一种基于相似度的 DDoS 攻击检测方法

何慧，张宏莉，张伟哲，方滨兴，胡铭曾，陈雷
(哈尔滨工业大学 计算机信息安全研究中心，黑龙江 哈尔滨 150001)

摘 要：在分析了网络流量构成的基础上，提出了基于相似度的 DDoS 检测方法。这种方法不是简单的根据流量的突变来检测网络状况，而是从分析攻击对流量分布的影响着手。首先对网络流量进行高频统计，然后对其相邻时刻进行相似度分析，根据相似度的变化来发现异常。从大量的实验结果可以看出基于相似度的检测方法能够比较有效的发现大流量背景下，攻击流量并没有引起整个网络流量显著变化的 DDoS 攻击，因此更适合大规模网络的异常检测。

关键词：异常检测；DDoS 检测；相似度；高频统计
中图分类号：TP 393 **文献标识码：**B **文章编号：**1000-436X(2004)07-0176-09

A DDoS intrusion detection method based on likeness

HE Hui, ZHANG Hong-li, ZHANG Wei-zhe, FANG Bin-xing, HU Ming-zeng, CHEN Lei
(Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin 50001, China)

Abstract: The paper proposes a DDoS intrusion detection method based on likeness through analyzing characteristics of the network traffic. This method detects the state of network not by burst net flow but by the impact of the traffic distribution. First, we focus on the high frequency statistics result, then analyze its likeness of adjacent time and detect the abnormality. According to a great number of experiments, the intrusion detection method based on likeness can find out the DDoS intrusion against the large scale network traffic, which does not arouse the sharp changes of the network traffic.

Key words: anomaly detection; DDoS detection; likeness; high frequency statistics

1 引言

随着 Internet 的日益普及与发展，网络与人们日常生活的关系越来越密切。但 Internet 是一把双刃剑，它给我们带来便利的同时，也给我们带来了诸多问题。在众多的问题当中，网络安全是首要问题。目前网络入侵的频率越来越高，入侵的危害性也越来越大，尤其是消耗网络资源的入侵行为愈演愈烈。而网络带宽作为一种宝贵的资源，直接影响到人们访问网络的质量。因此，如何保证带宽资源的有效利用，及时发现和防御恶意消耗网络带宽的行为是一个重要的研究方向。

从影响网络整体的性能来看，DDoS 是 Internet 目前面临最严峻的威胁之一。统计表明，

收稿日期：2004-02-10
基金项目：国家“863”高技术研究发展计划研究基金资助项目（2002AA142020）

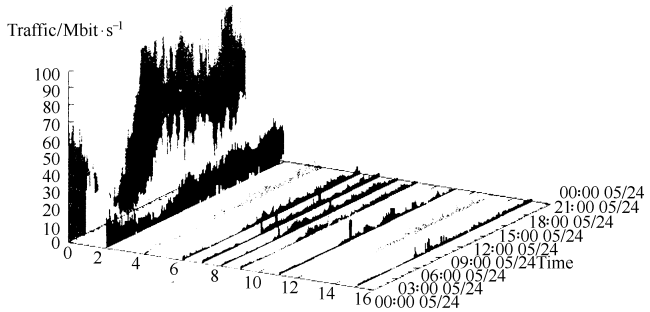
近年来 DDoS 攻击的数量一直呈快速增长趋势[1]。DDoS 攻击往往采用伪造、随机变化 IP 地址和端口方式，利用 TCP/IP 自身缺陷，产生大量合法数据包来攻击目标，使随机攻击流特征随机变化[2]。基于以上特征利用原有特征提取方式已经很难达到检测目的,而对于已经提出的马尔科夫模型[3]、神经元网络[4]等监测手段又很难适应本课题研究的大流量背景的需要。

因此，本文提出了更适合于大规模网络背景下的流量检测技术，即基于网络流量分布的相似度的统计方法。基于相似度的异常检测方法能很好地发现那些不引起流量显著变化的 DDoS 攻击，而在大规模网络下很多攻击开始都被大背景流量所掩盖，在这种情况下快速、及时地发现攻击将是检测 DDoS 攻击的关键所在。通过对校园网的大量长期实验发现，在正常情况下，网络流量的分布是相对稳定的，高频统计结果维持一个动态平衡，而当受到 DDoS 攻击时则会破坏这种稳定性和平衡状态。所以，本文提出对网络流量高频统计结果的相似度分析方法，将能够快速、有效的发现大流量背景下的 DDoS 攻击。

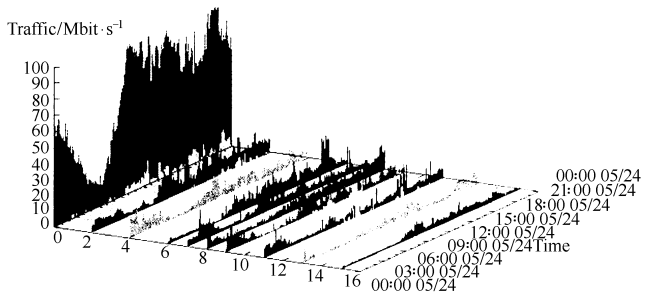
2　对流量的高频统计

为了了解真实网络流量的分布情况，本文对校园网出入口的实际流量从源 IP，目的 IP，源端口，目的端口四个方面进行了聚集分析。本文采用了 aguri[5]作为流量聚集工具。

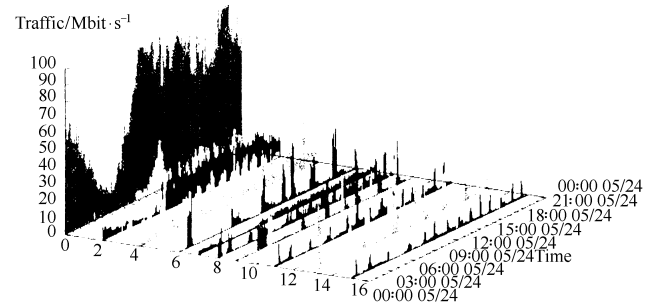
图 1 是利用 aguri 对某一时期校园网流量聚集结果显示。



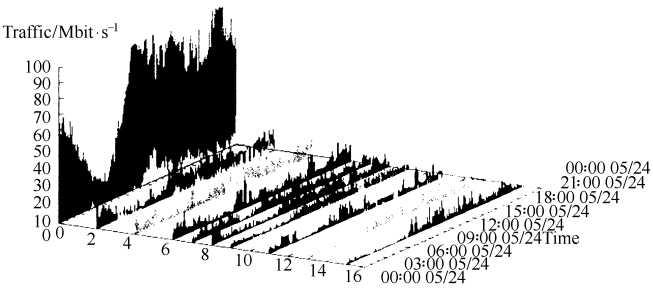
(a) 源地址聚集图



(b) 目的地址聚集图



(c) 源端口聚集图



(d) 目的端口聚集图

图 1　校园网流量聚集图

从图 1(a)中看出，对源 IP 进行流量统计，服务器 IP 能够作为高频事件被统计观察到。从图 1(b)目的地址流量聚集的结果来看，目的地址的分布是比较分散的，因此可以利用目的地址聚集的这种分散特性来发现 DDoS 攻击。从图 1(c)源端口聚集的结果来看，将能聚集出那些著名服务端口如 20（FTP data），80（HTTP）。从图 1(d)目的端口聚集的结果来看，发现端口的分布也是很分散的，因此可以利用目的端口聚集的这种分散特性来发现蠕虫攻击或某种固定端口 DDoS 攻击。

以上分析结果表明，首先了解网络流量的分布情况对进一步发现网络异常状况很有帮助，特别是流量的目的地址分布和目的端口分布。然后，采用相似度的方法对流量分布的聚集结果进行分析，尽早发现被大流量背景淹没的 DDoS 攻击。

3 相似度的分析方法

3.1 相似度的概念

相似度是概率统计中相关系数，是用于刻画两个随机变量分布的相似程度。其定义如下：

定义 1 量 $E\{[X-E(X)][Y-E(Y)]\}$ 称为随机变量 X 与 Y 的协方差，记为 $Cov(X,Y)$，即 $Cov(X,Y) = E\{[X-E(X)][Y-E(Y)]\}$。

定义 2 相关系数 $P_{xy}=\dfrac{Cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}}$，其中 $D(X)$，$D(Y)$ 分别为随机变量的方差。

本文用相似度的概念来刻画相邻时刻高频统计结果的相似程度。即在某相邻两时刻 T_1，T_2，分别做流量的高频统计，然后对聚集的结果进行相似度的分析。主要关注相邻时刻网络业务流量百分比在各个 IP 上的变化情况，即对 T_1 和 T_2 时刻的数据，作如下处理：

1) 列出 T_1 时刻的 IP 及其百分比数据。

2) 相对 T_1 时刻每个 IP 列出在 T_2 时刻的百分比数据，如果在 T_2 时刻不存在，其百分比数据定义为 0；(因为如果这个 IP 在 T_2 时刻未出现在前 N 名中，那么它的流量百分比应该是很小的一个值，近似为 0 是合理的)。

3) 对过程 1 和过程 2 得到的两组百分比数据求相关系数，得到参数 P_1。

4) 将上述 T_1 和 T_2 时刻的数据对调（即：T_1 时刻的数据看成 T_2 时刻的数据，T_2 时刻的数据看成 T_1 时刻的数据），重复过程 1），2），3）得到参数 P_2。

P_1 和 P_2 就是反映 T_1 和 T_2 时刻的流量分布相似程度的量值，P_1 和 P_2 接近 1 表示 T_1 和 T_2 时刻的分布越相似。每间隔一段时间统计一次这样的数据，通过比较相邻数据的相似度来发现相邻时刻的流量分布变化状况。

3.2 相似度的意义

如上文所述，每隔一个固定时间段统计一次数据，每次的 IP 项和其流量百分比项都可能发生变化，通过相似度的刻画就可以发现这种改变。这种变化有以下几种形式：1）前一时刻（以下记为时刻 T_1）某个 IP 在下一时刻（以下记为时刻 T_2）不存在或其流量百分比淡出前 N 位，这时在 T_2 时刻此 IP 项和对应的百分比项将都不存在；2）T_1 时刻的某个 IP 流量在 T_2 时刻发生增减的变化，此时这个 IP 在 T_2 时刻仍然存在，但其流量百分比发生了相应的增减变化。本文想要解决的问题就是及时发现和定位那些引起流量的剧增和骤减变化的 IP。

传统上解决此问题有两种途径，百分比的绝对值变化和百分比变化率。虽然这两种方法在一定程度上都能解决本文需要解决的问题，但是这两种方法本身都存在一定的缺陷。百分比的绝对值变化方法，主要定位在差值的变化上，不关心所比较基数的大小，会漏掉基数小

的大变化，而此种变化是本文流量检测关心的重点；判断百分比变化率的方法，主要定位在变化率上，这种方式又会忽略数值大的大变化。后文将进一步分析这两种方法的缺陷所在。

本文采用的相似度的方法既能很好的发现激增和骤减的现象发生，同时又可以准确的定位到发生激增和骤减现象的具体 IP。解决方案是：对两列数求相关系数，当相关系数超过预先设定的阈值时，认为异常。然后定位发生异常的具体 IP。本文采用的方法是分别将每个 IP 在 T_2 时刻的流量百分比数值还原成 T_1 时刻，同时再求两列数的相关系数，这时当相关系数发生变化最大的 IP 即是所求的导致异常现象发生的 IP。

下面考察一个例子，对这两组数据 X_{t1} 为（15, 10, 8, 7, 5, 3, 2, 1, 1, 0.8, 0.8, 0.7, 0.6, 0.6, 0.5, 0.3, 0.2, 0.1, 0.1, 0.1）和 X_{t2} 为（20, 11, 9, 5, 7, 3, 4, 0.8, 1, 0.6, 0.7, 0.8, 0.4, 0.5, 0.6, 0.2, 0.3, 0.2, 4.1, 0.1），得到的他们的相关系数为 0.960759，根据预定的阈值假设此相关系数超过了阈值，发现异常，然后定位具体的 IP，采取还原具体 IP 百分比的方法，忽略中间的百分比变化小的 IP 还原情况，对第一个 IP 的还原，求得的相关系数为 0.968970，对倒数第二个 IP 的还原得相关系数为 0.978467。可以看出传统的绝对值变化方法会将问题定位在 15->20,而实际分析表明，应该定位在 0.1->4.1。这个才是真正发生问题的 IP。上述分析结果表明，相似度的方法弥补了第一种方法的缺陷。

接着考察第二个例子，对两组数据 X_{t1} 为（15, 10, 8, 7, 5, 3，2，1, 1，0.8, 0.8, 0.7, 0.6, 0.6,0.5, 0.3, 0.2, 0.1, 0.1, 0.1）和 X_{t2} 为（5, 11, 9, 5, 7, 3, 4, 0.8, 1, 0.6, 0.7, 0.8, 0.4, 0.5, 0.6, 0.2, 0.3, 0.2, 1.0, 0.1），求得的相关系数为 0.803253，根据预定的阈值同样假设此相关系数超过阈值，发现异常。接下来采用还原 IP 百分比的方法来定位具体的发生问题的 IP，忽略中间的百分比变化小的 IP 还原情况，对倒数第二个 IP 还原，得到相关系数为 0.805832，对第一个 IP 还原得到相关系数为 0.979501。显然，传统的百分比变化率会定位在 0.1->1.0 上，而实际表明真正可疑 IP 是 15->5，可见通过相似度的方法，找到了真正发生问题的 IP。上述分析结果表明，相似度的方法弥补了第二种方法的缺陷。

综上所述，本文采用相似度的方法能够灵敏准确的反应流量百分比的激增和骤减的变化，并且能够准确的定位到发生问题的具体 IP，具有很大的优越性，能够解决前面提出的问题。

3.3　相似度的分析

从目前校园网出入口流量分布来看，少数几个 IP 占了总流量的 50%以上，而且相当稳定，它们每次都出现在高频统计中前几位，由于所占比例很大，这就决定了相似度的变化范围不能很大，从而降低了这种相似度判定方法的灵敏度。

可以从以下几方面利用相似度分析：

1) 对源地址做相似度分析：由于大量的数据往往是从服务器端返回的，如果以源地址做高频统计，往往得到的是服务器的 IP。可以通过相似度的变化（骤减变化）来发现 down 掉的服务器，这可能是攻击造成的后果。

2) 对目的地址做相似度分析：从高频统计实验观察，流量目的 IP 的分布并没有表现像源 IP 那样明显的聚类行为。通常相似度比较低，当发生攻击时，被攻击 IP 的流量会显著增加，而通常攻击会持续一定的时间，导致这个 IP 在后继的高频统计中仍然出现且占较大比例，从而相似度增大。这样可以通过相似度的变化过程来判断攻击。

3) 对源端口的相似度分析：源端口的分析与源地址分析类似。如果是骤减变化，那么有可能是受攻击后 down 机，同时通过查找流量骤减的端口，可以推断出受攻击的服务器类型；

4) 对目的端口的相似度分析：由于 DDoS 攻击通常采用随机端口，所以对目的端口的相

似性分析通常不能发现攻击，但蠕虫因为是针对特定的系统漏洞，通常只对漏洞相关的端口产生流量。因此目的端口相似度的变化过程往往可以用来发现蠕虫。

5) 对协议分布的相似度分析：那些利用固定协议的进行 DDoS 攻击的行为，可能导致协议分布相似度发生较大变化。

6) 对包尺寸分布的相似度分析：蠕虫爆发时往往是某种类型的包急剧增多，而这种包的大小相差不大，因而可以导致包尺寸分布的相似度发生较大变化。

4 基于相似度的 DDoS 异常检测系统

鉴于目的 IP 的相似度对 DDoS 攻击的敏感性，本文主要实现了基于目的 IP 相似度的异常检测系统（如图 2）。

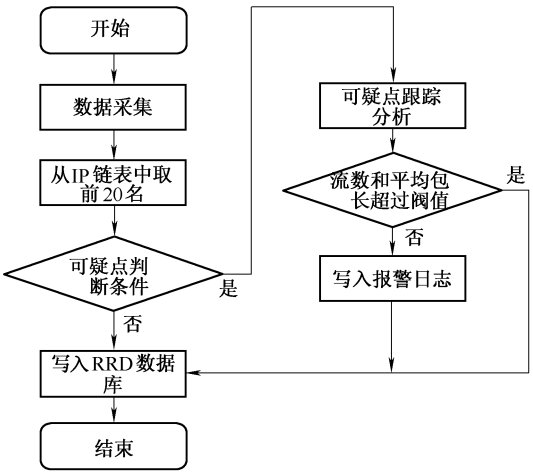


图 2 异常检测流程图

从整个系统流量分析过程来看，首先，从数据采集模块获得原始数据包，并对其进行高频统计，计算按流量排序的前 N 位目的 IP。然后，根据可疑点的判断条件，调用跟踪分析模块作判定。判定后，将数据写入 RRD 数据库，并根据判定结果决定是否产生报警。整个系统的关键模块集中在“可疑点的确定”和“流数、平均包长的判定”。

可疑点确定：分析一次 DDoS 攻击相似度的变化过程，T_i 时刻 DDoS 攻击导致某 IP 流量激增，导致相似度减小，这种变化分两种情况，一种是受攻击的 IP 上次统计中不在前 N 名中，但由于攻击在本次统计中进入流量前 N 名，致使两次流量分布很不相同，相似度减小；另一种是受攻击 IP 已经在上次统计的前 N 名中，但攻击使其相对于前 N 名中其他 IP 占有的流量比例显著变化，导致相似度的减小。由于攻击的持续，在 T_{i+1} 时刻受攻击 IP 继续在前 N 名中占有较高比例，导致相似度的值持续增大，接着 T_{i+2} 时刻相似度趋于稳定，直到 T_m 时刻攻击结束，受攻击的 IP 流量骤减，相似度会因前 N 名流量分布的再度变化而降低。

基于以上分析可以总结出可疑点的判断条件，采用相似度 P_2 的计算方法，$T_1,\cdots T_i,\cdots T_n$（$n<m$）这 $n+1$ 个采样点对应的相似度分别为 $P_1,\cdots P_i,\cdots P_n$。条件如下：

1) $p_i - p_{i+1} > q$，表示攻击开始时相似度的下降趋势；

2) $p_{i+2} - p_{i+1} > bq$，其中 $0<\hat{a}<1$ 表示攻击持续时相似度的上升趋势；

3) $|p_{j+1} - p_j| <$ ，其中 $i+2< j< n$ 表示攻击持续时相似度趋于稳定。

其中，q是指定的下降变化阀值，b是参数，e是攻击时的稳定阈值。如果 T_n 时刻满足这些条件，则 T_n 是可疑点。

为了更好地确定q 的值，本文采用了一种自适应的确定方法。用 ΔP_i 实际测得相似度的变化量，ΔQ_i 表示相似度变化量的估计值。

其计算公式如式（1）、（2）所示

$$DP_i = p_i - p_{i+1} \tag{1}$$

$$DQ_i = aDQ_{i-1} + (1-a)DP_i \tag{2}$$

由于只考虑下降趋势的影响，所以只有当 $\Delta P_i>0$ 时才用式（2）对 ΔQ_i 更新，否则 $\Delta Q_i=\Delta Q_{i-1}$。这样可以将上面的判定条件修改为

$$DP_i > DQ_i \tag{3}$$

$$\frac{1}{n-k+1}\sum_{j=k}^{n} p_j - p_1 > bDQ_i\text{，}\quad 0<b<1 \tag{4}$$

$$\left|DP_j\right| < gDQ_i\text{，}\quad k<j<n \tag{5}$$

对 2）和 3）的修改主要是从 T_k 时刻开始计算上升趋势和平稳趋势，这是由于在攻击开始时段，上升趋势和平稳趋势表现得并不明显，因此我们跳过攻击开始的前几个时刻，T_k 时刻开始计算。而且平稳阈值和上升阈值都归结到下降阀值上，用b和g两个参数来调整。

虽然通过相似度的变化可以发现网络的异常状况，但前面也提到了如果两台拥有高带宽的主机之间进行大文件传输，也会对相似度造成较大影响。为了识别出这种情况，本文采用一种附加的跟踪分析可疑 IP 的策略，这部分功能是由“ 流数、平均包长的判定 ”模块实现的。

流数、平均包长的判定：发现异常后进行可疑点的跟踪分析，通过比较 T_i 时刻和 T_{i+1} 时刻找出对相似度变化贡献最大的 IP，即流量变化最大的 IP，然后区分该 IP 是正在进行大文件传输，还是受到攻击而导致流量的剧变。通过分析单个 IP 的流量构成，可以很容易区别出高带宽大文件传输和 DDoS 攻击。DDoS 攻击时一般采用随机源 IP 来隐藏攻击源，所以流数多，且小包居多或者包长随机；而高带宽大文件传输时流数少，基本大包传输（1k 以上）。因此，区别这两种情况方法很简单，只需要分析这个 IP 在采样时间内的源 IP 数目和平均包长，如果超过阈值则可认为遭到攻击。本系统主要分析 T_{i+n+1} 时刻可疑 IP 的平均包长和访问该 IP 的源 IP 数目。每个采样周期的分析流程如图 2，下一个周期重复此过程，实现 DDoS 攻击检测。

5　模拟实验及结果分析

局域网模拟测试环境的构建，主要设备由一台 Cisco2950 交换机,两台曙光服务器(CPU PIII 800 X 2，内存 2GB，17GB SCSI 硬盘)作为流量分析机和制造背景流量的发包机，均为百兆比特网卡，还有两台 PC，一台作为攻击源，另一台作为受害者。将发包机和受害者 PC 所接交换机的端口流量映射到分析机的端口上。具体拓扑如图 3。

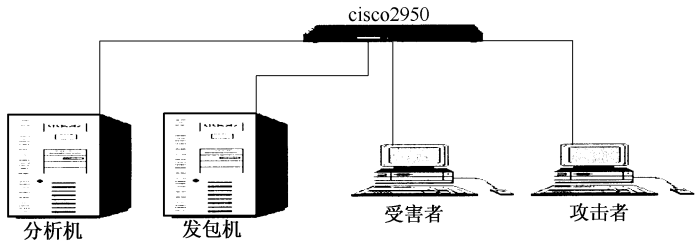


图 3 实验拓扑图

背景流量是哈尔滨某网络公司部分时期的 Internet 数据，流量大约 6~10Mbit/s。用 Netpoke 回放其数据作为背景流量。DoS 攻击工具采用 Hgod，该工具可以用最大线程数 100 向目标机发送指定协议，指定包长的数据包，而且可以采用随机 IP 源。

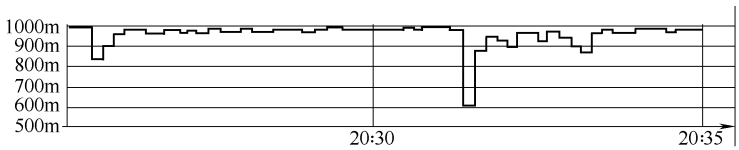
基于相似度的异常检测方法最大的优点是能够发现那些并不引起总流量显著变化的攻击，由于大规模网络背景流量很大，许多 DDoS 的攻击流量并不足以引起总流量的显著变化，但这些攻击流量却能给目标主机或目标主机所在的网络产生巨大影响，比如假设一网络出入口带宽 500Mbit/s，网内一服务器通常对外提供 5Mbit/s 的链接处理能力，一次 DDoS 攻击使该服务器流量增加到 10Mbit/s，这对总流量来所增加的幅度仅仅是 1%，可以认为是正常的流量波动，但在服务器来看流量增加了 100%，这可能是服务器难以承受的，特别是在背景流量越大的情况下，总体流量掩盖攻击的能力就越强。针对两种攻击情况分别做了试验，如表 1 所示。

表 1 实验数据表

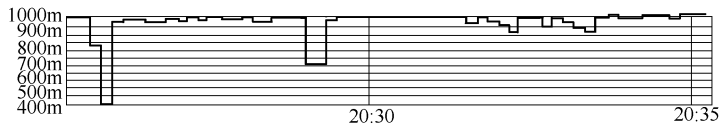
	实验一	实验二
实验开始时间	2003-06-01 20:26:13	2003-06-01 21:22:55
背景数据源	2003-05-19 日数据	2003-05-19 日数据
总流量（攻击前）	约 10Mbit/s	约 11Mbit/s
攻击开始时间	2003-06-01 20:29:02	2003-06-01 21:28:24
攻击结束时间	2003-06-01 20:31:26	2003-06-01 21:29:36
攻击强度	2 线程	10 线程
总流量（攻击后）	约 12Mbit/s	12~14Mbit/s
攻击前受害者所占流量比例	0%	4%
攻击后受害者所占流量比例	10%~14%	10%
其他 IP 所占的最大比例	6%	5%
相似度	0.66	0.82

实验的结果如图 4(a)，4(b)，4(c)所示，图 4(a)表示的相似度 P_1 在攻击过程中的变化情况。图 4(b)表示相似度 P_2 在攻击过程中的变化情况。图 4(c)反映的是总流量的变化曲线。从图 4(c)中可以看出在整个攻击过程中总流量的变化并不大，但在图 4(a)和 4(b)中关于目的 IP 的相似度都有一个明显的下凹，在两幅图最左边的下凹是由于开始放背景流量，使得网络中流量构成发生了巨大变化引起的，跟攻击无关，这也从另一个方面说明了相似度对流量的内部结构

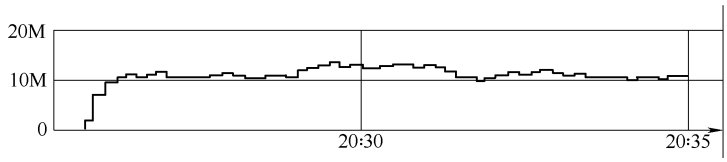
很敏感。图 4(a)的下凹发生在攻击结束时，这是因为它反映 P_1 的变化，从前面相似度的分析得知 P_1 对新 IP 加入引起的变化并不敏感，所以在攻击开始时刻并有很大的变化，但是在攻击结束时受害者 IP 的流量所占比例减小，退出了前 N 名，P_1 对这种变化很敏感，表现出剧烈的变化。图 3(b)的下凹发生在攻击开始时，这是因为它反映 P_2 的变化，从前面相似度的分析得知 P_2 对新 IP 加入引起的变化很敏感。



(a) 相似度 P_1 的变化



(b) 相似度 P_2 的变化



(c) 原始流量

图 4　实验结果图

从图 4(a)和 4(b)中可以观察到目的 IP 的相似度 P_2 稳定地保持在一个很高的水平上，这与大规模网络的相似度分布可能有些差异，在向该公司咨询后得知，所采集的数据的网络主要是由专线用户构成，所以导致了这种相似度分布。

目前，检测 DDoS 攻击的方法,有基于统计分析的方法，基于规则检测的方法，这些方法可以检测出一些采用简单、著名工具的 DDoS 攻击[6]，而对于采用其他方式的 DDoS 攻击，就显得无能为力。而基于“异常检测”和“特征检测”相结合的方法[7]，对于小规模网络检测比较有效，但对于大流量背景下的检测，尤其是在攻击流量被背景流量淹没的情况下，也有其固有的局限性，即依赖于攻击流量是否达到一定规模。而本文提出的相似度方法，是基于大规模网络流量的自相似特性[8]，采用相似度的分析方法发现流量异常，以达到提前检测攻击的目的。

6　结论

基于校园网大量实验发现流量的高频统计结果是相对稳定的，当受到 DDoS 攻击时这种稳定性遭到破坏。相似度可以用来表征高频统计结果的变化程度，并且能准确的定位导致剧变的因素。本文采用基于相似度的方法检测 DDoS 攻击，实验证明可以发现那些并不引起总流量显著变化的攻击。

参考文献：

[1]　CERT Advisory CA-20000-01. Denial-of-service developments[EB/OL]. http:// www.cert.org/ advisory/ CA-2000-01.html.2000.

[2] 李小勇，刘东喜. DDoS 防御与反应技术研究[J]. 计算机工程与应用，2003, 12(4):12-15.

[3] FOX K, HENNING R, REED J, SIMONIAN R. A Neural Network Approach Towards Intrusion Detection[R]. Harris Corporation, 1990.

[4] YE N. A markov chain model of temporal behavior for anomaly detection[A]. Workshop on Information Assurance and Security[C]. West Point,NY, 2000.

[5] KAIZAKIR. Aguri: an aggregation-based traffic profiler[EB/OL]. http://www.csl.sony.co.jp/person/kjc/kjc/software.html.

[6] 苏更殊，礼之堂. DDOS 攻击的分析、检测与防范技术[J]. 计算机工程与设计, 2002, 11(23):5-8.

[7] 李旺，吴礼发，胡谷雨 . 分布式网络入侵检测系统[J]. 软件学报, 2002, 13(8): 1723-1727.

[8] WILLINGER W. A bibliographical guide to self-similar traffic and performance modeling for modern high-speed networks[A]. Stochastic Networks :Theory and Applications[C]. 1996. 339-366.

作者简介：

何慧（1974-），女，吉林省吉林市人，哈尔滨工业大学博士生，主要研究方向为计算机网络安全、网络测量和网络模拟。

方滨兴（1960-），男，江西万年人，博士，研究员，中国科学院计算技术研究所博士生导师，哈尔滨工业大学兼职教授、博士生导师，国家计算机网络应急技术处理协调中心主任，主要研究方向为信息安全、计算机网络、并行计算。

张宏莉（1973-），女，吉林榆树人，博士，哈尔滨工业大学计算机科学与技术学院副教授，国家计算机网络与信息内容安全重点实验室副主任，主要研究方向为网络与信息安全、网络测量、网格计算等。

胡铭曾（1935-），男，江苏江阴人，哈尔滨工业大学教授、博士生导师，主要研究方向为高性能计算机体系结构、并行计算、计算机网络与信息安全。

张伟哲（1976-），男，河北吴桥人，哈尔滨工业大学助教、博士生，主要研究方向为网络安全和并行计算技术。

陈雷（1978-），男，四川达川人，哈尔滨工业大学计算机专业硕士生，主要研究方向为网络安全技术。