

基于时频分析的分布式拒绝服务攻击的自动检测

孙钦东, 张德运, 郑卫斌, 胡国栋

(西安交通大学电子与信息工程学院网络研究所, 710049, 西安)

摘要: 研究了分布式拒绝服务(DDoS)攻击的特点,定义了流连接密度(FCD)的概念,并证明了 FCD 时间序列的非平稳特性. 据此,提出了一种新的基于时频分析的自动检测 DDoS 攻击的方法,该方法采用平滑魏格纳2维利分布对 FCD 时间序列进行时频变换,将 FCD 时间序列转换为二维空间内的波动能量分布,并有效抑制了二次交叉项的影响,然后使用经过样本训练的 K 最近邻分类器进行攻击识别. 实验结果表明,该检测方法能够比较准确地识别 DDoS 攻击,识别误差主要出现在网络状态切换阶段,这对攻击识别的影响很小,识别误差率仅为 4126 %.

关键词: 分布式拒绝服务;时频分析;魏格纳2维利分布; K 最近邻

中图分类号: TP393 **文献标识码:** A **文章编号:** 0253 - 987X(2004)12 - 1247 - 04

Automatic Detection of Distributed Denial of Service Attacks Based on Time2Frequency Analysis

Sun Qindong, Zhang Deyun, Zheng Weibin, Hu Guodong

(Institute of Network, School of Electronics and Information Engineering, Xi an Jiaotong University, Xi an 710049, China)

Abstract: Based on the analysis of distributed denial of service (DDoS) attacks, the flow connection density (FCD) is defined and the characteristic of non2stationary of FCD time series is proved. A new method to detect DDoS attacks is proposed based on the time2frequency analysis of FCD. The proposed method detects DDoS at2tacks by transforming the time series of FCD with smooth Wigner2Ville distribution, to obtain the energy distri2bution of the time series in two2dimensional space and suppress the effect of the quadratic cross term, and then i2dentifying DDoS by using the K 2nearest neighbor classifier trained by samples. The experimental results show that the developed approach can detect DDoS attacks correctly, and identification errors mainly present to the switching stage of the network with little influence on the identification of DDoS attacks. Compared with the theoretic value, the identification error ratio is only 4126 %.

Key words: distributed denial of service; time2frequency analysis; Wigner2Ville distribution; K 2nearest neighbor

分布式拒绝服务(DDoS)攻击采用的是分布、协作的大规模攻击模式,这种攻击将导致目标主机网络和系统资源耗尽,无法为用户提供服务,甚至导致系统崩溃.随着 DDoS 攻击软件的出现^[1],发起 DDoS 攻击更为容易,对网络安全的威胁也就越大^[2].如何准确、及时地检测 DDoS 攻击,是有效防御攻击的基础.文献[3 - 5]分别使用管理信息库

(MIB)、卡尔莫哥洛夫复杂度及源地址过滤等方法来检测 DDoS 攻击,而这些检测方法有一些缺陷(要受到一定限制),如要求对 DDoS 攻击的协议类型有一定的先验知识^[3],难以区分突发正常流量与 DDoS 攻击^[4],以及要记录大量的历史记录^[5]等.针对上述问题,本文提出了一种基于时频分析的 DDoS 攻击检测新方法.

收稿日期: 2004 - 01 - 07. 作者简介: 孙钦东(1975 ~),男,博士生;张德运(联系人),男,教授,博士生导师. 基金项目: 国家信息化计算机网络与信息安全基金资助项目(2001 - 研 1 - 010).

1 DDoS 攻击分析与流连接密度定义

典型的 DDoS 攻击如图 1 所示,攻击主机经长时间的准备,先入侵大量的攻击从机,并在从机上安装 DDoS 攻击守护进程.当攻击从机接收到攻击命令后,会向目标主机发出大量的服务请求数据包,使目标主机网络和系统资源耗尽.

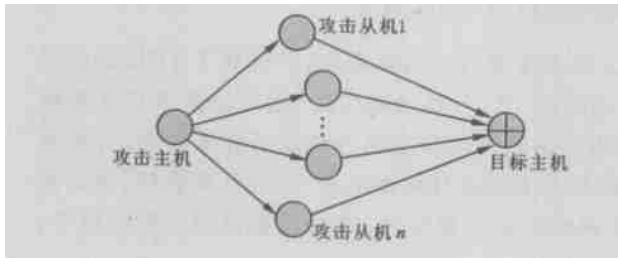


图 1 典型的 DDoS 攻击

DDoS 攻击通常采用对目标主机的某个端口请求大量的服务或对目标主机的多个端口请求服务,以消耗目标主机的资源.为了隐藏攻击者的真实位置,DDoS 攻击在实施过程中会随机伪造攻击数据包的源 IP 地址,或者使用大量的反射服务器,这会引发网络流量的某些特性发生改变.研究这些特性的变化,可以有效地检测 DDoS 攻击.

定义 1 $R = \{ p_1, \dots, p_i, \dots, p_j \}$ 为 IP 数据包集合,数据包元素为四元组形式,即 $p_i = (s_i, d_i, sp_i, dp_i)$,其中 s_i, d_i, sp_i 和 dp_i 分别表示数据包 i 的源 IP 地址、目的 IP 地址、源端口号及目的端口号.若 $p_1, \dots, p_i, \dots, p_j$ 的源、目的 IP 地址及目的端口号均相同,则称其为一组相关数据包,称集合 R 为相关数据包集合.相关数据包集合内的元素个数至少为 1.

定义 2 假设单位时间网络流量内的数据包集合为 $P = \{ p_1, p_2, \dots, p_M \}$,其内的相关数据包集合为 $\{ R_1, R_2, \dots, R_N \}$,则定义此网络流的流连接密度(FCD)为相关数据包集合的数量.

结合上述分析及定义 2 可以看出,DDoS 攻击会引起网络流的 FCD 异常增加.当然,合法的访问用户的增加也会使 FCD 增大,但合法用户在一定的时间段内的请求服务方式是单一的,或者请求服务的数量是有限的,而且其 IP 地址不会发生变化.因此,正常访问流量增加引起 FCD 上升的模式与发生攻击导致 FCD 变化的模式有明显区别,那么研究 FCD 随时间的变化规律,也就是对 FCD 时间序列的特性进行研究,这有助于检测到 DDoS 攻击.

2 FCD 时间序列的特性分析

对网络流 F 进行时间间隔为 t 的采样,并计

算每次采样的 FCD,得到 FCD 时间序列 $Z(N, t) = \{ a_i, i = 1, 2, \dots, N \}$, N 为序列长度.时间序列 Z 的 k 阶自相关系数为

$$\rho_k = \frac{\sum_{i=1}^{N-k} (a_i - \bar{a})(a_{i+k} - \bar{a})}{\sum_{i=1}^{N-k} (a_i - \bar{a})^2} \tag{1}$$

式中 \bar{a} 是时间序列 Z 的数学期望.

根据时间序列分析理论可知,随着 k 的增加,其对应的相关系数 ρ_k 始终不为 0,则称 Z 为非平稳时间序列.任取 FCD 时间序列,计算 ρ_k ,结果如图 2 所示.从图中可以看出,自相关阶数 k 从 1 增加到 50, ρ_k 仅从 0.1793 下降到 0.1641,因此 FCD 时间序列 Z 是非平稳时间序列.

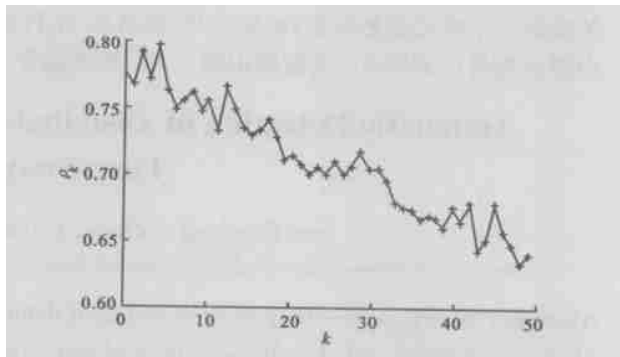


图 2 FCD 时间序列的自相关系数变化

时频分析法是一种有效的非平稳信号处理方法,它通过对时间、频率的联合分析形成一个二维域 (t, ω) ,并在时间频率平面内以强度的方式直观地反映信号的频率时变特性.对非平稳时间序列进行时频分析主要采用短时傅里叶变换(STFT)及魏格纳 2 维利分布(WVD)等方法.用 STFT 研究非稳时间序列,是假定序列在短时间内是平稳的,但为了提高分辨率又必须选取较长的观测时间,这样会破坏短时平稳的假设,使信号在时间和频率上模糊不清.WVD 是一种二次型的变换,能够克服 STFT 的缺陷,适合于分析 FCD 时间序列的特性.

3 FCD 时间序列的 WVD

FCD 时间序列 Z 是一个实数序列,频谱满足 $S(-\omega) = S^*(\omega)$,能量密度频谱总是相对于原点对称的,仅有一半频谱包含有用信息^[6],使用解析信号可以去掉此冗余.在计算 WVD 之前,要先把 Z 变换为解析序列,若 Z 被视为实信号 $R(t)$,那么它对应的解析信号为

$$R(t) = R(t) + j \hat{R}(t) \tag{2}$$

式中: $\hat{R}(t)$ 为 $R(t)$ 信号的离散希尔伯特变换,即

$$\hat{R}(t) = H[R(t)] = \frac{1}{j} \int_{-\infty}^{\infty} \frac{R(\tau)}{t - \tau} d\tau \tag{3}$$

Z 经过变换后的解析信号 $Z(t)$ 对应的 WVD 分布为

$$D(t, \omega) = \frac{1}{2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \left(t + \frac{\tau}{2} \right) \left(t - \frac{\tau}{2} \right) e^{-j\omega\tau} d\tau \tag{4}$$

根据式(4),输入一维信号 $Z(t)$,将在时频平面内得到一个二维分布图,该分布即为 FCD 波动能量的时频分布.由于变换属于二次型,所以 WVD 分布不是线性的,即两个信号之和的 WVD 不等于每个信号的 WVD 之和,它们之间存在一个交叉项.若 FCD 时间序列由 N 种信号叠加而成,那么交叉项的个数为 C_N^2 .交叉项是振荡的,幅度是自项的 2 倍,要利用 WVD 识别 DDoS 攻击,该交叉项的存在是一种干扰.基于上述原因,用 WVD 分析网络流量数据必须尽量减少交叉项的干扰.用核函数法^[6]对 WVD 进行时频平滑,即

$$D^p(t, \omega) = \frac{1}{2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h(\tau) g(s - \tau) \left(t + \frac{\tau}{2} \right) \left(t - \frac{\tau}{2} \right) e^{-j\omega\tau} ds d\tau \tag{5}$$

式中: $g(t)$ 和 $h(\omega)$ 分别为时间和频率平滑窗口.平滑可以降低交叉项的干扰,但会影响时频分辨率,所以在实际计算当中可根据需要选择合适的平滑窗口.设频率分辨率为 $\Delta\omega$,本文取时间平滑窗口为 $\Delta t / 10$ 的哈明(Hamming)窗口,频率平滑窗口为 $\Delta\omega / 4$ 的哈明窗口.提取不同网络状态下的网络 FCD 变化图,给定频率分辨率并对式(5)进行离散,可以得到不同状态下的时频特性图.

4 DDoS 攻击检测

时频特性图把 FCD 时间序列变换为二维空间向量,这样的识别流量状态可归结为基于向量空间模型的分类问题.本文采用 K 最近邻(KNN)分类算法构造分类器,其基本思想是:在训练样本集合中查找与待分类样本距离最近的 K 个样本,根据这 K 个样本所属类别来判定待分类样本的所属类别.该分类算法的理论错误率上限约为简单贝叶斯分类的 2 倍,具有较好的分类效果和明确的物理意义^[7].

分别获取网络在正常和发生 DDoS 攻击时的 FCD 时间序列,利用式(2)~式(5)可以得到二维空

间的训练样本,样本的类别标识为网络流所处状态,即正常或攻击.为每一个类别 j 定义一个类别集合 G_j ,所有属于该类别的训练样本都是集合 G_j 的元素.同样,计算待检测的 FCD 时间序列的 WVD,得到待分类的二维向量 (n) .在上述训练样本中寻找与当前样本距离最近的 K 个样本,而任意 2 个向量之间的距离采用余弦距离,即

$$Dis((i), (j)) = \frac{\langle_{m=1}^m(i) \mid \langle_{m=1}^m(j) \rangle}{\left[\sum_{m=1}^m \langle_{m=1}^m(i) \mid \langle_{m=1}^m(j) \rangle \right]^{1/2}} \tag{6}$$

所获得的最近邻集合用 K 表示. (n) 分别对所有的类别计算分类权重

$$W((n), G_j) = \sum_{(i) \in K} Dis((n), (i)) f((i), G_j) \tag{7}$$

式中: $f((i), G_j)$ 为类别判定函数.如果 $(i) \in G_j$,函数值为 1,否则为 0.计算所有类别的分类权重,待分类样本属于分类权重最大的类别,相应的状态也就是时间序列上的点的状态.

5 实验

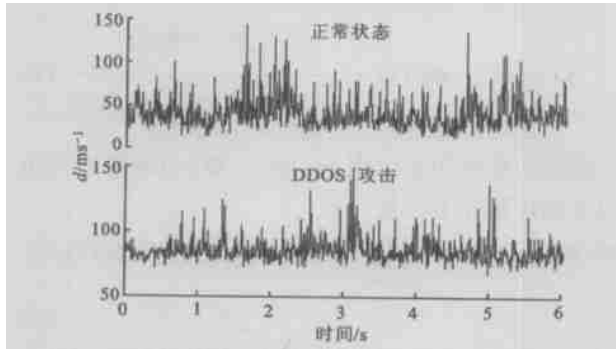
本文实验数据使用了 MIT 林肯实验室的 2000 年分布式拒绝服务攻击数据集 LLDOS21012^[8].为了使实验数据更具一般性,在攻击数据集的基础上增加了背景流量,背景流量取自 MIT 1999 年的数据集.

取正常状态及发生攻击时的流量作为训练样本,取样时间间隔为 0.101 s,取样次数为 600.分别计算 FCD,得到 FCD 时间序列样本如图 3 所示.根据式(5)计算时间序列的平滑 WVD 分布,频率分辨率取 256,即在频率轴有 256 个数据点,计算结果如图 4 所示.最后,使用获得的正常状态及攻击时的时频特性分布来训练 KNN 分类器,即根据式(6)、式(7)分别计算分类权重,确定相应所属类别.

待检测的时间序列样本如图 5 所示,取样时间间隔为 0.101 s,样本数为 1 200.根据式(5)计算待检测样本的平滑 WVD 分布,结果如图 6 所示,其中频率分辨率取 256.用训练过的 KNN 分类器对待检测时间序列的时频分布图进行分类.

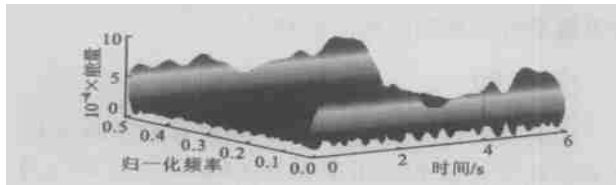
实验结果与理论值的对比如图 7 所示.实验结果显示,基于 FCD 时间序列的时频分析检测方法能够比较准确地识别 DDoS 攻击.与理论值相比,实验

误差率仅为 4126 %。在网络状态发生变化时,即攻击出现或结束时,分类的误差率比较高,同时检测过程中还伴有不规律的分类错误。经过分析发现,分类错误的来源主要有以下 2 个方面: 由随机噪声引起的系统状态偏移,使识别结果中出现少量的无规律的识别错误; 时频平滑引起分辨率下降,使在消除交叉项干扰的同时降低了分辨能力,由此造成在状态切换处出现连续的识别错误。

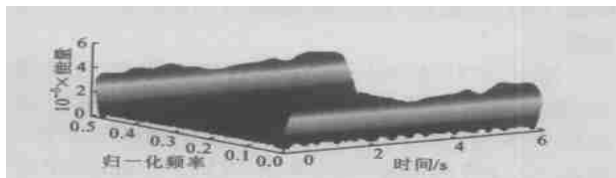


d 表示 FCD

图 3 FCD 时间序列训练样本

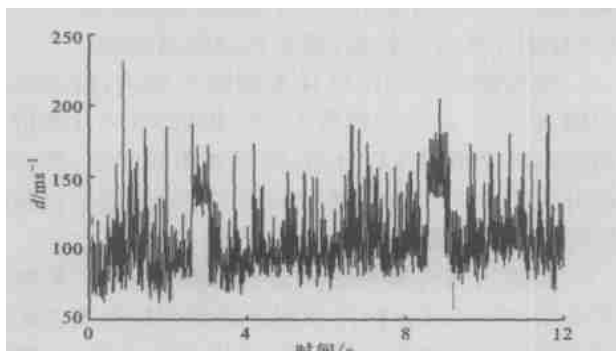


(a) 正常状态



(b) DDoS 攻击

图 4 训练样本平滑 WVD 分布



d 表示 FCD

图 5 待检测时间序列样本

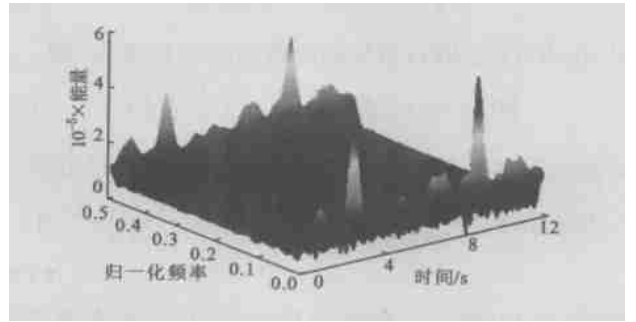


图 6 待检测时间序列平滑 WVD 分布

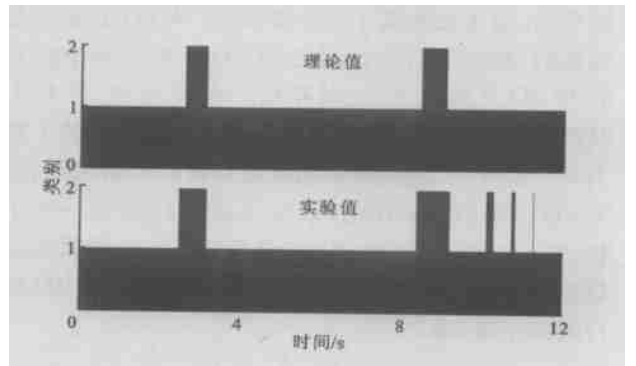


图 7 实验结果与理论结果对比

6 结论

本文分析了 DDoS 攻击的特点,定义了 FCD 的概念,并提出了基于 FCD 时间序列时频分析的 DDoS 攻击检测新方法。该方法用 WVD 对 FCD 时间序列进行变换,获得 FCD 时间序列在二维平面内的波动能量分布,并使用 KNN 算法将该波动能量与训练样本进行比较分类,实现了 DDoS 攻击自动检测。实验结果证明了该检测方法的有效性及其准确性。后续的研究将包括:使用其他的在线或离线数据集进一步试验;将本检测方法扩展到其他类型的异常检测中。

参考文献:

[1] Criscuolo P J. Distributed denial of service2trin00, tribe flood network [R]. Technical Report CIAC2319. Washington DC: Department of Energy, 2000.

[2] Lau F, Rubin S H, Smith M H, et al. Distributed denial of service attacks [A]. Proceedings of IEEE International Conference on Systems, Man, and Cybernetics [C]. Piscataway, USA: IEEE Press, 2000. 2 27522 280.

(下转第 1255 页)

参考文献:

- [1] Cader P D, Mohamed M A, Keller J M. Fusion of hand written word classifiers [J]. Pattern Recognition Letters, 1996, 17(6): 577 - 584.
- [2] Tahani H, Keller J M. Information fusion in computer vision using the fuzzy integral [J]. IEEE Trans on Systems, Man, and Cybernetics, 1990, 20(3): 733 - 741.
- [3] 杨 焯, 裴继红, 杨万海. 基于模糊积分的融合图像评价方法 [J]. 计算机学报, 2000, 24(8): 5 - 8.
- [4] Auephanwiriyaikul S, Keller J M, Cader P D. Generalized Choquet fuzzy integral fusion [J]. Information Fusion, 2002, 3(1): 69 - 85.
- [5] Sugeno M. Fuzzy measures and fuzzy integrals: a survey [A]. Fuzzy Automata and Decision Process [C]. New York: North-Holland, 1977. 89 - 102
- [6] Murofushi T, Sugeno M. A theory of fuzzy measures: representations, the Choquet integral, and null sets [J]. J Math Anal Appl, 1991, 159(2): 532 - 549.
- [7] Pawlak Z, Peters J F, Skowron A, et al. Rough measures: theory and applications [J]. Bulletin of International Rough Set Society, 5(1 - 2): 177 - 183.
- [8] Chiang J H. Aggregating membership values by a Choquet fuzzy integral based operator [J]. Fuzzy Sets and Systems, 2000, 114(3): 367 - 375.
- [9] Grabisch M, Sugeno M. Multiattribute classification using fuzzy integral [A]. The First IEEE Conference on Fuzzy Systems, San Diego, USA, 1992.
- [10] Keller J M, Osborn J. Training the fuzzy integral [J]. International Journal of Approximate Reasoning, 1996, 15(1): 1 - 24.
- [11] Borkowski M, Peters J F. Approximating sensor signals: a rough set approach [A]. Canadian Conference on Electrical and Computer Engineering, Winnipeg, Canada, 2002.
- [12] Grabisch M, Dispot E. A comparison of some methods of fuzzy classification on real data [A]. Second International Conference on Fuzzy Logic and Neural Networks, Lizaoka, Japan, 1992.
- [13] Moore R E. Interval analysis [M]. New York: Prentice Hall, 1966.
- [14] Lin T Y, Liu Q. First order rough logic: approximate reasoning via rough sets [J]. Fundam Inform, 1996, 27(2 - 3): 137 - 153. (编辑 苗 凌)

(上接第 1231 页)**参考文献:**

- [1] Ammann P, Wijesekera D, Kaushik S. Scalable, graph based network vulnerability analysis [A]. 9th ACM Conference on Computer and Communications Security, Washington DC, 2002.
- [2] Deraison R. Nessus [EB/OL]. <http://www.nessus.org>, 2003 - 02 - 15.
- [3] Stardust. 计算机网络系统安全漏洞分类研究 [EB/OL]. <http://www.xfocus.net/articles/200103/126.html>, 2003 - 03 - 03/2003 - 11 - 13.
- [4] Bishop M, Bailey D. A critical analysis of vulnerability taxonomies [R]. Technical Report 96 - 11. Davis, USA: Department of Computer Science, University of California, 1996.
- [5] Pawlak Z. Rough sets [J]. International Journal of Computer and Information Science, 1982 (11): 341 - 356.
- [6] Mell P. ICAT metabase: your CVE vulnerability search engine [EB/OL]. <http://icat.nist.gov/icat.cfm>, 2003 - 08 - 16. (编辑 苗 凌)

(上接第 1250 页)

- [3] Cabrera J B D, Lewis L, Qin Xinzhou, et al. Proactive detection of distributed denial of service attacks using MIB traffic variables: a feasibility study [A]. Proceedings of 2001 International Symposium on Integrated Network Management [C]. Piscataway, USA: IEEE Press, 2001. 6092622.
- [4] Kulkarni A B, Bush S F, Evans S C. Detecting distributed denial of service attacks using Kolmogorov complexity metrics [R]. Technical Report 1CRD176. New York: Research and Development Center, General Electric Company, 2001.
- [5] Tao Peng, Leckie C, Ramamohanarao K. Protection from distributed denial of service attacks using history based IP filtering [A]. IEEE International Conference on Communications, Anchorage, USA, 2003.
- [6] Cohen L. Time-frequency analysis [M]. Englewood Cliffs, USA: Prentice Hall, 1995.
- [7] Duda R O, Hart P E, Stork D G. Pattern classification [M]. 2nd ed. New York: Wiley, 2001.
- [8] MIT Lincoln Laboratory. 2000 DARPA intrusion detection scenario specific data sets [EB/OL]. <http://www.ll.mit.edu/IST/>, 2003 - 10 - 21. (编辑 苗 凌)