ChinaVis2016 网络数据可视分析

上海交通大学 樊昕 冯柱天 姜伟鑫

指导老师上海交通大学 董笑菊

1 背景介绍

WeSuCom 是一家知名的通信服务公司，近年来一直致力于为企业和政府机构提供定制化的通信服务与应用解决方案。2015 年 7 月，WeSuCom 公司为某商业集团股份有限公司（BigBusiness）部署了一套网络化业务支撑平台，同时还部署了一套最新研发的网络监控系统，该监控系统在 BigBusiness 公司的骨干通信链路上对数据包信息进行抓取，特别是它可以记录数据包在链路层、网络层和应用层的相关信息。通过一段时间试运行，WeSuCom 公司想了解新上线的业务支撑平台的运行状态，同时也想了解新研发的网络监控系统到底能帮助网络管理人员从监控日志中发现哪些有趣的模式，如何从应用层、网络层和链路层三个方面抓取的数据包信息中探索用户行为模式。

2 功能设计

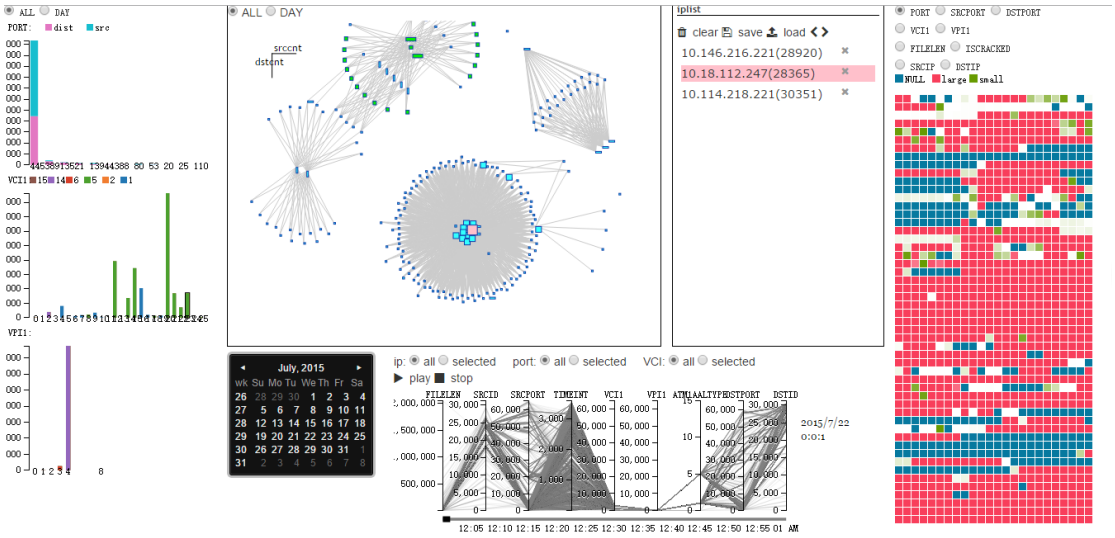

图 2.1

总体视图如图 2.1 所示。

2.1 日历视图

在日历中单击某一天，如果左侧条形图、中间力导向图的单选框选择的是 Day 的话，这两个视图就会重新得到该天的数据分布。

2.2 条形图

左侧条形图从上到下分别是单选框、port 条形图、VCI 条形图、VPI 条形图。

单选框用于切换条形图的数据来源是总体数据还是日历视图中选择的那天的数据。Port 只选择了使用次数最频繁的 1024 以下的端口。红色表示作为目的端口的次数，蓝色

表示作为来源端口的次数。VCI、VPI 的颜色对应 ATM 的类型。所有的条形图都可以点击以对力导向图视图做出筛选，把鼠标移上去可以得到具体数值提示。

2.3 力导向图

同样可以选择显示全部的或是选中日期的分布。主要用于显示网络的拓扑结构。每个节点都是一个小矩形，矩形的宽表示这个 ip 作为 srcip 的次数，长表示作为 dstip 的次数。当条形图做出筛选后，会用绿色高亮出经过筛选的 ip。

2.4 list 视图

力导向图中点击的 ip 会被加入到这个视图中，与力导之间会有高亮联动。可以用于保存重要的 ip，同时用于平行坐标视图中作为 selected ip。

2.5 矩阵视图

有几种数据来源可以选择：port、srcport、dstport、vci、vpi、filelen、iscracked、srcip、dstip。前三个（port、srcport、dstport）需要在条形图中选中某一 port，vci、vpi 也必须在条形图中选中，srcip、dstip 要在力导向图中点击某一具体 ip。

选择单选框来切换数据来源。

矩阵以小时为单位，横坐标为 1-24 小时，纵坐标为天数，这里是 53 天。蓝色表示数据为 0，红色表示相对比较大的数据量，绿色处于中间，根据数据量的大小从白色到绿色渐变。

单击某个小方块来选中具体的某一个小时。

2.6 平行坐标视图

显示的是矩阵视图中选中的一个小时的数据。可以显示这段时间里所有的数据，也可以进行筛选，只显示与 list 视图中的 ip 有关的数据或者选中的 port、VCI1。单击 list 中的 ip 在平行坐标中该 ip 的通信会以粉色高亮显示。

可以点击播放来以动画形式观察数据从网络层到链路层再到应用层的全过程，也可以手动拖动进度条。

3 分析方法

使用方法为从视图 2.1->2.2->…->2.6 层层递进筛选。

比如对于 ip，可以根据需求，在左侧直方图中选择某一数据，然后在力导向图视图筛选出的高亮 ip 中选择需要的加入到右侧的菜单中，然后在矩阵中观察这个 ip 的收发数据随时间的变化，找到值得观察的某一个小时单击选中，在下方的平行坐标视图中用动画的形式具体查看这一个小时的数据收发情况。

总之，2.1 日历、2.2 条形图用于筛选，2.3 力导向图用于显示拓扑结构，2.,5 矩阵视图用于查找异常。

4 结论总结

经过尝试，可以用整个系统比较有效地得到结论。

这个系统有以下几个特点：

（1） 对于网络层、链路层、应用层的数据都有比较好的表现。

（2） 采用的方法为层层筛选的方法。

（3） 易于发现异常和周期性行为。