基于小信号检测模型的LDoS攻击检测方法的研究

吴志军,裴宝崧
(中国民航大学电子信息工程学院智能信号与图像处理天津市重点实验室,天津 300300)

摘 要: 低速率拒绝服务LDoS(Low-rate Denial of Service)是一种新型的面向TCP协议的DoS攻击方式.LDoS攻击的平均流量仅占正常流量的10-20%,具有明显的周期性小信号特征,隐蔽性强.因此,检测LDoS攻击成为网络安全研究的一个难点.本文采用数字信号处理DSP技术,基于小信号检测理论,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30秒时间内(3000个采样点)到达的数据包个数进行统计;将统计值与设定的判决特征值门限比较,作为判断有无LDoS攻击的依据.如果判定成立,则通过特征值估算矩阵可较精确地计算出LDoS攻击的周期值.在NS-2环境中的仿真实验结果表明本文方法具有较高的LDoS攻击检测率.

关键词: 低速率拒绝服务攻击; 小信号; 检测; 漏值多点数字平均
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112 (2011) 06-1456-05

The Detection of LDoS Attack Based on the Model of Small Signal

WU Zhi-jun, PEI Bao-song
(*School of Electronics & Information Engineering, Tianjin Key Laboratory for Advanced Signal Processing, Civil Aviation University of China, Tianjin* 300300, *China*)

Abstract: Low-rate denial of service(LDoS) is a new class of DoS attack, which exploits the deficiencies of the minimum RTO of TCP to send out attack packets about 10%-20% of normal traffic in short periodic pulses to a victim. It is hard to be detected through traditional detection mechanism. In this paper, an approach of detecting LDoS attack based on the model of small signal is proposed. The proposed approach takes statistics on the packets arriving in 30 seconds (sampling time is 10ms, total of 3000 sampling points), and compares the statistical result with the characteristic judging value, which is settled as a threshold to indicate the difference between normal and attack flow. An eigenvalue-estimating matrix is established to estimate the attack period after LDoS attack being detected. Simulation results in NS-2 environment show that the proposed approach can detect the LDoS attack effectively.

Key words: low-rate denial of service (LDoS); small signal; detection; multiple sampling averaging based on missing sampling (MSABMS)

1 引言

低速率拒绝服务LDoS(Low-rate Denial of Service)攻击是一种新型的DoS攻击形式.它利用网络协议或应用服务中常见的自适应机制所存在的安全漏洞,通过周期性地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,从而降低被攻击端服务性能.这种间歇性攻击的特点,使得其攻击流的平均速率较低,而且完全融合在合法用户的数据流中,现有的检测方法对LDoS攻击很难进行检测和防范[1].

在合法TCP流和LDoS攻击流同时发送到相同的目的地址时,LDoS流表现出两个不同的重要行为:第一,LDoS流的最高速率将保持不变,而TCP流则呈线性增长;第二,LDoS流在相对固定的时间周期到达目的地,而TCP流则是连续到达.用现有的通信量分析方法,周期性脉冲很难在时间域被检测出来.这是因为平均共享的带宽并不是非常大.在分布式的情况下,成倍的傀儡机发起的攻击会更进一步降低单个通信量的速率,因此,就导致检测更加困难.分布式攻击发起者可以通过降低最高速率或者延长攻击周期来降低平均通信量[2].所以,用时间序列检测LDoS攻击是毫无效果的.目前的攻击检测手段基本是基于时间序列的,对LDoS攻击的检测是个盲点.

通过对单条TCP流和单个LDoS攻击流的研究发

收稿日期:2010-02-21 修回日期:2010-11-01
基金项目:国家自然科学基金委员会与中国民用航空总局联合资助(No.60776808);天津市应用基础及前沿技术研究计划(No.09JCYBJC00400);2010年度中央高校基本科研业务费中国民航大学专项(No.ZXH2010B004)

现:LDoS 攻击的平均流量较小,约占正常流量的 10% – 20%[1~3];而 LDoS 攻击的表现形式为周期性的脉冲序列.因此,相对 TCP 流量而言,可以将 LDoS 攻击定义为周期性的小信号,即周期小信号.进而可以采用小信号检测理论进行 LDoS 攻击检测方法的研究.本文在分析 LDoS 攻击特点的基础上,采用小信号理论,提出了基于小信号模型的 LDoS 攻击检测的方法.

2　TCP 和 LDoS 攻击流量时频域分析

在利用小信号模型进行 LDoS 攻击的检测方法中,背景噪声为 TCP 流量,而小信号则为 LDoS 攻击流量.因此,通过针对单条 TCP 和 LDoS 攻击流量的时频域分析,可以找出它们中间适用于检测的特点.

2.1　TCP 流量时域分析

通过对网络流量按照协议分析表明:网络流量中 80%以上的流量是 TCP[4].研究表明:正常的 TCP 流量,其数据包的传输与 RTT(Round-Trip Time)相关,呈现一定的周期性[4,5].TCP 的周期性如图 1 所示.

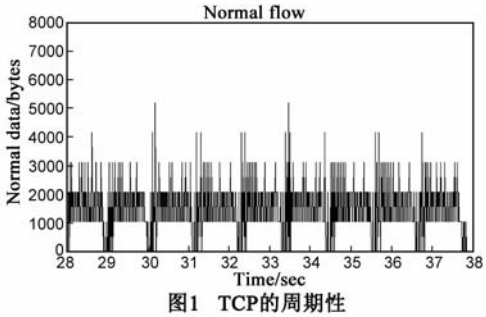

图1　TCP的周期性

本文针对 FTP(File Transfer Protocol)的应用,得到正常 TCP 流量随时间变化的统计结果如图 2 所示.

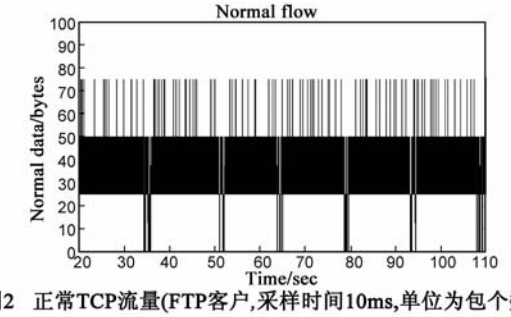

图2　正常TCP流量(FTP客户,采样时间10ms,单位为包个数)

2.2　LDoS 攻击流量时域分析

LDoS 攻击流量周期 T 为被攻击者的 RTO + 2 ~ 3RTT[5].选取 2 ~ 3 个 RTT 的原因是为了使 TCP 的 RTT 估算器恢复工作.其缺点是允许一部分 TCP 正常传送.攻击脉宽 L 取 1 ~ 2 个 RTT,攻击速率(即强度)R 取值接近瓶颈链路带宽,在中间路由器队列不是很大的情况下,这样选取 L 和 R,可使得攻击效果明显.

由于大部分网络系统的 TCP 的 minRTO 选取为 1s,因此,本文选取 $T > 1000$ms;瓶颈链路带宽选取 1Mb;中间路由器队列大小选取 100 个数据包;L 取值 250ms、R 取值 1Mb.在实验中,选取正常 TCP 流量作为背景流量(噪声);UDP(User Data Protocol)流量作为攻击流量.实验记录其中一次攻击中的攻击流量(UDP)和合法用户流量(TCP)随时间变化的统计图分别如图 3 和图 4 所示.

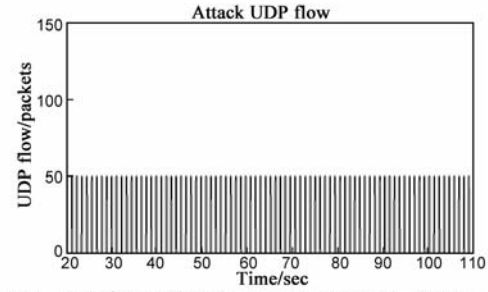

图3　攻击中UDP流量(R=1Mb,L=250ms,T=1100ms,采样时间10ms,单位为包个数)

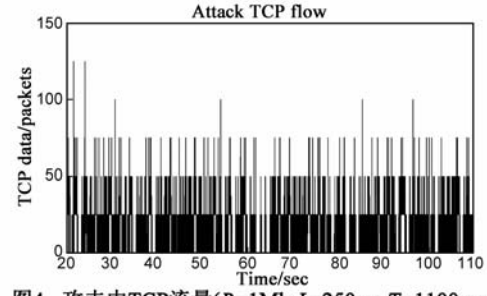

图4　攻击中TCP流量(R=1Mb,L=250ms,T=1100ms,采样时间10ms,单位为包个数)

正常流量与攻击流量的混合流量随时间变化的统计如图 5 所示.

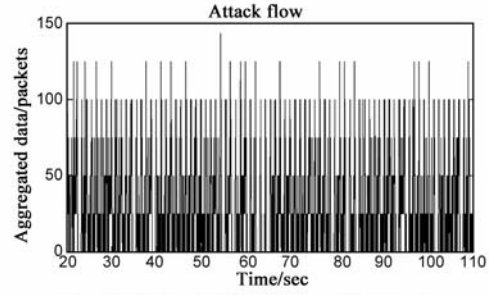

图5　混合流量(采样时间10ms,单位Byte)

比较图 4 和图 5 可以看出,它们之间的差异并不明显,攻击流量完全埋没在正常流量中.统计表明:每个攻击流量只占混合流量的 18.85%.

由上述分析可以将 LDoS 攻击定义为小信号,又由于 LDoS 具有一定的周期性,故称其为周期小信号.攻击方只需发送周期性的小信号便能达到攻击的目的.因此,从图 5 所示的混合流量中检测 LDoS 攻击的问题就变成了从背景噪声(正常 TCP 流量)中检测出小信号(LDoS 攻击)的问题[6,7].

3 漏值多点数字平均检测 LDoS 攻击

LDoS 攻击属于未知周期(从检测者角度来说)的周期小信号;背景噪声为正常流量(正常流量也属于周期信号,但其周期与攻击信号的周期不同),且远强于攻击信号.因此,本文检测 LDoS 攻击的方法需要解决的核心问题有 2 个:(1)从强背景流量中检测未知周期的 LDoS 攻击(小信号);(2)确定已检测到的 LDoS 攻击的周期.

3.1 检测未知周期的 LDoS 攻击

检测 LDoS 攻击周期的前提是必须首先检测出 LDoS 攻击的存在.在图 5 所示的混合流量中,假设 LDoS 攻击信号为 $Atk(t)$,其攻击周期是一个未知量 T;对其攻击包统计后得到其包个数的最大值和最小值的差为峰谷差值 P,即无论是单条或多条 TCP 流均会出现较大的峰谷差值(实际上,当没有 LDoS 攻击时,这种峰谷差值也存在,但其数值远小于存在 LDoS 攻击时的情况),即统计后的包个数相差较大.因此,通过流量分析得到的峰谷差值可以作为判决是否存在 LDoS 攻击的依据[7].

在 LDoS 攻击的检测中,攻击周期 T 的确定是通过多次的比较实验得到的.将每次统计的结果存入 $m \times n$ 维的包个数统计矩阵 $\boldsymbol{M}$.其中,行数 m 为实验的组数;n 为每组实验的次数(实验次数间隔与 T 有关).以 T 为迭加间隔进行漏值多点数字平均,即对 $\boldsymbol{M}$ 矩阵按列平均后分别得到向量的最大值和最小值,其差值即为流量包个数平均峰谷差值 $\bar{P}$.由于是同步迭加平均,所以 $\bar{P} = P$.

如果周期信号 $Atk(t)$不存在,或者周期不为 T,则 $\bar{P} \ll P$.利用这一特性可以判断是否检测到周期为 T 的信号.在检测中,设定一个门限 P_{Thr},如果 $\bar{P} \geqslant P_{Thr}$,则将该值记录在检测数组 P 中.信号周期搜索过程结束后取 P 中各元素的均值作为周期预测值;如果数组 P 不存在,则说明被检测信号为周期信号.门限 P_{Thr}的设置是根据 LDoS 攻击流量的最大和最小包个数,以及 TCP 背景流量的包个数统计决定.$\bar{P}$ 可称为 LDoS 攻击判决的特征值[7].

以一段时长为搜索间隔(后面将会从实验结果中看到:搜索间隔越小检测效果越佳),来不断地试探攻击周期.选取采样时间间隔为 10ms,采样点数为 3000 个,即每计算一次须 30 秒(经多次仿真知道,保证检测效果的最短时长为 30 秒).而攻击到达时未必在算法的时间边缘,所以完成一次检测需 30 秒(最佳状况,攻击到达时正好检测开始)至 60 秒(最坏状况,攻击到达时上次检测一次检测刚刚结束),即检测时长区间为 $[30,60)$.将这 3000 个采样数据点排列为 $m \times n$ 的矩阵 $\boldsymbol{M}$,再构造出判决特征值 $\bar{P}$.反复实验,得到可靠的判决门限 P_{Thr},即可有效地检测 LDoS 攻击.

3.2 确定 LDoS 攻击的周期

如果以搜索周期为间隔将时间轴分成若干段,则每段相同序号的采样值经过平均后,得到的数值仍然具备峰谷差值特性.因此,可以用采样值平均来确定 LDoS 攻击的周期.假定,LDoS 攻击的周期为 T,抽样间隔为 T_s,则有:$T = nT_s + \Delta T_s (0 \leqslant \Delta < 1)$.其中,$\Delta$ 表示时间偏差系数.对于 Δ 的取值有两种情况[7]:

(1)如果 $\Delta = 0$,则采样过程在时间上无偏差.LDoS 攻击和 TCP 背景流量各累加 m 次.包个数统计最大值远大于最小值,会产生较大的峰谷差值,表明:存在 LDoS 攻击,并且 LDoS 攻击的周期是采样间隔的整数倍关系.从而由采样间隔 T_s 周期就可以确定 LDoS 攻击的周期 T[7].

(2)如果 $\Delta \neq 0$,对于周期确定的 LDoS 攻击信号,由于其周期不是抽样间隔的整数倍,在时间上将产生误差积累,从而造成各周期抽样点数并不完全相同.为了确定 LDoS 攻击的周期,要求以各个周期具有相同抽样个数实现迭加.

在第 k 次抽样后(对第 k 个周期的抽样),重复采样和处理过程,即使每个周期都具有 n 个抽样点.在抽样过程中,为了保证每个周期内具有相同抽样点数,对抽样点数进行必要的重新整理,即舍去一些抽样点数据,此过程称之为漏值取样[7].

构造一个 $m \times n$ 的矩阵 N,每 n 个采样占据该矩阵一行,若采样点为 Sum 个,则 $m = \lceil Sum/n \rceil$.每个周期的抽样数据存放在 N 矩阵的一行.把各行中列号相同的样值进行迭加平均,即基于漏值取样的多点数字平均的方法—漏值多点数字平均[7].虽然相互迭加的样值并不一定完全是同相的,但是相差一旦超过 $\frac{T_s}{T}2\pi$,漏值取样将丢掉一个样值,使误差小于 $\frac{T_s}{T}2\pi$.而且,最大相差不随迭加次数增加而增加,即不存在误差积累.因此,相差均匀分布在 $(-\frac{2\pi}{n}, \frac{2\pi}{n})$之间,当迭加次数足够大时,其平均值趋近于 0,即迭加误差很大程度上相互抵消.从而到达确定 LDoS 攻击周期的目的[7].

4 实验和结果分析

本文检测方法利用网络仿真软件 NS-2 在搭建的网络环境中进行了测试.搭建的仿真网络拓扑结构如图 6 所示.

在图 6 中,客户、攻击者与检测路由器之间的链路带宽均为 10Mb/s,单向延时为 2ms;各路由器之间、路由

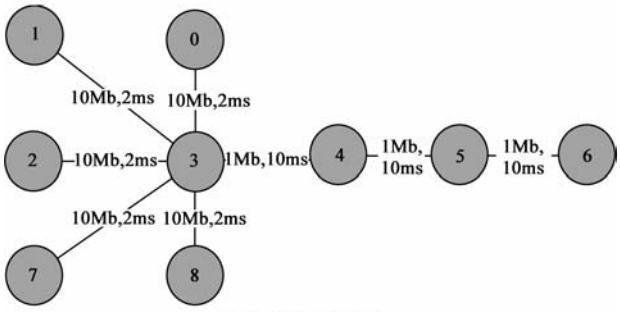

图6　仿真拓扑图

器 2 与服务器之间链路带宽均为 1Mb/s,单向延时为 10ms.且路由器的发送队列大小为 100 个数据包.LDoS 攻击的 3 个参数: L = 250ms、R = 1Mb、T = 1100ms 和 1075ms.

实验开始于 0s,结束于 110s.3 个正常流量(TCP)在 15s 后的某个随机时间开始生成;攻击流量(UDP)在 20s 开始生成;采样时间取 10ms;周期搜索范围从 1s 到 1.2s,搜索间隔分别为 10ms、20ms 和 50ms.选取 20s 到 50s 期间的流量为实验数据进行统计分析.

4.1　正常流量

为了模拟 Internet 流量,使攻击流量为正常流量的 10%—20%,仿真时将正常流量扩大 25 倍,这样攻击流量占正常流量的 18.846%.没有 LDoS 攻击(采样间隔 10ms)时的特征值分布如图 7 所示.

从图 7 中可以看到在各个周期预测点特征值 $\bar{D}$ 均处于较低水平(多次实验得到的分布图结果相同).

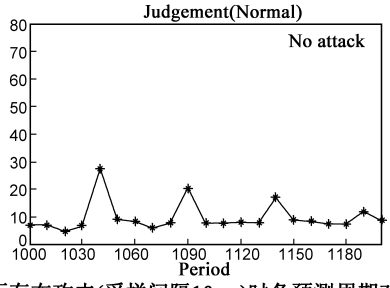

图7　不存在攻击(采样间隔10ms)时各预测周期对应$\bar{D}$值

4.2　异常流量

针对 LDoS 攻击时出现的异常流量,分别针对攻击周期、搜索间隔和采样间隔变化的情况进行了实验.

4.2.1　攻击周期不同

在采样间隔和搜索间隔均为 10ms,攻击周期分别为 T = 1100ms 和 1175ms 的两次实验中特征值 $\bar{D}$ 的分布如图 8 和图 9 所示.

从图 8 和图 9 中可以看到,对于 T = 1100ms 的攻击,最大 $\bar{D}$ 值准确出现在预测周期为 1100ms 处;对于 T = 1175ms 的攻击,最大 $\bar{D}$ 值出现在预测周期为 1170ms 和 1180ms 处.多次实验的结果均证明了上述结论.为了与实际情况相符,根据检测原理,选取均值 1175ms 作为预测攻击周期.

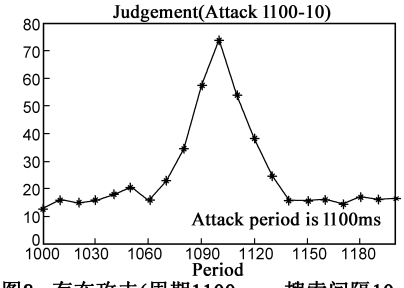

图8　存在攻击(周期1100ms、搜索间隔10ms、采样间隔10ms)时$\bar{D}$值分布图

4.2.2　搜索间隔不同

图 10 表示采样间隔 10ms、搜索间隔 ΔT = 20ms、攻击周期为 1100ms 的实验中特征值 $\bar{D}$ 的分布图.

此时(预测周期 1100ms 为搜索间隔 20ms 的整数倍),检测效果与 10ms 搜索间隔时差异不大.而当预测周期不为搜索间隔的整数倍时,效果较差,出现检测误差,甚至将无法实施检测.

攻击周期为 1175ms 和搜索间隔为 20ms 时的 $\bar{D}$ 值分布见图 11.从图 11 中可看到,出现相对误差(1180-1175)/1175 = 0.426%.

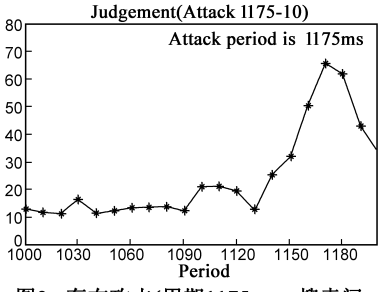

图9　存在攻击(周期1175ms、搜索间隔10ms、采样间隔10ms)时$\bar{D}$值分布图

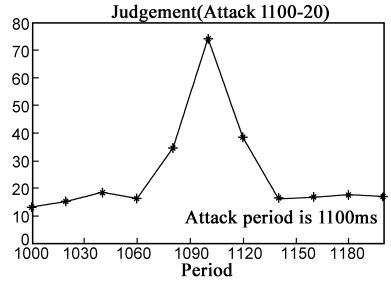

图10　存在攻击(周期1100ms、搜索间隔20ms、采样间隔10ms)时$\bar{D}$值分布图

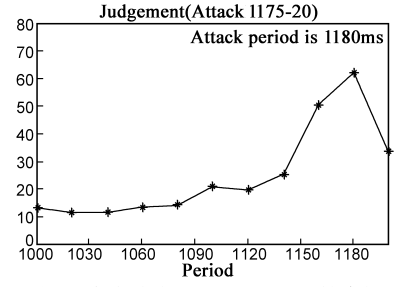

图11　存在攻击(周期1175ms、搜索间隔20ms、采样间隔10ms)时$\bar{D}$值分布图

攻击周期为 1175 和搜索间隔为 50ms 时的 $\bar{D}$ 值分布如图 12 所示.这时已无法检测.

4.2.3　采样间隔不同

采样间隔 7ms、搜索间隔 ΔT = 20ms 和攻击周期为

1175ms 的实验中特征值 $\bar{D}$ 的分布如图 13 所示.从图 13 中可看到,采样间隔的改变没有对检测结果产生影响.

在上述实验条件下,当攻击周期为 1100ms、搜索间隔为 10ms 时,按上述方法进行 100 次独立重复实验.100 次实验的最大判决特征值 $\bar{D}$ 统计图如图 14 所示.

在图 14 中,"*"状点表示存在攻击的最大 $\bar{D}$ 值;"□"状点表示不存在攻击的最大 $\bar{D}$ 值.

选取攻击判断门限值为 60,统计分析 100 次实验数据,其检测性能稳定:正确检测概率(P_D)为 100%;虚警概率(P_{FN})为 0;漏警概率(P_{FP})为 0.

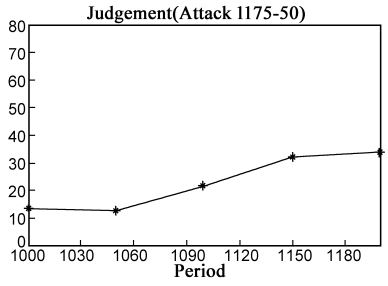

图12 存在攻击(周期为1175ms、搜索间隔为50ms)$\bar{D}$分布图

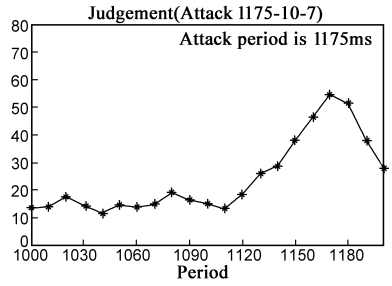

图13 存在攻击(周期为1175ms、搜索间隔为10ms、采样间隔为7ms) 时$\bar{D}$值分布图

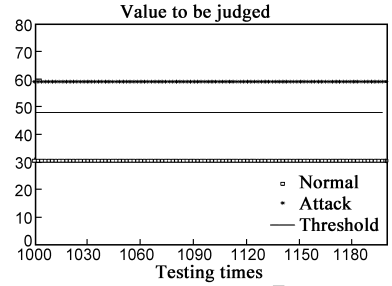

图14 100次实验的最大$\bar{D}$值统计

5 结论

基于小信号模型的 LDoS 检测方法主要把网络流量当作信号来处理,不涉及频域的变换,无须设计滤波器,每计算一次须 3000 个采样点,从而简化了检测算法复杂度,降低了系统消耗,而且具有良好的实时性与稳定性.

实验结果表明基于小信号模型的 LDoS 检测方法可以准确、高效地判断是否存在攻击,以及能够精确估计攻击周期.这为今后在攻击源端实现对 LDoS 攻击流的有效过滤的研究打下了基础.

参考文献

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

[2] 孙长华,刘斌.分布式拒绝服务攻击研究新进展综述[J].电子学报,2009,37(7):1562 – 1563.
Sun Changhua, Liu Bin. Survey on new solutions against distributed denial of service attack[J]. Acta Electronica Sinica, 2009,37(7):1562 – 1563.(in Chinese)

[3] 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):1590 – 1594.
Wu Zhijun, Yue Meng. Detection of LDDoS attack based on kalman filtering[J]. Acta Electronica Sinica , 2008, 36(8): 1590 – 1594.(in Chinese)

[4] Yu Chen, Kai Hwang, Yu-Kwong Kwok. Collaborative defense against periodic shrew DDoS attacks in frequency domain[A]. ACM Transactions on Information and System Security (TISSEC)[C]. Los Angeles, California, USA: ACM, 2005. 2 – 27.

[5] Allman M, Paxson V. On estimating end-to-end network path properties[J]. Computer Communication Review, 1999, 29(4): 263 – 274.

[6] 叶卫东,李行善.包络均值滤波算法实时检测微弱信号[J].北京航空航天大学学报,2010,36(8):909 – 912.
Ye Weidong, Li Xingshan. Real-time weak signal detection with envelope mean filter algorithm[J]. Journal of Beijing University of Aeronautic and Astronautics, 2010, 36(8): 909 – 912.(in Chinese)

[7] 张国杰.周期微弱信号的检测与跟踪[J].数据采集与处理,1991,6(1):16 – 22.
Zhang Guojie. Detection and tracking weak periodic signal[J]. Journal of Data Acquisition & Processing, 1991, 6(1): 16 – 22.(in Chinese)

作者简介

吴志军 男,1965 年生于新疆库尔勒,中国民航大学教授、博士生导师.主要研究方向为网络与信息安全.
E-mail: zjwu@cauc.edu.cn

裴宝崧 男,1984 生于辽宁辽阳,中国民航大学通信与信息系统专业研究生.主要研究方向为网络与信息安全.