DOI:10. 3969/j. issn. 2097-0706. 2022. 07. 001

面向智慧园区系统的网络攻击关联分析与防护策略研究

Network attack association analysis and attack protection strategy for smart park systems

李惠军[1],陆建强[2],周霞[2*],解相朋[2],万磊[2]
LI Huijun[1],LU Jianqiang[2],ZHOU Xia[2*],XIE Xiangpeng[2],WAN Lei[2]

(1.国电南瑞科技股份有限公司,南京 211106;2.南京邮电大学 碳中和先进技术研究院,南京 210023)
(1.NARI Technology Development Company Limited,Nanjing 211106,China;2.Institute of Advanced Technology for Carbon Neutrality,Nanjing University of Post and Telecommunication,Nanjing 210023,China)

摘 要:智慧园区系统内各层次时刻遭受网络攻击的威胁,为提高智慧园区系统面向网络攻击威胁的应对能力与恶意攻击事件识别的精度和效率,提出面向智慧园区系统的网络攻击关联分析方法,其是采用频繁模式增长(FP-Growth)算法的网络攻击异常事件关联规则分析技术。首先利用FP-Growth算法快速挖掘异常事件频繁项集,训练关联规则;其次利用灰色关联分析算法生成实时异常事件对于网络攻击异常表现形式的元素集合;接着结合关联规则实现网络攻击场景的在线识别;同时针对匹配的攻击场景所对应的环节提出网络攻击防护策略,进行网络攻击防御,消除攻击影响;最后在不同数据量下验证所提方法在关联规则训练方面效率的优越性,并以智慧园区系统负荷频率控制(LFC)业务为场景验证所提网络攻击防护策略的可行性和有效性。

关键词:智慧园区;综合能源系统;微电网;网络攻击;关联规则分析与匹配;灰色关联分析;攻击防护策略;负荷频率控制

中图分类号:TK 01:TM 73:TP 393.08 **文献标志码**:A **文章编号**:2097-0706(2022)07-0001-09

Abstract: Control system of smart parks at all levels are vulnerable to network attacks. In order to improve the system's coping capacities to network attacks and the identification accuracy and efficiency of malicious attack events, a network attack association analysis method for smart park systems is proposed. The method takes Frequent Pattern-Growth (FP-Growth) algorithm to detect the association rules of abnormal network attack events. FP-Growth algorithm can quickly mine the frequent item sets of abnormal events and train the association rules. Grey correlation analysis algorithm generates the abnormal manifestation set of real-time abnormal network attack events. Then, following the association rules, the network attack scenarios can be recognized on-line. Network attack protection strategy is made according to the links corresponding to the different attack scenarios to eliminate the impact of the attack. Finally, the efficiency of the proposed method in training association rules is verified by data of different volumes, and the feasibility of the network attack protection strategy is verified by the Load Frequency Control module of the smart park system.

Keywords: smart park; integrated energy system; micro-grid; network attack; association rule analysis and matching; grey correlation analysis; attack protection strategy; control on load and frequency

0 引言

综合能源系统中不同能源系统之间、电力网络与信息网络之间的耦合关系以及电力信息通信系统对电力物理系统的支撑作用不断提高[1-3]。智慧园区内部将风电、光伏等可再生能源与负荷终端以及储能设备组合成区域微电网,逐渐成为一种具有通信能力的多源信息物理系统[4-5]。然而,针对智慧园区系统的网络攻击行为在近年来不断发生,如虚假数据注入攻击[6]、拒绝服务攻击[7-8]等。同时,由于系统漏洞或工作人员误操作等原因,园区内部网络和设备现场智能终端上同样面临着网络攻击的威胁[9-10]。因此,如何挖掘异常事件与网络攻击之间的关联关系,对异常事件实时匹配,识别攻击场景,部署攻击防护策略消除攻击影响,保证智慧园区系统的安全稳定运行至关重要。

目前,关联规则分析技术已广泛运用于输电线

收稿日期:2022-03-22;**修回日期**:2022-05-20
基金项目:国家自然科学基金项目(61933005)

路缺陷状态预测[11-12]、安全分析[13]、网络攻击场景识别[14-17]等领域。文献[14]提出采用关联规则分析算法提取网络攻击报警事件的特征,生成网络攻击事件组合规则,实现对网络攻击行为的有效预警。传统电网环境下,经典关联规则分析Apriori算法能够有效地挖掘电网各层次频繁项集,生成电网网络攻击场景下的关联规则[15]。然而,传统Apriori算法在挖掘频繁项集的过程中,在内存占用、计算性能等方面具有一定局限性[16]。虽已有部分专家提出从减少数据库扫描次数,并利用频繁预选项剪枝的方式对传统Apriori算法进行改进[17],但面对智慧园区系统海量实时数据时容易产生过多的候选频繁项集,存储成本较大且实时性无法满足。同时,机器学习等智能算法也逐步运用于网络攻击关联分析当中,通过对电力通信侧异常事件初步分类,利用遗传算法自动生成对应不同网络攻击场景的关联规则,并基于时序逻辑实现关联规则的匹配[18]。但该方法需要对所有攻击场景内的关联规则依次进行匹配,异常事件匹配效率不高。文献[19]利用贝叶斯网络模型挖掘多步攻击间存在的关联规则,描述网络攻击场景图,实现网络攻击场景的预测。贝叶斯模型需要知道先验概率,假设的先验概率往往会影响预测结果,从而无法保证其可靠性。

针对不同网络攻击场景,科研人员提出了安全防护策略与防护技术,提高安全防护能力[20-21],保障电力通信系统的安全稳定运行。文献[22]针对网络攻击对信息侧与物理侧的影响,从时间维度上的事前防御和事后恢复出发,总结归纳了相关网络攻击防御手段,但并未指出如何识别相关网络攻击场景。文献[23]针对电力系统智能终端业务特征,总结提出了电力系统智能终端信息安全防护需要研究的关键技术,构建安全防护研究框架,但文中未考虑通信侧所受的网络攻击威胁[24]。

针对上述方法存在的问题,为了解决网络攻击场景识别效率慢、准确率低的问题。本文首先提出基于频繁模式增长(Frequent Pattern-Growth,FP-Growth)算法的网络攻击异常事件关联规则分析技术,相较于传统关联规则算法,大幅提高关联规则离线训练的效率,适应智慧园区系统海量数据的环境。其次,利用灰色关联分析算法实现实时异常事件与关联规则的在线匹配,有效提高了网络攻击场景识别效率与准确率。同时,针对匹配的攻击场景所对应的环节提出网络攻击防护策略,应用相应的攻击防护技术,进行网络攻击防御,消除攻击影响,提高智慧园区系统面对各层次网络攻击的应对能力。最后,与2种Apriori算法在不同数据量下的关联规则挖掘速度进行对比,验证所提方法的分析效率;以智慧园区系统负荷频率控制(Load Frequency Control,LFC)业务为场景验证本文所提网络攻击防护策略的必要性和有效性。

1 智慧园区系统下网络安全防护体系分析

现有的智慧园区系统内部主要按照“安全分区,网络专用,横向隔离,纵向认证”16字方针以提升智慧园区内外网络边界处的网络安全防护。然而,随着园区内终端接入数量的陡增,新型源网荷储智能终端友好互动需求不断增加,园区内部网络和设备现场关键测量和控制设备上同样面临着来自不同方面的威胁,智慧园区系统网络安全攻防体系示意如图1所示。利用操作系统漏洞、数据库漏洞、注入木马程序、监听\破解报文和第三方运维人员的违规操作等方式,针对不同环节产生不同网络攻击类型,如分布式拒绝服务攻击(Distributed Denial of Service,DDoS)、中间人攻击等,从而导致设备拒动误动或通信的中断,最终造成大面积停电事故的发生。

结合对智慧园区系统内网络安全防护体系的分析,对存在网络攻击威胁的攻击场景与异常表现形式进行归纳总结,见表1。针对智慧园区系统的网络攻击,以破坏网络安全3要素为目标。主要通过非法监听报文、会话劫持等方式破坏其保密性;通过修改配置参数、设备重启动等方式破坏其完整性;通过拒绝服务攻击、伪造控制指令等方式破坏其可用性。因此,智慧园区系统内信息侧的信息安全与物理侧的安全稳定运行均受到极大的影响,其异常表现形式复杂且多样,主要分为2类。

如何将智慧园区系统内实时异常事件与网络攻击场景进行在线匹配,根据攻击场景提出相应的网络攻击防护策略,消除攻击影响使智慧园区系统安全稳定运行,是目前亟须解决的问题。

2 智慧园区系统网络攻击关联分析方法

为了实现智慧园区系统内实时异常事件与关联规则的快速匹配,以实现对网络攻击场景的准确快速识别。本文借助FP-Growth算法和灰色关联分析算法构建智慧园区系统网络攻击异常事件关联分析框架,如图2所示。

2.1 智慧园区系统攻击关联规则生成

2.1.1 异常事件数据预处理模块

分析网络攻击异常事件需要获取有效且具有代表性的特征数据构成项集。根据上述多维度攻击异常表现形式、攻击场景分类、攻击对象分析可

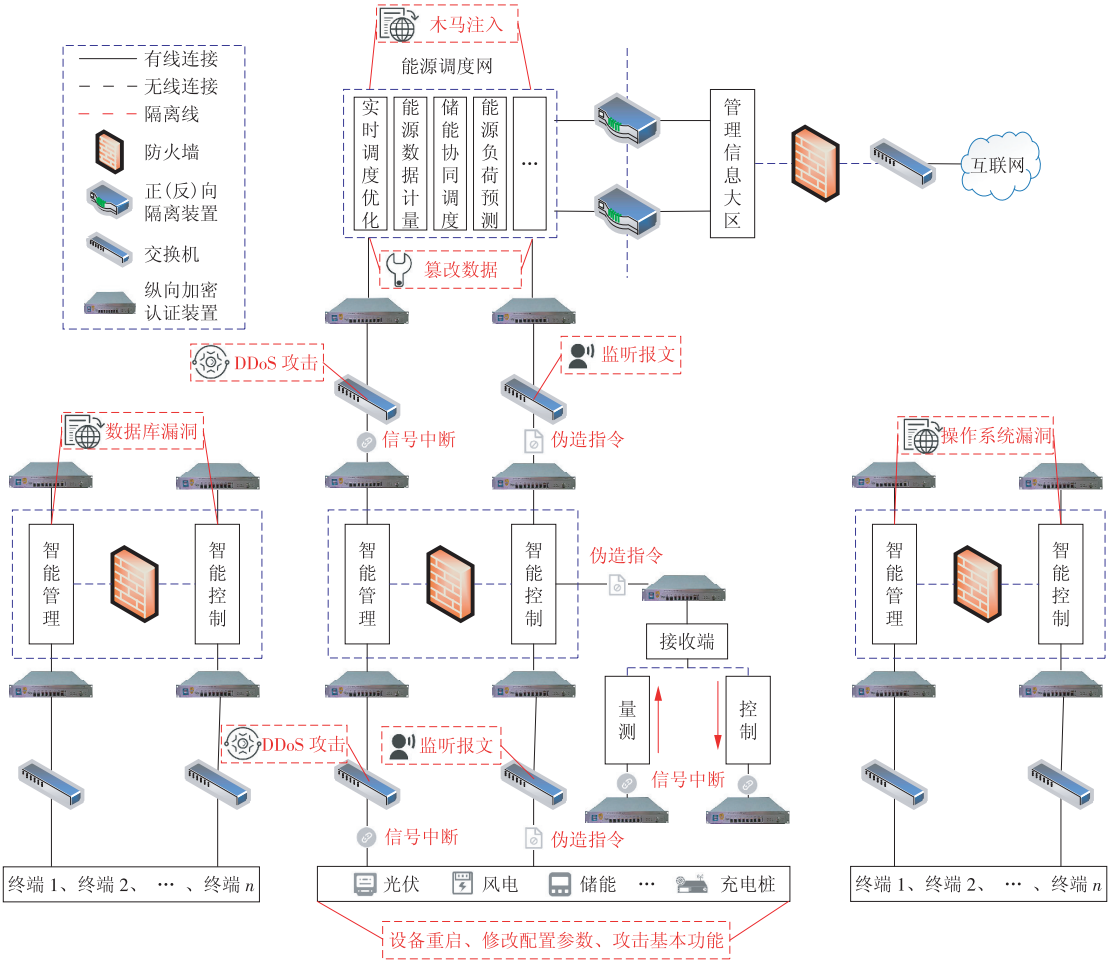

图 1　智慧园区系统网络安全攻防体系示意

Fig. 1　Security system of the smart park network

表 1　智慧园区系统网络攻击场景及异常表现形式

Table 1　Network attack scenarios and abnormal manifestations of the smart park system

攻击环节	攻击场景	异常表现形式
主站侧	修改配置参数 会话劫持 伪造控制指令	电压异常、电流异常、切负荷量异常、设备拒动/误动、电价异常
终端侧	篡改量测数据 设备重启动 设备锁控制	
通信侧	非法监听报文 恶意控制通信 拒绝服务攻击	网络流量异常、终端违规外联、业务应用拒绝服务、用户数据泄露

知,引起异常事件的攻击异常表现形式和攻击场景这 2 个数据量是分析网络攻击异常事件、提取关联规则的必需元素。由此可构建网络攻击异常事件关键因素集合

$$\boldsymbol{X}=\{\boldsymbol{S}_i,\boldsymbol{A}_i,\boldsymbol{O}_i\}, \tag{1}$$

式中:$\boldsymbol{S}_i$为攻击场景;$\boldsymbol{A}_i$为网络攻击异常表现形式;$\boldsymbol{O}_i$为数据来源对象。

归纳得出主要攻击场景有 9 类,包括修改配置参数、会话劫持、设备重启动、篡改量测数据、伪造控制指令、非法监听报文、恶意控制通信、拒绝服务攻击和设备锁控制;攻击异常表现形式主要包含 9 类,分别为电压异常、电流异常、切负荷量异常、设

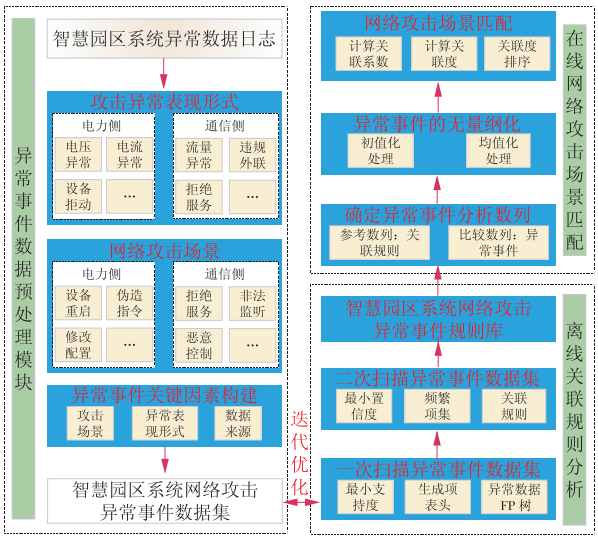

图 2　智慧园区系统网络攻击异常事件关联分析框架

Fig. 2　Association analysis on the abnormal network attack events in the smart park system

备拒动/误动、时变电价异常、网络流量异常、终端违规外联、业务应用拒绝服务、用户数据泄露。

读取智慧园区电力侧与通信侧终端设备的日志文件，对日志中异常数据进行编号。其中，电压异常、电流异常、切负荷量异常等9类攻击异常表现形式用1—9进行编号，而修改配置参数、会话劫持、设备重启动等9类攻击场景用A—I进行编号，每一条数据如E_1={A,1,C,D,3,6}。并将处理后的数据写入网络攻击异常事件数据集。

2.1.2　基于FP-Growth的关联规则训练算法

区别于传统利用Apriori算法实现频繁项集和关联规则挖掘，FP-Growth算法采用FP树存储数据集，减少数据集扫描次数，算法流程如下。

(1)1次扫描异常事件数据集，对每一条数据，统计S_i或A_i频繁1项集的个数，去除低于支持度阈值的S_i或A_i，建立异常事件项表头，如图3所示。

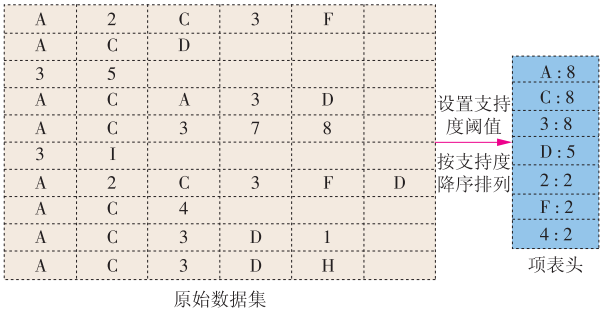

图3　网络攻击异常事件数据集1次扫描

Fig. 3　The 1st scan for the data set of abnormal network attack events

(2)2次扫描异常数据集，对每一条数据，剔除不在项表头中的S_i或A_i，并按照支持度降序排序，重新建立异常数据数据集，如图4所示。

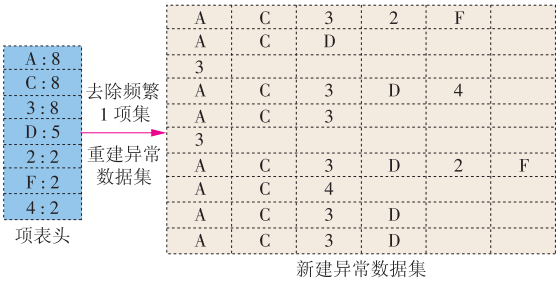

图4　网络攻击异常事件数据集2次扫描

Fig. 4　The 2nd scan for the data set of abnormal network attack events

(3)读取新建异常数据集，建立FP树，其中树中的每一个节点表示S_i或A_i和其在新建异常数据集中出现的次数，从根节点到叶子节点的每一条路径表示1条异常数据。同时可递归建立S_i或A_i对应的条件模式基，获得频繁项集，如图5所示。

基于FP-Growth算法实现的智慧园区系统网络

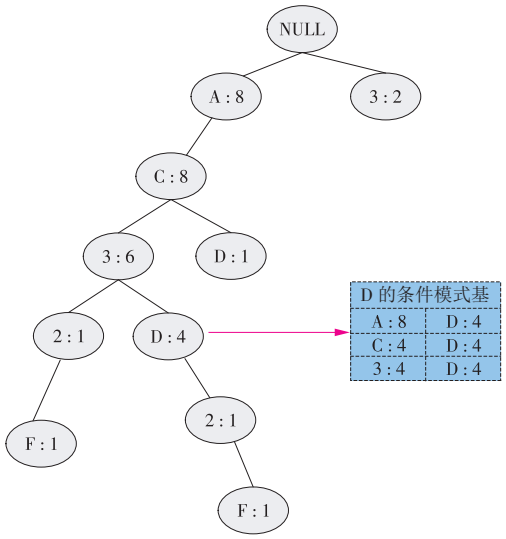

图5　FP树建立与条件模式基获取

Fig. 5　FP tree establishment and conditional pattern base acquisition

攻击异常事件的频繁项集，挖掘事件之间潜在的关联关系，建立网络攻击关联规则库，处理流程如图6所示。通过该方法，可以快速挖掘攻击场景S_i与网络攻击异常表现形式A_i之间满足最小置信度的频繁项集，获得二者之间的关联规则，写入网络攻击规则库，为在线网络攻击场景匹配提供基础。

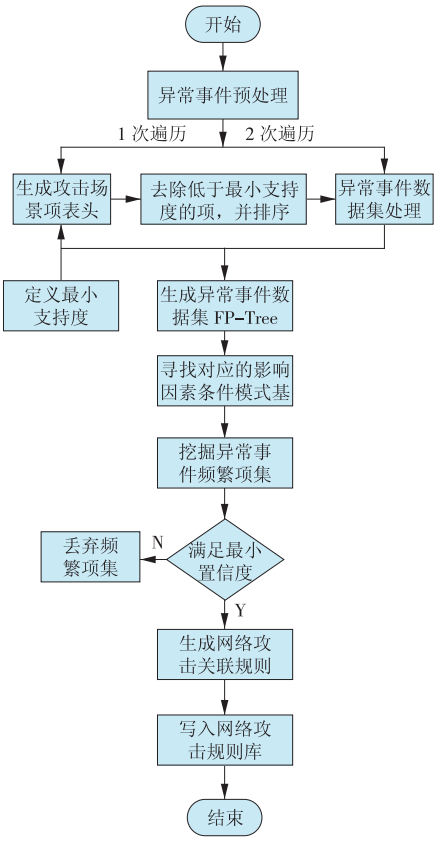

图6　基于FP-Growth的网络攻击关联规则挖掘流程

Fig. 6　Mining process of network attack association rules based on FP-Growth

例如，网络攻击异常表现形式$\boldsymbol{A}_i$中1和2与攻击场景$\boldsymbol{S}_i$中的C置信度较高，则可以生成关联规则：[1+2]→[C]，即表示电压异常和电流异常与伪造控制指令信号之间存在关联关系。

2.2　智慧园区系统攻击关联匹配模块

在生成关联规则后，需要将智慧园区系统内实时异常事件与关联规则进行快速匹配，以实现对攻击场景的快速识别。提出了基于灰色关联分析的智慧园区系统攻击关联匹配模块。

首先对于实时异常事件，选取表1中的9种网络攻击异常表现形式构成异常事件属性集$\boldsymbol{X}=\{x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9\}$；设置各指标的最优值（或最劣值）构成参考属性集$\boldsymbol{Y}=\{y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8,y_9\}$。同时，为了计算属性集中各属性与参考属性之间的关联度，建立了实时比较数列$\boldsymbol{X}_i(k)$与参考数列$\boldsymbol{Y}(k)$。

$$\boldsymbol{X}_i=\boldsymbol{X}_i(k)|k=1,2,\cdots,n;i=1,2,\cdots,9, \tag{2}$$

$$\boldsymbol{Y}=\boldsymbol{Y}(k)|k=1,2,\cdots,n, \tag{3}$$

式中：k为不同时刻；i为属性集中的不同属性。

由于各因素列中的数据的量纲存在不同，因此在评估实时异常事件各属性与参考属性之间的关联度之前需要对数据进行无量纲化处理，主要采用以下2种方法，分别为初值化处理和均值化处理：

$$x_i(k)=\frac{x_i(k)}{x_i(1)},k=1,2,\cdots,n;\ i=0,1,2,\cdots,9, \tag{4}$$

$$x_i(k)=\frac{x_i(k)}{\overline{x}_i},k=1,2,\cdots,n;\ i=0,1,2,\cdots,9。 \tag{5}$$

利用无量纲化处理后的数据计算各时段下的关联系数$\xi_i(k)$

$$\xi_i(k)=\frac{\min\limits_i\min\limits_k\left|y(k)-x_i(k)\right|+\rho\max\limits_i\max\limits_k\left|y(k)-x_i(k)\right|}{\left|y(k)-x_i(k)\right|+\rho\max\limits_i\max\limits_k\left|y(k)-x_i(k)\right|}。 \tag{6}$$

设$\Delta_i(k)=\left|y(k)-x_i(k)\right|$，则由式(5)可推出

$$\xi_i(k)=\frac{\min\limits_i\min\limits_k\Delta_i(k)+\rho\max\limits_i\max\limits_k\Delta_i(k)}{\Delta_i(k)+\rho\max\limits_i\max\limits_k\Delta_i(k)}, \tag{7}$$

式中：ρ为分辨系数。ρ越小，分辨力越大，通常取$\rho=0.5$。

最后，计算比较数列与参考数列在各个时刻的关联系数平均值，即为实时异常事件各属性与参考属性之间的关联度r_i

$$r_i=\frac{1}{n}\sum_{k=1}^{n}\xi_i(k)。 \tag{8}$$

对单个属性设定不同的阈值β，通过对比阈值β与对应属性的关联度r_i，判断该属性对应的异常表现是否发生。例如，对电流异常的关联度计算可以设定为

$$\begin{cases}r_i=0; & \text{未发生电流异常}\\ r_i\geqslant\beta; & \text{可能发生电流异常}\\ r_i=1; & \text{发生电流异常}\end{cases}。 \tag{9}$$

由此，可以得到实时异常事件对于网络攻击异常表现形式的元素集合，结合网络攻击规则库中的关联规则，将实时异常事件对应的异常表现形式与关联规则中的异常表现形式进行比对，实现对攻击场景的快速识别。

3　智慧园区系统网络攻击防护策略

智慧园区内部虽已普遍采用专网专用，区域之间采用纵向认证的方式进行防护，但园区内部多种能源种类在传输分配和储存消纳的过程中也同时衍生出园区内部网络攻击与设备现场攻击等新型网络攻击形式。本节基于所提出的网络攻击关联规则分析方法对异常事件进行匹配，针对匹配的攻击场景所对应的环节提出网络攻击防护策略，应用相应的攻击防护技术，进行攻击防御消除攻击影响。基于不同攻击场景的网络攻击防护策略如图7所示。

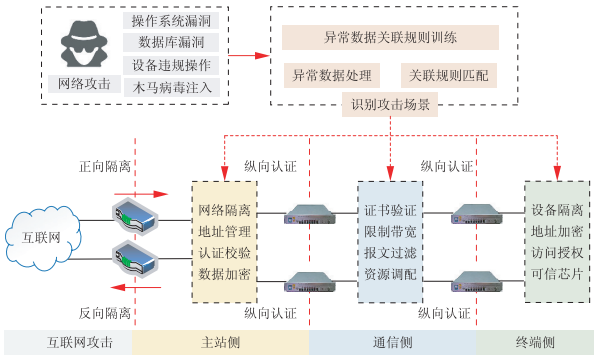

图7　基于不同攻击场景的网络攻击防护策略

Fig. 7　Network attack protection strategies for different attack scenarios

（1）主站侧的攻击防御防护技术包括网络隔离、地址管理、认证校验和数据加密等技术。

1）网络隔离：采用应用层数据提取技术和专用的数据传输协议，实现互联网与园区内部专用网络之间的数据交互，并进行审计、过滤，降低网络安全风险。

2）地址管理：对数据传输设备和站点分配可信固定地址，仅接收来自固定地址的数据，对异常数据来源的地址拉入黑名单，防止地址被攻击者所盗用。

3）认证校验：在检测到主站侧出现网络攻击之后，对下发的控制指令利用异或和、哈希算法等加密算法添加校验码，保证其完整性。

4)数据加密:对传输的数据进行加密,主要通过对称加密、非对称加密等形式。同时,为了保证指令下发的实时性,需要对密钥加密算法进行合理改进,保证其安全性。

(2)通信侧的攻击防御防护技术包括证书验证、限制带宽、报文过滤和资源调配等技术。

1)证书验证:在传输数据时,利用数字证书和CA去验证公钥持有者的身份,防止攻击方冒充。

2)限制带宽:为防止传输协议等洪泛攻击对通信的影响,对报文设置流量阈值,防止网络异常报文的大量涌入,占用带宽资源。

3)报文过滤:为防止大量重复性报文造成的网络堵塞,可通过识别报文类型,对报文进行过滤,滤除与业务无关的重复报文。

4)资源调配:面向优先级较高的通信业务,设置备用带宽资源,在检测到出现通信网络阻塞时启用备用带宽,实时消除攻击影响,保证通信顺畅。

(3)终端侧的攻击防御防护技术包括设备隔离、地址加密、访问授权、可信芯片等技术。

1)设备隔离:对出现异常的终端及时杀死进程,断开本地网络,同时去除物理地址绑定,关闭端口,增加访问控制策略。

2)地址加密:为了应对攻击方通过窃听获取主机地址信息,伪装自身地址下发虚假指令,利用地址跳变技术,实现主机地址的动态变化。

3)访问授权:在终端连接时需向服务器发送授权配置信息,并将终端登陆标识添加到目标终端通信目录当中,同时设置有效时限定时刷新。

4)可信芯片:在智能终端内部嵌入可信芯片,只有通过可信芯片的认证,才能确保终端连接、控制可信。

4 算例分析

本节首先针对网络攻击的关联规则分析方法在智慧园区系统大数据量状态下的训练速度进行分析,通过与传统算法在不同数据量下的训练时间进行对比,验证本文所提方法的有效性;其次,建立多电源区域互联电网模型,模拟智慧园区内以孤岛模式运行的微网系统,分析所提防护策略对LFC业务的影响。

4.1 关联规则训练算法效率分析

本文采用Java语言实现了FP-Growth算法、传统的Apriori算法和改进的Apriori算法,在同一台内存为16 GB,安装Windows 11的64位操作系统,部署JDK 1.8版本的主机下进行仿真。分别采用某智慧园区内异常数据集作为训练样本,通过设置不同数据量(1 000,3 000,5 000,10 000,50 000,80 000)的数据,进行关联规则的训练,并对训练效率进行对比,结果如图8所示。

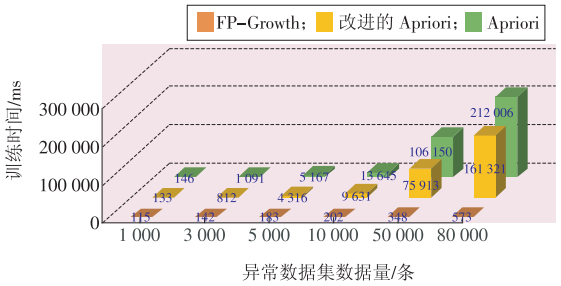

图8 不同数据量下3种算法训练时间对比

Fig. 8 Three algorithms´ training time with data in different volumes

由图8可知,相较于传统的Apriori算法和改进的Apriori算法,本文所提出的方法在不同数据量下,训练时间均有大幅度降低,可以有效降低异常事件关联规则的训练事件,提高训练效率。在大数据量下,本文所提方法在训练时间上的优势更为明显。例如在80 000条数据时,本文所提方法相较于传统Apriori算法效率提高了近370倍。随着数据量的增加,本文所提方法对于在训练时间上并没有大幅度的增加。从1 000条数据到80 000条数据,训练时间仅增加了不到5倍,更加适用于智慧园区系统海量数据的环境。

4.2 网络攻击防护策略效果分析

为了模拟智慧园区系统中以孤岛模式运行的微电网系统,本节在Matlab/Simulink平台搭建两区域互联微电网LFC模型。其中,将风电其作为扰动负荷加入互联系统当中。而飞轮储能通过与微电网进行有功/无功交换,提高LFC效果。利用标准单元模型对每个微电网进行建模,并利用分布式比例积分微分(Proportion Integration Differentiation,PID)控制器以区域控制误差(Area Control Error,ACE)信号通过通信网络传输到控制器中实现频率控制。同时考虑DDoS下对控制信号量传输时延的影响,多区域互联系统第i区域LFC模型如图9所示。

在两区域互联系统中,各微电源与联络线参数见表2。假设在区域2中从t为0 s时加入风电负荷扰动,在不施加任何控制策略时,两区域内稳态频率和联络线功率均有所下降,电能质量受到了影响。频率偏差Δf_i和联络线功率偏差$\Delta P_{\mathrm{tie}-i}$的仿真结果如图10所示。

设置在t为0 s时智慧园区系统开始遭受网络攻击,攻击方控制10个代理端向主站服务器发动DDoS攻击,从而导致服务器内存占比激增,通信系

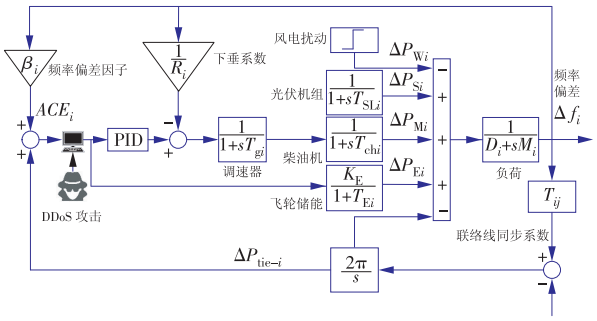

图 9　网络攻击下多区域互联系统第 i 区域 LFC 模型

Fig. 9　LFC model for the ith area of the interconnected multi-area system under cyber attacks

表 2　2 区域微电网互联电力系统参数

Table 2　Parameters of the interconnected power system for the two-region microgrid

区域	T_{gi}	T_{SLi}	T_{chi}	T_{Ei}	K_E	D_i	H_i	β_i	R_i	T_{ij}
1	0.10	1.30	0.30	0.30	5.00	1.00	10.00	21.00	0.05	0.50
2	0.08	1.30	0.32	0.30	5.00	1.00	11.00	18.00	0.05	0.50

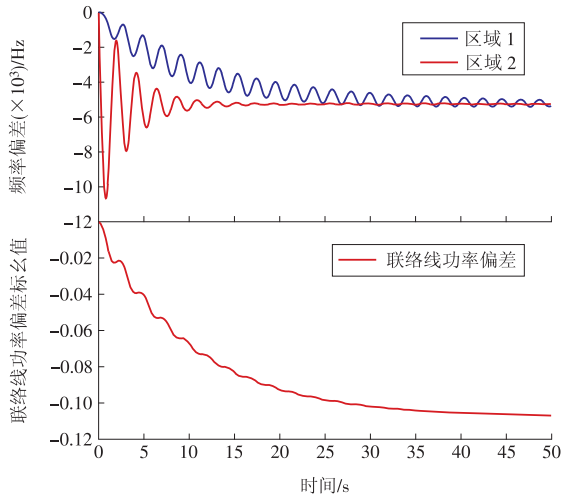

图 10　无控制器参与时频率与联络线功率偏差响应

Fig. 10　Response to frequency and tie-line power deviations without a controller

统收发流量急剧增加,以 ACE 的误差量作为控制器的输入量在传输过程中存在传输时延,从而导致 LFC 系统中被控对象不能及时反映系统所受扰动,超调量明显增加,系统稳定性变差。对两区域内分别添加风电功率扰动,同时设置两区域内传输时延分别为 0.28 s 和 0.08 s,对区域内频率偏差和联络线功率偏差进行仿真,并与未遭受 DDoS 攻击时的结果进行对比,如图 11 所示。

由图 11 可知,在未遭受 DDoS 攻击时,频率偏差和联络线功率偏差较小,能迅速恢复扰动前的状态。在延时较小时(区域 2),频率和功率的恢复时间和超调量有所增加,分别为 12.35 s 和 16.44 s。而在延时较大时(区域 1),系统稳定性明显降低,频率与功率偏差变化较大,系统分别需要 30.16 s 和

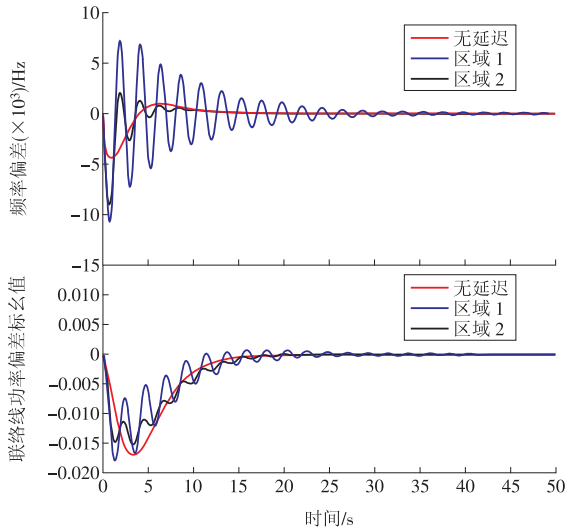

图 11　LFC 系统不同延时频率与联络线功率偏差响应

Fig. 11　Responses to the delay frequency and tie line power deviations of the LFC system

27.94 s 将频率和功率控制到稳定状态。同时,随着时延不断增加,频率最低点不断降低。

为了消除 DDoS 攻击对 LFC 业务带来的延时影响,保证控制策略的实时性,对延时较大的区域实施网络攻击防护策略:在通信侧,限制带宽设置报文流量阈值,对大量涌入的异常报文进行丢弃。同时,基于报文头部与相关信息对其进行分类,过滤恶意攻击报文。在终端侧,添加防火墙规则,仅接收来自可信名单内地址的数据。同时,对被感染的终端设备进行隔离,断开网络连接,防止被攻击方控制从而进行 DDoS 攻击。考虑网络攻击防护策略下的控制效果比较如图 12 所示。

由图 12 可知,在未添加防护策略时,频率和联络线功率恢复稳定的时间约为 28.40 s 和 26.10 s;

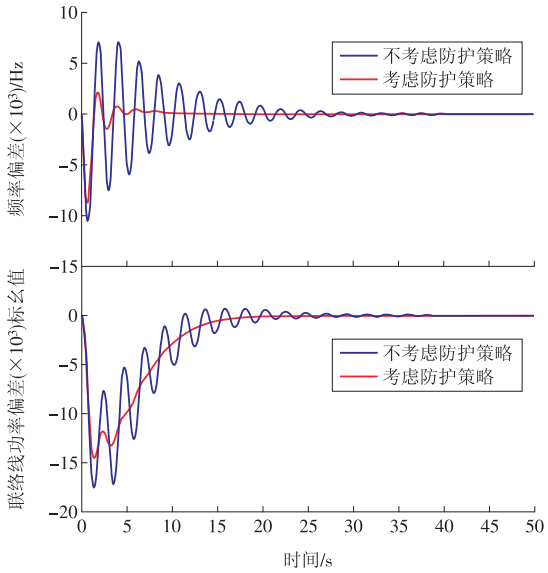

图 12　考虑网络攻击防护策略下的控制效果比较

Fig. 12　Control effects of the network attack protection strategy

添加防护策略后，频率和联络线功率恢复稳定的时间约为8.30 s和20.20 s，频率与功率偏差最低点也提高了约20%。可以看出，在添加防护策略后，系统频率超调量和稳定时间明显降低，LFC控制效果大幅提高。可见对于智慧园区内孤岛模式运行的多电源互联微电网系统，本文所提的网络攻击防护策略可以有效地改善网络攻击对LFC问题的影响，保证智慧园区内部微电网运行的稳定性与动态可靠性。

5 结论

随着智慧园区系统的不断发展，针对智慧园区内部网络和海量智能设备而进行的网络攻击手段更加多样、攻击影响越发严重。本文建立了网络攻击异常事件关联分析框架，提出了面向智慧园区系统的网络攻击关联分析方法，并针对不同攻击环节提出了相应攻击防护策略，消除网络攻击影响，保障智慧园区系统安全稳定运行。

(1)在智慧园区系统网络攻击关联分析方面，本文基于FP-Growth算法挖掘网络攻击异常事件频繁项集，与传统关联规则分析算法相比，进一步提高了网络攻击异常事件关联分析效率，大幅降低了训练网络攻击异常事件关联规则的时间复杂度；结合灰色关联度分析算法实现对异常事件与关联规则的在线匹配，有效提高了网络攻击场景识别的精度，具有重要工程实用价值。

(2)在攻击防护策略方面，本文结合网络攻击场景所对应的环节提出网络攻击防护策略，对园区内外网络和现场设备应用相应的攻击防护技术，进行攻击防御保护消除攻击影响。在智慧园区系统中，以LFC业务为场景验证了本文所提策略的必要性和有效性。

参考文献：

[1]王奖，邓丰强，张勇军，等.园区能源互联网的规划与运行研究综述[J].电力自动化设备，2021，41(2)：24-32，55.
WANG Jiang，DENG Fenqiang，ZHANG Yongjun，et al. Review on planning and operation research of park energy internet[J].Electric Power Automation Equipment，2021，41(2)：24-32，55.

[2]COLAK I，SAGIROGLU S，FULLI G，et al.A survey on the critical issues in smart grid technologies[J].Renewable and Sustainable Energy Reviews，2016，54(2)：396-405.

[3]秦羽飞，葛磊蛟，王波.能源互联网群体智能协同控制与优化技术[J].华电技术，2021，43(9)：1-13.
QIN Yufei，GE Leijiao，WANG Bo. Swarm intelligence collaborative control and optimization technology of Energy Internet[J]. Huadian Technology，2021，43(9)：1-13.

[4]钱峰，皮杰，刘俊磊，等.微电网建模与控制理论综述[J].武汉大学学报(工学版)，2020，53(12)：1044-1054.
QIAN Feng，PI Jie，LIU Junlei，et al.Review of microgrid modeling and control theory [J]. Engineering Journal of Wuhan University，2020，53(12)：1044-1054.

[5]KOTOWICZ J，UCHMAN W. Analysis of the integrated energy system in residential scale：Photovoltaics，micro-cogeneration and electrical energy storage[J].Energy，2021，227：120469.

[6]陈郁林，齐冬莲，李真鸣，等.虚假数据注入攻击下的微电网分布式协同控制[J].电力系统自动化，2021，45(5)：97-103.
CHEN Yulin，QI Donglian，LI Zhenming，et al.Distributed cooperative control of microgrid under false data injection attacks[J].Automation of Electric Power Systems，2021，45(5)：97-103.

[7]黄博南，詹凤楠，张天闻，等.一种针对电-热综合能源系统经济调度的DoS最优攻击策略[J].中国电机工程学报，2020，40(21)：6839-6854.
HUANG Bonan，ZHAN Fengnan，ZHANG Tianwen，et al.An optimal DoS attack strategy against the economic dispatch for electric-thermal integrated energy system [J]. Proceedings of the CSEE，2020，40(21)：6839-6854.

[8]余鹏，王勇.DTU与主站通信系统的DoS攻击研究[J].华电技术，2021，43(2)：34-39.
YU Peng，WANG Yong. Research on DoS attack to the communication system between DTU and master station[J]. Huadian Technology，2021，43(2)：34-39.

[9]张晓娟，曹靖怡，缪思薇，等.电力工控系统攻击渗透技术综述[J].电力信息与通信技术，2021，19(3)：49-59.
ZHANG Xiaojuan，CAO Jingyi，MIAO Siwei，et al.Overview of power industry control system penetration attack technology [J]. Electric Power Information and Communication Technology，2021，19(3)：49-59.

[10]何金栋，王宇，赵志超，等.智能变电站嵌入式终端的网络攻击类型研究及验证[J].中国电力，2020，53(1)：81-91.
HE Jindong，WANG Yu，ZHAO Zhichao，et al.Type and verification of network attacks on embedded terminals of intelligent substation [J]. Electric Power，2020，53(1)：81-91.

[11]叶万余，苏超，罗敏辉，等.基于关联规则挖掘的输电线路缺陷状态预测[J].电力系统保护与控制，2021，49(20)：104-111.
YE Wanyu，SU Chao，LUO Minhui，et al.Transmission line defect state prediction based on association rule mining[J]. Power System Protection and Control，2021，49(20)：104-111.

[12]陈勇,李胜男,张丽,等.基于改进Apriori算法的智能变电站二次设备缺陷关联性分析[J].电力系统保护与控制,2019,47(20):135-141.
CHEN Yong, LI Shengnan, ZHANG Li, et al. Association analysis for defect data of secondary device in smart substations based on improved Apriori algorithm[J].Power System Protection and Control,2019,47(20):135-141.

[13]高泽芳,王岱辉,王昀,等.基于告警事件特征的网络攻击行为实时预警研究[J].电信工程技术与标准化,2018,31(12):33-37.
GAO Zefang, WANG Daihui, WANG Jun, et al. Research on real-time warning of network attack behavior based on characteristics of alarm events [J]. Telecom Engineering Technics and Standardization,2018,31(12):33-37.

[14]黄悦华,邹子豪,张赟宁,等.基于FP-Growth算法的配电网薄弱点分析研究[J].电测与仪表,2020,57(17):79-84,135.
HUANG Yuehua, ZOU Zihao, ZHANG Yunning, et al. Research on weak point analysis of distribution network based on FP-Growth algorithm[J].Electrical Measurement & Instrumentation,2020,57(17):79-84,135.

[15]费稼轩,裴培,张明,等.电网工控网络攻击场景中的层次关联分析方法[J].南京理工大学学报,2020,44(6):715-723.
FEI Jiaxuan, PEI Pei, ZHANG Ming, et al. Hierarchical association analysis method in industrial control cyber attack scenario of power grid [J]. Journal of Nanjing University of Science and Technology, 2020, 44 (6): 715-723.

[16]余锐,郑亮,熊俊,等.基于改进Apriori算法的电力通信设备缺陷关联性分析[J].中国安全生产科学技术,2021,17(12):176-181.
YU Rui, ZHENG Liang, XIONG Jun, et al. Defect correlation analysis of power communication equipment base on improved Apriori algorithm [J]. Journal of Safety Science and Technology,2021,17(12):176-181 .

[17]孙学波,石飞达.基于Hadoop的Apriori算法研究与优化[J].计算机工程与设计,2018,39(1):126-133,145.
SUN Xuebo, SHI Feida. Research and optimization of Apriori algorithm based on Hadoop [J]. Computer Engineering and Design,2018,39(1):126-133,145.

[18]章锐,费稼轩,石聪聪,等.特定攻击场景下源网荷系统恶意攻击关联分析方法[J].中国电力,2019,52(10):1-10.
ZHANG Rui, FEI Jiaxuan, SHI Congcong, et al. Malicious attack correlation analysis method of source-grid-load system under specific attack scenarios[J].Electric Power, 2019,52(10):1-10.

[19]胡倩.基于多步攻击场景的攻击预测方法[J].计算机科学,2019,46(S1):365-369.
HU Qian. Attack prediction method based on multi-step attack scenario [J]. Computer Science, 2019, 46 (S1): 365-369.

[20]吕政权, 李朝阳, 王海峰, 等. 基于GRU-CNN的综合能源网络安全攻击检测方法[J]. 华电技术, 2021, 43(2): 9-14.
LYU Zhengquan, LI Zhaoyang, WANG Haifeng, et al. An intrusion detection method for integrated energy network based on GRU-CNN[J]. Huadian Technology, 2021, 43(2): 9-14.

[21]王海峰,李朝阳,吕政权,等.泛在电力物联网环境下网络安全攻击研究[J].浙江电力,2019,38(12):76-81.
WANG Haifeng, LI Zhaoyang, LV Zhengquan, et al.Survey on cyber attack in the context of ubiquitous power internet of things [J]. Zhejiang Electric Power, 2019, 38 (12): 76-81.

[22]汤奕,李梦雅,王琦,等.电力信息物理系统网络攻击与防御研究综述(二)检测与保护[J].电力系统自动化,2019,43(10):1-9,18.
TANG Yi, LI Mengya, WANG Qi, et al. A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection [J]. Automation of Electric Power Systems, 2019, 43 (10): 1-9,18.

[23]张涛,赵东艳,薛峰,等.电力系统智能终端信息安全防护技术研究框架[J].电力系统自动化,2019,43(19):1-8,67.
ZHANG Tao, ZHAO Dongyan, XUE Feng, et al. Research framework of cyber-security protection technologies for smart terminals in power system[J].Automation of Electric Power Systems,2019,43(19):1-8,67.

[24]张徐亮 , 万里冰 , 钱伟中 , 等. 基于区块链的电力大数据安全保障体系[J]. 华电技术, 2020, 42(8): 68-74.
ZHANG Xuliang, WAN Libing, QIAN Weizhong, et al. Security assurance system for electric power big data based on blockchain technology[J]. Huadian Technology, 2020, 42(8): 68-74.

(本文责编:张帆)

作者简介:

李惠军(1978),男,高级工程师,硕士,从事电网安全与控制研究,lihuijun@sgepri.sgcc.com.cn;

陆建强(1997),男,在读硕士研究生,从事电力通信研究,1098116508@qq.com;

周霞*(1978),女,高级工程师,博士,从事电力系统稳定方面的研究,zhouxia@njupt.edu.cn。

*为通信作者。