

分布式拒绝服务的可视分析

张毅凡, 董笑菊

(上海交通大学电子信息与电气工程学院, 上海 200240)

摘要: 首先, 对网络日志中提取出的 IP 地址进行可视分析, 设计完整的可视方案, 通过采取有效的可视化方法, 利用网页语言工具, 将网络日志数据以图形的形式有效表示出来。其次, 使用 IP 地址作为分析中心, 分别以源 IP、目的 IP 以及二者之间关联作为各个视图的重点, 向用户展现不同视角, 进而显示更多细节, 发现数据间的隐藏关联。在此方案的可视设计中, 加入了大量交互设计如联动等, 提高了视图的显示效率及可用性, 使各个视图间的关系更加清晰。最后, 分别采用 DDoS 发生后提取的实际网络日志与未发生时的网络日志作为源数据引入设计, 通过对比, 显示设计的实用效果及实际意义。

关键词: 网络安全; 数据可视化; 分布式拒绝服务攻击; IP 地址

中图分类号: TP311

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00135

Visualization analysis and design of DDoS attack

ZHANG Yi-fan, DONG Xiao-ju

(School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: Firstly, the IP address of the Web log were visualized, and an integral system was presented by using proper visualization methods. Secondly, the whole system was related to the IP address, containing source IP address, target IP address and their relationship respectively. It provided users with different views of data, which could show more details and undetected relations among massive data. Besides, some interactions were added into the system, which made it more effective and useful. Finally, it ended up with the comparison of the systems when loading data with the DDoS attack and without it. It made much sense in the application field.

Key words: network security, data visualization, DDoS attack, IP address

1 引言

可视化是利用计算机图形学和图像处理技术, 将数据转换成图形或图像在屏幕上显示出来, 并进行交互处理的理论、方法和技术^[1]。可视化概念的首次提出是在 1987 年美国国家基金会举办的可视化会议上^[2], 它将可视化定义成一种将抽象符号转换为具体几何关系的计算方法, 来弥补科学研究方法的不足。随后的二十几年, 随着

计算机技术的发展, 可视化开始与之结合起来。到近几年, 大数据的研究开始引入可视化, 推动可视化发展走向高峰。

网络安全可视化是一种利用可视化技术分析网络情况的应用。由于网络情况常用网络日志数据来表示, 该数据量大且复杂, 只对数字信息进行观察是不可行的。如果利用可视化处理多维复杂数据的能力, 将抽象的攻击数据以图形的方式展示出来, 那么就可以帮助网络管理者或研究者

收稿日期: 2016-12-03; 修回日期: 2017-01-05。通信作者: 董笑菊, xjdong@sjtu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61100053)

Foundation Item: The National Natural Science Foundation of China (No.61100053)

及时观察该网络的情况并识别异常信息,进而对网络攻击做出有效防护。此外,利用历史网络攻击数据还可以根据已出现的网络攻击情况总结规律,做出主动的防御,如对易受攻击的服务器或主机重点防御等。它不仅能将大量抽象的数据形象地转化成普通用户更易接受的图形图像,减轻了研究人员对大量数据分析的负担,避免因缺乏部分专业知识而造成分析偏差,还帮助网络管理者或研究者统计、分析并筛选所用数据,将一些重要细节进行标记,以使用户发掘隐藏的信息,同时赋予用户足够的自由度,允许用户多视角观察选定数据。

分布式拒绝服务(DDoS, distributed denial of service)攻击可视化是网络安全可视化的应用之一。Arbor networks 在其最新的《Worldwide Infrastructure Security Report》中指出,分布式拒绝服务攻击是最常见的攻击方式之一,且攻击次数逐年增长,并在2015年创下了单次攻击强度超过500 Gbit/s的记录,也成为了政府类网站的一个巨大安全隐患^[3]。因此,对DDoS攻击的可视化分析将对网络安全的研究产生意义,并将可视化技术的应用扩展至网络安全领域。在网络安全方面,研究者要了解DDoS攻击的原理与特点,根据所要研究的范围或区域选取合适的数据集,并明确着重提取的数据属性。可视化重要的特点之一是交互性,能够更好地实现数据间的关联与筛选。

目前,对DDoS攻击的研究主要集中在2个方面:一是对DDoS攻击监测方法的研究;二是对DDoS攻击防御方法的研究。在DDoS攻击的监测方法上,基于IP地址、流量、端口的监测算法是3种最常见的方法。Zhang等^[4]在论文中提出了一种基于IP行为的算法。通过比较TCP中的SYN、SYN/ACK、ACK及RST等分组,计算出客户端与服务端表示流量行为的参数值,进而标定折线图确定可疑IP地址。Mopari等^[5]在论文中指出,IP欺骗经常被DDoS攻击者使用,因此可以利用攻击者不能控制跳数的特点,生成一幅IP到条数的映像表(HCF, hop count filter)。根据该表格可以区分出攻击者的伪IP地址,达到检测DDoS攻击的目的。颜若愚^[6]提出一种基于流量矩阵的DDoS攻击监测方法,在DDoS攻击的防御

方法上,除防火墙等基础防御,最有针对性的是关闭敏感端口与过滤部分可疑IP。王伟等^[7]提出了基于端口监测的防御策略,通过获取IP分组中TCP分组头的端口信息,判定字段状态,进而判定是否丢弃该分组,实现对敏感端口的过滤。

而针对网络安全可视化的研究也在进行中,如Hideki等^[8]设计实现的SnortView系统。它是一种实时监控系统,可以将探测到的可疑IP以IP矩阵的方式列出。矩阵的横纵坐标分别表示时间轴与外部地址,矩阵中的点代表该时刻该位置受到了攻击。不同类型的攻击用不同形状的点表示,点的位置、颜色及形状等用于描述检测到的网络攻击细节。Chris等^[9]提出获取防火墙的日志信息作为基础数据进行可视化,并利用图、平行坐标、矩阵等各种基础图元对不同的网络攻击类型进行可视化。

本文的研究目的与意义是将对单一类型网络攻击的整理分析与可视化技术结合,通过选取适当的可视化方法,设计完整的用于DDoS攻击检测的可视化方案,大大减轻了研究者对于数据分析的工作难度;人机交互的简易性也使研究者更易发现数据间的潜在关系,发掘出数据潜藏的特点,为对DDoS攻击的主动防御做好准备,发挥出网络安全与可视化技术结合的真正作用。

为了实现对DDoS攻击的可视化分析,本文设计了一个针对DDoS攻击的可视化系统,根据网络日志中的IP地址等信息,检测并分析该网络是否遭受该种攻击,有助于分析攻击特点并及时采取相应的防御措施。此外,在系统实现方面,各视图间交互的运用,让各图间的关系更清晰,在帮助用户处理数据后,将重点数据与关系清楚标出,有助于用户的分析,还赋予了用户较大的自由度,让用户可以自行选择不同维度观察分析数据。同时,设计的各视图间采用多视角、多维度展示数据的特点,挖掘数据间的隐藏关系。

2 DDoS攻击可视化系统设计

拒绝服务(DoS, denial of service)攻击是指攻击者利用网络协议的缺陷进行攻击或直接消耗被攻击目标的资源,使被攻击者系统停止响应,进而无法正常使用。近年来,随着网络带宽的提

高、服务器处理速度的增长与内存的增加,出现有效的 DoS 攻击变得越来越困难,由此产生了更“高级”的攻击方式——分布式拒绝服务攻击。分布式拒绝服务攻击,指借助于客户/服务器技术,将多个计算机联合起来作为攻击平台,对一个或多个目标发动 DDoS 攻击,从而成倍地提高拒绝服务攻击的威力^[10]。DDoS 的攻击方法如图 1 所示。

2.1 设计需求

为了设计一个完整的 DDoS 攻击可视化系统,首先要明确该系统的设计目的,即用户需求。在确定用户需求之前,要先明确用户的群体。对于该系统的使用人群,大致分为 2 类:一类是对网络安全知识不甚了解,但想对所处网络环境有简单了解的普通用户;另一类是当前网络的监控者或研究者。对于普通用户来说,他最想得知该网络环境是否正常,是否出现 DDoS 攻击,即对网络环境整体情况的了解;对网络监控者来说,除了网络的整体情况,他还注重该网络环境下的各项细节,如易受攻击位置、攻击时刻、攻击强度、攻击位置的变化特点等,以便于监控者对该网络环境中受到攻击的情况有详细的了解,进而制定相应措施对网络进行防御;对网络安全的研究者来说,他会更注重攻击方的情况,如常用攻击 IP 或伪 IP 地址、单次攻击位置与强度等。

因此,根据以上情况,可以把设计框架确定为以下几点:① 根据用户需求的不同,系统要分别表示出网络的整体与局部情况,即采用总图与细节的展示方法;② 在细节的处理部分,需要将用户可能感兴趣的属性维度提取出来,便于今后用户对数据的观测与处理;③ 各个维度间增加交互,便于发现数据间的隐藏关系;④ 由于在网络攻击中,IP 地址提供的信息较为丰富,本文以数据的 IP 地址为焦点进行设计。

2.2 设计方案简述

根据设计需求,首先确定了使用总图与细节的可视化方法,将整个界面分为多个视图。考虑到数据集中的 IP 信息来源有 2 个部分:发动攻击的源 IP 地址与受到攻击的目标 IP 地址。将各个视图划分为 3 种类型,即分别以目标 IP、来源 IP 与两者间的关系为焦点的 3 种类型。在视图间的关系方面,将当前网络状况,即目标 IP 部分作为主视图,将来源 IP 与二者关系的部分作为辅助视图。此外,为了获得更好的用户体验,本文为各视图间加入了较多的交互。

本设计共分为 4 个视图,整体设计方案如图 2 所示。

2.2.1 视图 1: 目标 IP 矩阵

如图 3 所示,视图 1 为本设计的主视图,以目标 IP,即受害方 IP 为焦点,利用网络安全可视化中最经典的方法——IP 矩阵进行设计,辅以滑动

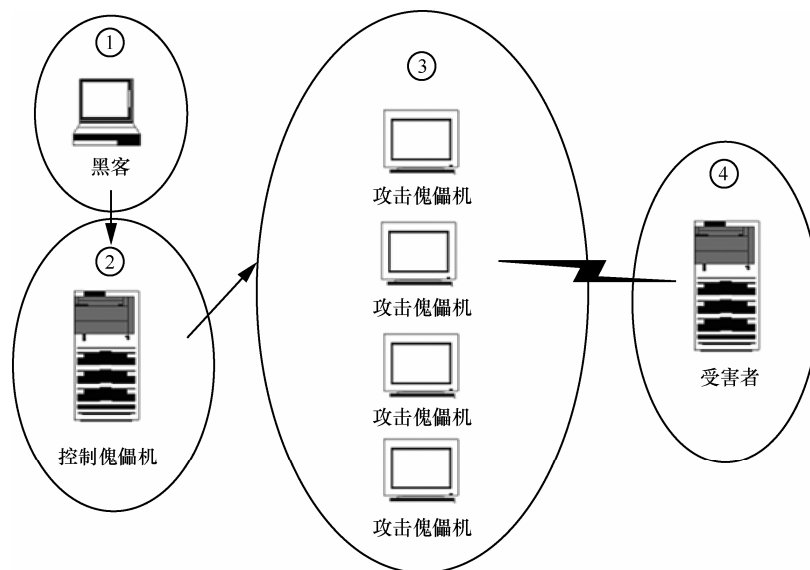


图 1 DDoS 攻击方法

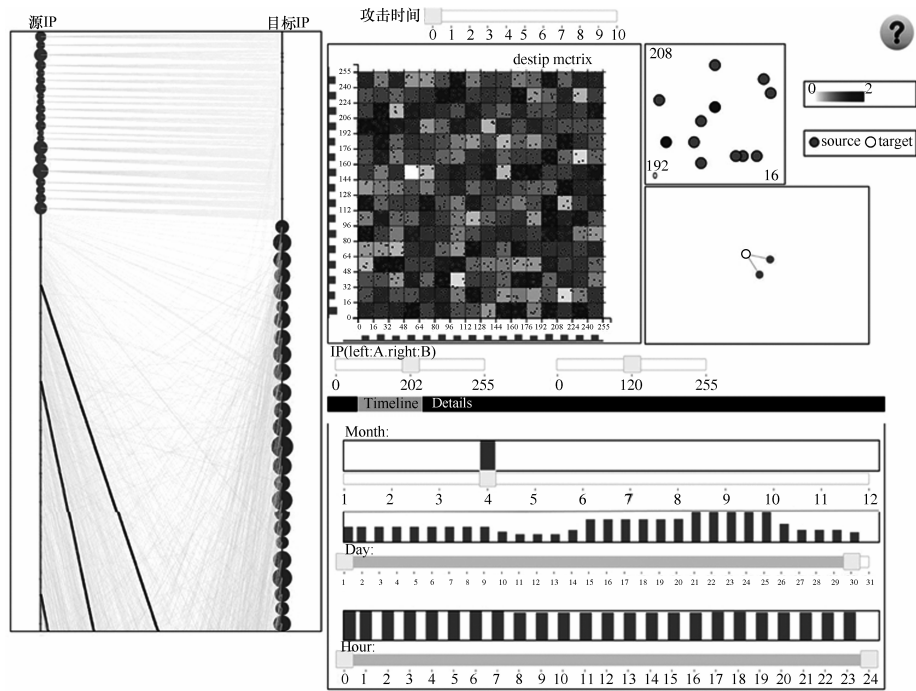


图 2 DDoS 攻击可视化系统总设计方案

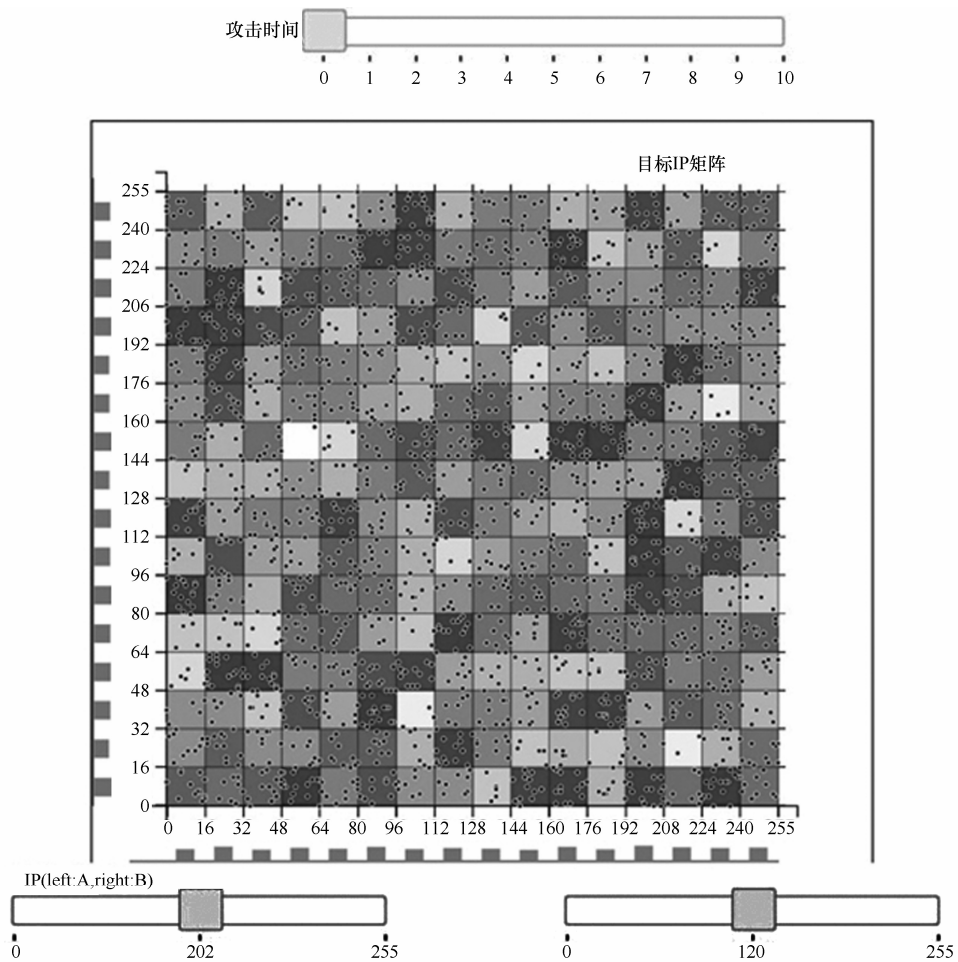


图 3 DDoS 攻击可视化系统视图 1: 目标 IP 矩阵

轴小组件进行可视化。由于IP地址是由4个字段组成,而二维矩阵并不能把4个维度表示在同一个矩阵中,那么就需要2个矩阵或加入辅助工具实现该功能。

对于经典的B类IP地址,前2个字段可以确定一个局域网的位置。结合用户需求,由于网络监测常常是一个机构、企业或学校等团体为了保护当下数据而进行的,网络监测者及研究者更关心自己所处位置的网络情况。而这些主机常常处于确定的局域网下,因此IP的前两字段的主要目的是为选取局域网区域。因此,如果将4个字段简单地拆分成2个相似的IP矩阵,是较浪费空间的做法。既然A、B段主要为实现筛选的目的,那么使用2条滑动轴作为辅助工具较为合适。这样做节省了较大的空间留给其余视图,可视化目的也更加明确。因此,将2条滑动轴组件放置于矩阵图下方相互关联,分别为IP前2段做出选择。

对于IP矩阵,横纵坐标分别代表IP地址的后2个字段。例如,如果数据集中出现以网络地址A.B.C.D为目标地址的信息,那么当用户拉动滑块并选定A与B后,可以观察到在A.B局域网下,上方矩阵中出现一个坐标点(C,D)。即该IP地址所对应的主机接收到了一个分组。由于IP地址的每一字段取值范围都是0~255间的正整数,因此将矩阵按照 16×16 的大小整体分块较为合理。在图3中,可以很清楚地看到, 16×16 的小矩形从白色到深灰色分别标记。这是在计算每个小矩形内IP地址的通信次数。若存在DDoS攻击,那么该矩形内的总次数就会明显高于其他矩形,于是该矩形会呈深灰色。结合图例中标记的最大通信次数与矩形颜色的深浅可圈定DDoS攻击可能发生的位置。该矩阵添加了放缩这种交互方法。用户通过滑动鼠标滚轮,可以在矩阵的任意位置进行放大或缩小,让矩阵更清晰、各种交互功能使用更方便。

IP矩阵的左端与下端分别是2组各16个小矩形组成的柱状图。16个矩形代表了16行或16列,每个矩形的长度是由该行或列与外界的通信次数决定的。由于DDoS攻击的特点,在连续攻击中,攻击者常连续攻击IP地址相邻的主机,这

些主机显示在矩阵中便是呈行或列连续的特点。即当某一行或列收到的通信次数远远多于其他行或列时,在这行或列上出现DDoS攻击的可能性较大。

此外,在矩阵上方还有一个标记为攻击时间(attack time)的滑动轴,这也是该视图的另一辅助工具。由于该系统的主要目的是观察某局域网下DDoS攻击的情况,并且所用的数据集全部来自网络日志,它记录了某段时间内该局域网与外网间的全部通信情况,而视图中的IP矩阵对所有信息都进行了点的标定,那么就要对一些不是DDoS攻击的信息进行过滤。根据DDoS攻击的特点,在短时间内会有大量数据分组涌向某地址,那么在该段时间内接受到较小量数据分组的主机就一定不是被攻击的位置,可以被排除掉。因此,本文设置该滑动轴,主要是实现数据筛选的作用,让用户可以更清晰地观察到可能被攻击的位置,便于及时做出防御。用户可拖动该滑块至选定值,在矩阵中过滤掉通信量小于该选定值的所有点。

2.2.2 视图2: IP通信关系总图

如图4所示,视图2位于整个系统的左半部分。从大小看,视图2要远大于其他3个视图,因为它从整体上对数据集的总结。无论用户如何筛选数据,本视图总默认显示全部数据集。视图2利用了可视化方法中经典的平行坐标轴方法,将数据集中的源IP与目的IP分列在左右两边,分别以正灰和正黑色的圆圈表示。一灰色圆圈与一黑色圆圈的连线代表2个IP间存在通信。源IP地址的分布按从左到右字段倒序分布,方便用户顺利找到某个可能存在的攻击者IP,并了解该IP的攻击情况。圆圈的大小代表所采集数据集内该IP成为目的IP或源IP的次数多少。值得注意的是,由于发生DDoS攻击后,部分IP的通信次数增多到较大值,受到网页大小的限制,圆圈大小不能仅凭通信次数线性增长,于是系统中设定了一个阈值。到达该阈值后,为保持视图的美观性,圆圈的大小停止增长保持不变。然而,该视图的重要功能之一是通过IP通信量对是否发生DDoS攻击、攻击者与被攻击者的IP信息等有整体的了解,阈值的设定会为判断带来一定的麻烦。为克服由此带来的缺点,将超过阈值一定比

例的点以颜色表示,即将原有的正灰色或正黑色变成深灰色或深黑色。这样改变后,就可以将数据集中通信量较大的点清晰地标识出来。

在本视图的细节方面,该视图共有3项交互。

- 1) 当用户单击某个圆圈时,鼠标旁显示关于该圆圈的详细信息,包括具体IP地址与通信次数。
- 2) 由于一份数据集中IP地址较多,在有限的区域内不能将全部信息显示出来,于是在该视图加入放缩与平移的方法。当用户想查看未进入视野的信息时,只需将鼠标向上或下方拖动视图即可。当由于数据较多影响查看效果时,只需放大该视图即可。
- 3) 视图1与视图2之间的交互。当用户单击视图1矩阵上的某一 16×16 的小矩形区域时,被点中的矩阵区域边缘高亮,同时视图2中与所选区域包含的目标IP地址有关的数据信息全部高亮,其余信息被弱化,如图5所示。通过高亮信息,可以发现与该区域有关的源IP的情况。通过对视图1、视图2的共同分析,结合DDoS攻击次数多、流量大的特点,可以判定该区域内是否发生了DDoS攻击以及攻击者的具体IP地址或者使用了哪些伪IP地址等信息。

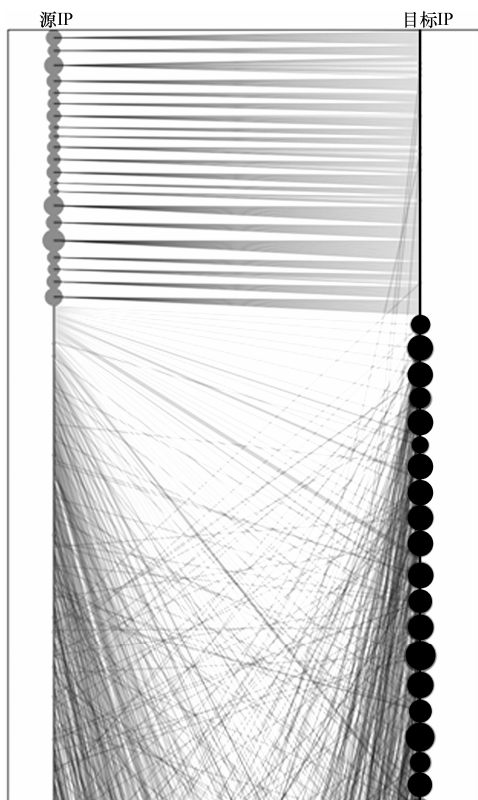


图4 DDoS攻击可视化系统视图2: IP通信关系总图

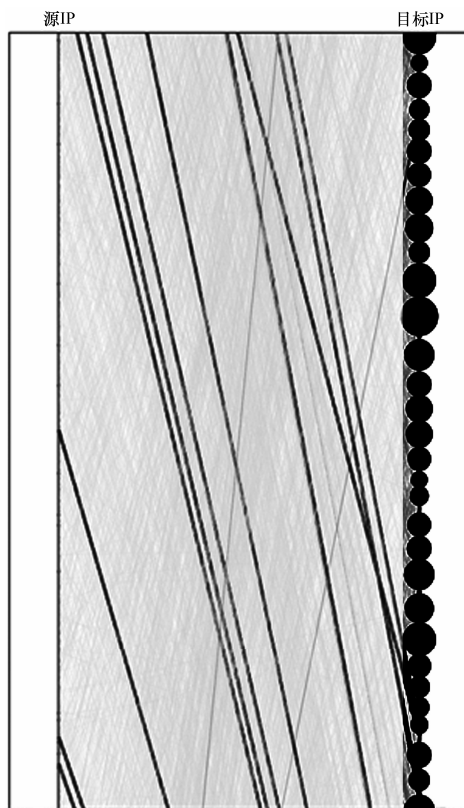


图5 IP通信关系总图部分信息高亮效果

2.2.3 视图3: 通信次数图

如图6所示,视图3位于整个系统的右上部分,属于视图1的辅助视图。由于视图1是根据目的IP后2个字段的数字转换成坐标来标记位置的,如果不同源IP地址都对应同一个目标IP,那也只会视图1内显示出同一个点。即使视图1中的每个小矩形用颜色表示出了各自通信次数的大小,但也只是说明该区域而不是某个点的具体情况。一个深色的区域往往可能有2种情况:一是某个点的通信次数很高而其他点较低,在这种情况下发生了DDoS攻击的可能性较高;二是区域内的点较多,但是每点次数较平均,这种情况下发生DDoS攻击的可能性相对较低。因此,要想确定是否真正发生DDoS攻击,还要结合单个点的情况,这便是视图3存在的原因。

作为辅助视图,视图1、视图3间必然会加入交互。当用户单击视图1中某个 16×16 小矩形区域后,在视图3中显示将选定区域等比例放大后的视图。视图3中左上、左下与右下角标记了视图1中选定区域边界的横纵坐标,起到一个提示的作用。区域中的点根据自身的通信次数多少

用深浅不同的灰色标定，颜色选取与视图1中灰色的渐进方式相同。此外，该视图还加入另外2种交互：一是当鼠标移到某点上，显示该点具体的通信次数；二是为防止相邻两点重复部分过多，通过鼠标滚动将该视图放大，进而便于查看所有点。

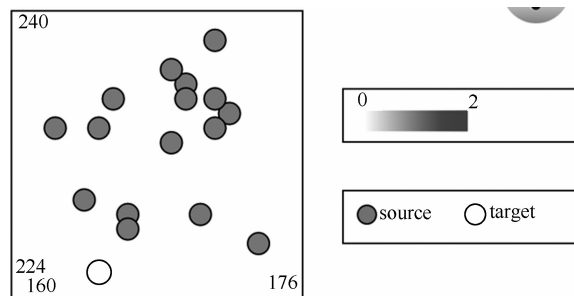


图6 DDoS攻击可视化系统视图3：通信次数

2.2.4 视图4：单目标IP通信关系图

如图7所示，视图4位于视图3的下方，属于视图1与视图3的辅助视图。视图3主要用可视化中力导向图的方法实现。其中，三角形代表目标IP地址，圆点代表源IP地址。两点间的连线表示二者有通信关联。该视图中的交互有3种：1) 当用户鼠标划过任意线，会显示对应两点间的通信次数，滑过点会显示具体的IP地址与点的编号；2) 当用户单击视图1中某一16×16的小矩阵后，视图4中显示该区域内通信次数最高点的力导向图；3) 当用户单击视图3中显示的某点，

视图4中会显示该点的力导向图，即该点和该点有关的所有源IP地址。之所以会选择力导向图这种可视化方法，是因为当某区域涉及的点较多时，用户可以手动改变点的位置，将其拖动到适合观察的区域使用鼠标滑动显示细节。

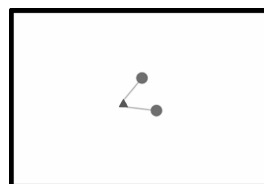


图7 DDoS攻击可视化系统视图4：单目标IP通信关系

2.2.5 其他

在4个视图之下还有一个区域，如图8和图9所示，该区域主要用来显示数据细节与时间轴。由于网页的空间有限，因此采取了区域复用，即鼠标滑过转换标签的方法。当用户打开网页后，该区域默认显示时间轴模块，鼠标滑过后可以转换为细节模块。时间轴的主要作用是对原数据集的筛选。时间轴共分为3个部分，从上到下依次为月份、日期与小时，用户可以自行滑动滑块对时间进行选择。时间轴模块与视图1中的矩阵有交互。当时间滑块停止后，视图1矩阵中会标记在目前选定的时间段内与外界IP有通信情况的由具体IP地址后两段字节组成的坐标点。

每个轴上有一个小型可视化交互柱状图：对于上方月份轴，显示了数据集中每月通信次数的

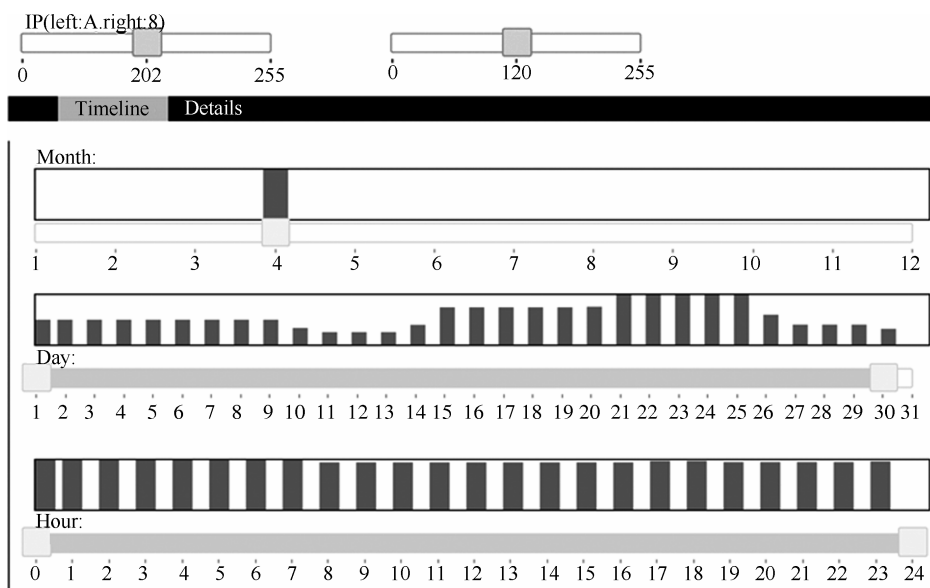


图8 DDoS攻击可视化系统时间轴模块

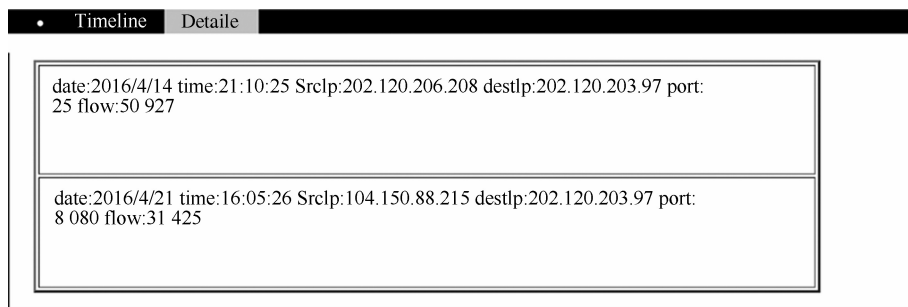


图9 DDoS 攻击可视化系统细节模块

多少, 一直保持不变; 中间日期轴显示了选定月份中每天通信次数的多少, 当选定的月份区间变化时, 日期轴上方柱状图跟随变化; 下方小时轴同理, 当选定的月份区间或日期区间变化时, 小时轴上方的柱状图也跟随变化。用户可以根据柱状图的提示清楚得知哪些时间段内的通信次数较多, 更易发生 DDoS 攻击, 进而将时间段选定在此区间内, 排除了正常通信的干扰。

该区域的另一模块为细节模块, 该模块与视图 1、3 有交互。当用户单击视图 1 或 3 中的某个点后, 可以在细节模块中显示该目标 IP 在数据集中的所有数据信息, 包括通信时间、源 IP 地址、通信端口、网址等。所用数据集不同, 显示的细节也不尽相同, 每条数据之间用矩形框区分, 使显示更加清晰。当用户再次单击其他点后, 会覆盖前一点的所有细节信息, 不保留历史记录。视图 1 中加入的放缩功能也是为该模块服务。当视图 1 中的点较密集时, 用户可以通过放大矩阵, 从而更易单击其中的特定点。

此外, 在整体设计的右上角有帮助图标, 当用户单击后, 显示该系统的使用说明, 指导用户进行操作。

综上, 时间轴与细节模块也是视图 1 的辅助视图, 通过较多交互让视图 1 作为主视图的功能更加完善。较多的交互是本系统设计的创新之处, 也是各视图间联系、各数据间关系的重要表现手段。它凸显了可视化的实际意义, 也让整个系统间的联系更加紧密。

3 系统应用

3.1 数据来源与处理

为了检验该 DDoS 可视化系统的实际效果,

采用了 3 份实际数据集加载入该系统中。其中, 有一份选取自中国可视化与可视分析大会 (ChinaVis) 2016 挑战赛的网路日志数据集; 另 2 份选取自某高校某实验室的真实网络日志, 包含一周确定遭受 DDoS 攻击的日志以及一周未遭受 DDoS 攻击的日志。引入某高校的真实数据, 是为了在已知是否存在 DDoS 攻击的情况下观察系统的实现效果, 总结与分析系统的实现情况; 引入 ChinaVis 的数据集, 是为了观察在引入普通数据后, 系统对 DDoS 攻击的敏感度, 用户是否能较明显地发现可能存在的攻击情况。

在对日志数据的处理上, 对源 IP 地址进行了分字段倒序排序, 为了减少在代码运行时的运算复杂度, 加快了系统处理大型数据的速度。

3.2 应用效果

3.2.1 效果 1

本次应用采用某高校某实验室受到 DDoS 攻击的特定周的网络日志数据集, 效果如图 10 所示。

通过效果图可以清晰地看出, 此时在选定的 IP 区域发生了 DDoS 攻击。因为根据 DDoS 攻击的特点, 攻击者喜欢利用傀儡机对受害方连续 IP 地址的区域发动攻击。在视图 1 的矩阵中, 可以明显看到, 在横轴 $x=162$ 处的纵轴上有连续的通信量出现, 且根据视图 3 每点显示的细节, 观测到每点的通信量都在千次以上, 这是典型的 DDoS 攻击的特点。此外, 根据下方时间轴的辅助柱状图信息, 可以得知 DDoS 攻击即有可能发生在 4 月 14 与 4 月 15 日 2 天, 因为这 2 天的通信量要远大于其他日期。

3.2.2 效果 2

本次应用采用某高校实验室未受到 DDoS 攻击的某一周的网络日志数据集, 效果如图 11 所示。通过效果图可以清晰地看出, 该周数据的通

信量较小且比较分散,许多IP地址的通信量都控制在10以下,无论从视图1矩阵,还是从视图3通信次数与视图2整体数据集的情况来看,都没有发现出现DDoS攻击的典型特点,因此可以基本判定,该周末发生DDoS攻击。

3.2.3 效果3

本次应用采用ChinaVis2016的部分网络日志数据集,效果如图12所示。通过效果图可以看到,视图2中有一目标IP呈深灰色,即受到了大量目标IP的攻击,这点也可从视图2的连线情况中得出。该视图状况符合DDoS攻击的规律。视图1中,用户选定了172.20区域,该局域网内只有某一小矩阵区域呈现了深灰色,而其他区域虽然也存在坐标点,但只采用了白色,说明深色区域的通信量极大,远大于其他区域,该视图状况符合DDoS攻击的规律。当用户单击深色小矩形区域后,辅助视图3中可以看到颜色最深的点具有上千的通信量。同时,在下方视图4中,可以清晰地看到选定区域内通信量最多的点的力导向图。这种典型的花朵似的图形更清晰地说明了该IP

地址发生了DDoS攻击。

综上所述,基本可以确定在2015年7月26日左右,位于172.20的局域网内发生了DDoS攻击。在用前2份数据在已知结论的情况下对系统进行了有效性检测后,该数据的加载效果更说明了该系统基本实现了设计目的,即用户能通过简单观察各个视图,发现是否存在DDoS攻击的情况。

3.3 效果分析与比较

3.3.1 系统优点

根据系统的实现情况来看,该系统具有以下优点。

1) 该系统相对于其他已存在的分析DDoS攻击的方法,使用了可视化技术,避免了大量繁琐的计算。区别于其他网络安全可视化系统,该系统主要针对DDoS攻击,且采用多视图多视角的方式进行可视化。

2) 从3.2节讨论的系统应用效果来看,该系统实现了判断DDoS攻击是否出现的功能,满足了用户的基本需求。用户通过阅读系统说明可以简单学会对系统的使用。

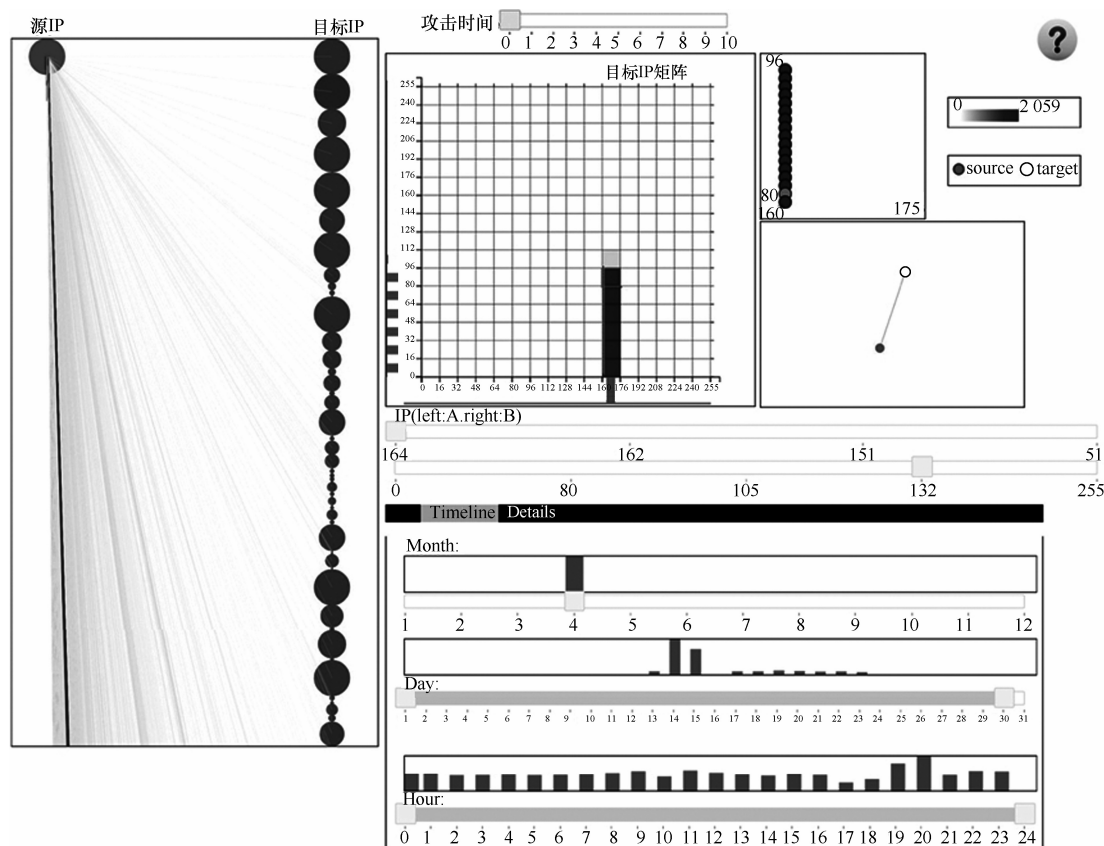


图10 某网络受到DDoS攻击的系统效果

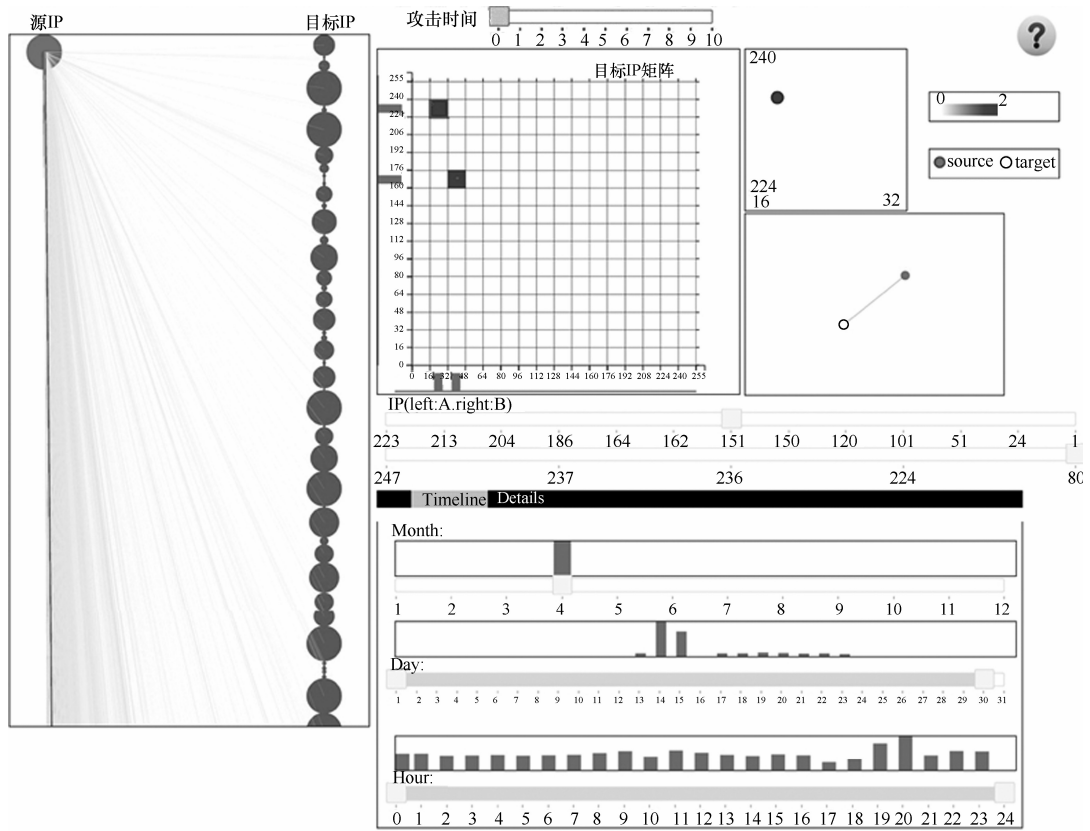


图 11 某网络未受到 DDoS 攻击的系统效果

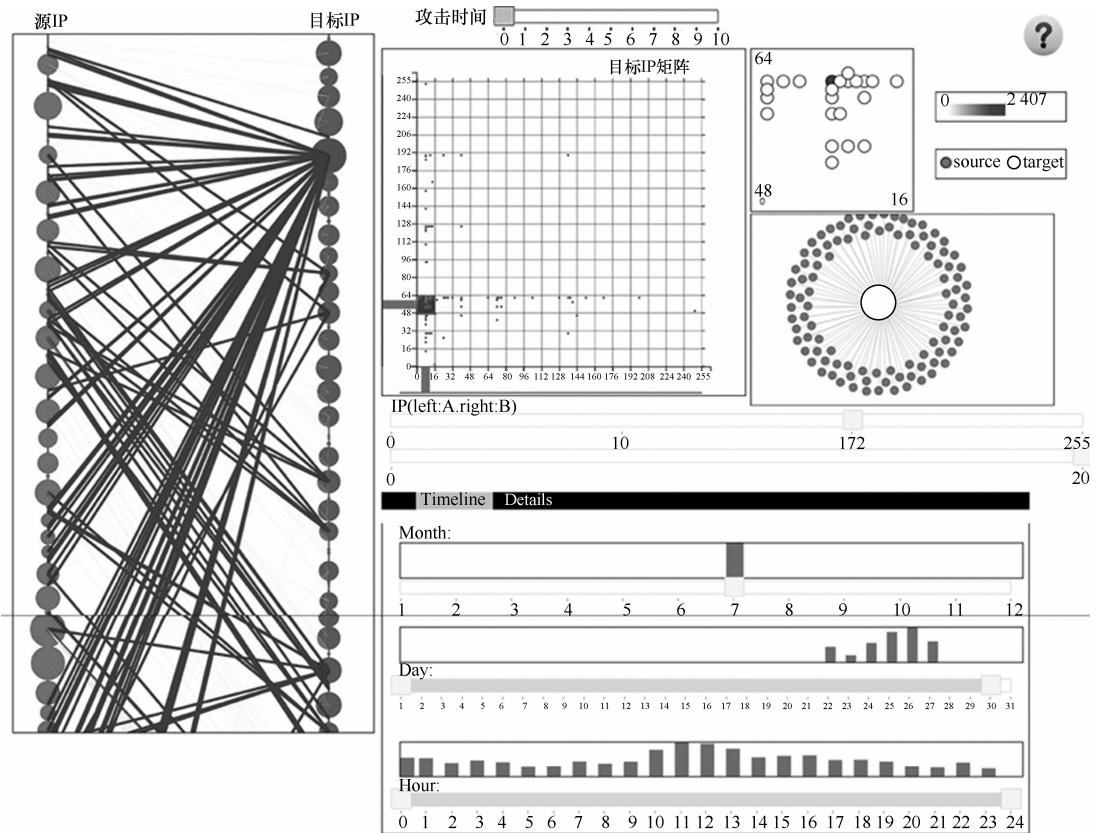


图 12 引入 ChinaVis 数据集的系统效果

3) 从设计的角度来看, 各视图功能各有侧重, 视图间排布较为合理, 有侧重点之分, 让人一目了然。

4) 从可视化的角度来看, 可视化的基本方法使用得当, 既保证了数据能完整、真实地显示在系统中, 不使数据冗余, 也不引入虚假关系, 又让数据清晰地表示出来。

5) 从交互设计的角度来看, 本系统将交互功能作为系统设计的重点, 增强了用户的体验。在主视图方面, 视图1分别与视图2、3、4各有交互, 也与时间轴、细节、IP选择等模块有直接交互, 赋予了用户较高的自由度, 让用户可以自行选择不同维度观察分析数据。对于其他视图, 相互间也有一些交互。例如, 视图4可以由视图3通过鼠标单击控制, 每个视图都有鼠标单击或滑过显示提示框交互等。通过较多交互, 不仅增强了用户体验, 强化了各视图间的关系, 更利于用户发现新问题, 进而发掘数据间的隐藏关系。

3.3.2 系统局限性

由于时间、技术等多种原因, 该系统依然具有一定的局限性。

1) 该设计作为一项系统应用, 并没有让数据由用户直接装载, 这大大降低了系统的实用性, 是下一步亟待解决的问题。

2) 当数据集超过百兆时, 系统的运算速度将大大减慢, 影响了用户体验。

3) 系统设计的细节问题。当加载的数据集较大时, 视图2的长度将变得很大, 虽然加入了拖拽交互与倒序排列, 但是也一定程度上影响了用户体验。同时, 若对某目标IP攻击的源IP数目过多, 在视图4力导向图上显示出的点数目过密, 影响了用户使用的便捷性与美观性。

4) 系统采用已导出的数据作为源数据集进行可视化, 缺少实时监测的能力。

3.3.3 系统可行性分析

1) 技术方面的可行性

本系统利用网页进行开发, 主要使用的语言是JavaScript、HTML与CSS, 使用的库为JavaScript中的D3库, 均属于常见的语言, 具有大量资料。通过查阅学习相关教程与官方文档, 开发人员可以基本熟悉所用语言。因此, 对于该系统的开发

人员没有太多技术上的困难。这3种语言对于开发环境的要求也不高, 只需在计算机上搭建小型服务器, 一般计算机都可顺利配置。

2) 经济方面的可行性

本系统开发成本由开发人员的时间精力与生活消耗组成。考虑到该系统的实用性较强, 可以给公司带来良好收益, 经济方面是可行的。

3) 后续维护方面的可行性

对于该系统的后续维护是较容易的。由于基本功能都已实现, 维护主要集中在未探测到的错误维护, 界面的UI设计与算法复杂度的降低方面, 这对熟悉该编程语言的开发人员是较容易的。

4) 用户操作可行性

除了系统开发方面的可行性, 用户使用方面的可行性也非常重要。一个好的系统设计需要让用户简单、顺畅地使用。对于本系统来说, 主要用网页进行实现, 不需用户自行下载安装软件。现在计算机网络的普及率很高, 所以对任意用户来说, 都可以简单地通过互联网进入系统, 简化了对软件的安装操作。在系统的使用方面, 操作简单, 只需用户操作鼠标单击与滑动即可使用。系统右上角有详细的使用说明, 用户可以随时查看。

综上所述, 该系统在各方面具有良好的可行性, 具备实际使用的价值。

3.3.4 系统前景与改进

目前, 该系统的基本功能都已实现, 但仍存在一些局限性。减少现有缺陷成为完善该系统的首要目标。

在3.3.2节中已提到过, 目前亟待解决的问题是数据的装载问题。对于任意实用系统来说, 系统需实现对数据集的选取功能。该问题的解决方法有2种: 一是当该系统运用于企业等团体机构后, 可以直接与该机构的网络日志系统连接, 将数据直接输入到该系统中, 不需人工加载处理; 二是对想要观察不同网络情况的研究者来说, 可以在系统中设置加载功能, 让用户自行上传想查看的数据到该系统中。解决了数据的装载问题, 可以大大提高系统的实用性与用户的自由度。

其次, 由于设计时间的局限性, 系统的细节部分还有待提高。例如, 系统的UI设计还比较粗糙, 不够精美。为了吸引用户的使用, 系统还需

要加强对细节部分的处理,如加入合适的图片提示、加入效果动画等。

再次,该系统在大数据方面表现还不够突出,今后在数据的筛选与计算方面应多做改进,降低系统的响应时间。

最后,该系统不应满足于已有的功能,在今后应多多开发新功能,为 DDoS 攻击可视化增添新的助力。例如,该数据集来源于网络日志中已统计过的数据,并没有对实时网络情况进行监控与分析,这就让使用者面对当下的 DDoS 攻击不能及时做出反应。因此,将网络日志中的实时数据直接导入系统可以大大增加系统的实用性,扩大用户范围。同时,对于实时监测到的 DDoS 攻击,该系统可以直接采取有效的防御措施,进行主动防御,大大减少了网络监控者的工作量。

以上几点改进都会大大增加系统的实用性与有效性,增加用户群体,增强用户体验,有利于系统的推广。由于网络安全与可视化结合本身就是新兴的研究方向,若能实现一个独立的具有独特创新性的系统,将会具有良好的发展前景,为可视化技术在网络安全方面的实践增添了助力。对分布式拒绝服务攻击进行可视化,是网络安全可视化的一个详细分支,也为今后的可视化研究提供了另一种方向,即对现有的可视化方向再细化,并设计出具体应用用于处理实际问题。相信这个方向也会是可视化技术由研究走向实际的必经之路。

4 结束语

在网络愈发重要的时期,用户对网络安全的要求就越高,那么对网络状态的监控就越必不可少。近年来,大数据的兴起带动了可视化的发展,将可视化技术带进了人们的视野中,衍生出了网络安全可视化这种新型研究方向。目前,网络安全可视化处于迅速发展的时期,研究者开发出了一系列新型的网络安全可视化工具,如 SnortView、NVisionIP 等,对可视化的应用以及网络安全的分析做出了较大的贡献。

本文对分布式拒绝服务攻击可视化进行了研究与系统设计。首先,介绍了网络安全与可视化的研究背景,阐明了 DDoS 攻击可视化的研究意

义。其次,介绍了 DDoS 攻击的基本概念,包括攻击原理、特点与防御方法等,让读者对该类型的网络攻击有一定的了解。接着,介绍了可视化在网络安全方面常用的一些基本方法,包括 IP 矩阵、平行坐标轴、环状图等,并重点阐述了可视化中的交互方法及其对可视化的重要意义,让读者了解了可视化技术中的一些方法。通过对基础知识的阐述以及研究背景的简介,引出了用于分析 DDoS 攻击的可视化系统的设计,并对该系统的整体设计情况、设计过程、各视图功能与视图间关系进行了详细的分析,包含各视图所运用的可视化方法以及交互在设计中的使用情况。最后,本文将 3 组实际网络日志数据,包括确定有攻击、确定无攻击以及一般的数据,引入了 DDoS 攻击可视化系统中,由前 2 组数据确定该系统在不同情况下的不同效果,并由一般数据检测了当系统应用于实际中的效果。根据系统的实际效果,本文提出了该设计存在的局限性,并有针对性地提出了改进方法。

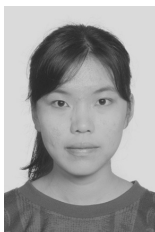
可视化技术作为近年来新兴的研究领域,还有许多方向有待挖掘。而网络安全可视化作为可视化应用的一个重要分支,也会快速向前发展。分布式拒绝服务的可视分析系统连接了两大研究方向,是网络安全可视化的一个具体应用。更加具体的研究内容带来了更加丰富的实际意义,这也是研究最终走向实践的必经之路。总之,在可视化技术飞速发展的当下,还会出现很多新生的理论研究。相信这些研究可以在大数据时代中,为可视化领域的发展、多领域间的交流做出重大贡献,为国家科技的发展带来良好的助力。

参考文献:

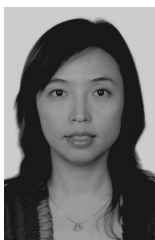
- [1] 陶传义. 科学计算可视化在物理光学教学中的应用[J]. 科教文汇旬刊, 2013(22):57.
TAO C Y. Application of visualization in scientific computing in physical optics teaching[J]. The Science Education Article Collects, 2013(22): 57.
- [2] 刘波, 马红妹, 徐学文. 20 年可视化发展历程对情报学的影响[J]. 情报理论与实践, 2008(1): 15-17.
LIU B, MA H M, XU X W. Impact of 20 years' development of visualization on information science[J]. Information Studies: Theort & Application, 2008(1): 15-17.
- [3] DARREN A, PAUL B, CHUI C F, et al. Worldwide infrastructure security report[R]. Arbor Networks, 2016.

- [4] ZHANG Y, LIU Q, ZHAO G F. A real-time ddos attack detection and prevention system based on per-IP traffic behavioral analysis[C]//IEEE International Conference on Computer Science & Information Technology. 2010(2): 163-167.
- [5] INDRAJEEET B M, PUKALE S G, DHORE M L. Detection of DDoS attack and defense against IP spoofing[C]//International Conference on Advances in Computing, Communication and Control. 2009: 489-493.
- [6] 颜若愚. 基于流量矩阵和Kalman滤波的DDoS攻击检测方法[J]. 计算机科学, 2014(3): 176-180.
YAN R Y. DDoS attacks detection method based on traffic matrix and kalman filter[J]. Computer Science, 2014(3): 176-180.
- [7] 王伟. 基于端口监测的DDoS攻击防御策略研究[J]. 安徽水利水电职业技术学院学报, 2010, 10(2): 62-64.
WANG W. A research on the attack of DDoS based on the port detection[J]. Journal of Anhui Technical College of Water Resources and Hydroelectric Power, 2010, 10(2): 62-64.
- [8] HIDEKI K, KAZUHIRO O. SnortView: visualization system of snort logs[J]. Workshop on Visualization & Data Mining for Computer Security, 2004: 143-147.
- [9] CHRIS P L, JASON T, NICHOLAS G, et al. Visual firewall: real-time network security monitor[J]. IEEE Workshop on Visualization for Computer Security, 2005: 129-136.
- [10] 张志国. 防止DDoS攻击的五个“大招”[J]. 计算机与网络, 2016(2): 53-53.
ZHANG Z G. Five methods to prevent DDoS attack[J]. Computer & Network, 2016(2): 53.

作者简介:



张毅凡(1993-), 女, 天津人, 上海交通大学硕士生, 主要研究方向为网络安全可视化。



董笑菊(1975-), 女, 吉林公主岭人, 博士, 上海交通大学副教授, 主要研究方向为信息可视化与可视分析、形式化方法。