Journal of Computer Applications
计算机应用,2013,33(10):2838-2841,2845
ISSN 1001-9081
CODEN JYIIDU
2013-10-01
http://www.joca.cn

文章编号:1001-9081(2013)10-2838-04
doi:10.11772/j.issn.1001-9081.2013.10.2838

基于流量行为特征的 DoS&DDoS 攻击检测与异常流识别

周颖杰[1,2*],焦程波[3],陈慧楠[1],马　力[1],胡光岷[1]
(1.电子科技大学 光纤传感与通信教育部重点实验室,成都 611731;　2.四川大学 计算机学院,成都 610065;
3.北京信息技术研究所,北京 100093)
(*通信作者电子邮箱 yjzhou@uestc.edu.cn)

摘　要:针对现有方法仅分析粗粒度的网络流量特征参数,无法在保证检测实时性的前提下识别出拒绝服务(DoS)和分布式拒绝服务(DDoS)的攻击流这一问题,提出一种骨干网络 DoS&DDoS 攻击检测与异常流识别方法。首先,通过粗粒度的流量行为特征参数确定流量异常行为发生的时间点;然后,在每个流量异常行为发生的时间点对细粒度的流量行为特征参数进行分析,以找出异常行为对应的目的 IP 地址;最后,提取出与异常行为相关的流量进行综合分析,以判断异常行为是否为 DoS 攻击或者 DDoS 攻击。仿真实验的结果表明,基于流量行为特征的 DoS&DDoS 攻击检测与异常流识别方法能有效检测出骨干网络中的 DoS 攻击和 DDoS 攻击,并且在保证检测实时性的同时,准确地识别出与攻击相关的网络流量。

关键词:异常检测;异常流识别;骨干网络;信息熵;流量分析
中图分类号:TP393.08　　**文献标志码**:A

Traffic behavior feature based DoS&DDoS attack detection and abnormal flow identification for backbone networks

ZHOU Yingjie[1,2*], JIAO Chengbo[3], CHEN Huinan[1], MA Li[1], HU Guangmin[1]
(1. *Laboratory of Optical Fiber Sensing and Communications, Ministry of Education, University of Electronic Science and Technology of China, Chengdu Sichuan* 611731, *China*;
2. *College of Computer Science, Sichuan University, Chengdu Sichuan* 610065, *China*;
3. *Beijing Information Technology Institute, Beijing* 100093, *China*)

Abstract: The existing methods for backbone networks only analyze coarse-grained network traffic characteristic parameters. Thus, they cannot guarantee both the premise of abnormal flow identification and the real-time detection for DoS (Denial of Service) & DDoS (Distributed Denial of Service, DDoS) attacks. Concerning this problem, a DoS&DDoS attack detection and abnormal flow identification method for backbone networks was proposed. First, it analyzed coarse-grained network traffic characteristic parameters to determine the time points that abnormal behaviors occur; then, fine-grained traffic behavior characteristic parameters were analyzed in these time points to find the destination IP addresses that correspond to abnormal behaviors; finally, comprehensive analysis was conducted for extracted traffic that correspond to abnormal behaviors to determine DoS and DDoS attacks. The simulation results show that, the proposed method can effectively detect DoS attacks and DDoS attacks in backbone networks. Meanwhile, it could accurately identify the abnormal traffic, while real-time detection is ensured.

Key words: anomaly detection; abnormal flow identification; backbone network; entropy; traffic analysis

0　引言

随着网络的不断规模化和复杂化,网络中拒绝服务(Denial of Service,DoS)攻击和分布式拒绝服务(Distributed Denial of Service,DDoS)攻击的发生频率也越来越高,给网络的正常运行带来了极大的威胁。为了保证网络的高效、安全运行,如何快速、准确地进行 DoS&DDoS 攻击检测已成为国内外学术界和工业界共同关注的热点问题之一。

国内外研究者提出了一系列方法以检测 DoS 攻击和 DDoS 攻击。按照数据源的不同,现有 DoS 攻击和 DDoS 攻击的检测方法主要可以分为两类:基于包信息的检测方法和基于网络流量行为特征的检测方法。

1)基于包信息的检测方法通过分析数据包中的特定信息或是用户日志等,建立判定规则,并根据实际的流量数据和这些规则的匹配关系来检测 DoS 攻击和 DDoS 攻击。典型的研究有:文献[1]提出一种基于主机日志分析的统计方法,通过分析主机的日志数据,利用统计理论对正常行为建模,并比较待检测行为与正常行为的偏离来检测网络 DoS 攻击。文献[2]提出了一种基于数据包包头信息综合分析的异常检测技术,通过分析目的 IP 地址或端口号在边沿路由器出口流量的关联检测异常。文献[3]利用 TCP 协议不同的控制报文在交互时呈现出的数学约束关系,提出了一种评价 TCP 流宏观平衡性的系统测度,并将之应用于异常检测。

2)基于网络流量行为特征的检测方法通过分析流量行为特征参数,如各种数据包包头信息(如 IP 地址、端口号等)聚合后计算得到的统计量,来进行异常检测。典型的研究有:

收稿日期:2013-04-10;**修回日期**:2013-07-05。　**基金项目**:国家自然科学基金资助项目(60872033,61201127)。
作者简介:周颖杰(1984-),男,四川成都人,博士,主要研究方向:网络异常检测与识别;　焦程波(1982-),男,河南郑州人,工程师,博士,主要研究方向:网络测量与安全;　陈慧楠(1986-),女,四川眉山人,硕士,主要研究方向:网络异常检测;　马力(1987-),男,四川成都人,硕士,主要研究方向:网络异常检测;　胡光岷(1966-),男,四川眉山人,教授,博士生导师,博士,主要研究方向:网络行为学、网络安全。

文献[4]提出使用数据包属性的分布描述网络流量行为,通过分析数据包属性分布的变化检测异常。文献[5]利用比例不确定性去确定一些诸如 IP 地址、端口号等属性的剩余值,提出一种剩余空间方法(Method of Remaining Elements, MRE)来检测异常流量;文献[6]将香农熵进行推广,提出了一种基于非扩展熵的异常检测方法;文献[7]提出基于经验熵的 DDoS 检测方法;文献[8]将网络流量幅值看作随时间变化的信号,利用小波分析区分出背景流量和异常流量,而后根据异常持续时间和信号频率的不同采用不同的方式来检测攻击;文献[9]使用连续小波变换检测 DoS 攻击引起的网络流量幅值变化;文献[10]通过对聚合后的网络流量进行小波分析检测 DDoS 攻击。

基于包信息的检测方法能分析出与攻击相关的异常流量,并具有检测准确度高的优点,适用于各种用户网络。然而,由于骨干网络中数据流量巨大,逐包分析将耗费大量时间,因而该类方法应用于骨干网络时无法满足异常检测的实时性要求。基于网络流量行为特征的检测方法检测效率较高,可以做到对 DoS 攻击和 DDoS 攻击的实时检测。然而,由于该类方法仅分析粗粒度的网络流量行为特征参数,即分析网络流量聚合后计算得到的各种统计量,而未涉及细粒度的网络流量行为特征参数,即原网络流量各子流上计算得到的统计量,因而无法识别出与攻击相关的异常流量,找出攻击者的确切 IP 地址,从而对异常流量进行过滤;其次,该类方法的漏检率也普遍较高。

针对上述问题,本文提出基于流量行为特征的骨干网络 DoS&DDoS 攻击检测与异常流识别方法。该方法采用粗、细粒度结合的思想,在粗粒度流量行为特征参数表现出异常的时间点分析细粒度的流量异常行为特征,从而在兼顾检测实时性的同时准确识别出与攻击相关的流量。

1　DoS 攻击与 DDoS 攻击

DoS 攻击是一种通过发送大量数据包使得计算机或网络无法提供正常服务的攻击形式。它可能在短时间内耗尽网络的可用带宽或被攻击对象的系统资源,使得正常的用户请求无法被处理,从而阻碍网络中的正常通信,给被攻击者乃至网络带来巨大的危害。

DDoS 攻击是一种隐蔽的拒绝服务攻击,攻击中的数据包来自不同的攻击源。与 DoS 攻击相比,DDoS 攻击在单条链路上的流量更小,难以被网络设备检测,因而更易于形成。另一方面,DDoS 攻击汇聚后的异常流量总量很大,极具破坏力。DDoS 攻击示意图如图 1 所示。

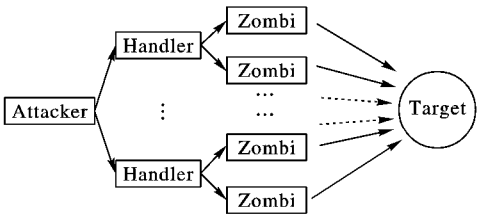

图 1　DDoS 攻击示意图

2　攻击检测方法

基于流量行为特征的骨干网络 DoS&DDoS 攻击检测与异常流识别方法使用粗细粒度结合的思想分析与 DoS&DDoS 攻击相关的流量行为特征参数。该方法通过对骨干网络流量分别进行粗、细粒度的流量行为特征参数分析,既能准确、实时地检测出骨干网络中的 DoS&DDoS 攻击,又能有效地识别出与攻击相关的网络流量,找出攻击者的确切 IP,从而使网络管理者能够在路由器进行设置,过滤掉攻击者发送的流量,防止其对目的主机造成危害。

基于流量行为特征的骨干网络 DoS&DDoS 攻击检测与异常流识别方法包括四个步骤:流量行为特征提取,异常时间点确定,异常目的 IP 确定以及异常流提取与攻击判定。具体流程如下:

1)从网络设备中获取原始数据,并从中提取出流量行为特征;

2)对粗粒度的流量行为特征参数进行处理,确定异常行为发生的时间点;

3)分析异常行为发生的时间点流量最大的 N 个目的 IP 在历史时间窗内所构成子流的细粒度流量参数,判定异常目的 IP;

4)找出历史时间窗内与异常目的 IP 对应的源 IP 并提取出相关异常流,综合分析异常流的行为特征参数在异常时间点的变化,判断引起该异常流的异常行为是否为 DoS 攻击或者 DDoS 攻击。

2.1　流量行为特征提取

首先,从实际的网络设备中获取骨干网络中的 Netflow 流量数据。由于 Netflow 数据是二进制流,难以直接进行操作,故需要将其转化为便于程序操作的文本形式,用于之后的检测和判别。得到上述文本后,从中提取与 DoS 攻击和 DDoS 攻击相关的流量行为特征。

通过对 DoS 攻击和 DDoS 攻击的特征进行调查,本文拟提取以下流量行为特征:流数量、包数量、字节数、源 IP 地址、目的 IP 地址、源自治域号、目的自治域号和目的端口号。其中,流数量、包数量和字节数从不同层次反映网络中各节点间的数据交换量,由于 DoS 攻击和 DDoS 攻击均会在攻击期间发出大量攻击包,因而大部分情况下会使网络中特定节点间的流数量、包数量和字节数上升,故这几项参数可作为判定 DoS 攻击和 DDoS 攻击的依据之一;源 IP 地址和目的 IP 地址反映网络中数据的流向,根据这两个参数能取得各主机间的流量,并判断攻击者和受害者;源自治域号和目的自治域号反映主机的分布情况,目的端口号反映攻击的性质,它们主要用于区分 DoS&DDoS 攻击和其他具有相似特征的网络流量异常行为。

2.2　异常时间点确定

在骨干网络中,如果将各个时间段数据包的统计过程看成是一个随机过程,将数据包中的各个属性看成是一个随机事件,那么引入信息熵的概念,就能表示各个属性分布的集中分散情况[11]。通过将时间分成一系列时间间隔,在每个时间间隔内统计网络的流量信息,属性 X 在该时间间隔内的信息熵定义如式(1)所示:

$$H(X) = -\sum_{i=1}^{N}(P_i \ln P_i) \tag{1}$$

式(1)中:P_i 为属性 X 中某个取值出现的概率,N 为属性 X 中所有可能的取值个数。本文中,使用信息熵作为粗粒度的网络流量行为特征参数。

通过对目的 IP 信息熵进行分析,能够确定异常行为发生的时间点。其算法描述如下:

算法 1　异常时间点检测算法。

输入　网络流量行为特征信息;

输出 异常行为发生的时间点。

1) 令 $a = a_0$;
2) 初始化当前时间点;
3) while {当前时间点属于待检测时间点}
4) 计算当前时间点的目的 IP 信息熵较前一时间点该值的变化值 h;
5) if $h > a$
6) 标记当前时间点为异常时间点;
7) end if
8) 当前时间点++;
9) end while

其中 a_0 由带标记的实际骨干网络流量数据训练得到。通过训练发现当 $a_0 \geq 0$ 时,a_0 的取值越小,异常时间点中包含 DoS 攻击和 DDoS 攻击的个数越多。即 a_0 越小,检测的漏检率越低。

2.3 异常目的 IP 确定

DoS 攻击和 DDoS 攻击的一个显著特点是,由于出口带宽几乎完全被攻击包占用,或者系统资源被大量无效请求耗尽,被攻击目的 IP 通常无法正常地响应用户访问。针对 DoS 攻击和 DDoS 攻击这一特点,本文提出使用服务率作为检测异常目的 IP 的流量行为特征。服务率反映目的 IP 响应用户访问的能力,本文将其定义为

$$Se(t) = ns(t)/nr(t) \tag{2}$$

式(2)中,$Se(t)$ 为待检测 IP 在时间点 t 的服务率,$ns(t)$ 为该 IP 在时间点 t 发送的数据包数,$nr(t)$ 为该 IP 在时间点 t 接收的数据包数。待检测 IP 的服务率下降越大,该 IP 遭受 DoS 攻击或 DDoS 攻击的可能性越大。

DoS 攻击和 DDoS 攻击的另一个特点是,DoS 攻击或 DDoS 攻击发生时,会引起被攻击目的 IP 对应的子流流量增大。为此,关注流数量、包数量、字节数这三个流量行为特征以检测异常目的 IP。流数量为 NetFlow 流的数量。NetFlow 流是具有相同 Netflow 信息记录的单向数据流。流数量反映了一对源 IP 地址和目的 IP 地址间在传输层的流量大小。包数量指同一源 IP 发给同一目的 IP 的数据包的个数,反映网络层的流量大小。字节数指同一源 IP 发给同一目的 IP 的字节数量,反映物理层的流量大小。DoS 攻击或 DDoS 攻击发生时,通常会引起对应子流的一个或多个上述参数显著上升。

将各目的 IP 对应子流的这四个流量行为特征作为细粒度的网络流量行为特征参数,通过分析异常时间点的细粒度流量行为特征参数,可以确定异常目的 IP。本文中,使用参数值变化比率判断细粒度流量行为特征参数是否体现出 DoS 攻击和 DDoS 攻击特点。参数值变化比率 R 定义如下:

$$R = \frac{|A - \bar{A}|}{A_{\text{var}}} \tag{3}$$

$$A_{\text{var}} = \sum_{i=1}^{k} \frac{|A_i - \bar{A}|}{k} \tag{4}$$

式(3)中:A 为待检测 IP 在异常时间点的流量行为特征参数值,$\bar{A}$ 为待检测 IP 对应子流的流量行为特征参数值在历史时间窗内各时间点的均值,其中,历史时间窗由该异常时间点及其之前的 k 个时间点构成。式(4)中,A_i 为待检测 IP 在历史时间窗内各时间点对应子流的流量行为特征参数值。将式(3)、(4)描述的参数值变化比率 R 分别应用于流数量、包数量、字节数和服务率这四个流量参数,通过使用带标记的实际骨干网络流量数据进行训练,我们确定了如下异常目的 IP 判定准则:当待检测 IP 对应子流的流数量、包数量、字节数这三个流量行为特征参数中至少有一个参数在异常时间点呈现出显著上升的变化趋势,且其参数值变化比率 R 大于给定门限;同时,待检测 IP 对应子流的服务率在异常时间点呈现出明显下降的变化趋势,且其参数值变化比率 R 大于给定门限,则判定待检测 IP 为异常目的 IP。上述准则中的相关门限均通过训练得到。另外,式(4)中 k 值的选取需要保证参数值变化比率对各个流量行为特征参数值突然改变的反映能力。通过使用实际骨干网络流量数据进行训练,发现当 $k \geq 5$ 时,参数值变化比率对各个流量行为特征参数值的突然改变具有较好的刻画能力。

各异常时间点的异常目的 IP 检测流程如图 2 所示。首先,将该异常时间点上各目的 IP 对应的流量大小进行排序,并提取流量排名前 N 的目的 IP;然后,对于每个筛选出的目的 IP,提取出历史时间窗内各时间点包含该目的 IP 的子流;接着,计算子流的各流量行为特征参数值及其变化比率;最后,根据各目的 IP 对应流量的流量行为特征参数值变化趋势和变化比率,判定异常目的 IP。

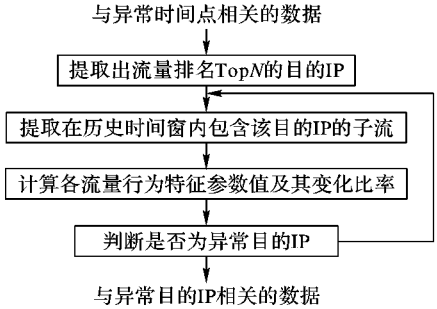

图 2 异常目的 IP 检测流程

2.4 异常流提取与攻击判定

异常流提取与 DoS&DDoS 攻击判定算法如下:

算法 2 异常流提取与 DoS&DDoS 攻击判定算法

输入 与异常目的 IP 相关的流量数据;

输出 与攻击相关的异常流量,DoS 攻击或 DDoS 攻击。

1) $q = q_0$; $p = p_0$;
2) 找出历史时间窗内与异常目的 IP 对应的源 IP 并提取出相关异常流;
3) for {所有待检测源 IP}
4) if 待检测源 IP 与异常目的 IP 之间流数量 > p & 流数量显著增加
5) if not α 攻击
6) 判定为 DoS 攻击;待检测源 IP 对应子流为与之相关的异常流;
7) end if;
8) end if;
9) if 存在与待检测源 IP 具有相似流量行为特征参数值变化趋势的其他源 IP
10) if 这些源 IP 与异常目的 IP 之间流数量 > q & 流数量显著增加
11) if not Flash Crowd
12) 判定为 DDoS 攻击;这些源 IP 对应的子流为与之相关的异常流;
13) end if;
14) end if;
15) end if;
16) end

其中,通过检查待检测源 IP 对应子流中涉及的端口号区分 DoS 攻击与 α 攻击。绝大部分 α 攻击都是对 5000 ~ 5050 以及 56117、1412 等特定端口进行攻击[12],而 DoS 攻击则主要对 0、110、113 以及 1433 等端口进行攻击。通过分析检查待检测源 IP 对应子流中涉及的自治域号区分 Flash Crowd 与 DDoS 攻击[12]。Flash Crowd 的攻击源在逻辑拓扑上往往集中于一个或几个自治域中,而 DDoS 攻击的攻击源则不具有该

特征。q_0 和 p_0 是通过使用带标记的实际骨干网络流量数据训练确定。

3　仿真结果与分析

使用美国 Abilence 网络[13] Losa 汇接点上的流量数据进行仿真实验。Abilene 网络使 Netflow 协议进行流量数据采集,采样率固定为 1%。出于隐私和安全考虑,采样流量数据 IP 地址的后 11 位二进制值在记录时被隐匿。Abilene 网络各汇接点的采样数据每 5 min 被记录一次,每个汇接点每天共有 288 个流量数据记录文件,即 288 个采样时间点。Losa 汇接点一周流量数据(2008-01-07—2008-01-13)的目的 IP 信息熵如图 3 所示。

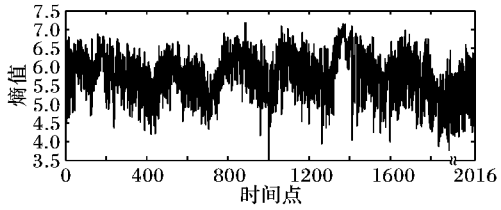

图 3　Losa 汇接点一周流量数据的目的 IP 信息熵序列

本仿真实验使用了美国 Abilence 网络[13] Losa 汇接点上的 1 月 1 日至 1 月 5 日的实际流量数据作为训练数据。根据文献[14]中所给方法,标出了训练数据中所有的 DoS/DDoS 攻击。通过分析在异常时间点计算得到的各参数值和在正常时间点计算得到的各参数值,确定了如下的参数设置。为保证尽可能小的漏检率,将 a_0 的值设为 0,即将所有目的 IP 熵小于前一时刻的时间点作为异常时间点。历史时间窗的宽度设为 5 个时间点。对于每个异常时间点,筛选出在该时间点上流量排名前 100 的目的 IP。之后,对于每个筛选出的目的 IP,提取出在历史时间窗内各时刻包含该目的 IP 的子流,并统计该子流的流数量、包数量、字节数和服务率四个流量特征。子流上流数量、包数量、字节数和服务率的参数值变化比率门限分别设为 2.2, 2.2, 2.2 和 6。判定为疑似 DoS 攻击的流数量门限 p_0 为 800,判定为疑似 DDoS 攻击的流数量门限 q_0 为 1 500。Losa 汇接点一周流量数据(2008-01-07—2008-01-13)的检测结果如表 1 所示。使用本文方法共检测出 21 个攻击。

为得到基于流量行为特征的 DoS&DDoS 攻击检测方法的性能指标,根据文献[14]中所给方法,标出了实验数据中所有的 DoS/DDoS 攻击。分析结果表明,本仿真使用的流量数据中共有 23 个 DoS/DDoS 攻击。将该结果与本文提出方法的检测结果进行比较,发现本文方法的漏检率为8.7%,误报率为 0%。另外,本仿真实验提取出的与 DoS/DDoS 攻击相关的网络流量全部正确。

为了进一步比较和解释以上检测结果,将它与基于小波的检测方法[9]进行比较。基于小波的检测方法共检测出 25 个 DoS/DDoS 攻击,其中 15 个为真正的攻击。表 2 列出了三种方法的检测结果。表 2 的结果表明本文方法的误检率明显低于基于小波的检测方法,因为本文方法在使用粗粒度信息分析以确定异常时间点的基础上,还对细粒度的流量行为特征参数进行分析,进一步确认了 DoS/DDoS 攻击。在漏检率方面,由于使用了较低的异常时间点判定门限,本文方法也明显低于基于小波的检测方法。

需要说明的是,虽然本仿真实验使用离线的 Netflow 流量数据来进行检测,但本文提出的方法能够满足在线检测的实时性要求。本仿真实验使用的 Losa 汇接点上一周流量数据,使用主流配置的个人计算机(处理器:奔腾双核 2.60 GHz,内存:2 GB)可以在 8 h 以内完成对 DoS/DDoS 攻击的检测和异常流的提取。

表 1　DoS 攻击和 DDoS 攻击检测结果

攻击时间点	攻击源	攻击目的	攻击强度(连接数)	攻击类型
116	129.49.88.0	220.113.8.0	1 581	DoS
229 ~ 232	129.79.136.0 等	220.113.8.0	1 522	DDoS
259 ~ 261	128.252.16.0 等	150.135.64.0	1 172	DDoS
267 ~ 268	198.202.112.0 等	129.114.48.0	1 770	DDoS
350 ~ 351	132.248.40.0 等	131.118.32.0	4 588	DDoS
357 ~ 358	132.248.40.0 等	131.118.32.0	24 985	DDoS
370 ~ 372	152.3.136.0 等	150.135.64.0	1 729	DDoS
407 ~ 409	203.72.64.0 等	130.85.24.0	2 989	DDoS
412 ~ 414	203.64.152.0	130.85.24.0	7 897	DoS
502 ~ 503	193.226.8.0 等	209.66.200.0	1 930	DDoS
573 ~ 577	202.120.8.0	128.186.120.0	28 487	DoS
573 ~ 577	202.120.8.0	128.186.120.0	28 487	DoS
619 ~ 620	152.3.136.0 等	150.135.64.0	1 249	DDoS
626 ~ 634	206.77.0.0	65.54.80.0	38 134	DoS
	65.54.80.0	206.77.0.0	41 314	DoS
	129.173.112.0	220.113.8.0	1 295	DoS
748	147.102.240.0 等	40.121.192.0	15 666	DDoS
755 ~ 757	202.120.8.0	130.15.96.0	23 836	DoS
763 ~ 768	202.120.8.0	130.15.96.0	25 991	DoS
1508	152.80.56.0	203.191.48.0	1 619	DoS
1662	202.249.24.0	195.176.176.0	8 255	DoS
1965 ~ 1969	163.27.176.0	81.180.216.0	83 505	DoS
2005	163.27.176.0	131.202.8.0	13 663	DoS

表 2　DoS/DDoS 攻击检测结果

方法	DoS/DDoS 攻击的数量	漏检率/%	误检率/%
本文方法	21	8.7	0
手工标定的结果(真实值)	23	—	—
基于小波的方法	25	34.8	40

本仿真实验的结果表明,基于流量行为特征的骨干网络 DoS&DDoS 攻击检测与异常流识别方法能有效检测出骨干网络中的 DoS/DDoS 攻击,并且在保证检测实时性的同时,能准确地提取出与 DoS/DDoS 攻击相关的网络流量。

4　结语

本文提出了一种基于流量行为特征的骨干网络 DoS&DDoS 攻击检测与异常流识别方法。该方法采用粗细粒度结合的思想,在粗粒度流量行为特征参数表现出异常的时间点分析细粒度的流量异常行为表征,从而在兼顾检测实时性的同时能够准确识别出与异常行为相关的流量。仿真实验结果验证了该方法的有效性。

参考文献:

[1] SMAHA S E. Haystack: An intrusion detection system[C]// Proceedings of IEEE 4th Aerospace Computer Security Applications Conference. Piscataway: IEEE, 1988: 37 - 44.

[2] KIM S S, REDDY A L N. Detecting traffic anomalies at the source through aggregate analysis of packet header data[EB/OL]. [2013-02-10]. http://www.ece.tamu.edu/~reddy/papers/skim_net04.pdf.

(下转第 2845 页)

侵采取相应的措施。

图 6 中,风险控制系统开启状态下,风险值小于报警阈值 0.2,系统不报警。当风险值大于报警阈值 0.2,系统开始报警。通过对比可知,相同网络风险条件下,风险控制系统的报警量明显低于 Snort 的报警量。由此可证明,在低风险情况下风险控制系统可以有效减少报警数量,降低误报率。

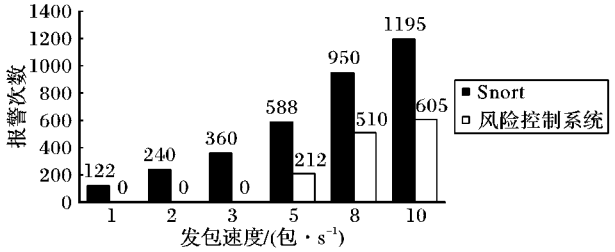

图 6　报警数量对比

3　结语

本文实现的基于抗体浓度的实时网络风险控制系统,在传统入侵检测系统 Snort 的基础上运用人工免疫理论中抗体浓度随网络入侵强度实时变化这一特点,实时、定量地计算出网络所面临的风险,解决了传统入侵检测系统无法定时定量地计算风险的问题。并通过设置阈值的方式,对不同风险的网络入侵采取通过、报警、丢包等有针对性的措施,同时此方式也能有效地降低 Snort 误报率。实验结果表明,本系统能够准确地反映出当前网络的实时风险状况,并且能够根据网络风险强度采取有效措施,同时降低了传统入侵检测系统误报率。

参考文献:

[1] LUO B, LEE D, LEE W C, *et al*. QFilter: fine-grained run-time XML access control via NFA-based query rewriting[C]// Proceedings of the 2004 ACM International Conference on Information and Knowledge Management. New York: ACM, 2004: 543 – 552.

[2] MURATA M, TOZAWA A. XML access control using static analysis [J]. ACM Transactions on Information and System Security, 2006, 9(3): 292 – 324.

[3] OZYER T, ALHAJJ R, BARKER K. Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criterion rule pre-screening[J]. Journal of Network and Computer Applications, 2007, 30(1): 99 – 113.

[4] XU Y, PAPAKONSTANTINOU Y. Efficient keyword search for smallest LCAs in XML databases[C]// Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2005: 527 – 538.

[5] 韦勇. 网络安全态势评估模型研究[D]. 合肥: 中国科学技术大学, 2009.

[6] 刘勃, 周荷琴. 基于贝叶斯网络的网络安全评估方法研究[J]. 计算机工程, 2004, 30(22): 111 – 113.

[7] 党德鹏, 孟真. 基于支持向量机的信息安全风险评估[J]. 华中科技大学学报: 自然科学版, 2010, 38(3): 46 – 49.

[8] 严俊龙, 李铁源. 基于 SVM 的网络安全风险评估模型及应用[J]. 计算机与数字工程, 2012, 40(1): 82 – 84.

[9] 王永杰, 鲜明, 刘进, 等. 基于攻击图模型的网络安全评估研究[J]. 通信学报, 2007, 28(3): 29 – 34.

[10] 方明, 徐开勇, 杨天池, 等. 基于攻击图的分布式网络风险评估方法[J]. 计算机科学, 2013, 40(2): 139 – 144.

[11] 陈亮, 潘惠勇. 网络安全风险评估的云决策[J]. 计算机应用, 2012, 32(2): 472 – 474, 479.

[12] 陈秀真, 郑庆华, 管晓宏, 等. 基于粗糙集理论的主机安全评估方法[J]. 西安交通大学学报, 2004, 38(12): 1228 – 1231.

[13] 李涛. 计算机免疫学[M]. 北京: 电子工业出版社, 2004: 119 – 131.

[14] 王益丰, 李涛, 胡晓勤, 等. 一种基于人工免疫的网络安全实时风险检测方法[J]. 电子学报, 2005, 33(5): 945 – 949.

[15] 李涛. 基于免疫的网络安全风险检测[J]. 中国科学 E 辑: 信息科学, 2005, 35(8): 798 – 816.

[16] 彭凌西. 基于 Snort 的实时危险评估模型[D]. 成都: 四川大学, 2008.

[17] LI T. An immunity based network security risk estimation[J]. Science in China Series F: Information Sciences, 2005, 48(5): 557 – 578.

(上接第 2841 页)

[3] 龚俭, 彭艳兵, 杨望, 等. TCP 流的宏观平衡性[J]. 计算机学报, 2006, 29(9): 1561 – 1571.

[4] LAKHINA A, CROVELLA M, DIOT C. Mining anomalies using traffic feature distributions[C]// Proceedings of the 2005 ACM SIGCOMM 2005. New York: ACM, 2005: 9 – 20.

[5] VELARDE-ALVARADO P, VARGAS-ROSALES C, TORRES-ROMAN D, *et al*. Detecting anomalies in network traffic using the method of remaining elements[J]. IEEE Communications Letters, 2009, 13(6): 462 – 464.

[6] ZIVIANI A, GOMES A T A, MONSORES M L. Network anomaly detection using nonextensive entropy[J]. IEEE Communications Letters, 2007, 11(12): 1034 – 1036.

[7] FEINSTEIN L, SCHNACKENBERG D, BALUPARI R, *et al*. Statistical approaches to DDoS attack detection and response[EB/OL]. [2013-01-20]. http://www.cs.unc.edu/~jeffay/courses/nidsS05/signal-proc/feinstein-stat-anal-03.pdf.

[8] BARFORD P, LLINE J, PLONKA D, *et al*. A signal analysis of network traffic anomalies[C]// Proceedings of the 2002 ACM SIGCOMM Internet Measurement Workshop. New York: ACM, 2002: 71 – 82.

[9] DAINOTTI A, PESCAPE A, GIORGIO V. Wavelet-based detection of DoS attacks[C]// Proceedings of the 2006 IEEE Global Telecommunications Conference. Piscataway: IEEE, 2006, 1 – 6.

[10] LI L, LEE G. DDoS attack detection and wavelets [J]. Telecommunication Systems, 2005, 28(3/4): 421 – 427.

[11] ZHOU Y J, HU G M. Network-wide anomaly detection based on router connection relationships [J]. IEICE Transactions on Communications, 2011, E94B(8): 2239 – 2242.

[12] LAKHINA A, CROVELLA M, DIOT C. Characterization of network-wide anomalies in traffic flows[C]// Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement. New York: ACM, 2004: 201 – 206.

[13] Internet2 Network[EB/OL]. [2013-01-20]. http://www.internet2.edu/network/

[14] LAKHINA A, CROVELLA M, DIOT C. Mining anomalies using traffic feature distributions[C]// Proceedings of the 2005 ACM SIGCOMM. New York: ACM, 2005: 9 – 20.