文章编号:2095－0411(2015)02-0059-05

基于时间序列分析的 DNS 服务器的 DDoS 攻击检测*

倪彤光, 顾晓清,王洪元
(常州大学 信息科学与工程学院,江苏 常州 213164)

摘要:分析了针对 DNS 服务器 DDoS 攻击的特征,提出了一种基于攻击流特征(A_{FC})时间序列的 DDoS 攻击检测方法。通过自适应自回归模型的参数拟合,将 A_{FC} 时间序列变换为多维空间内的自适应自回归 AAR 模型参数向量序列,然后使用支持向量机进行分类。实验结果表明,该方法能有效检测针对 DNS 服务器的 DDoS 攻击。

关键词:DNS 服务器;分布式拒绝服务攻击;时间序列;自适应自回归;支持向量机
中图分类号: TP 393.08 **文献标识码**:A **doi**:10.3969/j.issn.2095－0411.2015.02.013

Detection of DDoS Attack Towards DNS Server Based on Time Series Analysis

NI Tong-guang, GU Xiao-qing, WANG Hong-yuan
(School of Information Science and Engineering, Changzhou University, Changzhou 213164, China)

Abstract: Through the analysis of distributed denial of service (DDoS) attack towards the DNS server, a novel method to detect DDoS attack is proposed based on the A_{FC} time series, which is defined by attack flow characteristics. By approximating the adaptive autoregressive model, the A_{FC} time series are transformed into a multidimensional vector series. Furthermore, a support vector machine classifier is applied to identity the attacks. The experiment results show that this method can detect DDoS attacks effectively.

Key words: DNS server; distributed denial of service (DDoS); time series; adaptive autoregressive; support vector machine

DNS(domain name system,域名系统)服务器是 Internet 上最为关键的基础设施之一,其主要作用是提供主机名称和 IP 地址之间的转换,从而保障其他网络应用的顺利执行[1-3]。由于 DNS 协议设计之初存在着缺陷以及 DNS 服务器自身存在查询能力有限的缺点,在针对 DNS 服务器的各种攻击方法中,分布式拒绝攻击(DDoS)是攻击者最常用的手法,其影响力最大,攻击效果最明显[4]。如 2009 年 5 月发生的暴风影音事件,由于服务于暴风影音软件的域名服务器 DNS pod 遭到黑客的 DDoS 攻击而无法提供正常域名请求,导致了中国南方六省电信用户的大规模断网,预计经济损失超过 1.6 亿元人民币[5]。

防御针对 DNS 服务器的 DDoS 攻击的关键是如何快速准确地检测攻击,检测结果直接影响整个攻击防御的性能。目前,国内外学者提出了很多研究方法,Sun[6] 利用攻击流特征信息来识别攻击包,Subbulakshmi[7]、Vijayasarathy[8] 提出了基于机器

* **收稿日期**:2014-09-16。
基金项目:国家自然科学基金项目(61070121)。
作者简介:倪彤光(1978－),男,河北邢台人,博士生,讲师,主要从事机器学习和模式识别研究。

学习的检测技术,但这些方法在实际攻击环境下的准确率存在较大的不确定性。Lakhina[9] 提出了基于流特征分布熵的检测方法,Peng[10] 基于攻击产生大量新的源 IP 地址的现象,提出通过监视源 IP 地址数目的变化来检测攻击,但这些方法对攻击源数目较少而流量足够大的攻击不敏感。

为了克服以上方法的不足,本文提出了针对 DNS 服务器的 DDoS 攻击的攻击流特征(A_{FC})的概念和一种基于 A_{FC} 时间序列的 DDoS 攻击检测方法。它的基本思想是采用 A_{FC} 时间序列来描述 DNS 服务器数据流状态,从 DDoS 攻击会引发 A_{FC} 异常变化这一典型特征入手,利用 AAR 自适应自回归模型计算 A_{FC} 时间序列的多维参数向量,再用经过样本训练的支持向量机进行分类。

1 针对 DNS 的 DDoS 攻击分析

目前,针对 DNS 服务器的 DDoS 攻击可分为 2 类,查询式攻击和反弹式攻击。在查询式攻击中,攻击者通过傀儡机向目标 DNS 服务器发送大量的虚假源 IP 地址的 DNS 请求包,导致其资源耗尽甚至系统崩溃而无法响应正常的请求。当 DNS 服务器遭受查询式攻击时,随机伪造的攻击数据包经过 DNS 服务器解析以后的结果绝大多数都为"解析失败"。而在正常查询情况下,大多数查询域名来自用户在浏览器地址栏的输入或者相应网页上的点击访问产生,其为错误域名的比例很小。

在反弹式攻击中,攻击者通过傀儡机伪造受害 DNS 服务器的地址向网络上大量开放递归 DNS 服务器发送 DNS 查询请求报文。由于开放递归 DNS 服务器不对请求报文进行地址真实性验证,所有的应答报文会在受攻击 DNS 服务器处汇聚,形成 DDoS 攻击流。由于 DNS 协议请求报文和应答报文有成对出现的规律,因此当 DNS 服务器遭受反弹攻击时,应答报文的数目会明显多于请求报文。根据 DNS 协议的特点(RFC2617),DNS 应答报文的大小往往是请求报文的 10 倍乃至几十倍,比较而言,反弹式攻击造成的威胁更大。

2 时间序列分析的 DDoS 检测方法

2.1 A_{FC} 定义

由于 DDoS 攻击流具有突发性、流非对称性和数据包伪造性等本质特点,统计一段时间内 DNS 服务器的网络数据流中接收到的递归应答报文和发送的递归请求报文的比例可以作为服务器是否受到反弹式攻击的检测依据;而统计一段时间内域名解析失败报文和解析成功报文的比例可以作为服务器是否受到查询式攻击的检测依据。

定义 1 对 DNS 服务器数据流采样,设一个采样周期内到达的报文总数为 S,报文中接收到的递归应答报文和发送的递归请求报文的比例(answer/request number in T, A_{RN})为

$$A_{RN}=\sum_{T}\varphi_1/\sum_{T}\varphi_2 \tag{1}$$

其中:φ_1 表示接收到的递归应答报文,φ_2 表示发送的递归请求报文。

定义 2 报文 S 中,DNS 应答报文中域名解析失败的报文和解析成功的报文的比例(false/true number in T, F_{TN})为

$$F_{TN}=\sum_{T}\varphi_3/\sum_{T}\varphi_4 \tag{2}$$

其中:φ_3 表示域名解析失败的报文,φ_4 表示域名解析成功的报文。

定义 3 DNS 服务器数据流的攻击流特征(attack flow characters, A_{FC})为

$$A_{FC}=\theta\times A_{RN}+(1-\theta)\times F_{TN}\quad(0<\theta<1) \tag{3}$$

从上述定义可以看出,查询式攻击和反弹式攻击都会导致 DNS 服务器数据流中的 A_{FC} 异常增加。所以,A_{FC} 可以较好地反映针对 DNS 服务器的 DDoS 攻击流的状态特征,研究 A_{FC} 时间序列的特性能够检测针对 DNS 服务器的 DDoS 攻击。

2.2 A_{FC} 时间序列建模

自适应自回归(AAR)模型[11-12] 是一种时间序列分析模型,它较之传统的时间序列分析模型,具有突出的自适应性,模型的权系数是时间的函数,可以动态跟踪时间序列的变化。

对数据流进行时间间隔为 Δt 的采样,并计算每次采样的 A_{FC},N 次采样后获得 A_{FC} 时间序列样本,为任意 A_{FC} 时间序列定义 p 阶 AAR 模型,给定一个时间序列 $Z(N,\Delta t)=\{a_i,i=1,2,\cdots,N\}$,$a_i$ 为 i 时刻的样本值,N 为序列长度,则 AAR(p)模型的数学表示为

$$\boldsymbol{a}_i=\sum_{j=1}^{p}\varphi_j(i)\boldsymbol{a}_{i-j}+\varepsilon_i \tag{4}$$

其中:i 为当前样本的序号,φ_i 为权系数,是时间的函数,ε_i 为零均值、方差为 σ_ε^2 的高斯白噪声。模型表示将当前样本 i 可表示为前 p 个样本值的线性组

合。设 t 时刻 AAR(p)模型的参数向量为

$$\boldsymbol{\varphi}(i)=[\varphi_1(i),\varphi_2(i),\ldots,\varphi_p(i)]^{\mathrm{T}} \quad (5)$$

与其对应的样本数据向量为

$$\boldsymbol{A}(t-1)=[\boldsymbol{a}_{i-1},\boldsymbol{a}_{i-2},\cdots,\boldsymbol{a}_{i-p}]^{\mathrm{T}} \quad (6)$$

利用时间序列 $Z(N,\Delta t)$的观测样本拟合 AAR(p)模型,所得参数向量序列描述了网络流量特性在 p 维空间的改变。设 $t-1$ 时刻 $\boldsymbol{\varphi}(t-1)$的估计值为 $\hat{\boldsymbol{\varphi}}(t-1)$,则样本 i 对应的噪声估计值为

$$\hat{\boldsymbol{\varepsilon}}_i=\boldsymbol{a}_i-\hat{\boldsymbol{\varphi}}(i-1)^{\mathrm{T}}\boldsymbol{A}(i-1) \quad (7)$$

根据递推最小二乘[13]的估计,AAR(p)模型的增益向量 $\boldsymbol{k}(i)$为

$$\boldsymbol{k}(i)=\boldsymbol{T}(i-1)\times\boldsymbol{A}(i-1)/Q(i) \quad (8)$$

$$Q(i)=\boldsymbol{A}(i-1)^{\mathrm{T}}\times\boldsymbol{T}(i-1)\times\boldsymbol{A}(i-1)+1/(1-U) \quad (9)$$

式中 $\boldsymbol{T}(i-1)$ 为样本相关矩阵且为一个 p 阶方阵,U 为更新系数。$\boldsymbol{T}(i)$ 可用下面的公式计算

$$\boldsymbol{T}(i)=\boldsymbol{T}(i-1)-\boldsymbol{k}(i)\times\boldsymbol{A}(i-1)^{\mathrm{T}}\times\boldsymbol{T}(i-1)+U\times\boldsymbol{T}(i-1) \quad (10)$$

这样,样本 i 对应的 AAR(p) 参数向量估计值为

$$\hat{\boldsymbol{\varphi}}(i)=\hat{\boldsymbol{\varphi}}(i-1)+\boldsymbol{k}(i)^{\mathrm{T}}\times\varepsilon_i \quad (11)$$

如果给定 $\boldsymbol{A}(i-1)$,$\hat{\boldsymbol{\varphi}}(i-1)$以及 U 的初始值,根据式(7)-(11)就可以实现模型参数的递推估计。增益向量和相关矩阵的初始值对计算结果影响很小,可以分别取零向量和单位矩阵。更新系数 U 的值对参数估计的收敛速度影响较大,U 的值需要根据实验结果比较选取。

2.3 支持向量机分类检测 DDoS 攻击

支持向量机方法[14]建立在统计学习理论的 VC 维理论和 Vapnik 结构风险最小化原理基础上,在解决小样本、非线性及高维模式识别问题时有其独特的优势。支持向量机将实际问题通过非线性变换转换到高维的特征空间,在高维空间中构造线性判别函数实现原空间中的非线性判别函数,而且针对有限样本,能够得到现有信息下的最优解,即全局最优点。

A_{FC}时间序列经过 AAR(p)模型拟合后变换为 p 维向量来描述数据流的状态随时间变化的特征,识别流量状态归结为基于向量空间模型的分类问题。本文使用可支持大规模训练集的序列最小优化算法来训练支持向量机分类器。

3 实 验

3.1 实验数据获取

本文的实验数据来自我们设计的针对 DNS 服务器的 DDoS 攻击实验。实验运行在一个 100Mbps 的共享局域网下,受攻击 DNS 域名服务器为 Victim,操作系统为 Linux,内存为 4GB,域名服务器软件为 bind-9.4.1。为反映数据的真实性,采集某校园网 DNS 服务器的网络数据,利用 tcpreplay 工具把这些数据包重放到 Victim 作为背景数据,得到正常流数据集 T_0。通过 dns attacker 攻击程序,利用局域网中多台主机来模拟针对域名服务器 Victim 的 DDoS 攻击,包括:直接向 Victim 发送伪造源地址和非伪造源地址的查询式攻击,通过向开放递归的 DNS 服务器发送大量源地址为 Victim 的查询请求报文而实现的反弹式攻击。每次的攻击速率随机取(500~4 000)packet/s,每次攻击持续时间也各不相同,分别得到查询式攻击数据集 T_1和反弹式攻击数据集 T_2。

3.2 实验设置

实验中数据集的采样时间间隔 Δt 为 0.01s,时间段 Δt 为 0.5s,即样本长度 N 为 50,A_{FC}定义中的加权因子 θ 用来平衡 A_{RN}和 F_{TN}的比例,参照文献[7,11]的设置,θ 设为 1/2。实验中 500 次采样的正常流和攻击流的 A_{FC}时间序列比较如图 1 所示,其中 A_{FC}-1 表示正常流,A_{FC}-2 表示反弹式攻击流,A_{FC}-3 表示查询式攻击流。通过图 1 中正常流和攻击流的 A_{FC}时间序列比较,说明 A_{FC}能较好地反映正常流与 2 种攻击流不同的状态特征。

AAR(p)模型的定阶不能求出显式的表达,通常可采用计算相对残差方差来定阶,此外,阶数 p 太大将产生大的计算量,为了达到实时检测的目的并考虑阶数 p 的约束范围[12]

$$0\leqslant p\leqslant 0.1N \quad (12)$$

实验中选取 2 阶 AAR(p)模型,参数设为 $A1$,$A2$。更新系数 U 的值影响参数估计的收敛速度,U 小则振荡较小,但识别延迟会比较大,U 大可以减小识别延迟,但会引起剧烈的振荡,实验中 U 的值取 0.02。以图 1 中时间序列 A_{FC}-2 为例,在忽略了初始的震荡过程后,得到的拟合参数序列如图 2 所示。

将采集到的正常流数据集 T_0和攻击数据集(包含 T_1和 T_2)的 2/3 用作训练集,剩余的 1/3 数据作为测试集。训练集和测试集均按时间划分为若干个序列,以样本序列为单位进行训练和测试。实验中

将训练和测试样本序列的长度 N 设为 50,使用训练集 T_0、T_1和 T_2的 AAR 参数训练支持向量机分类器,训练数据的规模为 5 000 个样本,即 100 个样本序列,其中查询式攻击数据集 T_1共 22 个样本序列,反弹式攻击数据集 T_2共 20 个样本序列。支持向量机分类器采样高斯核函数,模型参数在训练集上采用 10 倍交叉验证寻优得到,使用最优参数在训练集上的分类结果作为本文所提方法的分类标准。

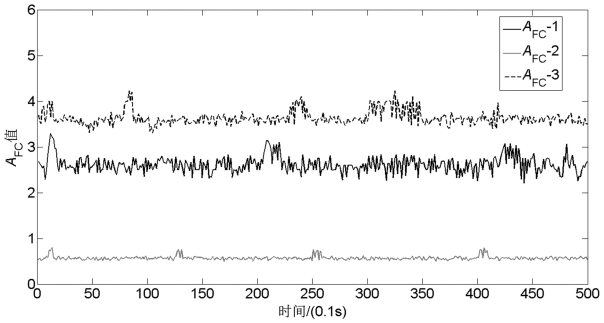

图 1 正常流和攻击流的 A_{FC}时间序列比较

Fig. 1 A_{FC} of normal traffic VS. A_{FC} of attack traffic

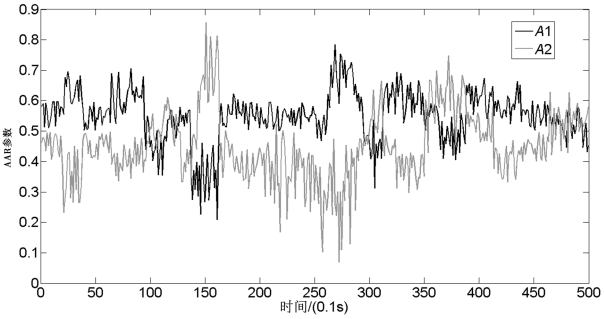

图 2 时间序列 A_{FC}-2 的 AAR 模型参数

Fig. 2 The parameters of AAR model of time series A_{FC}-2

3.3 实验结果分析

为了检测使用上述训练集获得的分类模型的决策能力,进行了 10 组实验,以正常流数据集 T_0为背景流,从测试集中按照 1,5,10,15,20 倍的规律增大背景流,分别得到 5 组实验的待测正常流 $T_{0i}(i=1,2,\cdots,5)$,将 T_{0i}分别与数据集 T_1混合得到 5 组实验的待测攻击流,由此得到 5 组用于检测查询式攻击的待测流 $F_{1i}(i=1,2,\cdots,5)$。用同样的方法将 T_{0i}分别与数据集 T_2混合得到 5 组实验的待测攻击流,得到 5 组用于检测反弹式攻击的待测流 $F_{2i}(i=1,2,\cdots,5)$。每组测试集均为连续的5 000 个样本,即 100 个样本序列,对待测流 F_{1i}和 F_{2i}分别进行采样并计算 A_{FC}时间序列,拟合后得到 10 个待测样本集,为了验证本文方法的有效性,将该方法与常用的检测方法神经网络(BP)算法[15]和 KNN 算法[16]进行了比较,表 1 和表 2 给出了 3 种方法对 10 组数据的检测结果。

设 T_P表示被正确标记的正常测试样本数,F_P表示被错误标记的正常测试样本数,T_N表示被正确标记的攻击测试样本数,F_N表示被错误标记的攻击测试样本数,则检测率 $D_R=T_N/(T_N+F_N)$,误报率 $F_R=F_P/(T_P+F_P)$,总错误率 $E_R=F_N+F_P/(T_P+F_P+T_N+F_N)$。

通过表 1 的数据可看出,在对查询式攻击的检测中,当背景流较小,即攻击流较大时,2 种方法的检测效果相差不大,但随着背景流的逐步加大,本文所提方法的优势逐渐显现,虽然检测率略有降低,但没有随着正常流的加大而明显下降,即使在背景流增大到 20 倍时,仍有 96%的检测率。5 组检测中,本文方法的平均误报率为 0.88%,平均错误率为 1.38%,测试结果中误报和漏检的主要原因是由于背景流的增加和网络的随机噪声引起了网络流状态的偏移。

表 1 3 种方法对查询式攻击的检测结果比较

Table 1 Comparison of three methods of detecting flooding attacks

%

		F_{11}	F_{12}	F_{13}	F_{14}	F_{15}
本文方法	D_R	100	99.2	98.3	97.1	96.0
	F_R	0.0	0.3	0.6	1.0	1.6
	E_R	0.0	0.4	1.0	1.7	2.4
BP	D_R	99.0	97.2	94.4	90.3	86.5
	F_R	0.3	0.4	1.0	3.3	6.5
	E_R	0.4	1.3	3.3	6.7	10.2
KNN	D_R	99.2	97.8	94.2	91.5	89.1
	F_R	0.3	0.5	1.5	3.1	6.3
	E_R	0.3	1.0	2.6	4.8	8.2

表 2 3 种方法对反弹式攻击的检测结果比较

Table 2 Comparison of three methods of detecting amplification attacks

%

		F_{21}	F_{22}	F_{23}	F_{24}	F_{25}
本文方法	D_R	100	99.7	99.0	98.2	96.4
	F_R	0.0	0.1	0.2	0.5	1.2
	E_R	0.0	0.2	0.4	0.7	2.2
BP	D_R	98.1	95.7	93.1	90.0	86.3
	F_R	0.6	1.0	1.4	3.1	5.7
	E_R	1.4	3.2	4.0	6.8	9.2
KNN	D_R	98.0	96.4	93.0	90.5	86.4
	F_R	0.7	0.8	1.6	3.4	5.0
	E_R	1.2	3.0	3.9	4.3	8.4

从表 2 可以看出,在 5 组反弹式攻击的检测实验中,本文方法的平均检测率为 98.8%,该结果表明,本文方法能较准确地识别含有反弹式攻击的异

常流,而且对攻击流引起的网络异常现象比较敏感。5 组检测实验中,本文方法的平均误报率为 0.50%,平均错误率为 0.88%。

如表 1 和表 2 所示,对 2 种 DDoS 攻击的检测结果中,BP 算法和 KNN 算法随着背景流的增加,检测率下降明显,同时误报率和总错误率明显上升,可见,本文方法更能准确地检测针对 DNS 服务器的 DDoS 攻击。

4 结 论

本文分析了针对 DNS 服务器的 DDoS 攻击形式及攻击发生时的流量特征,提出了针对流量结构特征变化的检测方法。通过等时间采样构成时间序列,使用 AAR 模型进行参数向量估计并用 SVM 进行分类。实验结果表明,该方法能较准确地识别出 DDoS 攻击流及其引起的网络流异常情况。

在后续的工作中我们会进一步分析检测方法中各参数对检测精度的影响,以及在实际应用场景中如何自适应地给出一种有效的参数设置。

参考文献:

[1]Li Weimin, Cao Xiaoguang, Liu Fang, et.al. Improving DNS cache to alleviate the impact of DNS DDoS attack [J]. Journal of Networks, 2011, 6 (2): 279-286.

[2]陈玉明,谢斐星,吴克寿,等.基于邻域关系的网络入侵检测特征选择[J].常州大学学报(自然科学版),2014,26(3):1-5.

[3]蔡艳婧,程晓红,程显毅.网络敏感信息动态特征的抽取方法[J].常州大学学报(自然科学版),2014,26(4):80-85.

[4]张永铮,肖军. DDoS 攻击检测和控制方法[J].软件学报,2012,23(8):2058-2072.

[5]徐阳.基于概率事件的无线传感网络能耗分析研究[J].常州信息职业技术学院学报,2014,13(3):33-35.

[6]Ye Xi, Ye Yiru. A Practical Mechanism to Counteract DNS Amplification DDoS Attacks [J]. Journal of Computational Information Systems, 2013, 9 (1): 265 - 272.

[7]Subbulakshmi T, Shalinie S M, Ramamoorthi A. Detection and classification of DDoS attacks using machine learning algorithms [J]. European Journal of Scientific Research, 2010, 47(3): 334-346.

[8]Farid D, Rahman S, Rahman C. Adaptive Intrusion Detection based on Boosting and Naïve Bayesian Classifier[J]. International Journal of Computer Applications, 2011, 24(3): 12-19.

[9]Wang W, Wu W. Online Detection of Network Traffic Anomalies Using Degree Distributions [J]. International Journal of Communications, Network and System Sciences, 2010, 3 (2): 177-182.

[10] Peng T, Leckie C, Kotagiri R. Proactively detecting distributed denial of service attacks using source IP address monitoring[C]// Proc of the 3rd Int IFIP-TC6 Networking. Berlin: Springer Verlag, 2004: 771-782.

[11] 孙钦东,张德运,高鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报,2005,28(5):767-773.

[12] 顾晓清,王洪元,倪彤光,等. 基于时间序列分析的应用层 DDoS 攻击检测 [J]. 计算机应用,2013,33(8):2228-2231.

[13] Vapnik V. The Nature of Statistical Learning Theory [M]. NewYork: Springer Verlag, 1995.

[14] Marina Throttan. Adaptive Thresholding for Proactive Network Problem Detection[C]//Proc of IEEE Internation Workshop on System Management, Rhode Island. NewYork: Springer Verlag, 1998: 108-116.

[15]Rastegari S, Saripan M I, Rasid M F. A detection of denial of service attacks against domain name system using neural networks [J]. UCSI International Journal of Computer Science, 2009, 15 (1): 23-27.

[16]Nasibov E, Peker S, Time series labeling algorithms based on the K-nearest neighbors' frequencies[J]. Expert Systems with Applications, 2011, 38 (5): 5028-5035.

(责任编辑:李艳)