网络洪流攻击的异常检测*

单蓉胜, 李建华, 王明政
(上海交通大学电子工程系, 上海 200030)

摘 要: 提出了一种新颖的网络洪流攻击的异常检测机制。这种检测机制的无状态维护、低计算代价的特性保证自身具有抗洪流攻击的能力。以检测 SYN 洪流行为为实例详细阐述了流量强度、对称性度量的检测方法。测试结果表明所提出的检测机制具有很好的检测洪流攻击的准确度, 并具有低延时特性。

关键词: 异常检测; 入侵检测; 拒绝服务攻击; 端口扫描
中图分类号: TP393 文献标识码: A 文章编号: 0529-6579 (2003) 06-0031-04

因特网在过去的几十年里经历了快速的增长。然而, 由于 TCP 协议固有的漏洞, 因特网极易遭受网络攻击。根据文献 [1] 大约超过 90%的拒绝服务攻击 (DOS) 是使用 TCP 协议。由于 DOS 攻击总是导致网络流量的特征产生偏差, 所以检测网络流量的异常变化是检测和防御 DOS 攻击的必要手段。目前, 许多管理员通过分析网络异常流量来人工识别这类攻击。通过网络流异常的可视化分析, 网络异常被分成两类:

网络操作异常: 是指由于配置的错误和网络流量达到环境限度时产生的异常行为。

网络滥用异常: 是指恶意的网络行为。DOS 攻击和快速扫描是两类常见的网络滥用异常。DOS 攻击是指恶意破坏网络在线的服务。端口扫描主要用于收集被攻击目标的有用信息。目前比较流行的 SYN-Flooding 和 SYN-Scan 攻击都是利用 TCP 协议 3 次握手的协议机制的漏洞。网络滥用异常是我们研究的重点。

为了克服 SYN-Flooding 攻击, 提出许多机制, 如 SYN cache[2], SYN cookies[3], SYN Defender[4], SYN proxying[5], 和 SYN-kill[6]。但是, 这些机制都是维护状态的, 也就是, 每个 TCP 连接需要维护状态, 并进行状态计算。SYN-Flooding 攻击商业网站的实验[7] 表明制服一个没有特别保护的网站的 SYN 速率要求达到 14 000 /s 个 SYN 请求。如果将这些检测系统集成网关设备上, 就会大大降低端到端 TCP 性能, 也会导致建立连接的延时增加。

上述基于 TCP 状态维护或复杂计算的解决办法使防御系统本身也容易遭受洪流攻击。本文提出了一种简单的检测机制。该检测机制运用基于指数平滑的时间序列分析方法, 并结合网络流的对称性特征来检测网络洪流攻击。这个方法能有效地检测那些产生突发网络流量的攻击, 如 SYN-flood, SYN 快速扫描等。基于 DARPA 评估数据的实验表明文中提出的机制有高检测率和高实时性。

1 基于网络流异常的洪流检测

根据网络滥用异常的特性, 我们定义了两类有利于检测洪流攻击的检测度量。

(1) 强度度量, 这些度量统计特征属性在固定的时间间隔内发生的次数, 用于检测突发活动的异常。

(2) 对称性度量, 这些度量描述在固定时间间隔内一对特征属性的对称关系, 用于检测对称性被破坏的异常网络行为。

1.1 强度度量异常检测

为了能实时检测网络异常的突发流量, 我们用强度度量表示相关业务的繁忙程度, 强度度量越大, 则相关的业务越繁忙。而且, 当网络异常行为发生时, 强度度量就会发生突变。然而, 象因特网这样动态、复杂的实体, 用一种简单的参数模型描述所有时刻的 TCP 连接模型是不可能的。因此, 我们利用基于指数平滑的时间序列分析方法, 并以 TCP 协议的 SYN 请求分组流量为实例, 说明流量强度突变的检测原理。设表示在固定时间间隔内 SYN 报文发生的计数, 随着时间而波动。通过对 1999 年 DARPA 评测网络入侵检测系统所使用的数据集[8] 的 1999 年第一周、第三周的正常数据的分

* 收稿日期: 2003-07-11
基金项目: 国家“863”高技术计划资助项目 (2001AA140214); 武器装备预研基金项目 (5143040301JW0301)
作者简介: 单蓉胜 (1971 年生), 男, 博士生; E-mail: srs-zh@263.net

析，x_t 不是一个稳态过程。图 1 描述了第一周第一天的 SYN 的统计数据。N 轴描述了采样间隔序列。图 2 描述了差分后 SYN 序列。

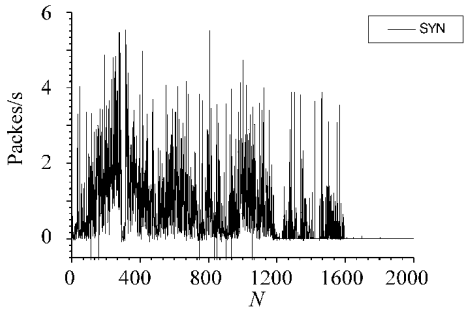

图 1 SYN 序列

Fig. 1 SYN sequence

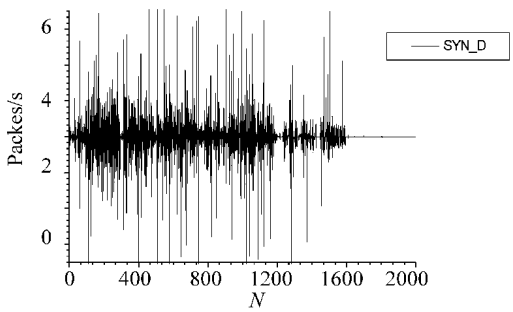

图 2 差分后的 SYN 序列

Fig. 2 SYN sequence after differencing

通过对序列 x_t 一阶差分，我们可以得到一个稳态过程 z_t，即

$$(1-B)x_t = z_t,\ t > 1,\ z_t \sim n(0,\ \sigma_t^2) \qquad (1)$$

其中，B 是一个后移算子，z_t 是一个零均值、方差为 σ_t 的正态过程，上、下限（UCL 和 LCL）分别如下所示：

$$UCL_t = 3\hat{\sigma_t},\ LCL_t = -3\hat{\sigma_t} \qquad (2)$$

我们所观察的数据流，如 SYN，SYNACK 报文发生率随时间变化大，当前观测的数值和邻近观测点紧密相关，与过去较长一段时间的数据关系不大。因此我们使用简单指数平滑（EWMA）方法来评估 σ_t 的值，即：

$$\hat{\sigma_t} = \sqrt{(1-\lambda)\sum_{j=0}^{\infty}\lambda^j z_{t-j}^2} \qquad (3)$$

式中，λ（$0 < \lambda < 1$）叫做衰减因子，其取值大小决定了相关样本的权重和有效样本的长度。这种方法的特点是对每个观测值给予不同的权重，离估计值越近的数据权重越大，越远的数据权重越小。用 EWMA 法估计时间序列的差分方差还有一个显著的特点，就是可以将方差的估计公式写成迭代形式，这将有利于应用计算机处理庞大的数据。迭代形式

$$\sigma_t^2 = \lambda\sigma_{t-1}^2 + (1-\lambda)z_t^2 \qquad (4)$$

因为 λ 的取值范围为：$1 < \lambda < 1$，故 z_{t-j}^2 的权重 $(1-\lambda)\ \lambda^j \to 0$（当 $j \to t$，$t \to \infty$ 时）。因此，定义容忍度 L_k：

$$L_k = (1-\lambda)\sum_{j=K}^{\infty}\lambda^j = \lambda^K \qquad (5)$$

其中，K 是有效数据的长度。上式阐明了 L_K，K，λ 三者之间的关系。

因此，在某容忍度 L_K 下，强度度量的突发判决函数为

$$f(z_t) = \begin{cases} 1 & z_t > 3\sqrt{(1-\lambda)\sum_{j=0}^{K-1}\lambda^j z_{t-j}^2} \\ 0 & |z_t| < 3\sqrt{(1-\lambda)\sum_{j=0}^{K-1}\lambda^j z_{t-j}^2} \\ -1 & z_t < 3\sqrt{(1-\lambda)\sum_{j=0}^{K-1}\lambda^j z_{t-j}^2} \end{cases} \qquad (6)$$

在测试过程中，如果某个观测点 z_t 大于控制上限 UCL，那么 $f(z_t)$ 的值为 1，并产生一个流突发事件的上跳变信号；如果 z_t 小于控制下限，那么 $f(z_t)$ 的值为 -1，并产生一个流突发事件的下跳变信号；如果观测点 z_t 的绝对值始终属于控制范围内，则 $f(z_t)$ 的值为 0，表明被检测的数据流平稳变化。

许多异常的网络行为在一段时间内存在。为了避免频繁报警，必须有效明确异常行为的起始时刻。强度度量突变的上、下跳变的识别有助于为确认异常事件的起始、终止时刻。

1.2 对称度量异常检测

许多网络流存在明显对称性现象。如，在正常条件下，SYN 和 SYNACK 的统计值的偏差和总的 TCP 连接请求相比很小。而且 SYN 和 SYNACK 的一一对应关系是不依赖于采样时间、网络站点。

设 y_t 表示在固定时间间隔内 SYNACK 报文发生的计数。显然，在正常的网络条件下，x_t 应该等于 y_t。图 3 描述了 DARPA1999 年评估数据的第一周第一天的 SYN 报文和 SYNACK 报文的统计数据。

SYN 和 SYNACK 报文的对称度量定义：

$$\varepsilon_t = \frac{|x_t - y_t|}{x_t} \qquad (7)$$

在正常的网络环境下，对称性度量的理想取值是 $\varepsilon_0 \to 0$。但是错误配置系统或误操作将导致对称性度量轻微偏移。而且，当异常事件发生，对称性会被严重破坏，ε_t 的值远离零点。为使 ε_t 可以更好地体现被观测度量的对称平衡能力，并区分操作

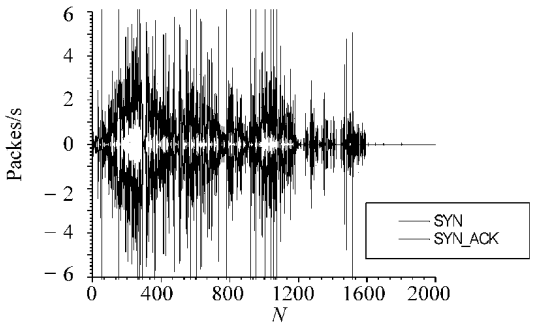

图 3　SYN 与 SYNACK 的对称性

Fig. 3　the symmetry of SYNs and SYNACKs

异常和滥用异常，需要采用比较灵活的对称性阀值定义。通过分析实际的网络流，我们发现当流量比较小的时候，异常事件发生的概率小，而流量比较大的时候，异常事件发生的概率大。因此，我们设计了具有自适应能力的对称性检测算法，其检测阈值能够随着网络流量的变化自动调整。自适应阀值定义为：

$$s_t = \frac{\beta \ln(x_t)}{x_t} s_t \in [0, 0.3] \qquad (8)$$

其中，β 是一个可调参数。通常情况，我们认为如果 ε 大于 0.3，对称性明显被破坏。因此 $\beta \leqslant 0.3 x_t / \ln(x_t)$，取 $\beta = 0.3\alpha / \ln(\alpha)$。α 表示网络流量的最大安全控制限度，而且 98% 的正常 x_t 是属于 [0, α]。当网络的流量强度小于 α，异常事件很少发生。对称性检测函数：

$$f(y_t, x_t) = \frac{|\varepsilon_t|}{s_t} = \frac{|x_t - y_t|}{\beta \ln(x_t)} > 1 \qquad (9)$$

如果上式成立，那么则我们认为该对称性度量的对称性被破坏。

为了避免采样时间间隔对测试精度的影响，我们改进了上述的对称性检测算法，增加了累积检测。当流量 x 在时刻 t_0 发生上跳变，且持续 N 个采样周期，设

$$\varepsilon_i = \frac{\sum_{t=t_0}^{t_0+i} |x_t - y_t|}{\sum_{t=t_0}^{t_0+i} x_t}, \quad s_i = \beta \log\left(\sum_{t=t_0}^{t_0+i} x_t \Big\backslash \sum_{t=t_0}^{t_0+i} x_t\right)$$

其中，$0 \leqslant i \leqslant N$，则累积检测的判决规则是

$$f_i(y_t, x_t) = \frac{\sum_{t=t_0}^{t_0+i} |x_t - y_t|}{\beta \log\left(\sum_{t=t_0}^{t_0+i} x_t\right)} \qquad (10)$$

如果上式成立，则发生对称性异常。显然，当 $i = 0$，式(9) 是式(10) 的特例。

2　实验分析

为了评估和验证我们的方法，我们在 DARPA1999 的评估数据上做了仿真实验。我们记录了每个观测间隔 t_0 内 SYN 和 SYNACK 的报文数目。t_0 决定了检测的分辨率。通常情况，Syn 请求分组第一次重发的时间约 6 s，第二次重发时间约 24 s[9]。因此，我们设定采样周期为 30 s。然而，采样周期是可调参数，而且我们的算法对采样周期不敏感。通过分析正常的 DARPA 评测数据，我们发现 98% 的 x 属于 [0, 3]。因此，设 α=3，得到 $\beta \approx 0.81$。而且，由于邻近观测点之间具有强相关性，所以设 λ=0.85，最小容忍度 L=0.001。根据式 (5) 得到 $k \approx 42$。

我们在 DARPA1999 的第五周第一天的数据上进行了检测实验。实验结果如图 4 所示。

图 4 (a) 是 SYN 一阶差分序列的强度度量的检测。UCL 和 LCL 是强度度量的控制上下线。图 4 (b) 是 SYN 与 SYNACK 对称性检测。检测到攻击如表 1 所示。

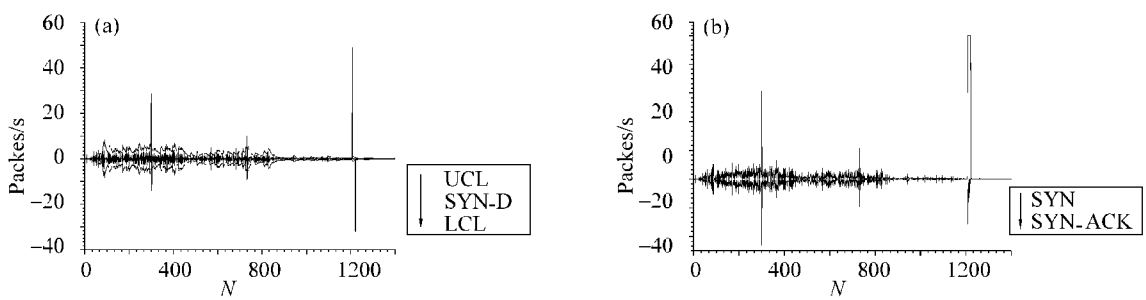

图4　DARPA 的第5 周第 1 天的数据

Fig. 4　The first day of DARPA evaluation date

(a) SYN-D 的强度检测；(b) SYN 与 SYNACK 对称性检测

表 1 检测结果

Fig. 1 the detection results

攻击次数	名称	发起时间	结束时间
1	Apache2	Mon Apr 05 10: 29: 51 1999	Mon Apr 05 10: 30: 51 1999
2	Apache2	Mon Apr 05 14: 05: 45 1999	Mon Apr 05 14: 06: 15 1999
3	neptune	Mon Apr 05 18: 04: 26 1999	Mon Apr 05 18: 10: 26 1999

在实验中, 我们的算法有效检测到第五周第一天的三次洪流攻击, 其中, 在 1999 年 4 月 5 日 10: 29: 51、1999 年 4 月 5 日 14: 05: 45, 发生了 Apache2 攻击; 在 1999 年 4 月 5 日 18: 04: 26, 发生了 neptune 攻击。Apache2[8] 攻击是 apache web 的拒绝服务攻击。攻击者发送带有很多的 http 数据头的请求分组, 导致系统速度减慢, 甚至死机。Netpune[8] 是典型的 SYN 洪流攻击, 可以攻击一个端口或者多个端口。不过, 该算法没有检测到 1999 年 4 月 5 日 9: 43: 11 的端口扫描行为。该扫描行为持续了近 4 min。这是因为该扫描行为是使用 SYN 的慢速扫描, 每隔 10 s 左右扫描一次, 没有形成突发流量。针对慢速扫描、异常扫描, 我们使用主动扫描技术检测, 已另外撰文描述。我们算法检测到的攻击的起止时间与真实结果略有不同, 即起始时间的和真实发生时间的误差小于一个采样周期。

3 结 论

本文提出了一个简单、健壮的网络流量异常检测方法。我们的方法的主要特征是: ①无状态和低计算负荷使自身对洪流攻击免疫; ②与网络业务的访问模式无关; ③累积检测使检测机制更健壮; ④同时运用强度和对称性度量使检测更准确。实验结果表明, 在检测的准确性、实时性方面效果比较理想。而且, 我们的算法能扩展检测 synKill 攻击, Ipsweep 扫描, NMAP 扫描、SATAN 等具有洪流性质且对称性被破坏的网络攻击。

参考文献:

[1] MOORE D, VOELKER G, SAVAGE S. Inferring internet denial of service activity // Proceedings of USENIX Security Symposium 2001 (Best Paper Award) [C]. Washington DC: USENIX, 2001: 9—22.

[2] LEMON J. Resisting SYN flooding DoS attacks with a SYN cache // Proceedings of USENIX BSDCon'2002 [C]. San Francisco CA: USENIX, 2002: 89—97.

[3] BERNSTEIN D J. SYN cookies [EB/OL]. http: //cr. yp. to/syncookies. html.

[4] Check Point Software Technologies Ltd. SynDefender [EB/OL]. http: //www. checkpoint. com/products/protect/firewall—1. html

[5] Netscreen Technologies Ltd. Firewall appliance [EB/OL], http: //www. netscreen. com/.

[6] SCHUBA C L, KRSUL I V, KUHN M G, et al. Analysis of a denial of service attack on TCP // Proceedings of IEEE Symposium on Security and Privacy [C]. Los Alamitos CA: IEEE Computer Society Press, 1997: 208—223.

[7] DARMOHRAY T, OLIVER R, Hot spares for DoS attacks [M]. Login, 2000.

[8] Lincoln Laboratory, Massachusetts Institute of Technology. DARPA Intrusion Detection Evaluation [EB/OL]. http: //www. ll. mit. edu/IST/ideval/index. html.

[9] STEVENS R W. TCP/IP Illustrated Volume: The Protocols [M]. New York: Addison-Wesley, 1994.

Anomaly Detection of Network Flooding Attacks

SHAN Rong-sheng, LI Jian-hua, WANG Ming-zheng

(Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030, China)

Abstract: A novel mechanism for detecting flooding-attacks is proposed. SYN-Flooding, as an instance of flooding-attack, is used to illustrate the theory of intensity anomaly and symmetry anomaly detections. Experiment shows that the mechanism has high detection accuracy and low detection latency.

Key words: anomaly detection; intrusion detection; denial of service