基于社区发现的网络异常检测方法

钱爱娟[1] 樊 昕[1] 董笑菊[1)*] 褚衍杰[2] 袁晓如[3),4)]

[1)]（上海交通大学计算机科学与工程系 上海 200240）

[2)]（盲信号处理国家级重点实验室 成都 610041）

[3)]（北京大学机器感知与智能教育部重点实验室 智能学院 北京 100871）

[4)]（大数据分析与应用技术国家工程实验室 北京 100871）

摘 要 随着互联网的不断普及与网络通信技术的不断进步，网络已经逐渐进入到人们生活的每一个层面，越来越多的网络应用应运而生.但是另一方面，随着当前网络结构的日益复杂，会引起各种各样的网络安全问题，对社会构成了巨大的威胁和挑战.因此，网络安全问题至关重要.其中网络异常检测得到了研究人员的普遍关注.多年来，虽然已有许多异常检测的工作可以一定程度上发现和抵御网络攻击，但是有些方法难以适用于无标签的数据集，有些方法则训练成本过高，无法应用于实时场景.此外，对于细微异常的检测也是现有方法面临的一大问题.考虑到模型可解释性对于很多场景的必要性，本文以可视分析作为基础，提出了基于社区发现的网络异常检测方法，通过一个较为合适的粒度来提高系统对于细微异常的检测能力.该方法首先使用多层常量玻茨模型(CPM)算法对移动时间窗内的网络数据检测社区，并以社区为单位提取特征向量，然后用社区匹配方法将相邻时间步的社区关联起来，通过监控各社区特征的变化情况来检测异常.这种方法既考虑了网络数据作为动态图的特性，又能从一个比较合适的粒度提取特征.此外，系统提供可视化界面来帮助用户确认异常点前后的网络情况、关联异常事件.通过在Vast Challenge 2013挑战三的NetFlow数据集上的实验证明了该方法能够有效地检测更加细微的网络异常，验证了所提方法的有效性.

关键词 网络异常检测；可视分析；社区发现；社区匹配

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2022.00825

Network Anomaly Detection Method Based on Community Detection

QIAN Ai-Juan[1)] FAN Xin[1)] DONG Xiao-Ju[1)] CHU Yan-Jie[2)] YUAN Xiao-Ru[3),4)]

[1)](*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240)

[2)](*National Key Laboratory of Science and Technology on Blind Signal Processing, Chengdu* 610041)

[3)](*Key Laboratory of Machine Perception (Ministry of Education), and School of Artificial Intelligence, Peking University, Beijing* 100871)

[4)](*National Engineering Laboratory for Big Data Analysis and Application, Beijing* 100871)

Abstract In the rapid development of today, network has gradually integrated into the layers of human lives, and more and more network applications have emerged. However, as the current network structure becomes more and more complex, it will inevitably lead to the occurrence of various network security risks and loopholes, posing a huge threat and challenge to society. In recent years, the number and the strength of network attacks are gradually increased, and the intrusion methods are also updated, making the network information security problem more and more serious and crucial. Therefore, the issue of network security is of utmost importance.

收稿日期：2021-01-25；在线发布日期：2021-09-06.本课题得到国家重点研发计划项目(No. 2017YFB0701900)、国家自然科学基金(No. 61100053)资助.**钱爱娟**，硕士研究生，主要研究领域为可视化、机器学习.E-mail：qaj-16@sjtu.edu.cn. **樊 昕**，硕士研究生，主要研究领域为可视化、网络安全. **董笑菊**(通信作者)，博士，副教授，中国计算机学会(CCF)杰出会员，主要研究领域为信息可视化与可视分析、数字人文、形式化方法.E-mail：xjdong@sjtu.edu.cn. **褚衍杰**，博士，副研究员，主要研究领域为网络数据分析. **袁晓如**，博士，研究员，中国计算机学会(CCF)杰出会员，主要研究领域为可视化、可视分析、人机交互.

Among them, network anomaly detection has received widespread attention from researchers. Over the years, although there have been some anomaly detection researches that can discover and defend network attacks to a certain extent, some of them are difficult to apply to unlabeled datasets, and some methods are too expensive to train and cannot be applied to real-time scenarios. Besides, the detection of subtle anomalies is also an important problem of existing methods. In recent years, the continuous development of network security automated detection technology has reduced a lot of manpower expenditure, while there are also many problems. On the one hand, the scale of training data has brought huge storage costs and time costs; on the other hand, the complex network environment and the concealment of attack methods have led to many false negatives. Therefore, it is necessary to involve humans in the analysis process to make more accurate judgments. In this process, how to systemize and structure the massive and complex data is a key issue, and the cross-cutting research field of network security visualization has emerged as the times require. Given the necessities of model interpretability under several scenes, based on visual analysis, this paper proposes a network anomaly detection method based on community detection, which improves the ability of to detect subtle anomalies through an appropriate level of granularity. This method first utilizes the multi-layer constant Potts model (CPM) algorithm to detect the community of network data in the moving time window and extracts the feature vector with the community as the unit. Then it uses the community matching method to correlate the communities of adjacent time steps and detects the anomaly by monitoring the changes of the characteristics of each community. This method not only considers the characteristics of network data as a dynamic graph, but also can extract features from a suitable granularity. In addition, this paper provides a visual interface to help users confirm the network situation before and after the exception point and correlate the exception events. Experiments on the NetFlow dataset of Vast Challenge 2013 challenge 3 prove that this method can effectively detect more subtle network anomalies. It further verifies the effectiveness of our system in network anomaly detection, which can help users explore the abstract and complex network data conveniently and intuitively. In summary, our method based on community discovery and visualization technology is feasible and effective for detecting network anomalies.

Keywords network anomaly detection; visual analysis; community detection; community matching

1 引 言

随着互联网的不断普及与网络通信技术的不断进步,网络已经逐渐进入到人们生活的每一个层面.同时,各类攻击事件出现了爆发式的增长,引起了网络安全研究者的普遍关注.其中,网络入侵检测是重点研究方向.对于入侵检测的研究可以分为两个类型:误用检测和异常检测.误用检测依赖于网络安全专家预先确定的规则和签名,而异常检测建模正常的网络活动或行为,不符合模型表示的即为异常.这两种检测的主要区别在于异常检测则能够适应未知的攻击形式,但是相对而言准确率较低.本课题关注异常检测,旨在适应日益复杂的网络攻击形式.

在过去的十几年中,已经有很多工作对网络异常检测进行了研究,还有一些工作给出了异常检测方法的综述[1-2].根据使用的核心算法,可以将异常检测算法分为基于统计和机器学习[3-4]、图论[5]、信息论[6-7]等的方法.这些方法从不同的角度进行异常检测,各有其优缺点.例如,许多以机器学习为核心的异常检测方法虽然能在实验数据上获得较高的检测率,但是存在可解释性方面的问题,即分析的过程不够直观,分析人员无法判断模型的结果是否正确,也无法确定当前的参数是否合适.为了实现分析过程的直观、有效,一些研究人员利用可视化方法[8-9],对网络日志进行提取,并将大量抽象的文字数据转换成图像,帮助研究人员分析对应的网络状态,识别是否存在网络攻击.另外,有监督的机器学习算法在训练模型时对带

标注的数据需求很大.然而,网络安全领域中,很多情况下难以直接得到适用的公开标记数据集.

对于网络异常的检测,无论是使用有监督还是无监督学习,特征提取都是必不可少的一步.然而,现有的特征提取步骤大部分是针对一个时间窗内的整体数据[10]或者针对单条连接[11].这些方法存在以下两个问题:(1)粒度不合适.粒度太粗会导致细微的异常难以检测,例如同时发生分布式拒绝服务攻击(DDoS)攻击和IP扫描时,由于DDoS导致的特征向量的变化比IP扫描的大得多,因此IP扫描可能难以被检测出来.而粒度太细又会产生过多的数据量,增加分析的成本和难度;(2)没有充分利用网络数据本身的特性.将网络连接或请求作为边,IP作为顶点,网络数据可以构成拓扑图(顶点与边的集合),加上时间属性后是一种动态图,即前一时刻的顶点和后一时刻的顶点存在联系,但大部分特征提取方法忽略了这一联系.

针对上述问题,本文从图论的角度对网络数据进行分析,首先对移动时间窗内的网络数据检测社区,并以社区为单位提取特征,然后用社区匹配方法将相邻时间步的社区关联起来,通过监控各社区特征的变化情况来检测异常.这种方法既考虑了网络数据作为动态图的特性,又能从一个比较合适的粒度提取特征.此外,系统提供可视化界面来帮助用户确认异常点前后的网络情况、关联异常事件.现有的一些基于图论的异常检测方法大多依赖于社区结构的变化或者边的属性变化[12],但是在网络安全领域,网络结构和边的权重经常在变动,而这些变动很多情况下并不代表异常.本文提出的方法虽然以社区为异常的检测单位,但是并不关注社区结构或是连接情况这些细节变化.

本文的主要贡献如下:

(1)将社区发现方法应用于网络安全领域,提出以社区为粒度提取特征并检测网络异常,相比现有方法,能够检测到更加细微和隐蔽的异常.

(2)设计并实现了基于社区发现的网络异常检测系统,以可视化的形式展示了网络异常检测的整个过程和结果.

(3)通过系统分析可以帮助用户将异常事件和异常IP进行关联,使分析过程更清晰可靠.

2 相关工作

本文研究的课题涉及网络异常检测以及社区发现,接下来我们将介绍这两个领域的相关工作.

2.1 网络异常检测方法

网络异常检测作为热点研究领域,近几十年来研究人员提出了很多优秀的工作,这些工作将各个学科的理论知识应用于网络安全领域,从不同角度分析网络数据.由于本文从图论的角度对网络数据进行分析,因此本节对基于图论的网络异常检测方法的相关工作进行了梳理.

已有一些工作给出了基于图的异常检测的综述.Ranshous等人[12]描述了在动态图中出现的四种异常类型,提出一种检测异常的两阶段通用方法,在第一阶段生成数据特征,第二阶段在第一阶段的基础上应用异常检测器.Akoglu等人[5]总结了对于不同类型的图的异常检测方法并介绍了其在不同领域的实际应用.

在网络安全领域,考虑到网络数据的时间属性,网络数据IP的连接图本质上也是动态图的一种.Idé等[13]监控节点的活跃向量的变化来标记异常,如果一个节点连接到多个活跃节点,那么这个节点的活跃值较高.Sun等人[14]用CMD (Compact Matrix Decomposition)方法分解网络图的邻接矩阵,用重构误差来度量网络快照随时间的变化[15].Akoglu等人[16]对不同时间步的每个顶点提取特征,然后计算移动时间窗内每个特征上节点对之间的相关系数,通过矩阵主成分的变化程度来检测突变点.Ding等人[17]监控跨社区的通信行为来发现网络入侵,但是误警率较高,约为50%.

将网络动态图进行可视化也是探索网络异常的一个方向.时间-时间映射[18]通过动画按顺序播放各时间片的数据,在演变过程中发现IP的出现、消失和IP团体的变化;时间-空间映射[19]将动态图的不同时间片排布到视图的不同空间区域,可以跨时间片进行比较;时间-属性映射[20]将不同时间片重叠在同一个视图里,通过顶点或边的颜色、形状、记号等区分时间片.

2.2 社区发现方法

网络中的社区是由互相紧密连接的一组节点构成的,而社区发现算法的主要作用在于从网络中获得有意义的社区信息.Fortunato等人[21]对社区的定义、衡量标准、检测方法等提供了一个全面的概览.Yang等人[22]使用LFR基准测试了常用的社区发现算法,提供了为给定网络选择合适的社区发现算法的准则.

静态社区发现方法主要有基于图分割[23]的方法、

基于模块度(Modularity)的方法[24]、基于图嵌入的方法[25]和基于深度学习的方法[26]等.其中,模块度优化是最著名的社区发现方法之一,然而,模块度优化是一个NP-hard问题,因此已经提出了许多启发式算法.其中,Louvain算法[27]是最流行的一种算法,它也是比较分析[28]中速度最快、性能最好的算法之一.

虽然模块度优化算法似乎能够准确识别已知的社区结构,但它存在一个固有问题,即分辨率限制[21],这可能会阻止它检测到相对于整个网络规模较小的社区.为了克服这个问题,Traag等人[29]推导出了无分辨率限制方法的一些基本属性,并提出了CPM(Constant Potts Model)质量函数:

$$H=-\sum_{ij}\left[A_{ij}w_{ij}-\gamma\right]\delta\left(\sigma_i,\sigma_j\right) \tag{1}$$

其中,A_{ij}表示对应顶点之间是否存在边,w_{ij}是对应边的权重,σ_i代表顶点i所属的社区,$\delta(\cdot,\cdot)$判断两数是否相等.其基本思想是试图最大化社区内部边的数量,同时保持相对较小的社区.

对于动态社区发现问题[30],静态算法也存在对应的变体.最简单的策略是对每个快照检测静态社区,然后通过Jaccard相似度[31]进行社区匹配,但是存在划分结果不稳定的问题.另一种策略进化聚类(evolutionary clustering)方法[32]引入一个成本函数,目标是在快照t的划分质量和快照t与$t-1$的划分相似性之间取得平衡.多层模块度方法[33]是基于进化聚类的一种算法,将模块度函数扩展到了动态图(多层网络).该方法可以处理一般的多层网络,但由于该方法基于模块度优化,因此它具有分辨率限制的缺点.

3 系统介绍

本文设计的基于社区发现的网络异常检测系统的流程图如图1所示,主要分为两大模块:算法模块以及可视化模块.下面从可视分析方法、算法描述以及可视化设计三个部分具体介绍该系统.

3.1 可视分析方法

如图1所示,算法模块和可视化模块相互联系、相互支撑.下面简要介绍可视分析的大致流程.

算法模块中使用的原始数据为NetFlow格式,首先,根据时间窗t_w和时间步t_s,将数据按时间戳字段分成T个时间片,并获得对应时间片的网络数据;接着以时间片为单位,分别用社区发现算法在其中检测社区;然后,提取所有时间片中的社区特征向量,并与前一个时间片相匹配社区的特征向量求差分作为新的特征向量;在最终的特征矩阵上,通过离群点检测算法可以获得异常的社区和时间区间.迭代地求取能最大程度改变异常特征向量的节点,可以得到导致异常的IP.对这些IP进行聚类,将异常IP与异常事件相关联.

算法模块完成后,可视化模块则会使用相关数据和检测结果并通过可视化界面呈现给用户.可视化整体界面如图1右下方所示.用户通过视图A选择异常时间区间,视图B会显示出该异常前后网络拓扑结构的缩略图对比,选中的缩略图会在右侧视图C中详细显示.用户可以在视图C中选择节点查看端口信息,其他视图中对应的节点会高亮联动.此外,用户可以在视图D中修改参数(如时间步长)来重新开始整个异常检测算法.

算法模块和可视化模块在分析过程中的具体数据交互在图1中使用实线以及文字标注.此外,可视化界面中的关键动作在图1中使用实线标出.

3.2 算法描述

算法模块主要包含六部分,分别是网络图预处理、社区发现、社区匹配、特征提取、异常检测以及异常关联.

3.2.1 网络图预处理

考虑到网络数据的特性,我们在应用社区发现方法之前增加网络图数据的预处理步骤.与网状结构的社交网络不同,在网络数据形成的图中,大多数连接是由客户端向服务器发起请求形成的,而客户端和客户端之间一般不会有联系,即社区内除了中心节点(服务器)之外的其他节点之间的连接并不紧密,社区主要表现为星型或树型结构.

因此,为了使得传统应用于社交网络的社区发现方法在网络安全数据上也能获得较好的效果,我们根据节点的相似度在图中增加虚拟边:如果节点i和节点j的公共邻居节点的比例大于一定阈值,就在两个节点之间增加一条边,权重设为相似度.这种衡量方式其实就是求节点i,j和其邻居节点组成的集合的Jaccard系数,其计算公式如下所示:

$$J_{ij}=\frac{N_i\cap N_j}{N_i\cup N_j} \tag{2}$$

其中N_i代表节点i及其邻居节点的集合.

3.2.2 社区发现

分辨率限制是基于模块度算法的固有问题,因此,我们使用CPM优化代替多层模块度方法[33]中的模块度优化以避免这一缺陷.多层模块度方法使用

两个主要参数，一是分辨率系数，这个系数越大，划分出的社区数目会越多；二是耦合系数，代表各个时间片之间的耦合权重，系数越大，不同时间片的检测结果越相似.

3.2.3　社区匹配

虽然在社区发现算法执行之后，每个时间片的节点都有了所属的社区，但是不同时间片的社区数目和社区编号都不对应，如果要分析社区随时间的动态演变，就必须将相邻时间片的社区关联起来. 根据文献[34]，可以使用Jaccard系数(公式(2))计算时间片t中社区和时间片$t-1$中社区之间的相似度以寻找匹配社区，这一策略也是目前主流的追踪网络社区演化的方法.

对于时间片t中的每个社区i，遍历时间片$t-1$中的所有社区j，计算两者的Jaccard系数. 如果系数大于一定阈值τ，则认为这两个社区之间存在对应关系，如果存在多个系数大于阈值τ的社区，则取Jaccard系数最高的作为匹配社区.

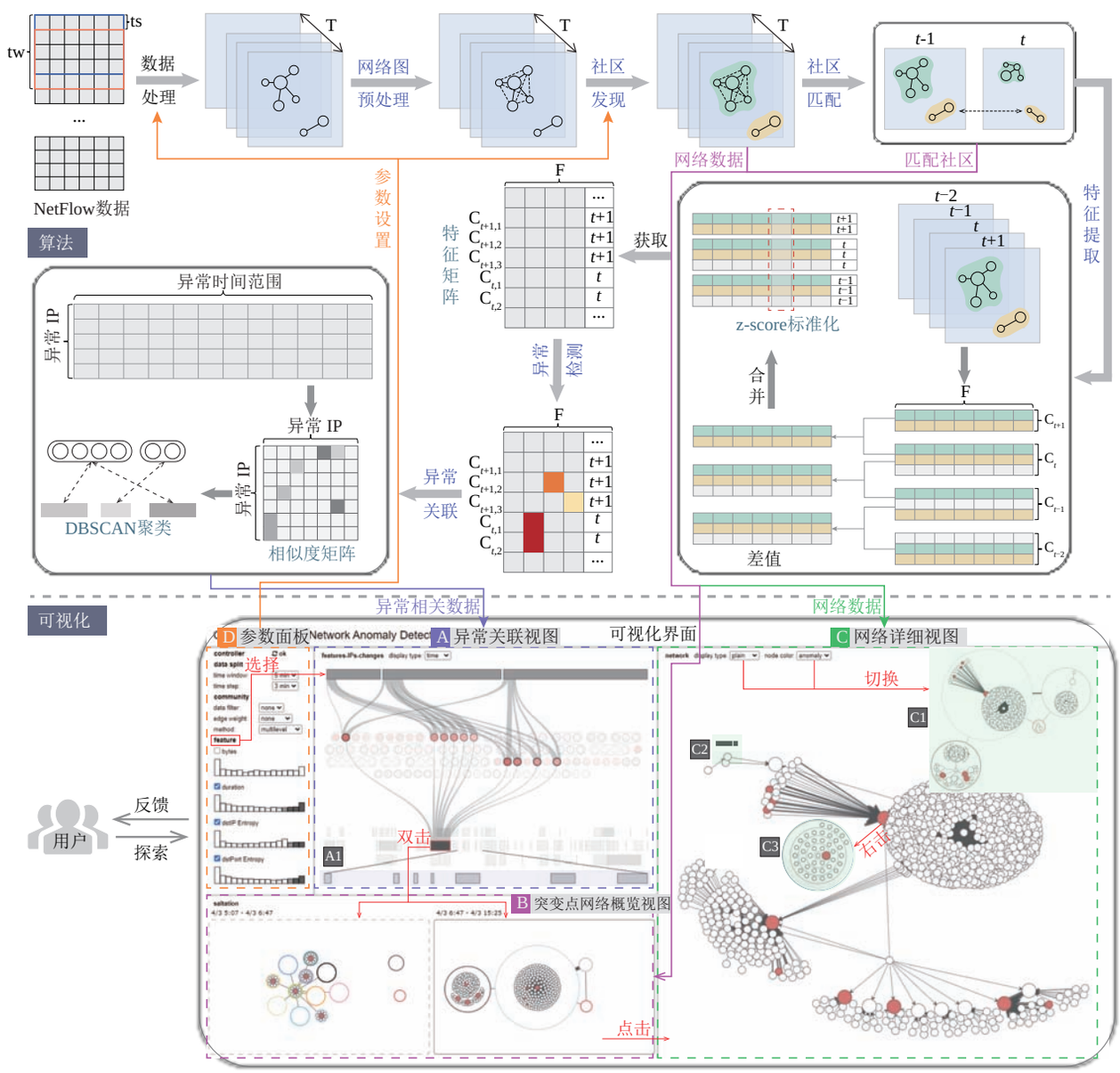

图1　基于社区发现的网络异常检测系统流程图

由于在网络数据中，内网的服务器是相对固定的，而访问服务器的客户端经常发生改变，在这种情况下，虽然社区内部的成员可能发生了较大的改变，但是只要中心的服务器和社区的基本结构不改变，就可以认为社区依旧匹配. 针对这一特点，系统在计算Jaccard系数时对不同类型的IP使用不同的权

重，对内部服务器采取较大的权重，而对外网客户端给出较低的权重.

此外，文献[34]中因为关注的是社区的演化过程，所以会将当前社区与之前多个时间步的社区进行比较，而我们目前只关注社区前后的特征变化情况，即突变点，因此在本系统中时间片t的社区只和时间片$t-1$的社区进行比较.考虑如果一个社区在时间片$t-2$时出现，在时间片$t-1$消失，在时间片t又出现，用原始的匹配方法[34]虽然可以在时间片$t-2$找到匹配社区，但是监控时间片t和匹配到的时间片$t-2$中的社区的特征变化反而会忽略其中间消失的异常情况.

3.2.4 特征提取

整个特征提取的过程如图1中相应部分所示，其中$F=21$表示特征维数，C_t表示时间片t的社区数.首先对每个时间片的每个社区提取特征，然后用社区的特征向量和前一个时间片相匹配社区的特征向量求差值，最后将所有时间片的特征矩阵合并后，执行标准化操作，作为最终的特征矩阵.

1）获取特征矩阵：在决策树算法中，通常使用信息增益[35]进行特征选择.根据NSL-KDD[36]数据中具有最大信息增益（>0.4）的8个特征[37]，我们对社区提取相似的属性.社区中的每条边存在属性：cnt（请求次数），dst host（目的主机IP），service（端口），src bytes（源字节数），dst bytes（目的字节数），duration time（会话持续时间）.其中，对于cnt，src bytes，dst bytes，duration time属性，统计它们的均值、方差、最小值和最大值（不统计总和是因为总数会受到社区规模的影响）.然后再计算下面的属性：整个社区的目的IP的信息熵，社区内所有IP访问的目的IP的信息熵的最大值、整个社区的目的端口的信息熵、社区内所有边的目的端口的信息熵的最大值.最终对每个社区可以得到共20维（4×4+4）的特征向量.对每个时间片，可以将这个时间片内的社区的特征向量组合起来，形成一个社区数（行）×特征数（列）的二维特征矩阵.

2）计算特征（差值）矩阵：由于检测突变点只需要考虑特征的变化情况，所以我们将时间片t中每个社区的特征向量与时间片$t-1$中匹配的社区的特征向量相减，得到一个社区数（行）×特征数（列）的相邻时间片的特征差值二维矩阵，其中第i行第j列表示时间片t中第i个社区的第j维特征和时间片$t-1$中相比的差值.T个时间片的数据可以得到$T-1$个这样的矩阵.每个相邻时间片的特征差值矩阵的列数都是特征数，但行数因为各时间片社区数不同而不同.因此将所有相邻时间片的特征差值矩阵按行进行拼接，同时增加一个时间步标识维度，就可以得到特征矩阵.

3）标准化特征：为了度量各特征，使特征之间具有可比性，需要在特征上执行标准化操作.由于异常样本的数量远小于正常样本，加上考虑的是特征差值，我们选择z-score这一受离群值影响较小的方法，转换函数为

$$\bar{x}=\frac{x-\mu}{\sigma} \tag{3}$$

其中μ为特征均值，σ为标准差.

3.2.5 异常检测

首先将特征分为四组，第一组$attr_1$：和流量相关的cnt，src bytes，dst bytes；第二组$attr_2$：和时间相关的duration time；第三组$attr_3$：目的IP的信息熵；第四组$attr_4$：目的端口的信息熵.其中，第一组和流量相关的特征可能代表DDoS之类的攻击，第二组和持续时间相关的特征可能和重定向有关，第三组目的IP信息熵通常代表IP扫描，第四组通常代表端口扫描.从而，可以更好地区分出不同类型的异常.

使用One-ClassSVM[38]对每组特征分别检测离群数据，将离群程度大于阈值（$\mu+\sigma$）的数据视为异常.这里离群数据指的是特征矩阵中的单元格，即具体某一时间片中的某一个社区的某一维特征.接着，将每组特征在时间上连续的异常合并.例如：如果在时间片3，4，5，6，10，11存在异常，就合并为区间[3，6]，[10，11].然后对所有特征组$attr_i$的每个异常时间区间，计算导致社区异常的主要IP.根据之前离群点的检测过程，突变点前后异常社区的特征向量的距离会比正常情况大，而如果从异常社区中去除异常节点，那新的特征向量相比异常时间区间的特征向量应该会发生较大程度的变化，通过这种方法我们可以定位到异常IP.具体计算方法见算法1，在本文中，μ取0.5，K取5.

如算法1所示，首先求突变点前后的异常社区的特征向量，将两者的差值乘以μ作为阈值.然后将异常区间内的数据合并成图G.由于重新计算去除每个节点后的特征向量的复杂度较高，这里我们采取的方式是选取入度和出度最大的K个节点作为排查对象.不断地从异常图G中去除候选节点和它的邻节点来重新统计特征向量，如果新的特征向量和异常特征向量的差值大于阈值，那么认为这个节点

是导致异常的IP之一，将其加入异常IP集合A. 这里的异常IP可能是攻击者，也可能是受到攻击的IP.

另外，考虑到存在多个攻击者和一个受害者的情况，例如DDoS攻击，用上述方法可能只能找到受攻击对象，而难以找到攻击者，所以对于这种情况，即找到的异常节点都是受攻击IP(属于入度最大的候选节点)时，将该异常IP的邻居节点和所有入度/出度最大的排查对象的交集也认为是异常IP(可能的攻击者). 最后得到某个时间段内基于特征组$attr_i$的异常IP集合A.

算法1.　异常IP检测

输入：特征组$attr_i$、异常区间、原始特征向量

输出：异常IP集合A

1. 集合$A=\emptyset$，其元素为异常IP
2. 取异常区间内异常社区的原始特征向量的均值f_{now}
3. 取所有异常社区在突变点前对应社区的原始特征向量，求均值f_{pre}
4. 设定阈值：$thre=\mu\times\left\| f_{now}-f_{pre}\right\|_{attr_i}$，其中第二项是$f_{now}$和$f_{pre}$在特征组$attr_i$上的欧式距离
5. 将异常时间区间内的图合并成图G
6. 对$\forall n\in\bigcup_j C_j$，$C_j$是异常社区，取入度和出度最大的$K$个节点$s_1, s_2, \cdots, s_K$
7. FOR$k\in[1,K]$DO
8. 构建s_k的邻节点集合N_{s_k}
9. 令$G_{new}=\bigcup_{s\in G, s\notin N_{s_k}} s$，重新提取$G_{new}$的原始特征向量$f_{new}$
10. 计算$d_k=\left\| f_{new}-f_{now}\right\|_{attr_i}$
11. IF $d_k>thre$ THEN
12. $A=A\cup s_k$
13. END IF
14. END FOR
15. IF 集合A中元素都是入度最大的节点 THEN
16. $A=N_A\cap\left(\cup s_j\right)$
17. END IF

3.2.6　异常关联

为确定异常IP之间是否存在联系，与哪些类型的异常事件相关联，我们对结果进行聚类分析.

根据异常检测的结果，可以得到每个异常IP出现的时间段. 即可获得一个二维矩阵B，矩阵的行是异常IP，列是异常时间区间，单元格的值代表对应异常时间区间的长度. 随后在该矩阵基础上构建各IP之间的相似度矩阵. IP_i和IP_j之间的相似度为

$$sim_{i,j}=1-\frac{\sum_k\left|B_{ik}-B_{jk}\right|}{\sum_k\max\left(B_{ik},B_{jk}\right)} \tag{4}$$

对相似度矩阵，使用DBSCAN[39]算法进行聚类，以获得异常IP的分组.

3.3　可视化设计

如图1所示，可视化模块主要包含四个视图：异常关联视图(图1A)；突变点网络概览视图(图1B)；网络详细视图(图1C)；参数面板(图1D，设置算法模块参数).

3.3.1　异常关联视图

图1A异常关联视图，以桑基图的形式展示异常IP之间的关联、异常IP与异常事件的关联. 为用户提供异常在全体数据中的分布信息，可以此作为分析的入口.

整个视图分为3排，最上排的是左侧选中的各个特征组的异常总数. 根据3.2.5节所述，我们在特征提取环节将所有特征分为4组，每个特征组都代表了一定类型的攻击. 将攻击数目映射成宽度可以迅速判断出当前网络中主要的攻击形式. 第二排是异常IP，这些IP是使用如3.2.6节描述的方法对当前异常时间区间中的异常IP进行聚类后的结果. 每个IP用一个圆表示，粗边框的圆表示内网服务器，细边框的圆表示其他IP，圆的颜色代表异常程度，同一组的IP用一个方框框起来. 第三排是选中的各组特征的具体时间分布，横坐标代表异常开始的时间点，宽度代表持续时间，颜色表示异常程度，颜色越深，异常程度越高，鼠标悬浮可以查看具体的时间范围. 此外，考虑到有些异常时间片由于宽度太窄难以选中，我们还提供了放大功能，将点击处周围的时间片在下方放大(如图1A1所示).

点击异常事件，视图会高亮显示与该事件相关的IP，也可以点击单个IP或一组IP来查看与它们相关的异常事件. 通过这种交互方式，用户可以了解到各种攻击在时间上的顺序、异常IP之间的关联、哪些IP主导哪些异常，这对于理解大规模攻击事件以及及时打击攻击者都是非常有帮助的.

3.3.2　突变点网络概览视图

当用户在图1A中双击选中某个时间片，图1B会展示该突变时间前后的网络概览. 左侧概览图的时间段为前一个突变的结束时间到选中突变点的开始时间，右侧概览图的时间段为选中突变的时间区间. 在两个概览图中，用户可以看到突变前后网络的大致分布，其中每一个圆圈表示一个社区，圆圈的

大小表示社区内IP的数目.由于异常一般只与少数IP相关,为便于分析,这里省略了社区内的正常节点.但是对于异常IP以及它们的邻节点,还是会正常显示,且用红色表示异常IP.注意这里的异常IP指的并非是图1A中的全局异常IP,而是导致该突变的异常IP.

点击概览图可以切换需要在图1C中详细显示的时间段,实线边框表示选中,虚线表示未选中.点击概览图中的某一个社区,其在另一个概览图中的匹配社区、在图1C中的对应社区会进行高亮.选中IP节点也有类似的交互,如果点击的是异常IP,在图1A中也会联动显示.

3.3.3 网络详细视图

用户可以通过图1C网络详细视图查看某一时间段的详细信息,深入获取部分细节数据.

图1C默认显示力导向布局.每个节点代表一个IP,其中使用颜色编码IP所属的社区,大小编码IP类型---服务器或客户端.节点之间的连线表示两个IP之间存在通讯,箭头表示通讯的方向,边的粗细映射为流量大小,流量越大,边越粗.由于力导向布局方法在网络规模较大、社区中节点过多的情况下,有难以比较不同社区之间联系的问题,因此系统还提供另一个聚合视图,可以通过视图上方的下拉菜单在两种视图之间进行切换.

在如图1C1的聚合视图中,每个社区用一个圆圈包裹在内,社区内的结构显示在圆圈内部,而社区间通信,即一个社区中的节点和另一个社区中节点之间的通信,聚合起来用单条连接表示.该聚合视图的布局实现采用的是双层力导向布局,首先对每个社区内的节点应用力导向布局,然后把社区作为节点再次应用力导向布局,社区节点的大小和社区内节点数目成正比.通过这种方式,用户可以更清晰地看到社区之间的通信情况.

此外,在该视图中还可以查看端口数据.如图1C2所示,点击某个IP,在周围会用矩阵的形式展示这个IP被访问的目的端口分布.每个格子表示一个端口,格子的宽度映射为被访问的次数,鼠标悬浮可以查看具体数据.

对于社区内节点过于密集难以选中的情况,类似图1A的异常关联视图,我们提供了放大功能.当右击某个节点时,将这个节点和周围一定范围内的其他节点用同心圆按照IP地址的十进制顺序排列出来,如图1C3,大小代表与该IP相关的流量,用户可以在放大的节点上进行操作.

如果只关注异常IP,可以在下拉菜单进行切换,这样红色显示导致当前时间片异常的IP,白色显示正常IP.

4 实 验

4.1 数据集

我们选用Vast challenge 2013挑战三[40]第一周的网络流量数据(NetFlow)作为实验数据集,总数据量大约为5 GB.在NetFlow数据中,两台计算机之间的一系列消息被合并成一个流量记录.表1列出实验中所使用的11个字段.

表1 系统中使用到的NetFlow数据的字段

字段	说明	示例
TimeSeconds	标准UNIX时间	1365034326
ipLayerProtocol	IP协议号	6
firstSeenSrcIP	源IP地址	10.0.3.76
firstSeenDestIP	目的IP地址	172.10.0.5
firstSeenSrcPort	源端口	34796
firstSeenDestPort	目的端口	80
durationSeconds	会话持续时间(s)	4
firstSeenSrcTotalBytes	源字节总数	466
firstSeenDestTotalBytes	目的字节总数	1571
firstSeenSrcPacketCount	源数据包计数	5
firstSeenDestPacketCount	目的数据包计数	3

4.2 实验设置

系统实现为一个可交互的Web应用程序.前端可视化用CSS、JavaScript和D3,后端算法主用Python实现.具体来说,选用Tornado服务端框架,用igraph和networkx库表示和处理图数据.同时,使用louvain库提供的多层CPM算法进行动态网络的社区发现.运行环境是Intel(R) Core(TM) i7-8550U CPU、16 GB RAM和Windows 10.分割时间片的参数设置,时间窗t_w默认值5分钟,时间步t_s默认值2分钟,在可视化界面中可以调整这两个参数.多层CPM社区发现算法的参数,根据实验和相关研究结果,分辨率系数设为0.001,耦合系数设为0.1.

4.3 案例分析

首先,从如图2所示的总体异常分布上看,目的IP和目的端口信息熵异常的出现频率较高,且存在一定重复度,推测是由于IP扫描和端口扫描通常同时进行.流量异常主要集中在4月3日和4日,最早出现在4月2日上午.这一结果符合攻击特点,攻击者一般会在用扫描类的方式探测到足够多的信息后开始流

量攻击或数据窃取行为.连接持续时间的异常通常伴随其他类型的异常出现,但从4月4日晚间开始多次独立出现,推测可能存在一些特殊的异常行为.

图2　总体异常分布

4.3.1　扫描

如图3所示,选中目的IP信息熵和目的端口信息熵的特征组,首先查看发生在4月1日上午10:42-11:15的一个异常.从最左侧的异常关联视图上可以看出这个异常和服务器172.30.0.3-172.30.0.7以及IP10.6.6.6和10.7.7.10有关.点击该时间段查看网络详细视图,发现这两个外部IP 10.6.6.6和10.7.7.10多次访问了服务器172.30.0.3-172.30.0.7.从边的粗细上看,对172.30.0.3的访问次数尤其多,在半个小时的时间内有409次连接.接着,我们点击IP查看端口信息,可以发现特点:10.7.7.10主要访问25端口,10.6.6.6主要访问80端口,且172.30.0.3主要是25端口被访问,而其他几个服务器则主要是80端口被访问,因此可以推测出172.30.0.3是邮件服务器而其他几个是HTTP服务器.由于从异常关联视图上看,172.30.0.3的异常程度最高,因此,选择这个IP,查看与它关联的异常时间.如图3最右侧,可以看到该服务器从4月1日到4月7日的每天上午都存在异常,是一种很有规律性的模式,而且同时存在被端口扫描和IP扫描的可能.

在观察信息熵异常的过程中,还会发现在多个异常时间段存在如图4所示的情况,10.3.1.25访问了172.10.0.3很多次.从172.10.0.3的端口使用情况上推测该服务器同样是邮件服务器,但是除了25端口外,多个其他端口被访问.接着我们右击节点10.3.1.25,可以发现它访问了从18526开始的多个连续端口,是一次典型的端口扫描.

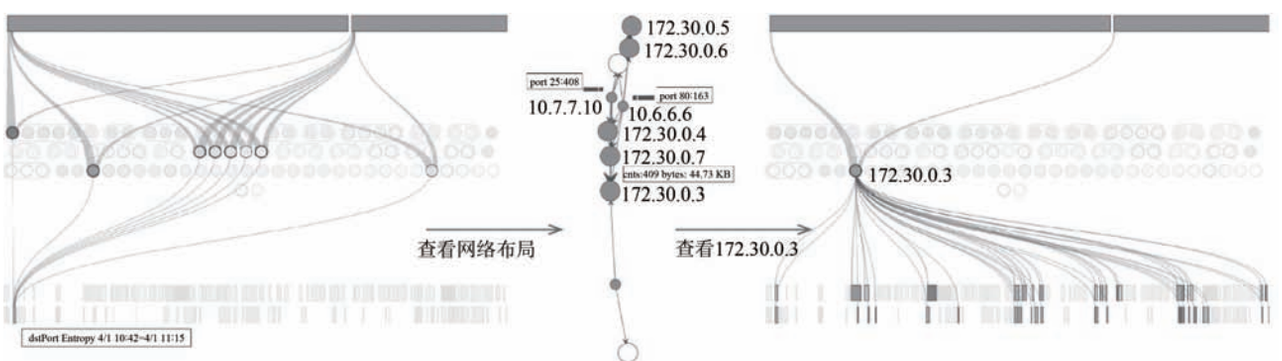

图3　选取目的端口信息熵异常程度最高的时间段，接着查看其网络布局，最后点击172.30.0.3查看与其关联的异常时间

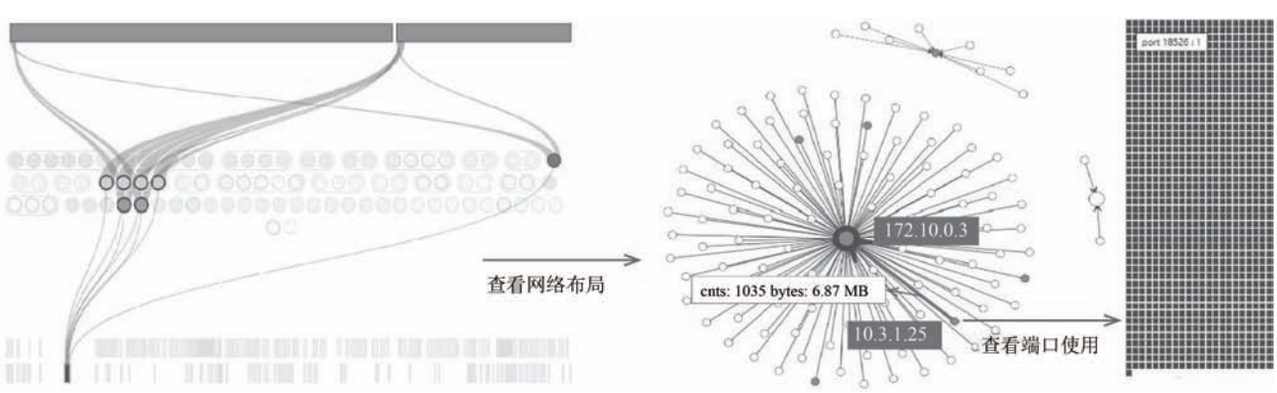

图4　选取信息熵异常的某一时间段,接着查看其网络布局,最后右击10.3.1.25查看其端口使用情况

此外,扫描类的异常还经常会造成网络社区的大幅度变化.如图5,左侧网络概览图中最大的社区在右侧分裂成了多个社区.查看网络详细情况,可以发现,左侧大社区中大部分成员是内网工作站,工作站之间互相存在一些通信(类似右侧概览图中的结构),但是由于有几个外网IP频繁地访问这些内网工作站的多个端口,导致右侧正常的多个社区结构被聚合成了单个社区.

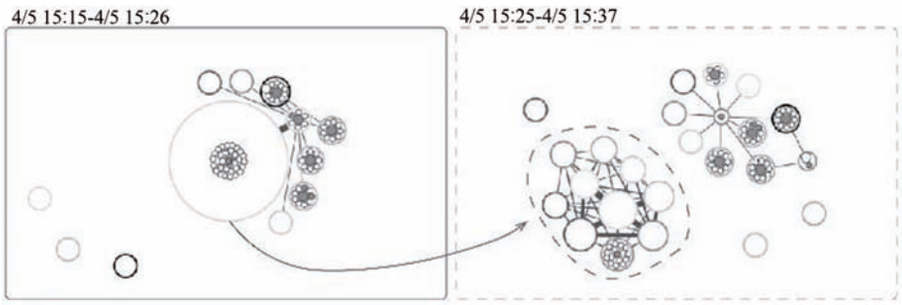

图5 信息熵异常某一时间段的突变点网络概览视图

4.3.2 DDoS

选择和流量相关的特征组，从异常关联视图上看，从4月3日上午到4月4日上午有大量异常事件.如图6所示，选取一个异常程度最高的时间段4月3日的9:28—10:57，并查看其网络布局.可以发现有多个粗箭头指向172.20.0.4和172.30.0.4这两个服务器以及工作站172.20.0.15，这说明它们被大流量的访问，鼠标悬浮可以确认具体流量大小总共在3 GB左右，可以判断是一次DDoS攻击.

由于图6的异常关联视图中除了172.30.0.4，其他几个IP都聚合为了一类(说明有相似的行为)，因此进一步确认172.30.0.4，发现它在这次攻击之后一直到4与6日之前都不再出现，可能是因为这次攻击导致其暂时崩溃.

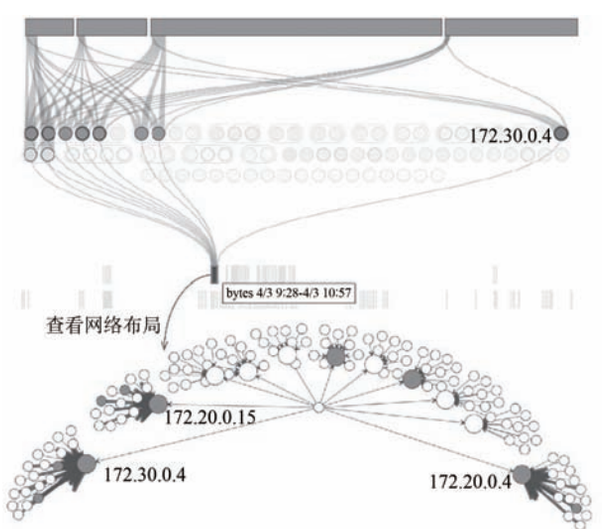

图6 选取流量异常程度最高的时间段并查看其网络布局

4.3.3 重定向

点击4月4日上午5:42—7:15的异常时间段，从概览视图中可以观察到网络结构发生了很大的变化，接着我们查看其详细网络布局.如图7所示，与服务器172.20.0.4发生通信的大量内部IP与外部IP10.7.5.5都发生了连接.事实上，这个异常是由

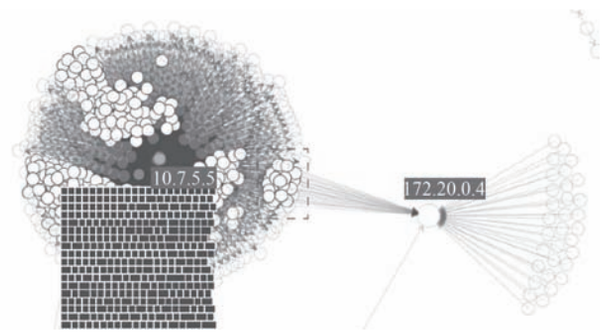

图7 4月4日上午5:42—7:15时间段的网络布局

于服务器172.20.0.4被植入了恶意软件，所有连接这个网站的访问者都被重定向到了恶意的外部IP 10.7.5.5，导致访问者也受到感染.

4.4 方法对比

我们与Vast challenge 2013挑战三的两个获奖作品，即中南大学和北京大学参赛队的作品，从以下四个方面进行了分析比较：

1) 设计目标：这两个队伍的作品主要是针对于比赛要求进行设计的，而我们的系统旨在提出一种新的网络异常检测方法以检测到更加细微的网络异常；

2) 数据格式：这两个获奖作品除了使用NetFlow数据之外，还使用了比赛方提供网络和主机状态的日志数据.考虑到系统的通用性，我们只利用NetFlow数据进行分析；

3) 关键方法：这两个获奖作品的可视化设计相对丰富和复杂，一方面是由于数据格式丰富，另一方面是因为他们主要通过可视化界面进行网络安全态势感知.而我们的系统主要侧重于利用后端的算法发现可能的异常事件、IP，接着通过可视化界面进一步验证和发现异常；

4) 分析结果：除了通过日志数据发现的异常之外，我们的系统几乎可以发现这两个获奖作品找到的其他异常，甚至可以相较于他们检测到更加细微的网络异常(如重定向).但是，他们的可视化设计比较丰富，可以根据统计分析视图发现FTP泄露这类

异常.因此,我们可以考虑在后期的工作中丰富可视化设计.

4.5 用户评估

为了进一步验证所提出系统的有效性,我们设计并进行了用户评估.实验中,我们邀请了5名具有计算机背景但不了解网络攻击的用户.由于DDoS攻击相较于其他攻击容易被用户消化和理解,因此我们在实验中主要观察用户在规定时间内发现DDoS攻击的次数.

具体地,我们首先为用户讲解可视化界面的视觉编码以及使用流程,用时15分钟.在用户熟悉界面操作后,我们请用户利用该系统在10分钟之内发现尽可能多的DDoS攻击.最后,用户反馈结果表明,所有人都发现至少2例DDoS攻击,甚至有用户发现4例DDoS攻击.因此,本系统对于不具备专业知识的用户来说也是有效的.

5 结 论

在本文中,我们提出了一种全新的网络异常检测方法,该方法将图论中的社区发现方法和传统统计方法相结合,应用于网络安全数据检测,首先对时间窗内的网络划分社区,然后以社区为粒度提取特征并监控特征的变化情况来获取离群程度较高的异常点,之后通过一个迭代算法进一步检测导致社区异常的网络节点并聚类.此外,提出算法检测导致社区特征异常的IP.这些结果通过高度可交互的可视化界面呈现给用户,使得用户可以更好地掌握全局异常情况,提高态势感知能力.

案例分析部分表明,相对其他方法,该方法能够检测到更加细微的网络异常.但是该方法的一个问题是缺少详细信息例如特征的具体变化情况的可视化模块等,在对于异常的佐证方面较为欠缺.当前异常检测的阈值是基于均值和方差,可以考虑将异常值的分布提供给用户,交由用户来决定阈值的方式.此外,该方法对全体数据检测一次异常的耗时较长,在未来的工作中,可以考虑增量的异常检测方法和动态社区检测方案.

参 考 文 献

[1] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey.ACM Computing Surveys (CSUR), 2009, 41(3): 1-58

[2] Bhuyan M H, Bhattacharyya D K, Kalita J K. Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials, 2013, 16(1): 303-336

[3] Buczak A L, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 2015, 18(2): 1153-1176

[4] Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection//Proceedings of the 2010 IEEE Symposium on Security and Privacy. Oakland, USA, 2010: 305-316

[5] Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: a survey. Data Mining and Knowledge Discovery, 2015, 29(3): 626-688

[6] Muelder C, Ma K L, Bartoletti T. A visualization methodology for characterization of network scans//Proceedings of the IEEE Workshop on Visualization for Computer Security, 2005VizSEC 05. Minneapolis, USA, 2005: 29-38

[7] Tsuge Y, Tanaka H. Quantification for Intrusion Detection System Using Discrete Fourier Transform//2016 International Conference on Information Science and Security (ICISS). Pattaya, Thailand,2016: 1-6

[8] Shiravi H, Shiravi A, Ghorbani A A. A survey of visualization systems for network security. IEEE Transactions on Visualization and Computer Graphics, 2011, 18(8): 1313-1329

[9] Ying Z, Xiaoping F, Fangfang Z. A survey on network security data visualization. Journal of Computer-Aided Design and Computer Graphics, 2014, 26(5): 687-697

[10] Theron R, Magán-Carrión R, Camacho J, et al. Network-wide intrusion detection supported by multivariate analysis and interactive visualization//Proceedings of the 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). Phoenix, USA, 2017: 1-8

[11] Sultana A, Jabbar M A. Intelligent network intrusion detection system using data mining techniques//Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). Bangalore, India,2016: 329-333

[12] Ranshous S, Shen S, Koutra D, et al. Anomaly detection in dynamic networks: a survey. Wiley Interdisciplinary Reviews: Computational Statistics, 2015, 7(3): 223-247

[13] Idé T, Kashima H. Eigenspace-based anomaly detection in computer systems//Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA,2004: 440-449

[14] Sun J, Xie Y, Zhang H, et al. Less is more: Compact matrix decomposition for large sparse graphs//Proceedings of the 2007 SIAM International Conference on Data Mining. Minneapolis, USA,2007: 366-377

[15] Sun J, Xie Y, Zhang H, et al. Less is more: Sparse graph mining with compact matrix decomposition. Statistical Analysis and Data Mining: The ASA Data Science Journal, 2008, 1(1): 6-22

[16] Akoglu L, Faloutsos C. Event detection in time series of mobile communication graphs//Proceedings of the Army Science Conference. Orlando, USA, 2010: 1

[17] Ding Q, Katenka N, Barford P, et al. Intrusion as (anti) social communication: characterization and detection//Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA, 2012: 886-894

[18] Bach B, Pietriga E, Fekete J D. Graphdiaries: Animated transitions andtemporal navigation for dynamic networks. IEEE Transactions on Visualization and Computer Graphics, 2013, 20(5): 740-754

[19] Farrugia M, Quigley A. Effective temporal graph layout: A comparative study of animation versus static display methods. Information Visualization, 2011, 10(1): 47-64

[20] Archambault D, Purchase H C, Pinaud B. Difference map readability for dynamic graphs//Proceedings of the International Symposium on Graph Drawing. Berlin, Germany: Springer, 2010: 50-61

[21] Fortunato S, Hric D. Community detection in networks: A user guide. Physics Reports, 2016, 659: 1-44

[22] Yang Z, Algesheimer R, Tessone C J. A comparative analysis of community detection algorithms on artificial networks. Scientific Reports, 2016, 6(1): 1-18

[23] Satuluri V, Parthasarathy S. Scalable graph clustering using stochastic flows: applications to community discovery// Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA, 2009: 737-746

[24] Clauset A, Newman M E J, Moore C. Finding community structure in very large networks. Physical Review E, 2004, 70(6): 066111

[25] Cavallari S, Zheng V W, Cai H, et al. Learning community embedding with community detection and node embedding on graphs//Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. New York, USA, 2017: 377-386

[26] Xin X, Wang C, Ying X, et al. Deep community detection in topologically incomplete networks. Physica A: Statistical Mechanics and its Applications, 2017, 469: 342-352.

[27] Blondel V D, Guillaume J L, Lambiotte R, et al. Fast unfolding of communities in large networks. Journal of Statistical Mechanics: Theory and Experiment, 2008, 2008(10): P10008.

[28] Lancichinetti A, Fortunato S. Community detection algorithms: a comparative analysis. Physical Review E, 2009, 80(5): 056117

[29] Traag V A, Van Dooren P, Nesterov Y. Narrow scope for resolution-limit-free community detection. Physical Review E, 2011, 84(1): 016114

[30] Spiliopoulou M. Evolution in social networks: A survey// Proceedings of the Social Network Data Analytics. Boston, USA:Springer, 2011: 149-175

[31] Palla G, Barabási A L, Vicsek T. Quantifying social group evolution. Nature, 2007, 446(7136): 664-667

[32] Chakrabarti D, Kumar R, Tomkins A. Evolutionary clustering// Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA, 2006: 554-560

[33] Mucha P J, Richardson T, Macon K, et al. Community structure in time-dependent, multiscale, and multiplex networks. Science, 2010, 328(5980): 876-878

[34] Greene D, Doyle D, Cunningham P. Tracking the evolution of communities in dynamic social networks//Proceedings of the 2010 International Conference on Advances in Social Networks Analysis and Mining. Odense, Denmark, 2010: 176-183

[35] Quinlan J R. Induction of decision trees. Machine Learning, 1986, 1(1): 81-106

[36] Tavallaee M, Bagheri E, Lu W, et al. A detailed analysis of the KDD CUP 99 data set//Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. Ottawa, Canada,2009: 1-6

[37] Aljawarneh S, Aldwairi M, Yassein M B. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 2018, 25: 152-160

[38] Schölkopf B, Williamson R C, Smola A J, et al. Support vector method for novelty detection//Proceedings of the 12th International Conference on Neural Information Processing Systems. Denver, USA, 1999, 12: 582-588

[39] Ester M, Kriegel H P, Sander J, et al. A density-based algorithm for discovering clusters in large spatial databases with noise//Proceedings of the Second International Conference on Knowledge Discovery and Data Mining. Portland, USA, 1996, 96(34): 226-231

[40] VAST Challenge 2013 Homepage. http://www.vacommunity.org/vast+challenge+2013

QIAN Ai-Juan, M.E. candidate. Her research interests include machine learning and visualization.

FAN Xin, M.E. candidate. Her research interests include visualization and network security.

DONG Xiao-Ju, Ph. D., associate professor. Her major research interests include information visualization and visual analysis, digital humanities, formal methods.

CHU Yan-Jie, Ph. D., associate professor. His major research interest includes network data analysis.

YUAN Xiao-Ru, Ph. D., professor. His major research interests include visualization, visual analysis and human-machine interaction.

Background

Network has gradually integrated into the layers of human lives, providing modern information technology support for every walk of life. But in other instances, the increasingly complex and large network attacks have made increasing network security risk, which is a serious threat to the whole society. Although there exist some anomaly detection researchers that can discover and defend network attacks to some degree, some of them have high training costs that conflict with the demand of real-time scenes, others are difficult to apply to unlabeled datasets. Besides, the detection of subtle anomalies is also an important problem of existing methods.

Consequently, we propose a network anomaly detection method based on community detection, which improves the ability to detect subtle anomalies through an appropriate level of granularity. This method first utilizes the multi-layer CPM algorithm to detect the community of network data in the moving time window, extracts the feature vector with the community as the unit, and then uses the community matching method to correlate the communities of adjacent time steps, and detects the anomaly by monitoring the changes of the characteristics of each community. This method not only considers the characteristics of network data as a dynamic graph, but also can extract features from a suitable granularity. In addition, we provide a visual interface to help users confirm the network situation before and after the exception point and correlate the exception events. Experiments and case studies prove that our method is feasible and effective.

This work is supported by the National Key Research and Development Program of China (Grant No. 2017YFB0701900), the National Nature Science Foundation of China (Grant No. 61100053) and the Key Laboratory of Machine Perception in Peking University (K-201K-2019-09).