计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(8):203−208 [doi: 10.15888/j.cnki.csa.006473]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

融合本体理论的电网动态威胁数据模型与可视感知①

梁晶亮, 黄军胜, 白树军, 王　鹏, 李　睿

(贵州省遵义市供电局 信息中心, 遵义 563000)
通讯作者: 梁晶亮, E-mail: 853863364@qq.com

摘　要: 网络安全威胁可视化, 深度融合网络状态和攻击形式, 将网络中安全态势感知与可视化技术结合, 实现全域网络可信状态下受到威胁的可视化表征. 电力数据网络威胁可视化技术仍存在传统数据模型的表征能力受限以及状态特征冗余和离散导致表达可用程度低的问题. 本文提出了融合本体理论与态势演变的电网动态威胁网格化可视感知, 通过设计实体化的三阶段统一攻击威胁行为模型, 有效解决了电力数据网络安全特征表征模糊问题. 设计基于本体特征的深度内容检测方法, 形成电网安全数据的紧密关系特征集, 从而降低了状态特征的冗余程度, 精细化处理后的网络威胁数据将通过态势阶梯, 实现攻击行为的图形表征平滑渐变. 通过贵州省遵义市供电局电网威胁可视化实验, 验证本文方法提升网络安全威胁监测错误 4%.

关键词: 会商电力数据网络; 安全威胁; 数据可视化; 本体理论

引用格式: 梁晶亮,黄军胜,白树军,王鹏,李睿.融合本体理论的电网动态威胁数据模型与可视感知.计算机系统应用,2018,27(8):203–208. http://www.c-s-a.org.cn/1003-3254/6473.html

Dynamic Threat Data Model and Visual Perception of Power Grid Fused Ontology Theory

LIANG Jing-Liang, HUANG Jun-Sheng, BAI Shu-Jun, WANG Peng, LI Rui

(Information Center, Zunyi Power Supply Bureau, Guizhou Province, Guizhou 563000, China)

Abstract: Visualization of network security threats, deep integration of network status, and attack patterns, combine the security situational awareness and visualization technology, can realize the visualization representation of the global network under the trusted state. The technologies of network threat visualization still have the problem of limited representation ability of traditional data models, and the low availability of state feature redundancy and dispersion. In this study, dynamic threat data model and visual perception are proposed, which combines the ontology theory and the situation evolution. Unified attack behavior model with three solid states can help improve the problem of unclear description of network security characteristics. By designing deep content detection based on ontology features, the tight relationship characteristics set reduces the redundancy of security features. The refined network threat data will pass through the situation ladder to achieve the smooth gradient of the graphical representation of the attack behavior. The tests on Zunyi Power Supply Bureau of Guizhou Province verify the proposed method to improve the network security threat monitoring error by 4%.

Key words: power data network; security threat; data visualization; ontology theory

态势可视化, 是将事物运动剧烈程度进行高度抽象数据化, 并将复杂和抽象的事物状态和形式以非量化的、直观的形式呈现给用户, 实现用户对态势的可信、可靠、可用感知.

① 基金项目: 遵义供电局网络威胁主动发现和预警研究项目 (06030020170301O2XX00001)
Foundation item: Network Threat Active Detection and Early Warning Research Project of Zunyi Power Supply Bureau (06030020170301O2XX00001)
收稿时间: 2017-12-13; 修改时间: 2018-01-04; 采用时间: 2018-01-11; csa 在线出版时间: 2018-07-28

网络安全威胁可视化, 深度融合网络状态和攻击形式, 将网络中安全态势感知与可视化技术结合, 实现全域网络可信状态下受到入侵风险、法律风险、通报风险、漏洞风险等威胁时[1], 网络安全性变化趋势的可视化表征.

电力数据传输网络是连接管理中心、数据中心、用户中心、发电中心、输配电中心的连接通道, 是地区电网的基础设施. 2016 年, 习近平在网信工作座谈会上明确指出需要构筑网络安全防线.

世界各国均将网络安全确定为科技竞争的战略制高点. 2013 年美国政府推动“数据美国”项目形成包括网络安全在内的数据可视化工具. 2015 年, IEEE 组织包括态势感知 (Situation awareness)、协助主动安全配置和部署 (Assisting proactive security configuration and deployment)、逆向工程与恶意软件分析 (Reverse engineering and malware analysis) 等网络安全可视化主题会议. 2017 年度信息安全大会中 Redseal、Skybox、FireMon、Tufin、Algosec、安博通等公司展示了整网路径计算、漏洞评级、策略管理、风险分析、流量分析等网络安全状态分析可视化工具和性能. 2016 年, 英国建立基于 DNS 的国家防火墙, 阻止钓鱼邮件使用恶意域名进行网络犯罪.

调查统计表明, 2015 年全球信息安全市场规模已突破 1100 亿美元, 而 2017 年由于网络攻击造成系统瘫痪和信息泄露导致经济损失达到上万亿美元.

由此, 如何高效地监测网络安全威胁引起了世界各国的关注. 网络安全威胁可视化, 是当前预测网络安全事件发展趋势和保障网络稳定的发展趋势, 如图 1.

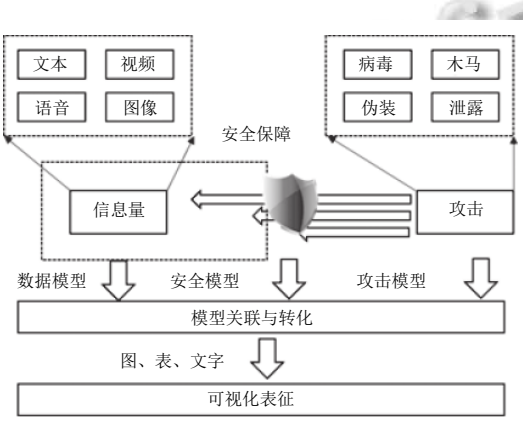

图 1 网络安全威胁可视化的特点示意图

其主要包括基于网络流量数据、时间序列数据、边界网关协议、日志数据等可视化技术. 基于网络流量数据的可视化技术, 主要采用点阵图、网格图、饼状图等对端口流量以及总体变化趋势进行显示监测[2], 实现数据的静态与动态统计分析和多方式显示流量特征, 直观的显示网络状况[3]、网络异常和攻击行为. 基于时间序列数据的可视化技术, 利用层次关系的树图进行不同的数据维度的展示[4,5]. 其能够描述一个包含多个状态转换的事件, 每个状态都具有时间属性, 且状态之间的转换存在多条路径[6,7]. 通过多视图协作, 支撑由整体到个体、由点到面以及由历史到未来的网络流量时序数据分析过程. 基于边界网关协议的可视化技术, 是可视化网关协议的路径变化、通告, 以及路由跟踪等信息, 及时告警网络异常行为和攻击[8]. 通过简易抽象描述方法, 使用 Promela 构建协议模型可视化, 能够有效分析攻击对路径的正确选择[6]. 使用柱状图识别每个特定类型的如路由器配置错误及蠕虫攻击的 BGP 异常行为表征. 基于日志数据的可视化技术, 通过图形元素与监测数据进行属性关联, 有效地向用户展示网络中蕴涵的态势状况[9,10]. 基于 Echarts 可视化技术对电力数据网络报警日志进行处理[11], 分别从统计和分布的角度实现报警信息的可视化.

综上所述, 电力数据网络威胁可视化技术仍存在以下难题:

(1) 传统数据模型的表征能力受限, 难以表达多状态、多阶段、多维度的电力数据网络威胁. 电力数据网络中包含静态和动态数据, 文件、多媒体、控制数据的格式和结构差异性大, 需要进一步建立能够描述网络攻击威胁的行为模型.

(2) 大型复杂网络的安全状态特征冗余和离散, 导致可视化的图元关系混乱, 网络安全态势表达可用程度低. 电力数据网络是一个综合性网络, 包括产电、输电、配电、售电和用电全过程, 特征相互混叠且冗余, 相互关系交叉非独立, 即使以图元可视化展现, 安全态势复杂性反而增加, 因此, 需要有效聚类安全特征.

为此, 针对传统数据模型的表征能力受限以及状态特征冗余和离散导致表达可用程度低的问题, 本文提出了融合本体理论与态势演变的电网动态威胁网格化可视感知. 首先设计了统一攻击威胁行为模型, 基于不同的网络攻击行为和电力网络数据, 形成了静态启发式规则、动态攻击生命周期、行为潜伏等效转化的数据模型实体化, 实现了对电力数据网络的安全特征准确描述. 提出了基于本体特征的深度内容检测方法,

从统一攻击威胁行为模型进一步抽象出威胁本体特征, 实现本体的数据关联处理和检测. 精细化处理后的网络威胁数据将通过态势阶梯, 实现攻击行为的图形表征平滑渐变. 通过搭建网络环境, 验证本文方法在表征复杂度和内容检测精度等方面的性能提升.

1 统一攻击威胁行为模型

1.1 静态启发式规则的数据模型

数据是所有可视化的基础. 电力数据网络的应用程序数据流异构多源, 其包括 P2P 流量、实时通讯流量以及流媒体流量. 而业务数据封装在传输帧结构中, 在传输过程中不经过解封装是无法判断业务内容. APT (Advanced Persistent Threat) 攻击将大量威胁代码构筑在静态文件中, 特别是相互传输的文档、日志和压缩包. 因此, 只有通过静态数据模型构建, 在不对静态文件传输形态进行解封装时, 即可对内容特征文件进行可视化感知.

将一个文件集合 F 细分为 N 个子文件集合 $F=\{F_1,F_2,F_3,\cdots,F_K\}$, 恶意文件的执行代码长度下限为 L_K, 则有 $0<K<sum(F)$. 假定恶意文件与正常文件同时接入可信网络, 即 F 整体均服从相同的业务源模型, 其包括用户行为到达过程和业务行为过程.

静态启发式规则的数据模型主要包括静态文件传输会话到达过程、静态文件会话呼叫数目、静态文件会话呼叫间隔、单静态文件会话文件数、子文件的到达间隔、文件包大小, 如图 2 所示.

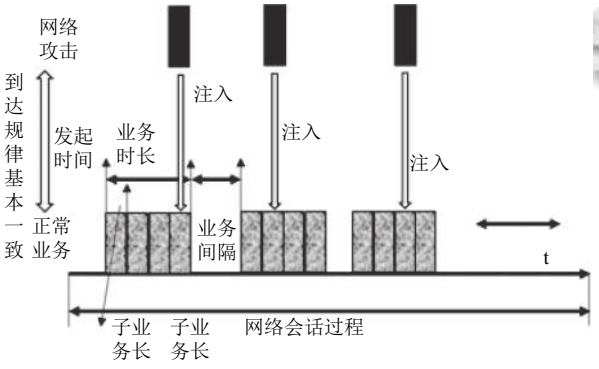

图 2 统一攻击威胁行为模型

数据模型可进一步描述如下:

(1) 静态文件传输会话到达过程: 静态文件传输发起事件的规律, 约定传输开始时间 T_{start} 服从泊松分布, 随机参数 λ 根据传输的应用类型有所不同, 则有到达过程,

$$P(K(T_{\text{start}}))=e^{-\lambda}\frac{\lambda^K}{K!} \tag{1}$$

(2) 静态文件会话呼叫数目: 同时需要处理的请求业务数量, 服从几何分布, 均值为 μ_N.

(3) 静态文件会话呼叫间隔: 由于特定时间内, 呼叫数目服从几何分布, 因此呼叫间隔也服从几何分布, 均值为 μ_D.

(4) 单静态文件会话文件数: 从整体文件进行细分后, 单事件同样服从几何分布, 均值为 μ_K.

(5) 子文件的到达间隔: 为了保持数据模型的整体性, 子文件的到达间隔同样服从几何分布, 均值为 μ_{ft}.

(6) 文件包大小: 每个子文件服从截断的 Pareto 分布, 其标准分布如下:

$$f_x(x)=\frac{\alpha*k^\alpha}{x^{\alpha+1}},x\geqslant k \tag{2}$$

其均值和方差如下:

$$\begin{cases}\mu=\frac{k\alpha}{\alpha-1},\alpha>1\\ \sigma^2=\frac{k^2*\alpha}{(\alpha-2)(\alpha-1)^2},\alpha>2\end{cases} \tag{3}$$

其中, α 为 Pareto 分布的定值, 设定 m 为最大允许的分组大小. 则当分组大小满足 $x>m$, 则文件包大小的均值为:

$$\mu_{fK}=\int_{-\infty}^{\infty}xf_x(x)dx=\int_k^m x\frac{\alpha*k^\alpha}{x^{\alpha+1}}dx=\frac{\alpha k-m(k/m)^\alpha}{\alpha-1} \tag{4}$$

2.2 动态攻击生命周期的数据模型

动态攻击生命周期的数据模型, 是将在静态分析或行为检测中发现的可疑文件放入可持续攻击的生命周期模型搭模型中, 并判定攻击的危险程度[12].

动态攻击初始植入阶段可分为攻击者攻击入侵过程以及终端接入过程. 攻击者攻击入侵的随机性低, 因此分布规律主要由终端接入过程控制. 电力网络用户使用电网进行数据传输的到达服从泊松分布, 持续时长服从指数分布, 则有动态攻击初始植入阶段的持续时间 t_{sa} 概率密度函数为:

$$f_Z(t_{\text{sa}})=\lambda_{\text{sa}}e^{-\lambda_{\text{sa}}t_{\text{sa}}} \tag{5}$$

将 λ_{sa} 设定为非随机变化, 即在持续时间 t_{s1} 内 APT 初始植入事件可数, 假定为 N_{sa}.

动态攻击信息收集阶段是一个多参量的分层并发事件. 由此, 可以构造观察向量 $\vec{T}_{sb}$,

$$\vec{T}_{sb}=\left\{t_{sb1},t_{sb2},\cdots,t_{sbN_{sb}}\right\} \tag{6}$$

其中, N_{sb}为分层并发事件数量. 按照参数估计理论可以构造指数分布参数λ_{sb}的似然函数, 其表征在参数λ_{sb}为定值前提下, 观察向量$\vec{T}_{sb}$的概率密度函数, 则有

$$f_Z(T_{sb}|\lambda_{sb})=\prod_{i=1}^{N_{sb}} f_Z(t_{sbi}|\lambda_{sb})=(\lambda_{sb})^{N_{sb}}e^{-\sum_{i=1}^{N_{sb}}\lambda_{sb}t_{sbi}} \quad (7)$$

由此可以得到, 动态攻击信息收集阶段下潜入威胁将总能获得导致攻击事件发生的伺机概率.

当处于动态攻击发起阶段, 攻击模型可以从可信系统的边界安全进行可逆计算, 为:

$$f_Z(T_{sc})=2^{1-\log_2 f(d_{trust_i})} \quad (8)$$

2.3 行为潜伏等效转化的数据模型

由于 APT 攻击采用社会工程学等巧妙手法, 要想完全防止入侵是十分困难的. 为了掌握潜伏在网络内的威胁, 需要对攻击进行危险度转换, 其依托是基于正常数据行为模型, 通过该模型, 可视化异常数据及可疑行为关联.

不同生命周期下所有的危险程度与信息量 I、攻击性强度 A 和安全策略强度 S 具有以下关系:

$$D=I*A*S^{-1} \quad (9)$$

当电网数据的信息量 I 越大, 则遭受网络攻击和安全风险将随之增大. 网络攻击性强度 A 越大, 则数据被泄露的风险越大. 安全策略强度 S 越大, 则数据将获得更大的保障, 安全风险降低. 信息量 I、攻击性强度 A 和安全策略强度 S 均能根据网络安全事件进行细分, 即$I=\{I_1,I_2,I_3,\cdots,I_k\}$, $A=\{A_1,A_2,A_3,\cdots,A_k\}$, $S=\{S_1,S_2,S_3,\cdots,S_k\}$. I, A 与 S 及其子集应为相互独立.

2 基于本体特征的深度内容检测

2.1 电力网络的威胁本体特征

基于统一攻击威胁行为模型, 形成信息量、攻击性强度和安全策略强度的数据模型及其子集, 并具有静态启发式规则、动态攻击生命周期、行为潜伏等效转化的数据模型实体化, 实现了对电力数据网络的安全特征准确描述. 模型的具体化也带来了电力网络安全特征的冗余, 导致可视化处理的细粒度模糊.

从大量冗余特征中遴选出核心要素的方法通常包括层次分析法、加权评估法等等. 这些方法都依赖于强先验概率下的专家知识库, 与系统特性关联紧密, 数据结构化差, 语义难以跨平台适用, 且对动态变化的本体描述能力低. 而在 APT 威胁下, 突发攻击将长时潜伏隐匿的漏洞威胁瞬态激发, 将会造成跨平台、多时段、多应用的系统崩溃. 因此, 在进行 APT 深度内容检测时, 构建的知识库需要能够满足在不同建模方法、范式、语言和软件工具下的快速转换. 由于本体理论[13]是面向对象的形式化描述重要实体、属性、过程和相互关系的跨数据关联理论, 其将能更适合无健全专家知识体系的网络. 因此, 本文将进一步引入本体理论, 挖掘电网动态威胁关联最紧密的特征.

将前述威胁数据模型、周期和行为统一转化为本体描述特征, 即

$$O=\{I,A,S,E_I,E_A,E_S,E(\cdot)\} \quad (10)$$

其中, E_I为信息量之间的关系, E_A为攻击量之间的关系, E_S为网络安全保障之间的关系, $E(\cdot)$为信息量、供给量和安全保障之间的关系. 可以具体化为 $E(I, A)$、$E(I, S)$ 和 $E(A, S)$, 分别信息量与攻击量之间的关系, 信息量与安全保障之间的关系, 攻击量与安全保障之间的关系.

2.2 基于本体的数据聚类关联处理和检测

可由电力网络的威胁本体特征集合中任意选定需要可视化的特征组成待考察组合. 与利用 k-means 算法[14]可以将目标威胁本体特征群分为k'个簇.

步骤一: k'个初始聚类中心是$O=\{o_1,o_2,\cdots,o_n\}$. 传统 k-means 算法随机选定点作为初始类簇中心点, 聚类性能稳定差. 为了提升威胁本体特征集合的聚类效果, 通过加大初始类簇中心点的平均相对欧氏距离, 增加最优解的全局性能. 因此首先选定初始类簇中心点o_1, 然后选定距离该点最远的那个点作为第二个初始类簇中心点o_2, 再选择距离o_1与o_2的距离最大的点作为第三个初始类簇的中心点o_3. 此时选择聚类最大迭代次数 m; 确定迭代结束的最小目标威胁函数 T.

步骤二: 根据欧氏距离公式, 计算每个数据到簇的距离, 将各数据分到最小距离的簇中, 其中计算距离公式为:

$$d(x_j,o_n)=\sqrt{\sum_{n=1}^{l}(x_{j1}-o_{n1})^2} \quad (11)$$

$d(x_j,o_n)$是第 j 个威胁本体特征数据到第 n 个聚类中心的距离.

步骤三:重新计算k'个聚类的中心值$O=\{m_1,m_2,\cdots,m_n\}$, 其计算公式为:

$$m_j=\frac{1}{n}\sum_{x_j\in O_n}x_j \quad (12)$$

其中, m_j为第 j 个聚类的聚类中心.

步骤四: 若迭代次数等于 m, 则结束聚类, 否则判断聚类结果是否满足小于给定参数 T, 如果满足则结束, 不满足重复步骤二、三[15]. 本体特征深度内容无标度聚类如图 3 所示.

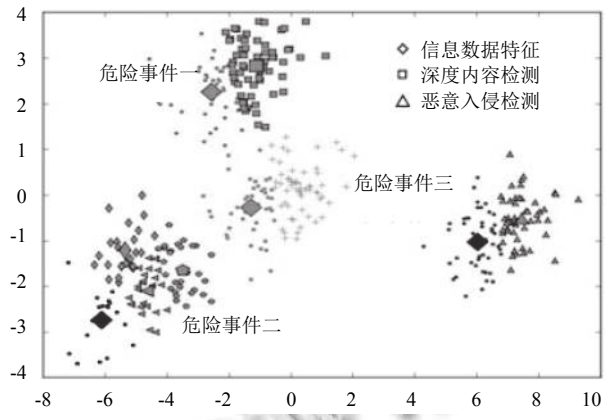

图 3 本体特征的深度内容检测无标度聚类

3 仿真与性能分析

3.1 网络安全可视化环境构建

为了验证本文动态威胁模型和可视化感知的效果, 新方法将基于贵州省遵义市供电局的电网进行验证. 可视化效果验证环境包括攻击模拟设备、电网数据中心、电网网络中心、电网服务中心、安全路由以及威胁监控平台, 如图 4 所示.

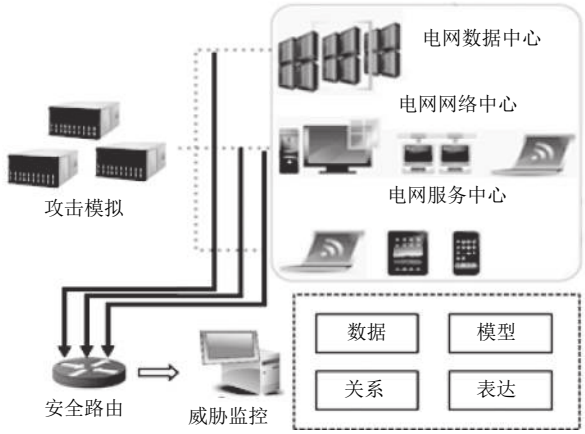

图 4 网络安全可视化环境构建

威胁监控平台能够实现数据、模型、关系和表达的综合处理, 并可以根据攻击模拟出适用的人机交互方案, 包括功能流程设计、运行监测模式设计以及可视化决策主体页面设计等. 攻击模拟设备的模拟攻击事件包括 P2P 流量、实时通讯流量以及流媒体流量[16], 具体设定如表 1 所示.

表 1 攻击模拟设备的模拟攻击事

攻击事件	应用程序	攻击威胁
P2P 流量	Ares、Bittorent、Blubster、eDonkey、Kazaa、Gnutella、Winny、Foxy	违规链接远端控制
实时通讯	AIM、Goggle Talk、MSN、Skype、Yahoo Messenger	隐形通道安全证书、伪造
流媒体	RTMP、RTSP、SHOUTCast、WMSP	植入恶意代码零日漏洞

实验中将从表 1 中任意选定三种攻击事件, 组成不同的应用程序下的攻击威胁事件发现. 将流量监测方法以及日志跟踪方法, 与本文方法共同配置到威胁监控平台. 通过长时间观察, 分析不同方法在监测误差以及监测表达能力的性能表现.

3.2 网络安全威胁监测错误分析

图 5 为不同方法的网络安全威胁监测错误分析. 由图 4 中可以看出, 基于本体的网络威胁感知错误率要低于流量监测方法以及日志跟踪方法的感知错误率. 当并发任务数量为 40 个时, 基于本体的网络威胁感知错误率为 9.86%, 流量监测方法以及日志跟踪方法的感知错误率分别为 13.9% 以及 14.2%, 分别提升了 4.04% 以及 4.34%.

4.3 监测表达能力分析

监测表达能力分析实验, 从表 1 中选取三个攻击事件作为观察对象. 攻击事件一 (Bittorent, 违规链接)、攻击事件二 (Goggle Talk, 隐形通道)、攻击事件三 (RTMP, 零日漏洞). 收集监测表达能力的数据, 利用蒙特卡洛分析法和均方根误差 (Root Mean Square Error) 分析监测表达的准确度, 预测结果如图 6 所示.

由图 6 中可以看出, 基于本体的网络威胁表达能力 RMSE 要低于流量监测方法以及日志跟踪方法的威胁表达能力 RMSE, 这是由于新方法引入本体理论, 挖掘电网动态威胁关联最紧密的特征, 降低了可视化构建的特征冗余度. 可视化监测威胁的实际效果如图 7 所示.

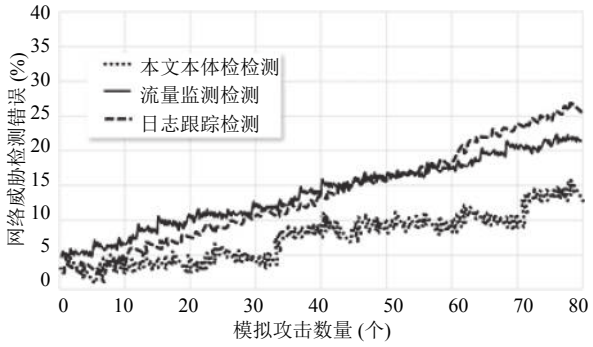

图 5 网络安全威胁监测错误分析

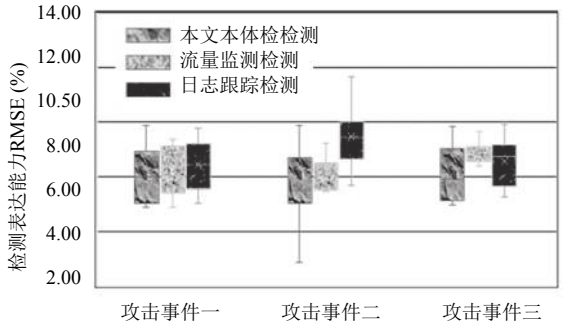

图 6 网络安全威胁监测错误分析

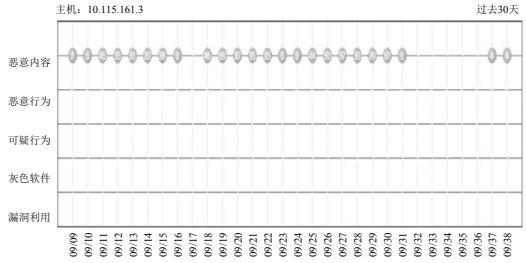

图 7 网络安全威胁可视化实际效果

4 结论

本文提出了融合本体理论与态势演变的电网动态威胁网格化可视感知. 基于不同的网络攻击行为和电力网络数据, 形成了静态启发式规则、动态攻击生命周期、行为潜伏等效转化的数据模型实体化, 实现了对电力数据网络的安全特征准确描述. 提出了基于本体特征的深度内容检测方法, 从统一攻击威胁行为模型进一步抽象出威胁本体特征, 实现本体的数据关联处理和检测. 精细化处理后的网络威胁数据将通过态势阶梯, 实现攻击行为的图形表征平滑渐变, 优化了网络安全威胁监测错误和监测表达能力, 有效解决了传统数据模型的表征能力受限以及状态特征冗余和离散导致表达可用程度低的问题.

参考文献

1 龙震岳, 钱扬, 邹洪, 等. 电网企业网络信息安全的威胁与攻防新技术研究. 现代电子技术, 2015, 38(21): 100–104.

2 张翠香, 蒋宏宇, 沈代瑶, 等. 基于网络流量数据的多视图协同交互可视分析系统. 西南科技大学学报, 2017, 32(2): 66–72. [doi: 10.3969/j.issn.1671-8755.2017.02.013]

3 Mateo CM, Gil P, Torres F. Visual perception for the 3D recognition of geometric pieces in robotic manipulation. International Journal of Advanced Manufacturing Technology, 2016, 83(9-12): 1999–2013. [doi: 10.1007/s00170-015-7708-8]

4 刘轶, 武妮, 张晗. 一种网络流量统计分析与可视化系统. 微电子学与计算机, 2007, 24(6): 153–155. [doi: 10.3969/j.issn.1000-7180.2007.06.045]

5 Moon D, Im H, Kim I, *et al*. DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. The Journal of Supercomputing, 2017, 73(7): 2881–2895. [doi: 10.1007/s11227-015-1604-8]

6 杨欢欢, 李天瑞, 陈馨茹. 基于螺旋图的时间序列数据可视化. 计算机应用, 2017, 37(9): 2443–2448.

7 Yang HP. Method for behavior–prediction of APT attack based on dynamic Bayesian game. Proceedings of 2016 IEEE International Conference on Cloud Computing and Big Data Analysis. Chengdu, China. 2016. 177–182.

8 赵颖, 王权, 黄叶子, 等. 多视图合作的网络流量时序数据可视分析. 软件学报, 2016, 27(5): 1188–1198.

9 黄吴丹, 陈哲. 边界网关协议安全性的模型检验方法研究. 小型微型计算机系统, 2017, 38(6): 1187–1191. [doi: 10.3969/j.issn.1000-1220.2017.06.004]

10 吴建建. 电力系统数据挖掘可视化平台的关键技术研究与实现[硕士学位论文]. 郑州: 郑州大学, 2016.

11 孙磊, 陈璇, 唐红, 等. 基于 GBrowse 的多源长非编码 RNA 数据可视化系统. 计算机系统应用, 2017, 26(3): 81–85. [doi: 10.15888/j.cnki.csa.005633]

12 Li MC, Huang W, Wang YB, *et al*. The study of APT attack stage model. Proceedings of 2016 IEEE/ACIS 15th International Conference on Computer and Information Science. Okayama, Japan. 2016. 1–5.

13 高建波. 本体模型及其在信息安全评估领域的应用研究[博士学位论文]. 上海: 上海交通大学, 2015.

14 Choi JH, Choi C, You I, *et al*. Polymorphic malicious javascript code detection for APT attack defence. Journal of Universal Computer Science, 2015, 21(3): 369–383.

15 于海波. 基于规则和本体的应用安全策略研究[博士学位论文]. 长春: 吉林大学, 2006.

16 龚钢军, 陈志敏, 陆俊, 等. 智能用电用户行为分析的聚类优选策略. 电力系统自动化, 2018, 42(2): 58–63.