基于网络通信异常识别的多步攻击检测方法

琚安康，郭渊博，李涛，叶子维
（战略支援部队信息工程大学密码工程学院，河南 郑州 450001）

摘 要：针对企业内部业务逻辑固定、进出网络访问行为受控等特点，首先定义了 2 类共 4 种异常行为，然后提出了基于网络通信异常识别的多步攻击检测方法。针对异常子图和异常通信边 2 类异常，分别采用基于图的异常分析和小波分析方法识别网络通信过程中的异常行为，并通过异常关联分析检测多步攻击。分别在 DARPA 2000 数据集和 LANL 数据集上进行实验验证，实验结果表明，所提方法可以有效检测并重构出多步攻击场景。所提方法可有效监测包括未知特征攻击类型在内的多步攻击，为检测 APT 等复杂的多步攻击提供了一种可行思路，并且由于网络通信图大大减小了数据规模，因此适用于大规模企业网络环境。

关键词：多步攻击；网络异常；通信子图；小波变换
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019142

Multi-step attack detection method based on network communication anomaly recognition

JU Ankang, GUO Yuanbo, LI Tao, YE Ziwei
Department of Cryptogram Engineering, Strategic Support Force Information Engineering University, Zhengzhou 450001, China

Abstract: In view of the characteristics of internal fixed business logic, inbound and outbound network access behavior, two classes and four kinds of abnormal behaviors were defined firstly, and then a multi-step attack detection method was proposed based on network communication anomaly recognition. For abnormal sub-graphs and abnormal communication edges detection, graph-based anomaly analysis and wavelet analysis method were respectively proposed to identify abnormal behaviors in network communication, and detect multi-step attacks through anomaly correlation analysis. Experiments are carried out on the DARPA 2000 data set and LANL data set to verify the results. The experimental results show that the proposed method can effectively detect and reconstruct multi-step attack scenarios. The proposed method can effectively monitor multi-step attacks including unknown feature types. It provides a feasible idea for detecting complex multi-step attack patterns such as APT. And the network communication graph greatly reduces the data size, it is suitable for large-scale enterprise network environments.

Key words: multi-step attack, network anomaly, communication graph, wavelet analysis

1 引言

根据近年来国家互联网应急中心发布的中国互联网网络安全报告，个人信息泄露、网络钓鱼等安全事件数量呈上升趋势；网络基础设备、域名系统等基础网络和关键基础设施依然面临着较大的安全风险，网络攻击事件多有发生，针对重要信息系统的高强度、有组织的攻击威胁形势日益严峻，多步攻击已经成为网络攻击的主要方式[1]。

网络攻击是尝试破坏资源完整性、保密性和可用性的行为集合。当攻击行为具有独立的、不可分

收稿日期：2018−09−06；**修回日期**：2019−05−22
基金项目：国家自然科学基金资助项目（No.61501515）
Foundation Item: The National Natural Science Foundation of China (No.61501515)

解的攻击目的时，被称为单步攻击。多步攻击是将单步攻击按照一定的逻辑关系进行排列，在特定的时间和空间中形成一个攻击序列，从而实现仅用单步攻击无法实现的攻击意图[2]。

与传统攻击方式相比，多步攻击采用的手段更加丰富，不仅包括拒绝服务（DoS, denial of service）攻击、Web 渗透（如跨站脚本攻击等）、扫描攻击、暴力破解等常见攻击方式，还包括隐蔽式木马、新型僵尸网络等新型攻击手段。采用新型攻击手段的多步攻击以复杂网络攻击[3]和 APT（advanced persistent threat）[4]为典型代表，其造成的危害更加严重且检测难度较大，是影响当前网络安全状况的重要因素。APT 是一种具有高度复杂性、强隐蔽性的多步攻击，其检测问题已成为网络安全领域关注的重点，也是近年来学术研究的热点课题[3,5]。

告警关联分析[6-8]、攻击图[9]等技术为多步攻击检测提供了很好的解决思路，但这些方法都建立在已知攻击特征的检测技术基础上，依赖于多步攻击模式的专家知识，针对未知特征的攻击行为没有很好的检测效果。异常检测技术是应对 APT 等未知威胁的可行方法，但传统单点检测的方法只能发现某阶段的局部异常事件，无法从局部异常事件还原出整体攻击过程；同时，由于异常检测技术本身误报情况严重，如何降低误报是异常检测技术研究的关键问题。

GBAD（graph-based anomaly detection）在社区发现、模式识别等众多领域得到广泛应用，在入侵检测领域同样有着诸多研究成果[10]。结合典型企业网络环境与攻击链模型，本文提出了一种通过检测网络通信异常来识别多步攻击的方法。分别采用基于图的异常分析和小波分析方法识别多步攻击带来的 2 类共 4 种网络异常行为，并给出关联重构多步攻击场景的方法，为检测复杂网络攻击、APT 等定制化多步攻击提供方法。

2 多步攻击示例与威胁模型

本节首先给出典型企业网络部署示例，并举例说明企业网络环境下的多步攻击实施过程，在此基础上给出基本定义和多步攻击威胁模型。

2.1 典型企业网络环境及多步攻击示例

企业网络环境下多步攻击场景可用击杀链模型进行刻画。击杀链模型[11]是对攻击行为的一种通用性描述，它最早由 Jeffrey Carr 于 2008 年提出，并在 2013 年经 Lockheed Martin 公司优化进而形成模型。击杀链模型将攻击概括为目标侦察、武器定制、投递、利用、安装、建立通道、行动实施等攻击步骤。击杀链实施过程如图 1 所示。

图 1 击杀链实施过程

击杀链实施过程具体描述如下。攻击者在采取攻击行动之前，首先要对攻击目标的相关情报进行收集，对目标网络有一定的了解后，定制相应的攻击工具，开始实施攻击行为。初始入侵阶段采用社会工程、漏洞利用等方法，对目标网络中的弱点主机渗透侵入，并以此建立立足点。对立足点主机实现持续控制后，通过立足点主机对内网进行探测，分析网络拓扑和可利用漏洞。之后向内网中弱点主机植入恶意软件，提升用户权限，并逐步向内网渗透。在收集获取到目标数据后，将数据通过层层跳板外传，最后清除日志掩饰攻击行为。

典型企业网络环境如图 2 所示。攻击者为获取系统内部敏感数据，可通过下述步骤对数据进行窃取。1) 在攻击之初，攻击者对目标网络进行扫描探测，渗透侵入 DMZ（demilitarized zone）中的 Web 服务器，并以此作为继续侵入内部系统的立足点；2) 攻击者以 Web 服务器为立足点，逐步渗透侵入内部关键数据节点；3) 攻击者在关键数据节点加载恶意软件，提升用户权限并获取关键数据，然后通过远程访问服务在内部数据节点与外部主机之间创建网络隧道；4) 利用网络隧道，将关键文件或数据传输至 DMZ 中的 Web 服务器，并通过各个跳板，将敏感数据传输至外部站点，最终实现数据窃取目的。

一般来说，在每一个活动步骤中，攻击者虽然有意识地在目的达成后擦除系统日志等攻击痕迹，设法伪装自己，然而网络通信行为必然会在各类网络设备中留下行为痕迹，也会在网络通信日志中留下活动记录，并且攻击者的网络通信行为与正常用户操作会有差别，这为检测出攻击行为提供了可能。另一方面，在企业内部网络环境中，由于业务逻辑较为固定，且在网络边缘部署内容过滤产

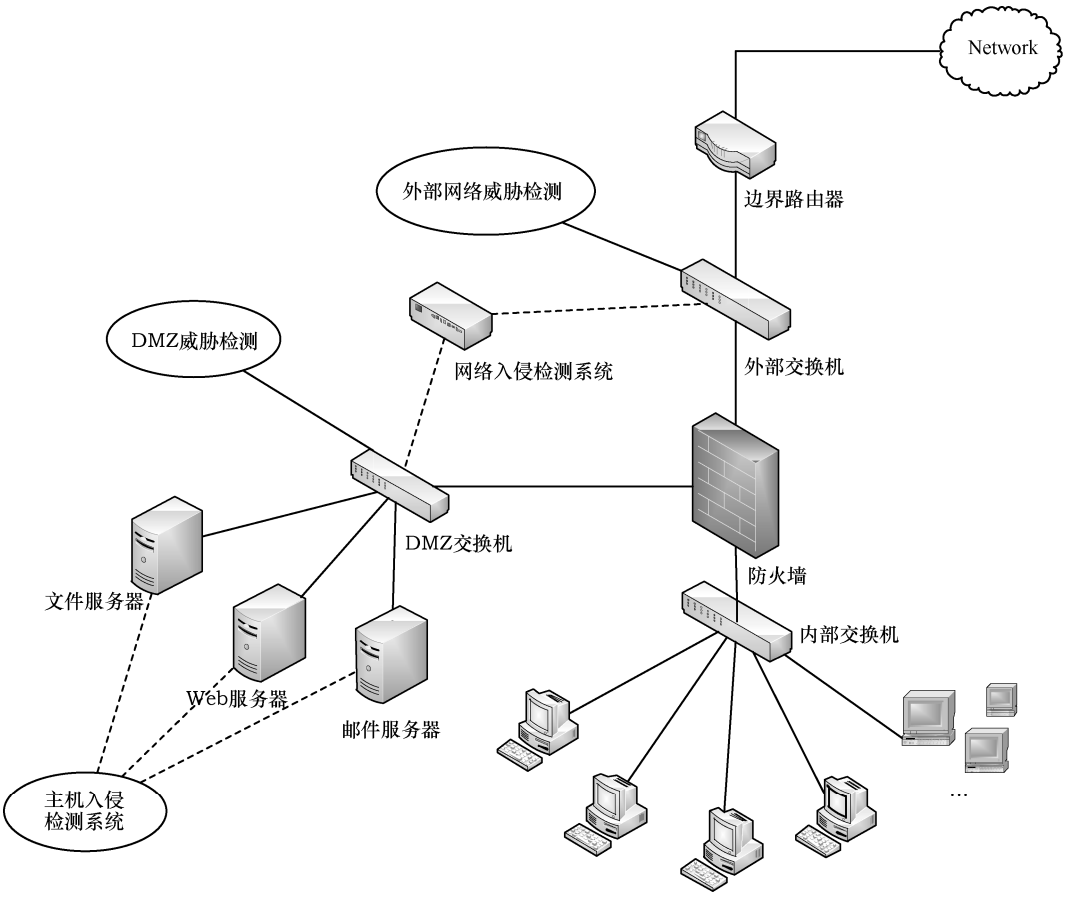


图 2　典型企业网络环境

品分析网络数据分组并对网络内容进行过滤，从而使进出网络的访问行为受限，因此通过检测异常网络通信行为来识别多步攻击场景的方法是可行且有效的。

由于攻击活动的实施会在网络通信日志中留下记录，且与企业网络环境中正常业务逻辑有明显区别，根据上述分析可以得出采用基于网络图的方法检测多步攻击网络通信异常行为的检测依据：多步攻击的发生，会在受攻击主机、中间节点、受攻击对象等各类网络实体之间引入额外的通信流量，且攻击活动会带来与正常业务相区别的通信模式。

基于上述检测依据，本文提出基于检测网络通信异常行为的多步攻击检测方法，识别异常通信子图并结合通信数据量的统计异常情况，确定异常主机并关联分析得出多步攻击事件，通过后续综合分析得出多步攻击场景，以发现系统潜在安全威胁，保护系统资源的完整性、保密性和可用性。

2.2　威胁模型

为便于后续描述，给出下述基本定义。

定义 1　多步攻击事件集。攻击者为实现最终攻击目的而实施的攻击事件集，是由多个基本攻击事件构成的攻击事件集合。

定义 2　多步攻击场景。具有特定攻击目的并由攻击者发起的一次有计划的、完整的攻击过程，通常由多步攻击事件集按照一定逻辑关系排列构成，是集合中各攻击事件按照一定的时间或空间关系组成的攻击序列。

在正常的工作状态下，主机的网络通信行为有着一定的规律性。例如，有些主机之间没有直接通信关系、平时通信量较少或只有单向连接关系等；而在多步攻击实施过程中，攻击发起主机或受感染主机的网络通信行为与正常业务主机的行为有所偏离[12]。4 种最为常见的多步攻击事件类型介绍如下。

1) 拒绝服务攻击（DoS）。攻击者通过控制僵尸网络发动 DoS 攻击，以达到致瘫目标节点的目的，在攻击发动阶段会有多个 IP 向单个主机发起连

接。基本攻击事件之间具有并列关系，其网络通信行为呈现汇聚形态。

2) 扫描探测（scan）。攻击者向内网渗透的首要工作是扫描探测以查找弱点主机，扫描一定范围的内网节点，查找具有开放服务和可利用漏洞的弱点主机，在这一过程中，攻击者会从单个主机向内部网络中多台主机发起网络通信。基本攻击事件之间具有并列关系，其网络通信行为呈现发散形态。

3) 内网渗透（penetrate）。攻击者从立足点主机出发，逐步向内网迁移渗透，寻找存储关键数据的目标主机，是由弱点主机一步一步探测并向目标主机迁移的过程。基本攻击事件之间具有依赖关系，其网络通信行为呈现连续的发散形态。

4) 数据获取（get）。在得到关键节点的高级权限后，攻击者提取目标数据并通过跳板节点向网外传输，会带来通信流量的数据异常。基本事件之间具有选择关系，其网络通信行为呈现明显突发性变化。

在上述 4 种攻击示例中，示例 1)~示例 3)都是特殊的通信子图形式，通过对一定时间窗口内的网络通信情况进行分析，得出异常子图并对其分析验证；示例 4)需要对 2 个节点之间的正常通信数据进行建模分析，找出通信行为统计规律，计算通信过程在各时刻的异常值，从而发现异常的数据通信。

与上述 4 种多步攻击事件相对应的网络通信特征如图 3 所示。其中，图 3(a)为 in-star，即多条连接指向单个节点；图 3(b)为 out-star，即单个节点发出多条连接；图 3(c)为 k-path，即攻击者向目标节点逐步渗透；图 3(d)为 red-edge，即通信边的数据流量突发性异常。

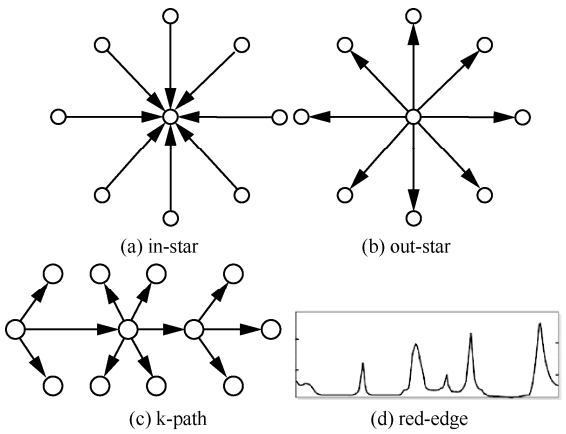


图 3 4 种网络异常通信特征

攻击链模型中各攻击阶段描述与图 3 中对应的异常通信特征如表 1 所示。

表 1 各攻击阶段及异常通信特征

攻击阶段	阶段描述	异常通信特征
扫描探测	目标网络扫描探测，获取网络拓扑及漏洞信息	out-star
内网迁移	以 Web 服务器为立足点，逐步渗透侵入内部关键数据节点	k-path
建立通道	在内部数据节点与外部主机之间创建网络隧道	k-path
攻击达成	关键文件或数据通过各个跳板传输至外部站点	red -edge、in-star

通过上述对 4 种类型多步攻击实施过程的分析，可以归纳出下述 3 种基本攻击事件之间的逻辑关系。

1) 并列关系。多个单步攻击以任意次序全部成功，才是下一步攻击实施的前提。

2) 依赖关系。一个单步攻击的成功是另一个单步攻击实施的前提条件。

3) 选择关系。多个单步攻击中任意一个成功实施，即为另一个单步攻击创造了前提。

上述 3 种关系概括了大多数多步攻击实施过程中各原子事件的基本逻辑关系，在多步攻击实施过程中，一个完整的多步攻击可能是多种类型多步攻击事件的组合。

上面给出了典型企业网络环境及多步攻击示例，在实际检测过程中，需要先根据异常网络通信行为检测出多步攻击事件，再将多步攻击事件进行关联分析，从而得出多步攻击场景，最终达到检测出多步攻击的目的。

3 检测思路及算法

本文通过分析对应于网络图的各类异常子图模式，识别多步攻击带来的异常网络通信行为。针对多步攻击带来的异常通信特征，采用基于图的异常检测方法，检测滑动时间窗口内的异常通信子图；并基于小波变换的方法分析检测网络攻击行为在持续控制阶段、数据外传阶段产生的异常通信行为，然后通过对 2 种异常的关联分析得出主机的异常值评分，并通过对各个异常事件的关联重构出多步攻击场景。

本节首先介绍网络通信模型的基本定义，在此基础上给出基于网络异常识别的多步攻击检测解

决方案。

3.1　网络通信模型

对网络通信模型进行如下定义。整体网络通信数据可表示在一个时间与通信图的叉乘空间 $S=T\times G$ 内[13]，其中，通信图 $G=(V,E)$，节点集 V 包括网络内所有通信主机，边集 E 包括所有具有网络通信行为的通信边。对于每条边 $e\in E$，在任意的离散时间点 $t\in\{1,\cdots,T\}$，都可以得到一个数据过程 $X_e(t)$，时间 T 内所有时间窗口 $\Omega=\{(s,s+1,\cdots,k):\ 0\leqslant s<k\leqslant T\}$，给出包含时间 T 内的所有时间窗口集合的全集 $\Gamma=\{\{\omega_1,\omega_2,\cdots,\omega_i,\cdots,\omega_n\}:\omega_i\in\Omega\}$。通常只研究包含约束的时间窗口集合 $\tau\in\Gamma_R$，将在一定的时间窗口 τ 内的通信边 e 表示为 $X_e(\tau)$。研究的整体数据空间可表示为 $S=\{(\omega,g)\,|\,\omega\in\Omega,g\in G\}$，其中，$\omega$ 为时间窗口，g 是在该时间窗口内的通信图。

3.2　基于滑动时间窗口的异常通信子图检测算法

本节检测第一类异常——异常子图，对应于图 3(a)～图 3(c)所示的 3 种异常。采用基于滑动时间窗口的异常通信子图检测算法，在特定时间窗口内匹配与这 3 种异常相对应的子图模式，并根据匹配度计算异常值，异常值计算方法需满足以下条件。

1) 在一定时间窗口内，某一节点的度大于正常情况，且入度远大于出度，二者的值相差越多，异常值越大。

2) 在一定时间窗口内，某一节点的度大于正常情况，且出度远大于入度，二者的值相差越多，异常值越大。

3) 若干个节点出度大于入度，且形成连续渗透的图状结构，时间上有先后约束关系。由于路径过短不能反映出多步攻击的实施特点，路径过长的多步攻击发生可能性较低，且可以被短路径检测结果涵盖，综合考虑实际攻击案例，本文选择异常路径长度为 3。

整体数据空间 $S=\{(\omega,g)\,|\,\omega\in\Omega,g\in G\}$，其中，时间窗口 ω 与时间窗口内的通信图 g 在上文中已有定义，这里考察异常子图集合 $S'\subseteq S$。引入异常值函数 f 的定义，$f:S\to R$，且 $\forall s'\in S'$，有 $|f(s')-\widehat{f}|>c_0$，其中 c_0 为异常阈值，异常值函数 f 的计算过程遵照上述原则。

异常子图生成算法思想为：对滑动时间窗口内的通信图 g 计算其异常值，若 g 满足异常子图模式且异常值大于设定阈值，则将其加入异常子图列表。此算法目的在于，检测出在一定时间区间内与特征模式相匹配的所有异常通信子图，计算出相应置信度和节点异常值，并生成异常子图列表。异常子图生成算法如算法 1 所示。

算法 1　异常子图生成算法

输入　(G,Ω)

输出　(graph_list)

```
while t!=
{
  renew( G );
  for each subgraph  g  in  G
    compute  f(g);
    if  | f(g) − f̂ | > c0
      tag  g  with timstamp and add  g  to graph _ list ;
      else continue;
    end if
  end for
  t=t+slide_window;
}
return  graph _ list ;
```

与 Neil 等[13-14]以天为时间单位进行异常分析的方法不同，由于以天为单位不符合多步攻击带来网络通信的短时间变化，为更加细粒度地分析攻击实施细节，本文选取的时间窗口为 7 200 s，即 2 h；时间窗口每次滑动 1 800 s，即 30 min。

对于有 n 个通信节点、e 条通信边的通信图 G，检测 T 时间内的所有异常子图（假设时间窗口为 t_w，每次滑动 t_s），其算法复杂度为 $O(\frac{t_w}{t_s}Tn)$。

3.3　基于小波变换的网络通信异常分析算法

本节检测第二类异常——异常通信边，即图 3(d)所示的异常。使用泊松模型描述网络突发量时存在较大误差，现有研究表明，正常网络流量具有自相似性，而网络攻击行为产生的异常流量会对网络流量的自相似性产生明显的影响[15]。Hurst 指数是反映网络流量长相关和自相似性的重要指标。因此，为有效地检测出单个通信边的数据量异常，本文采用小波分析的方法，求解正常通信流量的 Hurst 指数，检测出网络通信中的异常点，返回异常通信边列表 edge_list。

小波变换通过将时域中的通信数据变换到小波域内对数据进行预测，再将预测值转换到时域

中。目前，主要有 3 种利用小波变换求解 Hurst 指数的方法：能量法、小波分析法和谱估计法。本文选择小波分析法进行求解，算法原理描述如下。

给定一个时间序列 $X_i, i=1,2,\cdots,n$，对其进行二进制小波变换。

$$d_X(j,k)=2^{\frac{j}{2}}\sum_{i=1}^{n}X_i\psi(2^{-j}n-k), j=1,2,\cdots,2^{-j}n$$

其中，$\psi(\cdot)$ 为母小波函数，$d_X(j,k)$ 为小波变换系数，j 为尺度参数，k 为平移参数。若 X_i 为二阶平稳过程，则

$$E[d_X(j,k)^2]\approx\int f(v)2^j\left|\psi(2^jv)\right|^2\mathrm{d}v$$

其中，$f(v)$ 和 $\psi(v)$ 分别为 X_i 的功率谱和 $\psi(\cdot)$ 的傅里叶变换，而且

$$E[d_X(j,k)^2]\sim 2^{j(2H-1)}C_fC(H,\psi)$$

其中，$C(H,\psi)=\int|v|^{-(2H-1)}\left|\psi(v)\right|^2\mathrm{d}v$ 是依赖于 H 和 ψ 的常数，C_f 是尺度变换系数。若 X_i 长度为 n，则在尺度 j 上，小波变换系数的个数 $n_j=2^{-j}n$，则有

$$\mu_j=E[d_X(j,k)^2]\approx\frac{1}{n}\sum_{k=1}^{n_j}\left|d_X(j,k)\right|^2$$

于是有

$$\mathrm{lb}\mu_j\approx\mathrm{lb}\left[\frac{1}{n}\sum_{k=1}^{n_j}\left|d_X(j,k)\right|^2\right]\sim(2H-1)j+c$$

其中，$c=\mathrm{lb}[C_fC(H,\psi)]$，采用最小二乘法线性拟合得到的斜率为 $\alpha=2H-1$。

Mallat 算法是计算离散栅格上小波变换的快速算法，其时间复杂度和空间复杂度均为 $O(N)$，其中 N 为待分析序列的长度，这里选取 Mallat 算法对通信序列进行离散小波变换，以实现求解 Hurst 参数过程中小波系数的快速提取。

3.4 异常关联分析

3.1 节~3.3 节完成了对异常子图和异常通信过程的建模分析，分别得出异常子图列表 graph_list 和异常通信边列表 edge_list。为降低误报率，还需要采用异常关联算法，将 2 类异常进行关联分析，得出置信度和完整性更高的攻击场景。异常关联算法通过综合评估多步攻击事件异常值，得出节点异常值评分结果，进而生成异常列表以便于后续检索分析，最后生成按置信度大小排列的多步攻击场景列表，如算法 2 所示。

算法 2 异常关联分析算法

输入 (graph_list,edge_list)

// graph_list 是异常子图列表

// edge_list 是异常子图通信边列表

输出 (node_list,senoria_list)

// node_list 是异常节点列表

// senoria_list 是多步攻击场景列表

```
for g in graph_list
for n in g
{
//参照 g 的异常值标记相关节点
compute n.outlier ;
//给节点添加时间标记和异常类型
tag n with timestamp and type ;
add n into node_list ;
  }
for e in edge_list
{
//参照 e 的异常值，标记相关节点
compute n.outlier in e;
tag n with timestamp and type ;
add n into node_list ;
}
//对 node_list 进行归约和聚合
correlate and aggregate node_list ;
//关联分析得出多步攻击场景列表 senoria_list ;
return node_list and senoria_list .
```

用户可以以异常主机为索引进行检索查询和完善验证，具体应用过程如图 4 所示。

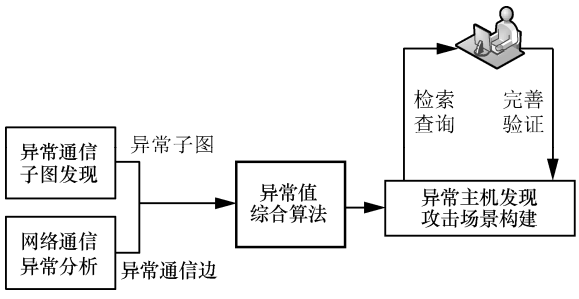


图 4 应用过程

4 实验与结果分析

为验证所提方法，本文分别对 LLDoS1.0 数据集和 LANL 数据集开展实验，验证方法的有效性和扩展性，算法实现分别使用 Python 包 NetworkX（版

本号 1.11）和 PyWavlets（版本号 0.5.2）。

4.1　数据集选取

目前，在入侵检测技术的相关研究中，检测数据源的问题一直比较突出。虽然目前文献中已经有学者研究讨论了入侵检测数据集陈旧的问题，然而，这些数据集仍然被近来的多数研究采用；同时也有课题组给出自己的数据集模拟生成方法，产生 testbed 数据集[16]，针对生成的 testbed 数据集开展实验，以方便其他研究人员使用或参考生成满足需求的测试数据集。总体来说，现有的公开数据集不能满足新型攻击检测及验证需求，而模拟数据不能反映网络攻击的现实情况。当前在入侵检测领域常用的数据集如表 2 所示。

表 2　　入侵检测领域常用数据集

数据来源	数据集名称	简称
网络流量	DARPA1998 TCPDump 数据集	DARPA98 TCPDump
	DARPA 1999 TCPDump 数据集	DARPA99 TCPDump
	KDD99 数据集	KDD99
	10% KDD99 数据集	KDD99-10
	Internet Exploration Shootout Dataset	IES
用户行为	Unix User Dataset	UNIXDS
系统调用序列	DARPA 1998 BSM 数据集	DARPA98 BSM
	DARPA 1999 BSM 数据集	DARPA99 BSM
	University of New Mexico Dataset	UNM

其他较新的入侵检测数据集有 ISCX、MAWI、NSA Data Capture、Internet Storm Center 等。然而即使在最近的文献中，这些新数据集的使用率也并不高，原因在于没有一个较权威的认证使其他研究者认可其可靠性，而 KDD 99、DARPA 99 等数据集虽然较老旧，但仍是大部分研究者选用的数据对象。

综合考虑现有方法，本文选取了 DARPA 2000 LLDoS1.0 数据集和 LANL 实验室的公开测试数据集作为实验对象。以较权威的 DARPA 2000 数据集中的 LLDoS1.0 数据集检验方法的有效性；为检验大型网络中未知特征的攻击检测效果，选取 LANL 数据集对方法的分析效率和扩展性进行进一步分析。

4.2　基于 DARPA 2000 数据集的实验

DARPA 2000 数据集[16]是 MIT Lincoln 实验室在 2000 年进行 IDS 评测时获得的数据集，具有较强的权威性和代表性。数据集包含 2 个多步攻击场景，分别为 LLDoS1.0 和 LLDoS2.0.2。为验证本文方法的有效性，采用 LLDoS1.0 Inside 数据开展实验，该数据中包括了漏洞探测、非法访问、程序安装以及攻击发起等多种多步攻击事件，LLDoS1.0 数据集共包含 5 个阶段的数据：IPsweep、Probe、Breakin、Installation、Action。LLDos 1.0 攻击过程如图 5 所示。

2 种算法实现分别使用 Python 包 NetworkX（版本号 1.11）和 PyWavlets（版本号 0.5.2）。算法在实现中使用的核心函数是 degree_centrality(G) 、in_degree_centrality(G) 、out_degree_centrality(G) 、strategy_largest_first(G, color)、max_degree (int)，其功能是对网络图 G、节点集合中所包含子图及节点出入度的排序输出。通过对网络通信图的分析，得出异常子图列表和异常通信边的排序列表，经过可视化分析后，由 graphviz 绘出检测结果。

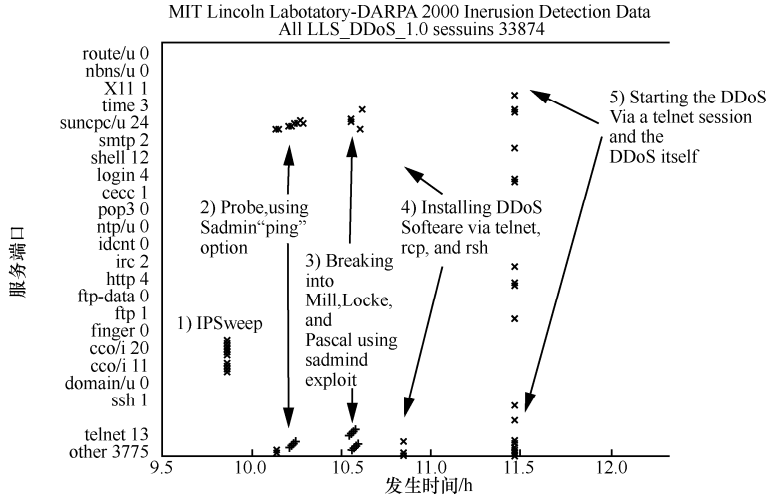


图 5　LLDoS1.0 攻击过程

异常子图检测算法实现过程如下。首先定义网络图对象 G，分别读取 LLS_DDoS_1.0-inside.dump 文件中的 tcpdump 记录，按时间顺序并将其加入 G 中（这里以 IP 地址为节点标识），其中 G 表示了在时间窗口内的网络图连通情况（选取时间窗口为 30 s），分别计算时间窗口内各个子图的异常值，将异常值过高的子图输出。

经过本文提出的检测算法，得到异常子图 a（攻击发起主机）和异常子图 b（受害主机）分别如图 6 和图 7 所示。然后，经过异常值关联分析得出多步攻击事件，通过对网络通信图的分析，得出异常子图列表和异常通信边的排序列表，经过可视化分析后，由 graphviz 绘出检测结果，最终得到一个由原始攻击组成的攻击场景。

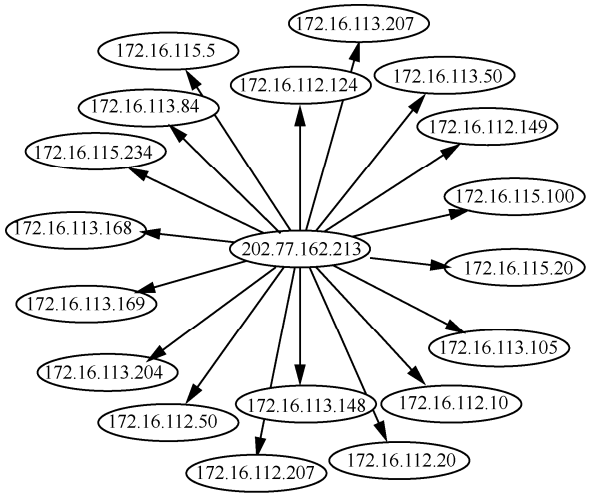


图 6 异常子图 a（攻击发起主机）

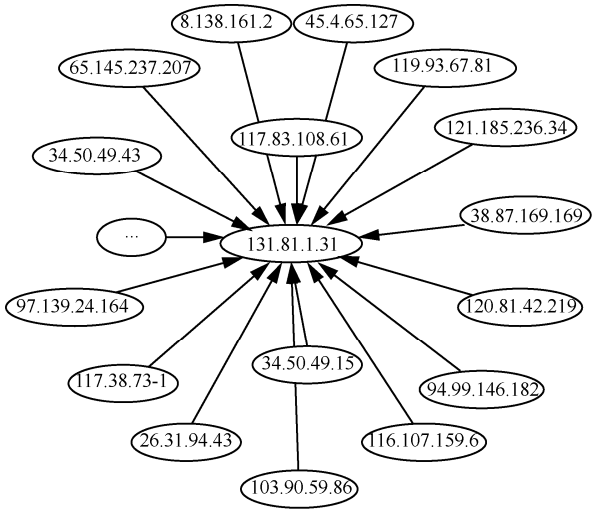


图 7 异常子图 b（受害主机）

对 LLDoS1.0 inside_dump 数据的实验结果表明，此方法可有效检测出探测渗透过程、异常数据通信（安装）、DDoS 实施过程 3 个攻击事件，经过关联分析得出整体攻击场景，如图 8 所示。

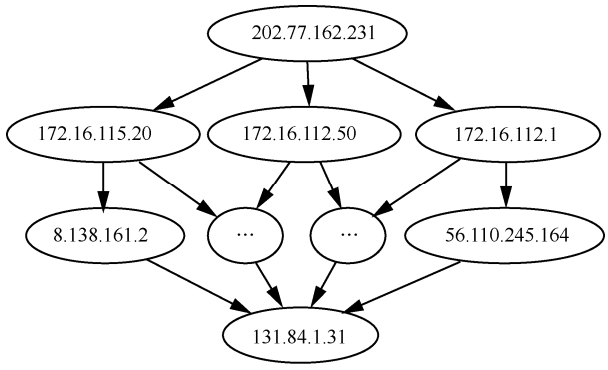


图 8 LLDoS1.0 攻击场景

针对 LLDoS1.0 数据集的实验结果与数据集中标注的攻击情况一致，即与图 5 表示的攻击过程中漏洞探测、攻击发起等步骤均一致，与攻击场景吻合。此方法可有效检测出探测渗透过程、异常数据通信、DDoS 实施过程的多步攻击事件，并经过关联分析得出整体攻击场景。由上述检测结果可知，针对多步攻击检测场景，本文所提方法可以有效检测出可疑子图和可疑通信边，通过将各类异常子图按照过程关联，可以得出整体多步攻击场景。

4.3 基于 LANL 数据集的实验

为进一步验证本文所提方法的扩展性，验证其在大规模网络中的应用效果，选取 LANL 数据集的 flows 数据作为实验对象，对所提方法的分析效率和扩展性 2 个方面进行测试。

对 LANL 数据集的 flows 数据实验与上述实验略微有所不同。因为 LANL 数据集是经过匿名化和预处理的，数据格式规整，对数据集的具体描述如下。

LANL 数据集[1]是 2010 年由 Los Alamos National Laboratory 在其内部网络数据采集而来，其中，flows 数据分组包括 29 天内由 NetFlow 记录产生的通信数据，共有 426 045 096 条数据记录，一共包含 12 027 个主机节点，99 433 条有效通信边（用 IP 地址区分不同节点，不同的源 IP 和目的 IP 看作不同的通信边），目前对此数据集发表的成果较少。

LANL 数据集中的 flows 网络流量数据采集自关键路由器上搜集的网络流量数据，其数据字段为：时间、持续时间、源主机、源端口、目的主机、目的端口、协议类型、数据分组数、字节数。网络流量数据示例如图 9 所示。

```
1,9,C3090,N10471NC3420,N46,6,3,144
1,9,C3538,N2680,C3371,N46,6,3,144
2,8,C4316,N10199,C5038,443,6,2,92
```

图 9　flows 网络流量数据示例

flows 数据整体概况如图 10 所示。

图 10　flows 数据整体概况

算法实现基于核心函数 graph. subgraph(nodes)、degree_centrality(*G*) 、 in_degree_ centrality(*G*) 、out_degree_centrality(*G*)、strategy_ largest_ first(*G*, color)、max_degree (int)，其功能是计算节点的出入度中心性、返回按度降序排列的节点列表以及计算图中节点的最大连通度。

本文采用 PyWavelets 对通信边进行数据处理，将 LANL 数据集中前 14 天数据用作训练集，后 15 天数据用作测试集，以 C17693 为例，异常通信边的分析结果如图 11 所示。

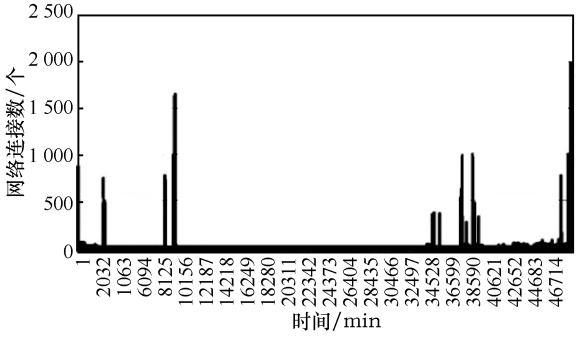


图 11　异常通信边的分析结果（C17693）

由于 LANL 网络流量数据集中主机节点数较多，数据量相对较大，采用基于网络图的通信异常检测方法分析检测 LANL 网络数据中的异常子图，计算负担较小，可以有效识别出网络图中的通信异常情况。图 12 为一个异常子图检测结果示例。

上述检测结果表示的多步攻击场景是：C12304、C8735 等主机对主机 C10202 进行 DoS 攻击，导致服务器瘫痪并获得主机 C10202 的权限后，利用其作为内部渗透的跳板主机，然后进入 C6677，最后利用盗用的认证凭证登录到 C7490 中获取数据并将数据传出。

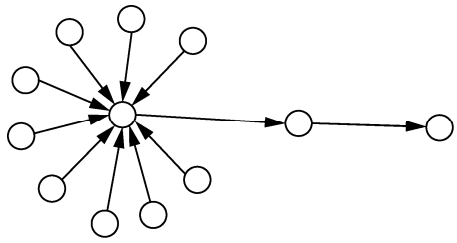


图 12　LANL 异常子图检测结果示例

5　结束语

针对以 APT 为代表的多步攻击，本文提出了一种基于网络通信异常识别的多步攻击检测方法。采用基于图的异常检测算法，检测滑动时间窗口内的异常通信子图；并基于小波变换分析检测网络攻击行为在持续控制阶段、数据外传阶段产生的异常通信行为；然后对多源异常进行关联分析，以异常主机为索引进行检索查询和完善验证，进而重构出多步攻击场景。分别针对 DARPA 2000LLDoS1.0 数据集和 LANL 数据集开展实验，验证本文方法的有效性和扩展性。实验结果表明，本文方法可以有效检测出异常通信子图和异常通信边，并通过多源异常关联分析，关联得出 DDoS、数据窃取等多步攻击场景。采用基于通信异常识别的方法，不仅可以检测出已知行为特征的网络攻击类型，对于未知特征的多步攻击类型同样具有检测效果。本文提出的多步攻击检测方法，主要具有以下优点。

1) 采集数据量小，减小对网络带宽的负担。

2) 通过多维数据关联，提高检测的准确度。

3) 整体方法采用异常检测的思路，可应对未知类型的多步攻击威胁。

4) 适用于大规模网络环境。

本文所提方法的意义在于检测出攻击带来的网络异常行为，但是由于 LANL 数据集适用性不足，实验结果有以下不足：LANL 的 flows 数据缺乏对网络拓扑的说明，由于数据来源的局限性，在 LANL 数据集给出的 redteam 数据中，异常事件以认证授权异常事件为例，缺少其他异常行为的对比验证数据，实验部分缺乏对异常检测效果的说明验证。

未来的工作有：1) 结合其他维度数据提高检测准确度，比如可与主机进程数据、IDS 告警数据、

防火墙日志、域名解析结果等信息结合分析，得出更全面更准确的多步攻击场景，进一步提高检测准确度；2) 由于实验数据集本身的局限性，缺少对实验结果的验证，后续可通过对多步攻击实例的分析，给出实际网络环境的 testbed 数据集[18]；3) 数据规模较大时功能受限，存在性能制约因素的影响，可与大数据平台结合应用，提高算法效率和可扩展性；4) 添加网络通信量作为边的权重，对检测算法改进也是下一步研究工作的方向。

参考文献：

[1] NAVARRO J, DERUYVER A, PARREND P. A systematic survey on multi-step attack detection[J]. Computers & Security, 2018, 76(6): 214-249.

[2] 王莉.网络多步攻击识别方法研究[D].武汉:华中科技大学, 2007.
WANG L. Study on method of network multi-stage attack plan recognition[D]. Wuhan: Huazhong University of Science and Technology, 2007.

[3] GREGORIO-DE S I, BERK V H, GIANI A, et al. Detection of complex cyber attacks[C]//Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V. International Society for Optics and Photonics, 2006: 6201-6209.

[4] CHEN P, DESMET L, HUYGENS C. Study on advanced persistent threats[M]. Berlin: Springer, 2014: 63-72.

[5] MA Z, SMITH P. Determining risks from advanced multi-step attacks to critical information infrastructures[C]// International Workshop on Critical Information Infrastructures Security. Springer, 2013:142-154.

[6] HOLGADO P, VILLAGRA V A, VAZQUEZ L. Real-time multistep attack prediction based on hidden Markov models[J]. IEEE Transactions on Dependable & Secure Computing, 2017, PP(99):1.

[7] 刘威歆, 郑康锋, 武斌,等. 基于攻击图的多源告警关联分析方法[J]. 通信学报, 2015, 36(9):135-144.
LIU W X, ZHENG K D, WU B, et al.Alert processing based on attack graph and multi-source analyzing [J]. Journal on Communications, 2015, 36(9):135-144.

[8] ELSHOUSH H T, OSMAN I M. Alert correlation in collaborative intelligent intrusion detection systems-a survey[J]. Applied Soft Computing, 2011, 11(7):4349-4365.

[9] WANG L, ISLAM T, LONG T, et al. Attack graph-based probabilistic security metric[C]//XXII, IFIP WG 11.3 Working Conference on Data and Applications Security. DBLP, 2008:283-296.

[10] AKOGLU L, TONG H, KOUTRA D. Graph based anomaly detection and description: a survey[J]. Data Mining and Knowledge Discovery, 2015, 29(3):626-688.

[11] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. Leading Issues in Information Warfare & Security Research, 2011, 1(1): 80.

[12] KIM Y H, PARK W H. A study on cyber threat prediction based on intrusion detection event for APT attack detection[J]. Multimedia Tools and Applications, 2014, 71(2): 685-698.

[13] NEIL J, HASH C, BRUGH A, et al. Scan statistics for the online detection of locally anomalous subgraphs[J]. Technometrics, 2013, 55(4): 403-414.

[14] NEIL J, STORLIE C. Statistical detection of intruders within computer networks using scan statistics[M].London: Imperial College Press, 2014: 71-104.

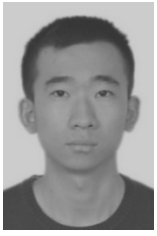
[15] 钱叶魁, 陈鸣, 叶立新, 等. 基于多尺度主成分分析的全网络异常检测方法[J]. 软件学报, 2012(2): 361-377.
QIAN Y Q, CHEN M, YE L X, et al.Network-wide anomaly detection method based on multiscale principal component analysis[J]. Journal of Software, 2012(2): 361-377.

[16] MCHUGH J. Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by lincoln laboratory[J]. ACM Transactions on Information and System Security, 2000, 3(4): 262-294.

[17] KENT A D. Cyber security data sources for dynamic network research[M].World Scientific Publishing. 2016: 37-65.

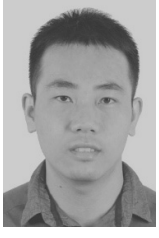
[18] CSUBÁK D, SZÜCS K, VÖRÖS P,et al. big data testbed for network attack detection[J]. Acta Polytechnica Hungarica, 2016, 13(2): 47-57 .

[作者简介]



琚安康（1995− ），男，河南辉县人，战略支援部队信息工程大学博士生，主要研究方向为多步攻击检测、异构安全数据融合。

郭渊博（1975− ），男，陕西周至人，博士，战略支援部队信息工程大学教授、博士生导师，主要研究方向为大数据安全、态势感知。



李涛（1992− ），男，甘肃甘谷人，战略支援部队信息工程大学博士生，主要研究方向为网络威胁语义建模。

叶子维（1990− ），男，吉林通化人，战略支援部队信息工程大学博士生，主要研究方向为网络安全、态势感知。