不存在 LDoS 攻击,H_1表示网络遭受到 LDoS 攻击.设 H_0 的值是均值等于 u_0、方差等于 σ_0^2 的正态分布;H_1 的值是均值为 u_1、方差为 σ_1^2 的正态分布.统计 3 000 个ξ值得到:u_0=0.2993, σ_0^2 =0.0236;u_1=0.0349, σ_1^2 =6.4009×10^{-4}.

图 16 为网络正常和有攻击状态时的ξ值分布情况,可以根据ξ值的不同分布来判断网络的状态.由图 16 中可知,有攻击和正常状态曲线的交集很少,说明漏警率与虚警率都很小,由此能够很好地判断网络的状态情况.由于在实际环境中,不同的网络模型、攻击参数以及选取的指标阈值的不同都会影响到本文检测方法的性能,在ξ分别取值不同的情况下计算得出检测率 P_D、漏警率 P_{FN} 和虚警率 P_{FP},结果见表 5.

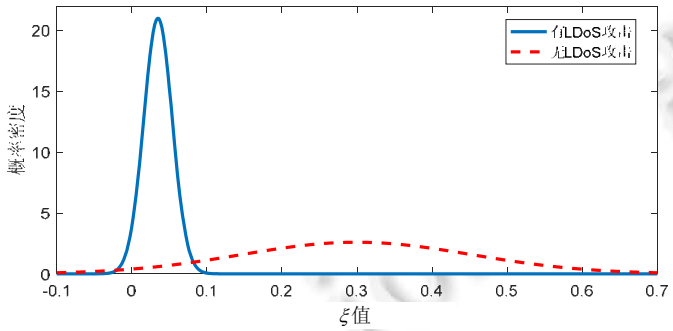


Fig.16 Value distribution of ξ

图 16 ξ值的分布

Table 5 Detection performance corresponding to different ξ values

表 5 不同ξ值对应的检测性能

	ξ						
	0.05	0.06	0.07	0.081 8	0.12	0.17	0.20
P_D	72.47%	83.94%	91.73%	96.81%	99.96%	1.000 0	1.000 0
P_{FN}	27.53%	16.06%	8.27%	3.19%	0.04%	0	0
P_{FP}	5.22%	5.95%	6.76%	7.83%	12.14%	19.98%	25.88%

由表 5 可知,ξ取不同的值对检测性能的影响非常大.图 16 中两条正态分布曲线的交点就是判决阈值的最佳位置,这时的ξ=0.0818.表 6 对基于 NCPSD[9]、卡尔曼滤波[22]、粒子滤波[23]和多重分形[10]的检测方法性能进行了比较.

表 6 对比了几种常用的 LDoS 攻击的检测方法,分别从检测率、漏警率和虚警率这 3 个方面做了统计.分析对比可知,基于网络测量的 LDoS 攻击检测方法相对于其他检测方法在减少漏警率和虚警率的情况下,同时提高了检测率,检测性能良好.

Table 6 Performance comparison of different detection methods

表 6 不同检测方法性能比较

检测方法	检测率(%)	漏警率(%)	虚警率(%)
NCPSD	88.00	12.00	16.70
卡尔曼滤波	89.60	10.40	12.60
粒子滤波	97.68	2.32	4.23
多重分形	91.00	9.00	10.00
网络测量	96.81	3.19	7.83

图 17 是基于粒子滤波的 LDoS 攻击检测和基于网络测量的 LDoS 攻击流量检测结果对比图.由图 17 可知,虽然粒子滤波的检测率较高,但由于粒子滤波算法在估算过程中存在大量的蒙特卡罗抽样操作,使得粒子滤波算法的复杂度比其他算法要高.鉴于本实验的网络环境相对简单,假设的网络状态模型也是在比较理想情况下的,下一步工作要丰富实验环境,完善网络状态模型参数,以更好地贴近实际网络状况.

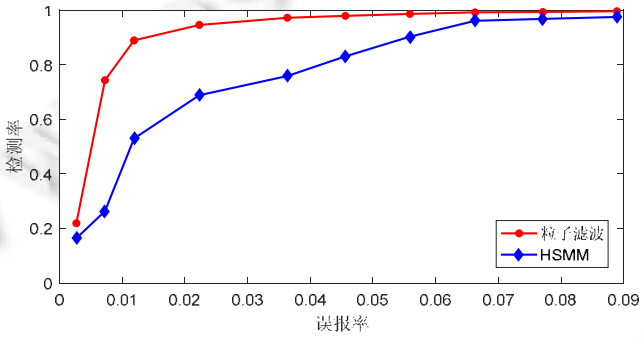


Fig.17 Comparison of detection results between particle filtering and network measurement

图 17 粒子滤波与网络测量的检测结果对比

5 结 论

“互联网+”时代信息技术日新月异,随之带来的网络安全问题也越来越多.LDoS 攻击是一种高级形式的 DoS 攻击,其低速率的特点使其具有很强的隐蔽性,使得常规的检测方法很难奏效.所以,研究 LDoS 攻击的检测方法具有挑战性和应用前景.

本文的主要创新性工作体现在:对网络链路中的数据包进行定量分析,提取包数量的小波能谱熵特征,通过采用 HSMM 网络模型设计状态判别模型,将小波能谱熵的观察值序列作为 HSMM 模型的输入检测 LDoS 攻击.基于此,提出了基于网络测量的 LDoS 攻击检测方法.通过搭建 NS-2 仿真实验拓扑和在 Test-bed 平台采集真实网络环境下的实验数据进行实验,证明算法检测性能较好,具有很好的可用性.通过大量数据验证算法的有效性,对比其他检测算法,说明检测性能良好.

本文方法研究的对象是一种典型的 LDoS 攻击形式,其周期是固定值.而针对攻击周期按照 RTT 指数变化的情况(属于同步攻击方式)以及变速率 LDoS 攻击类型,本文方法并没有进行验证.因此,本文方法在针对不同类型的 LDoS 攻击和建立精确的非线性网络流量模型方面需要改进.今后的研究工作的研究思路如下.

(1) 需要进一步改善非线性网络流量建模的精度,准确刻画网络流量的特点,提高 LDoS 攻击的检测精度.

(2) 由于 HSMM 模型假设的前提比较理想化,在实际网络状态转移情况更复杂可能会导致检测效能降低.下一步调整 HSMM 模型参数,更好地构建网络状态的模型参数来提高检测的性能.

(3) 随着云计算、云存储和大数据技术的不断发展,针对它们面临 LDoS 攻击威胁的问题,开展针对云端的 LDoS 攻击检测与防范的研究.

References:

[1] Wu ZJ, Pei BS. The detection of LDoS attack based on the model of small signal. Acta Electronica Sinica, 2011,39(6):1456−1460 (in Chinese with English abstract).

[2] Luo JT, Yang XL, Wang J, Xu J, Sun J, Long KP. On a mathematical model for low-rate shrew DDoS. IEEE Trans. on Information Forensics and Security, 2014,9(7):1069−1083. [doi: 10.1109/TIFS.2014.2321034]

[3] Kuzmanovic A, Knightly EW. Low-rate TCP-targeted denial of service attacks. Proc. of the ACM SIGCOMM, 2003,14(4):75−86. [doi: 10.1145/863965.863966]

[4] 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 with English abstract). http://www.jos.org.cn/1000-9825/4520.htm [doi: 10.13328/j.cnki.jos.004520]

[5] 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 ICCNMC. 2005. 423−432. [doi: 10.1007/11534310_46]

[6] Zhang J, Hu HP, Liu B, Xiao FT. Detecting LDoS attack based on ASPQ. Journal on Communication, 2012,33(5):79−84 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-436X.2012.05.010]

[7] Wu N, Mu ZY, Zhang LC. Distributed denial of service covert flow detection based on data stream potential energy feature. Computer Engineering, 2015,41(3):142−146,161 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-3428.2015.03.027]

[8] Luo JT, Yang XL. The new shrew attack: A new type of low-rate TCP-targeted DoS attack. In: Proc. of the Int'l Conf. on Communications. 2014. 713−718. [doi: 10.1109/icc.2014.6883403]

[9] Chen Y, Huang K, Kwok YK. Collaborative defense against periodic shrew DDoS attacks in frequency domain. ACM Trans. on Information and System Security, 2005. https://www.researchgate.net/publication/228703297

[10] Tang D, Chen K, Chen XS, Liu HY, Li XH. Adaptive EWMA method based on abnormal network traffic for LDoS attacks. Mathematical Problems in Engineering, 2014,(3):166−183. [doi: 10.1155/2014/496376]

[11] Wu ZJ, Zhang LY, Yue M. Low-rate DoS attacks detection based on network multifractal. IEEE Trans. on Dependable and Secure Computing, 2016,13(5):559−567. [doi: https://doi.org/10.1109/tdsc.2015.2443807]

[12] Tang YJ, Luo Xp, Hui Q, Rocky KC. Modeling the vulnerability of feedback-control based Internet services to low-rate DoS attacks. IEEE Trans. on Information Forensics and Security (TIFS), 2014,9(3):339−353. [doi: 10.1109/tifs.2013.2291970]

[13] Zhu HL, Yang YX, Wu QX, You FC. A novel distributed LDoS attack scheme against Internet routing. China Communications, 2014,11(13):101−107. [doi: 10.1109/cc.2014.7022532]

[14] 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. 24−28. [doi: 10.1109/icc.2007.204]

[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] He YX, Liu T, Cao Q, Xiong Q, Han Y. A survey of low- rate denial- of- service attacks. Journal of Frontiers of Computer Scicence and Technology, 2008,2(1):1−19 (in Chinese with English abstract). [doi: 10.3778/j.issn.1673-9418.2008.01.001]

[17] He YX, Cao Q, Liu T, Han Y, Xiong Q. A low-rate DoS detection method based on feature extraction using wavelet transform. Ruan Jian Xue Bao/Journal of Software, 2009,20(4):930−941 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/20/930.htm [doi: 10.3724/SP.J.1001.2009.03302]

[18] Wu ZJ, Yue M. Research on the performance of low-rate DoS attack. Journal on Communication, 2008,29(6):87−93 (in Chinese with English abstract). [doi: 10.3321/j.issn:1000-436X.2008.06.014]

[19] Zeng QH, Qiu J, Liu GJ, Tan XD. Equipment degradation state recognition method and its applications based on wavelet feature scale entropy and hidden semi-Markov models. Acta Armamentarii, 2008,29(2):198−203 (in Chinese with English abstract). [doi: 10.3321/j.issn:1000-1093.2008.02.015]

[20] Jain R, Abouzakhar NS. Hidden Markov model based anomaly intrusion detection. In: Proc. of the Int'l Conf. for Internet Technology and Secured Transactions. 2012. 528−533.

[21] Kuzmanovic A, Knightly EW. Low-rate TCP-targeted denial of service attacks and counter strategies. IEEE/ACM Trans. on Networking, 2006,14(4):683−696. [doi: 10.1109/tnet.2006.880180]

[22] Wu ZJ, Yue M. Detection of LDDoS attack based on kalman filtering. Acta Electronica Sinica, 2008,36(8):1590−1594 (in Chinese with English abstract). [doi: 10.3321/j.issn:0372-2112.2008.08.021]

[23] Wu ZJ, Jiang J, Yue M. A Particle filter-based approach for effectively detecting low-rate denial of service attacks. In: Proc. of the Int'l Conf. on Cyber-enabled Distributed Computing and Knowledge Discovery (CyberC). 2016. 86−90. [doi: 10.1109/cyberc.2016.25]

附中文参考文献:

[1] 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):1456−1460.

[4] 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 [doi: 10.13328/j.cnki.jos.004520]

[6] 张静,胡华平,刘波,肖枫涛.基于 ASPQ 的 LDoS 攻击检测方法.通信学报,2012,33(5):79−84. [doi: 10.3969/j.issn.1000-436X.2012.05.010]

[7] 吴娜,穆朝阳,张良春.基于数据流势能特征的分布式拒绝服务隐蔽流量检测.计算机工程,2015,41(3):142−146,161. [doi: 10.3969/j.issn.1000-3428.2015.03.027]

[16] 何炎祥,刘陶,曹强,熊琦,韩奕.低速率拒绝服务攻击研究综述.计算机科学与探索,2008,2(1):1−19. [doi: 10.3778/j.issn.1673-9418.2008.01.001]

[17] 何炎祥,曹强,刘陶,韩奕,熊琦.一种基于小波特征提取的低速率 DoS 检测方法.软件学报,2009,20(4):930−941. http://www.jos.org.cn/1000-9825/3302.htm [doi: 10.3724/SP.J.1001.2009.03302]

[18] 吴志军,岳猛.低速率拒绝服务 LDoS 攻击性能的研究.通信学报,2008,29(6):87−93. [doi: 10.3321/j.issn:1000-436X.2008.06.014]

[19] 曾庆虎,邱静,刘冠军,谭晓栋.基于小波特征尺度熵-隐半马尔可夫模型的设备退化状态识别方法及应用.兵工学报,2008,29(2):198−203. [doi: 10.3321/j.issn:1000-1093.2008.02.015]

[22] 吴志军,岳猛.基于卡尔曼滤波的 LDDoS 攻击检测方法.电子学报,2008,36(8):1590−1594. [doi: 10.3321/j.issn:0372-2112.2008.08.021]

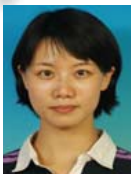
吴志军(1965－),男,河南固始人,博士,教授,博士生导师,CCF 专业会员,主要研究领域为网络信息安全.

张景安(1989－),男,硕士,主要研究领域为低速率拒绝服务攻击的检测.

李红军(1992－),男,学士,主要研究领域为网络信息安全.

岳猛(1984－),男,博士,讲师,主要研究领域为网络信息安全.

刘亮(1991－),男,硕士,主要研究领域为网络信息安全.



雷缙(1982－),女,讲师,主要研究领域为网络信息安全.