第47卷 第12期 计 算 机 工 程 2021年12月
Vol.47 No.12 Computer Engineering December 2021

·网络空间安全· 文章编号：1000-3428(2021)12-0131-10 文献标志码：A 中图分类号：TP309

面向电力系统网络安全的多层协同防御模型研究

王 梓[1,2]，王治华[3]，韩 勇[1,2]，金建龙[1,2]，黄天明[1,2]，朱 江[1,2]

（1.南瑞集团有限公司（国网电力科学研究院有限公司），南京 211106；2.南京南瑞信息通信科技有限公司，南京 211106；
3.国网上海市电力公司，上海 200122）

摘 要：为满足电力监控系统组网架构及网络安全协同防护的需求，提出一种多层次且纵深分布的主动安全协同防御模型，并从模型架构、功能机制等方面设计一整套实现方案。基于域内自防御和跨域协防的特性，通过基于灰色关联分析的最高关联度防御决策，并协同安全防护设备间协作，实现从主机层、安防设备层到网络层的网络安全多级防御。通过电力监控系统典型现场对网络安全应用场景进行实验验证，结果表明，该协同防御模型增强了各层级间安全防护能力，能够提供更高效的安全风险监测、安全事件响应及动态处置的手段。

关键词：电力系统网络安全；主动防御；多层协同防御；协同防御模型；灰色关联决策

开放科学（资源服务）标志码（OSID）：

中文引用格式：王梓，王治华，韩勇，等.面向电力系统网络安全的多层协同防御模型研究[J].计算机工程，2021，47(12)：131-140.

英文引用格式：WANG Z，WANG Z H，HAN Y，et al.Research on mulit-layer cooperative defense model oriented to network security of power system[J].Computer Engineering，2021，47(12)：131-140.

Research on Mulit-Layer Cooperative Defense Model Oriented to Network Security of Power System

WANG Zi[1,2]，WANG Zhihua[3]，HAN Yong[1,2]，JIN Jianlong[1,2]，HUANG Tianming[1,2]，ZHU Jiang[1,2]

（1.NARI Group Corporation（State Grid Electric Power Research Institute），Nanjing 211106，China；
2.NARI Information & Communication Technology Co.，Ltd.，Nanjing 211106，China；
3.State Grid Shanghai Municipal Electric Power Company，Shanghai 200122，China）

【Abstract】The security control and production management of the power system are highly dependent on the network communication between the levels of regulatory agencies，and cyberspace security events always threaten the stable operation of the power grid.In order to meet the needs of power monitoring system architecture and network security collaborative protection，a multi-level，deep distributed collaborative defense model is designed and proposed，and a set of implementation methods are given from the perspective of model architecture，technical methods and functional mechanisms of each module.Based on the characteristics of self-defense and cross-domain cooperative defense in the domain，the model cooperates with security protection devices to perform multi-level active collaborative defense from the host layer，security device layer to the network layer by the highest degree of correlation defense decision-making based on the gray correlation decision.Through the analysis，it is found that the model has the capability of real-time monitoring of network security risks，rapid response to security threats，and dynamic handling of cyber security events，which can effectively improve the level of network security protection of power monitoring systems.

【Key words】network security of power system；active defense；multi-layer collaborative defense；collaborative defense model；gray correlation decision

DOI：10. 19678/j. issn. 1000-3428. 0059716

0 概述

随着计算机、网络及通信技术在建设坚强智能电网中的广泛应用，现代电力系统已发展成为由物理电力系统和信息通信系统构成的复杂耦合网络系统[1-3]。其中，电力监控系统是基于计算机及网络技

基金项目：国家电网有限公司总部管理科技项目“电力监控系统网络空间脆弱性分析与威胁探测关键技术研究”。

作者简介：王 梓（1988—），男，高级工程师、硕士，主研方向为电力监控系统、网络空间安全；王治华、韩 勇，高级工程师；金建龙，工程师；黄天明、朱 江，高级工程师。

收稿日期：2020-10-13 **修回日期：**2020-12-16 **E-mail：**wangzi@sgepri.sgcc.com.cn

术的业务系统及智能设备，作为基础支撑的通信及数据网络，被用于监视和控制电力生产及供应过程。作为整个电力系统的神经网络和控制中枢，电力监控系统对保障电力系统的安全稳定运行和电力可靠供应具有重要的意义[4]。近年来，针对电力监控系统的网络攻击频繁爆发，呈现出专业化、高危害、国际化、高持续威胁等特点[5-7]，电力监控系统安全防护的迫切性已被提到国家安全层面[8]，相关部门明确了“多道纵向防线”联合防御的要求[9]。

研究人员基于传统信息安全角度，通过借鉴国内外成熟的安全防护模型引入协同的概念，从理论上提出网络安全协同防御模型[10]、体系[11]或机制[12]，此外还针对特定场景[13-14]下的模型实现或方案设计，为协同防护模型的实现提供了一定的指导及参考价值。然而，电力监控系统与传统信息系统在安全防护上存在明显差异[15]，通用信息安全防护方法并不能完全适用于电力监控系统。现阶段针对电力监控系统网络安全防护研究成果大多聚焦在建立适用于电力系统的纵深防护架构[16]、防御技术剖析应用[17]或极端事件的风险评估与防范[18]方面。但以上成果均未考虑在电网实际组网环境下结合多层级协同防御思想的网络安全防护框架及实践研究，且缺乏全面、细致、有效的协同机制和实现方法的描述。鉴于此，本文设计并提出一整套安全、有效的网络安全协同防御模型及实现机制，以提升电力监控系统网络安全事件的应急管控能力。

1 研究背景

1.1 现有电力监控系统网络安全防护

电力监控系统网络主要由电力调度数据网承载，拓扑一般以双星型为主。其组网节点具有数量多、连接复杂的特点，通常按照IP网络的层次化进行设计[19]。为保障电力系统安全稳定运行，建立和完善电网、电厂计算机监控系统及调度数据网络的安全防护体系，国家和行业相关部门先后提出并发布了电力监控系统安全防护的相关要求[20-21]。其中，电力监控系统网络安全以《电力监控系统安全防护总体方案》作为行业最新的电力系统安全规范文件，以“安全分区、网络专用、横向隔离、纵向认证”为原则，通过综合采用防火墙、入侵检测、主机加固、病毒防护、日志审计、统一管理等多种手段，建立了以省级以上调度中心、发电厂、变电站、配电等组成的电力监控系统安全防护架构。

以重点防护的生产控制大区为例，目前在省调、地调、变电站及电厂选择性部署了纵向加密认证、物理隔离装置、硬件防火墙、防病毒/防恶意代码、入侵检测防御系统以及漏洞扫描、网管、安全审计等一系列围绕业务安全、通信安全、边界安全的安全防护设备和系统，其所涉及的安防技术主要包括加密、身份认证/数字签名、可信接入、入侵检测、基于角色访问控制、防火墙、安全隔离、虚拟专用网络、安全隧道、报文过滤/拦截等，其逻辑关系如图1所示。

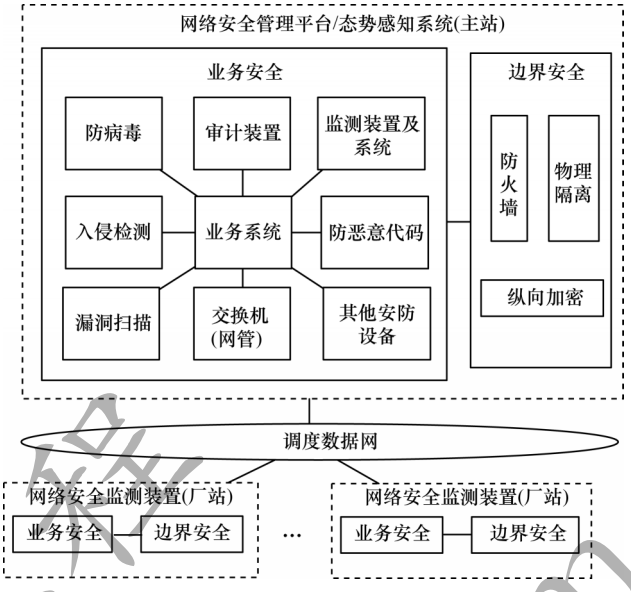

图1 电力监控系统网络安全总体防护架构

Fig.1 Network security protection structure of existing power monitoring system

1.2 电力监控系统网络安全防护需求

通过各类安防设备的部署和安全技术的应用，在一定程度上提升了网络安全防护能力。但网络系统的整体安全并不能通过安全设施或技术的简单堆叠实现，而应取决于安全防御能力最薄弱的环节或组成部分[22]。目前安全技术的静态叠加、安防设备孤立的部署方式、单一固化的防御手段已不能满足新威胁背景下动态管控、纵深防御的主动式电网安全发展需求[23]。因此，结合电力监控系统组网结构特点，通过协调安防设备或技术以共同抵御各种威胁攻击是提升网络安全防御能力的重要实践方向。

1)协同各安类安防能力互补

目前部署的各类安防设施主要依靠设备自身固化策略或针对不同的安全目标作业，相互间协同性较低。通过协同各类具备不同安防能力的安全实施进行通力合作，可有效提升全网的安全防御能力，实现1+1>2的安全防护效果。比如通过入侵检测设备实时监测，并通知防火墙设备立即阻断风险源的非法访问可实现安全协同防御能力的提升。

2)安全信息的共享

及时、正确、有效的安全数据是安防设施提供安全保障能力的前提。通过对各类安全操作信息、设备运行信息、数据日志信息数据的采集、融合、处理及下发，实现安全威胁信息的快速分发与共享，可有效地提升安防设施相互协作的效率。按照安全数据信息由下级向上级逐层传递，由上级筛选、过滤和整合，再将威胁信息从上级往所需的下级传送的原则，可最大程度上发挥安防设施的效能并减少威胁告警信息的漏报和误报的情况。

3)多层级的协同防御

针对各类异常网络攻击或安全事件，目前电力

监控系统以各层级为核心,通过应用各类安防设施及技术并尽可能多地采用禁止手段来进行安全防御。但当本级遇到安防设施失灵、防御手段失效或无法抵御的网络攻击时,通过多层级的协同防御模式及上级结合多层次的安全防御技术对安全攻击进行实时、主动的协同防御,并在必要时将风险源切除可有效处理整体安全与局部安全的关系。

2　模型设计

2.1　模型框架

本模型将各层级中每一节点为中心划分为本地自治域,按照本级节点域内自防御及层级间跨域协防以实现核心层、汇聚层、接入层对电力监控系统网络安全事件进行多层协同防御的目的。同时,通过各层级间安全信息的快速传递及共享,有效地协同节点内或层级间的各类安全防护设备、域内设备级协同防御、级间策略级协同防御等工作。如图2所示,多层协同防御模型主要包括核心层中的主站自治域及协同防御控制模块、汇聚层中的区控自治域及区控协防模块、接入层中的自治域及自治域模块。

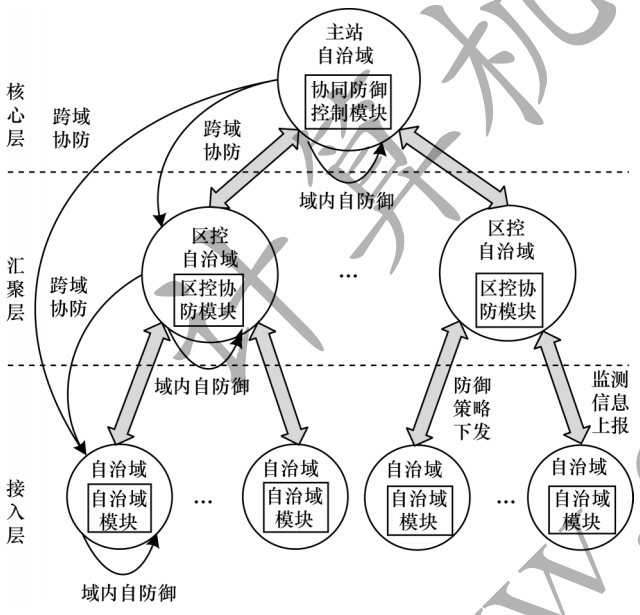

图2　多层协同防御模型总体框架

Fig.2　Overall framework of multi-layer cooperative defense model

模型框架包括以下3个方面:

1)主站自治域

核心层节点以省级或以上级别单位划分为主站自治域,域内包含本地安全防护设备,并下辖若干区控自治域及自治域。主站自治域内部署协同防御控制模块不仅具备自治域模块的监测及域内自防御能力,而且支持通过协同防御机制下发安全防御策略至所辖各区控自治域,并和自治域的安全协同设备完成协同防御。如单主站自治域以省级调度为单位,支持对所辖若干的地级调度及各地级所辖的若干变电站或电厂间进行协同防御的能力。

2)区控自治域

汇聚层节点以地市级为单位划分为区控自治域、域内包含本地安全防护设备及其下所辖若干自治域。区控自治域内部署区控协防模块不仅具备自治域模块的监测及域内自防御能力,而且支持接受、执行来自上层主站自治域分发的消息和协同防御策略,并对所辖各自治域完成防御响应动作。如单区控自治域节点以地级调度为单位,可实现对所辖若干的变电站或电厂协同防御。

3)自治域

接入层以本地为单位划分为本地自治域、域内包含各类本地安全防护设备。自治域内部署自治域模块通过监测本地网络安全信息,可协同本地安全防护设备对域内网络安全事件进行本地自防御。

2.2　模型分析

模型分析包括以下3个方面:

1)域内自防御

域内自防御通过相对独立的自治域模块可实现本地域内安全事件的快速响应及处置。域内自防御主要面向局部的网络安全问题,能使各域内拥有独自防御的能力。例如,当域内模块本地监测到网络威胁信息后,通过控制本地安全防护设备的安全策略进行本地化防御。各层级的自治域、区控自治域和主站自治域都具备域内自防御能力并优先采取该能力抵御本地安全威胁。

2)跨域协防

跨域协防是由区控协防模块或协同防御控制模块通过获取各所辖域内监测上传的相关安全信息,能生成并下发安全协同防御策略以完成域间的协同防御。跨域协防主要面向域内自防御无效、需多层级协同共同抵御或未有对应策略处置的网络安全威胁。例如,当域内安全协同设备未具备网络安全事件的响应策略、防御能力或域内自防御措施失效时,主站自治域、区控自治域可实现精准防御策略的下发及跨域协同防御。当区控自治域未具备域间协同防御能力时,可支持请求所属上层主站自治域替代区控自治域下发策略至自治域以完成跨域协防。

3)协同模式

各层级域间的协同防护是基于域内实时监测的本地相关安全信息,通过消息的方式将监测到的威胁信息由下层域向上层域上报。区控协防模块和协同防御控制模块控制所辖各域安全防护设备间的协作,能实现以分布式自治为基础的全局性安全多层协同防御模式。上级自治域模块能保障对本域的安全防护,同时可与所辖域模块通信以实现对下层域安全事件的监控与处置。

3　模型机制

通过设计数据采集、分发与共享、协同防御及联动、防御策略下发等机制的共同协作,以实现网络安全多层协同防御模型。

3.1 数据采集

电力监控系统覆盖发、输、变、配、用、调6大电力环节,涉及的与安全相关的数据种类多、体量大、结构复杂,且大多均基于多元异构数据[24],因此很难用一种方式获取所需的信息。所以,针对不同的应用场景应综合利用以下5种方式进行数据采集:

1)Syslog协议

Syslog协议以日志方式实现网络设备操作和安防设备防护等触发式安全日志信息的标准化采集[25]。如交换机设备的登录操作、设备间地址冲突、纵向加密设备的隧道错误、不符合安全访问、防火墙设备的攻击事件、入侵检测设备的入侵保护事件、防病毒设备的病毒事件等。

2)SNMP协议

对于网络设备自身运行状态信息,以SNMP(Simple Network Management Protocol)形式可周期性地采集交换机及连接于每台交换机上活跃设备的相关信息,如在线时长、处理器/内存利用率、网络丢包率、误码率网口状态等。同时,可采用SNMP trap方式以主动的形式采集网络设备配置变更或设备接入、上线等触发式信息,如用户登录口令管理、具体操作等。为保证采集的安全性,SNMP协议应采用安全性较高的v3版本。

3)Agent程序

针对业务服务器、工作站类主机,通过Agent方式实现主机硬件配置、系统运行状态、用户登录/退出、外设/外联操作、硬件异常监视等信息的采集。

4)Web Service方式

Web Service是SOA(Service-Oriented Architecture)的核心基础之一,具备服务架构理念及松耦合特性[26]。目前,电力系统中已广泛采用了Web Service方式并封装了系统的接口[27]。通过对接口进行集成,可实现对第三方应用的定制化数据采集。

5)流量方式

流量方式可弥补通用安防设备无法采集的缺憾,对符合电力系统特点的或对实时性要求更高的网络安全信息可进行实时监测和异常解析,及时发现网络中存在的常见网络攻击、工控协议规约异常、网络流量异常等信息。

3.2 分发与共享

经各层级采集到的威胁信息及安全事件数据通过分发与共享模块统一标准化后向各层级进行快速的转换和分发,以实现从更高层级或甚至全局的角度对威胁信息及安全事件的协同处置提供信息支持。

1)总线模式

为实现网络安全威胁事件的快速分发与共享的目标,本模型采用采集上报与决策下发的实时总线机制。通过对各类异构数据采集数据量大、实时性高的需求,采用上报和下发的消息总线,以实现基于网络安全威胁事件的实时消息发布、订阅功能。例如各域内的“生产者”通过采集机制发布威胁事件的消息到总线,消息总线通过主题标签的方式对事件信息进行合理分组。同一个消息主题支持各层级多“生产者”发布及“消费者”订阅。当“消费者”订阅此类威胁事件的消息后,消息总线会将此类消息高速、实时地进行推送。

2)自下至上的威胁上报

通过将监测发现并逐层上报的威胁安全事件进行标准化分类,以实现更快速的信息分发及共享,以便上层控制中心安全风险的快速决策或处置。威胁安全事件的部分分类如表1所示,包括安全事件类、运行异常类、设备故障类、人员操作类。威胁信息等级从低到高分为一般、重要和紧急3种。

表1 监测上报的威胁信息样例

Table 1 Sample of monitoring threat information reported

威胁类型	威胁信息内容	等级	事件描述
安全事件	网络入侵事件	紧急	安防设备或流量分析出的网络安全入侵事件
运行异常	数据库空间不足	重要	数据库磁盘、表空间不足

3)自上至下的策略下发

多层协同防御模型中的区控协防模块和协同防御控制模块通过策略下发总线实现策略下发的功能。面向电力监控系统的安全协同防御策略按主站自治域向区控自治域或自治域、区控自治域向自治域以自上至下的方向分为访问控制、安全接入、入侵防护3类,策略的优先级从低到高分为低、中、高3级。对于出现的威胁事件采用优先级高的的协同防护策略,当自治域收到的由主站自治域和区控自治域区同时段对同目标对象下发的同类型协同策略时,经过策略的优化和合并应优先响应高层级下发的策略。部分安全协同防御策略如表2所示。

表2 下发的安全协同防御策略样例

Table 2 Sample of secure collaborative defense strategy

策略类型	防御策略对象	优先级	协同防御策略描述
访问控制	主站自治域向区控自治域或自治域	高	协同边界防护设备控制网络流量及并发连接数
安全接入	区控自治域向自治域	中	禁止未授权、有安全风险的设备节点接入网络

3.3　协同防御

当业务节点出现安全威胁或触发网络安全事件时,需及时下发防御指令并控制安全问题的扩散。这些业务节点大多是指服务器、工作站、监控主机等主机类设备,当对存在安全风险的主机设备进行协同控制时,需要综合利用服务禁用、逻辑阻断、物理隔离等防御措施,结合网络设备、安防设备、Agent程序代理等安全防护设备进行逐级协同防御控制,如图3所示。

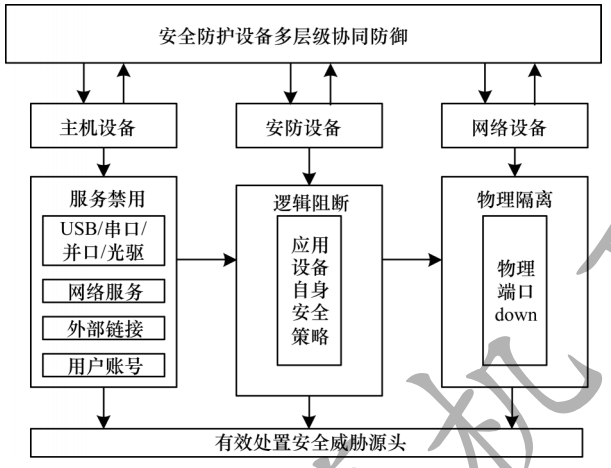

图3　安全防护设备协同防御机制

Fig.3　Cooperative defense mechanism of safety protection equipment

协同防御主要包括以下3种方式:

1)服务禁用

通过采集分析发现节点主机设备有未授权的USB接入、串口/并口接入、光驱加载、可疑的用户登录、用户危险操作、违规的外部链接或登录会话等操作事件发生时,需要对主机设备下发防御控制指令,由Agent程序执行,及时控制安全威胁的进一步蔓延。服务禁用的防御机制采用数字签名的方式以实现被控制端的身份认证,防止伪造命令的下发。其防御动作包括USB外设禁用、串口禁用、并口禁用、光驱禁用、用户强制登出、限制外部连接、主机相关的网络服务禁用等,并通过返回结果持续监测防御动作的执行效果。

2)逻辑阻断

针对违规的外部连接、危险的远程登录操作等安全威胁、以服务禁用的防御方式作用失效等场景,使用逻辑阻断的方法。逻辑阻断通过对相应安防设备下发逻辑阻断策略的方式进行连接限制甚至阻断。例如,通过对纵向或防火墙设备下发指定IP地址、端口或协议报文过滤策略进行协同,以及持续监测不符合安全策略的访问告警信息,以验证逻辑阻断的防御控制效果。

3)物理隔离

为消除当服务禁用、逻辑阻断等协同防护措施防御效果不佳、经分析判定业务主机或整个域节点存在多起安全隐患等情况发生,通过采取隔离手段实现对主机源甚至局部的网络阻隔,切断其与整个网络的联系。在物理隔离防御控制过程中,主要通过对网络设备的策略协同完成对目标风险源或区域物理网络隔离。例如,基于网络拓扑确认所有与安全风险相关节点主机直接相连的交换机端口或路由器时隙端口后,通过SNMP协议下发指定端口关闭的防御控制指令,断开风险节点与网络的连接。同时,持续监测后续网络设备防御指令返回或主动查询端口状态以确认物理隔离措施的效能。

3.4　协同联动

协同联动包括以下3种方式:

1)协同联动判定

通过将不同监测手段发现的安全事件信息互为印证、相辅相成,从而实现对网络安全事件的协同判定。例如当某主机向本地网络发动DDoS网络流量攻击时,主机所在域模块会同时监测到主机安全监测软件发出的主机异常操作行为信息、网络设备发出的主机流量异常信息及安全设备发出的网络攻击信息。通过对以上威胁信息的源主机网络IP地址、网络连接目的地址、端口号、异常流量等信息的相互匹配和验证,可对此类网络安全问题进行协同联动判定。此外,如出现本域无法判断的情形时,该消息会同时向其上层域进行上报,由上层域模块通过比对其他可能相关的监测信息进行协同判断并联动下发经决策后的协同策略。

2)协同联动控制

通过给多种协同安全设备下发联动的协同防御策略实现对所发现网络安全威胁信息的协同控制,限制危险源在一定的规则条件下运行。例如当已判定域内某主机发生DDoS网络流量攻击时,域内安全协同设备会联动进行安全控制防护,包括利用防火墙执行相应报文过滤、网络设备执行流量和并发数限制、主机监控软件执行指定IP地址、端口号的访问控制等策略。此外,当本域出现策略无效或无可执行策略的安全协同设备时,该信息将同时向其上层域进行上报,由上层域模块下发协同防御策略或在该域相邻的域,即更大范围内的安全协同设备间采取联动的协同防御策略控制。

3)协同联动阻断

根据监测到的并完成协同判定确认的,或基于安全协同控制服务无效的威胁信息,通过下发协同防御策略协同各安全协同设备联动执行阻断操作,以杜绝危险源可能造成的进一步危害。例如在已判定域内某主机发生DDoS网络流量攻击并对其进行域内自防御或协同控制无效的场景下,可通过联动多种安全防护设备的协同阻断措施切除危险源。具体来说,针对出现的威胁事件对应所属域按上层级向下层级从高优先级向低优先级的顺序执行联动的协同安全防御策略,直到监测的威胁信息不再上报

为止。此外，当本域出现策略无效或无可执行策略的安全协同设备时，该信息将同时向其上层域上报，由上层域或与该域相邻域模块下发协同防御策略，即在更大范围内的安全协同设备间实现联动的协同防御策略阻断。

3.5 关联决策下发

借鉴灰色系统理论[26]，结合网络安全事件的业务影响度、威胁程度、防御动作可靠性及时效性、频次或持续时间以及与其他安全事件的关联度等影响因子，通过构造决策集合、赋值确定参考序列、计算关联系数及加权关联度等步骤对网络安全事件各因子与防御策略进行关联度分析，对特定并满足条件的网络安全事件，选取关联度最高（即决策优先级最高）的防御措施下发执行。

1）决策集合

针对特定网络安全事件，分析及制定各影响因子与防御策略的关联性，并设 n 个影响因子数据序列形成如下矩阵，其中 m 为可行的安全防御动作的个数。

$$(X_1',X_2',\cdots,X_n')=\begin{pmatrix} X_1'(1) & X_2'(1) & \cdots & X_n'(1) \\ X_1'(2) & X_2'(2) & & X_n'(2) \\ \vdots & \vdots & & \vdots \\ X_1'(m) & X_2'(m) & \cdots & X_n'(m) \end{pmatrix} \tag{1}$$

其中：X_n' 为某网络安全事件下第 n 个影响影子对应的 m 种防御措施集合；$X_n'(m)$ 为该事件第 n 个影响因子的第 m 种防御措施。

2）对决策集合赋值并确定参考序列

根据该网络安全事件各影响因子的具体描述，对式（1）中 n 个影响因子对应的 m 种可行防御措施进行初始化指数赋值，数值越高，该关联系数越大。同时，以构造决策集合中各影响因子指标的最优值（即安全风险的关联系数最小值）为标准构建对应各类影响因子的参考序列，如式（2）所示：

$$\boldsymbol{X}_0'=\left(X_0'(1),X_0'(2),\cdots,X_0'(m)\right) \tag{2}$$

其中：X_0' 为某网络安全事件下安全风险指数的参考序列；$X_0'(m)$ 则为第 m 种安全措施的安全风险理想值。

3）关联系数

通过式（3）分别计算决策集合与参考序列对应元素的关联系数，并形成关联系数矩阵，计算公式如式（4）所示：

$$\boldsymbol{S}_i(k)=\frac{\min_i\left|X_0'(k)-X_i'(k)\right|+\rho\times\max_i\left|X_0'(k)-X_i'(k)\right|}{\left|X_0'(k)-X_i'(k)\right|+\rho\times\max_i\left|X_0'(k)-X_i'(k)\right|} \tag{3}$$

$$\boldsymbol{S}_i(k)=\begin{pmatrix} S_1(1) & S_2(1) & \cdots & S_n(1) \\ S_1(2) & S_2(2) & \cdots & S_n(2) \\ \vdots & \vdots & & \vdots \\ S_1(m) & S_2(m) & \cdots & S_n(m) \end{pmatrix} \tag{4}$$

其中：$i=1,2,\cdots,n$；$k=1,2,\cdots,m$；$X_i'(k)$ 及 $X_0'(k)$ 分别为决策集合及参考序列第 i 个影响因子下第 k 中安全防御措施的安全指数值。在逐个计算决策集合每个安全指数与参考序列对应元素的绝对差值后确定最小最大标准化参数，最终得到关联系数矩阵。其中，ρ 为分辨系数，$0<\rho<1$，若 ρ 越小，则关联系数间差距越大，结果差异也越大。在本次防御决策关联度计算中，ρ 取中间值0.5，使关联系数的偏差保持一致。

4）加权关联度

通过综合评估每类影响因子在本次网络安全事件中所占权重，根据式（5）对关联系统矩阵计算各影响因子每种防御措施的安全指数，及参考序列对应元素的关联系数均值，以反映各种防御手段与参考序列的关联关系，最终列出本次网络安全事件与各安全防御策略间的相应关联度。

$$r_i'=\frac{1}{m}\sum_{k=1}^{m}W_k\times S_i(k) \tag{5}$$

其中：$i=1,2,\cdots,n$；$k=1,2,\cdots,n$；W_k 为各影响因子的在影响权重占比；r_i' 为本次安全事件第 i 个防御策略的加权平均关联度。

以厂站侧发生某业务主机USB无线网卡接入的单点网络安全事件为例。表3通过最高关联度决策算法验证该算例，计算结果表明，“网卡禁用”处置措施的关联度最高。

表3 网络安全事件防御决策关联度决策算例

Table 3 Example of decision-making on the degree of relevance in the defense of network security events %

“USB无线网卡接入”事件	业务影响度	安全威胁程度	策略可靠性	发生频次或持续时间	与其他事件相关性	关联度（r_i'）
网卡禁用	100	100	60	100	100	92.94
上联交换机端口关闭	90	100	80	80	90	79.23
纵向隧道阻断	70	80	90	50	70	61.67
主站路由端口阻断	40	50	100	10	40	49.97
权重占比	20	20	15	20	35	—

3.6 协同防御模型比对

以目前国内外信息安全应用较为广泛的一种经典动态安全P2DR模型[27],包括Policy、Protection、Detection、Response等多个主要构成要素为基准,对部分文献中提及的关于协同防御模型的实现方式进行对比,如表4所示。

表4 各安全协同防御模型的实现对比

Table 4 Implementation comparison of security collaborative defense models

对比项	本文模型	模型1[28]	模型2[29]	模型3[30]	模型4[13-14]
策略	基于协同防御策略库的最高关联度动态决策机制	基于静态策略库的全局和本地策略2类	基于动态更新策略库的控制、通信及整体安全策略3类	基于静态策略库的策略生成及协同控制器的分发	静态安全策略库
防护	协同安防、网络及主机设备Agent,通过服务禁用、逻辑阻断、物理隔离等措施	默认为网络设备	协同漏扫打补丁、蜜罐/蜜网系统	协同防火墙、交换机、路由器及蜜罐设备	协同网络伪装系统、防火墙
监测	Syslog/SNMP协议、主机Agent、WebService及流量等底层方式	入口部署监控节点,未论述监测方式(默认为网络设备)	依靠入侵检测、防火墙、入侵阻止等系统或设备	依靠部署入侵检测、防火墙、交换机镜像口探测器等设备	依靠入侵检测等设备
响应	基于多层级协同的威胁上报及决策下发	一个全局集中式安全域管控其他二级各域的防护响应,域间支持信息交互	实现入侵监测与防火墙联动、蜜罐的重定向,未涉及层级关系	各域内节点平等,自主防御响应,无层级关系	依靠审计及事故恢复系统

对比文献中所提模型的实现大多是在静态安全策略控制的指导下,综合运用传统网络安防或固有设备的监测及防御能力,通过中心节点管控或各域内自治的方式驱动整个系统的安全协同防御,但都未涉及多级间协同的防御方式。本模型以最高关联度策略的动态决策作为防御核心,通过各类协议及流量镜像等底层信息采集方式,支持协同多层级主机Agent、网络设备、通用或专用安防设备实时的威胁响应及风险处置。通过对比可知,本模型数据采集方式丰富、协同防护手段全面、防御措施支持动态决策,可快速适应电力调度数据网多层级网络拓扑架构,在实现网络安全协同防御的全覆盖的同时,可满足电力监控系统网络安全协同防护及管控要求。

4 实验验证

4.1 总体设计

根据面向电力监控系统网络安全多层的协同防御模型及其实现机制,从电力系统网络安全防护需求出发,并采用如图4所示的多层架构和模块化设计。该设计包括数据采集、威胁分析与识别、协同防御、防御策略库、公共服务等模块。各模块间结构相互独立,便于独立部署或单元测试。基于上述模型功能框架结构上,遵从高内聚、低耦合的原则实现模块化设计,选择成熟的Web技术路线,使用Java、JavaScript、Flex等语言开发,采用分层技术和面向接口和服务的技术架构,通过支持主流中间件,融合主流、成熟的开源软件,实现基于面向电力监控系统的多层协同防御原型系统。

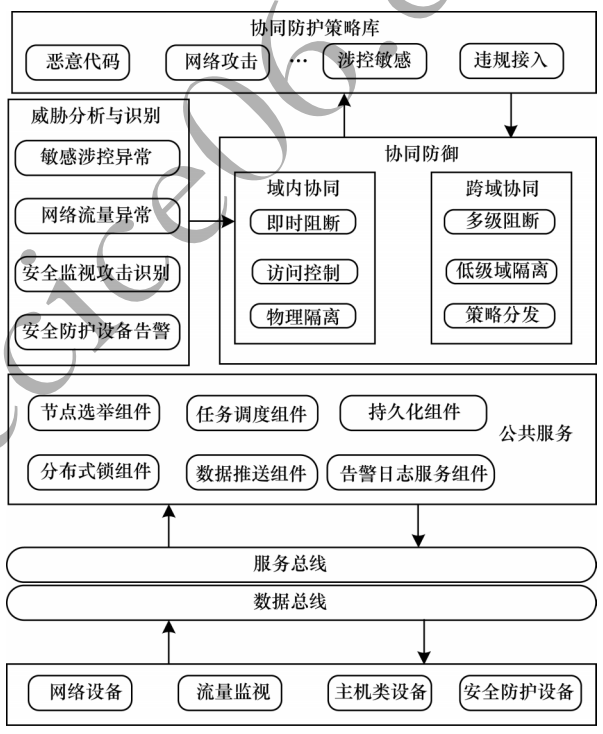

图4 协同防御模型模块化设计

Fig.4 Modular design of collaborative defense model

此系统目前已在调度主站及所辖数个厂站完成试点应用,并对所设计的框架模型及软件功能进行了应用测试。通过对本级调控机构全网网络安全事件的梳理,在已知明确的单点网络安全事件、复杂情景下的网络安全事件及以上情形防御失效的3个典型场景进行了功能验证。

4.2 已知明确安全事件场景

针对触发原因明确、业务影响度较低且由单台设备引起的紧急网络安全事件，本地自治域模块通过阻断ssh链路、禁用主机物理网卡服务及其上联交换机端口下电方式有效地对风险源进行处置。

验证场景1 通过阻断ssh链路的方式，以实现站内现场运维人员在登录会话中操作涉敏违规操作命令或非法外联链接场景下的安全处置。

验证场景2 通过禁用主机物理网卡服务及断开其上联交换机端口的方式应对无线网卡接入、恶意代码感染、网络攻击或入侵、违规设备接入、主机或端口扫描、DDoS攻击、SMB服务访问异常、不符合策略的安全访问或异常服务访问等紧急安全事件。如图5所示，×表示成功的防御动作。

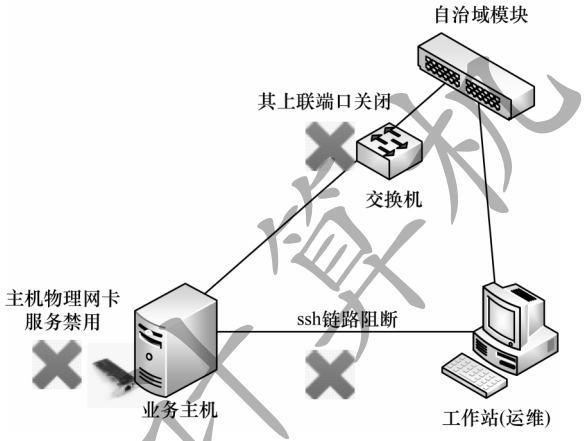

图5 明确网络安全事件下的防御模型验证场景

Fig.5 Defense model verification in clear network security event scenario

4.3 复杂安全事件场景

针对一段时间内爆发的数起复合型非紧急类安全事件或不能直接定位攻击或风险源的事件，区控协防模块通过匹配协同防御策略库中预制规则，按安全事件的情节轻重程度触发主动防御动作。

验证场景3 通过模拟同时段内相同主机爆发USB外设接入、非法登录尝试、用户权限变更、关键文件或目录变更、违规操作、设备开发非法端口等组合型安全事件时，成功执行网卡禁用及上联交换机端口阻断的防御动作。

验证场景4 通过模拟同厂站内不同业务设备在同时间段内触发紧急复合型安全事件，执行该厂站纵向设备隧道阻断动作，以成功切断单站网络，从而实现局部隔离。如图6所示为复杂网络安全事件下的防御模型验证场景。

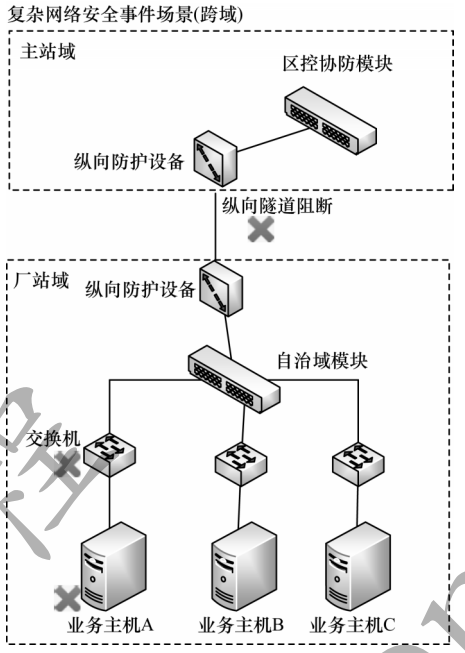

图6 复杂网络安全事件下的防御模型验证场景

Fig.6 Defense model verification in complex network security event scenario

4.4 安全防护失效场景

通过人工干预，在模拟以上场景安全防御失效的场景下，协同防御控制模块通过各类影响因子的关联计算，执行防御决策优先级最高的防御动作。如图7所示，随着灰色域逐步加深，防御动作逐层启动，网络空间安全防御的处置范围也正逐级扩大，直至切除局部或整个域为止，以保障电网的整体安全。

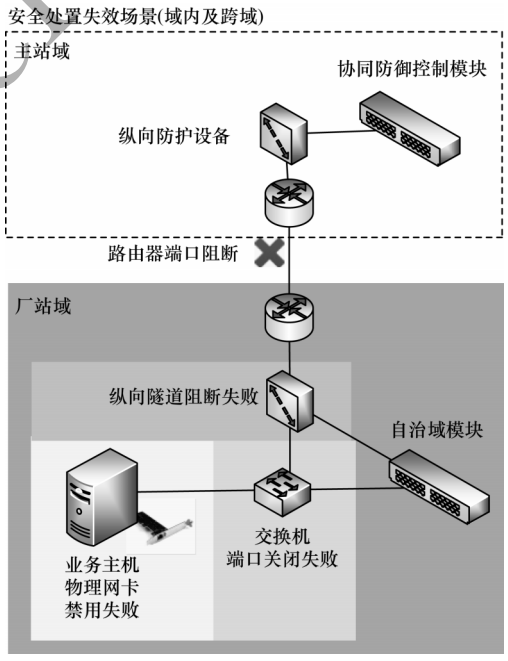

图7 失效场景下的多级防御模型验证

Fig.7 Verification of multi-level defense model in failure scenario

验证场景5　模拟主机物理网卡禁用执行失败情形下，成功下发并执行其上联交换机端口阻断动作。

验证场景6　模拟上联交换机端口阻断失败条件下，成功下发并执行了对应区域纵向设备的断隧道动作。

验证场景7　模拟厂站区域纵向设备的断隧道动作失败的情形下，主站成功下发并执行了主站侧路由器对应端口的关闭动作，实现厂站侧区域隔离，防止安全威胁向主站的传播可能。

现场典型场景验证结果表明，该系统能够通过网络安全事件信息共享、协同防御策略库的快速决策，有效协同并处置了各类场景下的网络安全事件，从而避免了安全风险进一步扩散。下一步协同防御策略库在试运行期间所积累的网络安全事件成功处置策略集将部署于省级以上调度主站，并协同开展省-地-厂站3级协同防御机制的应用测试及功能验证。

5　结束语

多层协同防御是提升网络空间安全防护的一种有效途径，在电力监控系统网络攻击专业化、国际化、攻击频繁爆发及高持续威胁的背景下，多层协同防御模型可动态处置电力监控系统网络安全在防御广度和深度方面存在的不足。本文结合电力监控系统多层级星型组网特点及安全防护需求，提出基于自治域面向电力监控系统的多层协同防御模型及实现机制。该模型通过各层级域内自防御、跨域协同防御的特性，从主机层、安防设设备层和网络层对安全威胁及风险进行分级、多层次的主动防御。实验结果表明，该模型能较好地满足目前电力监控系统安全防护要求，提高网络安全防护能力，实现由被动式防御向主动式防御的转变，具有较高的理论研究和实践推广应用价值。下一步将继续验证适应省级以上调度机构协同防御模型的现场测试工作，同时开展“国-分-省-地-厂站”5级网络安全协同防御模式的探索。

参考文献

[1] 董朝阳，赵俊华，文福拴，等. 从智能电网到能源互联网：基本概念与研究框架[J]. 电力系统自动化，2014，38(15)：1-11.
DONG Z Y，ZHAO J H，WEN F S，et al. From smart grid to energy internet：basic concept and research framework[J]. Automation of Electric Power Systems，2014，38(15)：1-11. (in Chinese)

[2] 赵俊华，文福拴，薛禹胜，等. 电力CPS的架构及其实现技术与挑战[J]. 电力系统自动化，2010，34(16)：1-7.
ZHAO J H，WEN F S，XUE Y S，et al. Cyber physical power systems：architecture，implementation techniques and challenges[J]. Automation of Electric Power Systems，2010，34(16)：1-7. (in Chinese)

[3] 赵俊华，文福栓，薛禹胜，等. 电力信息物理融合系统的建模分析与控制研究框架[J]. 电力系统自动化，2011，35(16)：1-8.
ZHAO J H，WEN F S，XUE Y S，et al. Modeling analysis and control research framework of cyber physical power systems[J]. Automation of Electric Power Systems，2011，35(16)：1-8. (in Chinese)

[4] 辛耀中，石俊杰，周京阳，等. 智能电网调度控制系统现状与技术展望[J]. 电力系统自动化，2015，39(1)：2-8.
XIN Y Z，SHI J J，ZHOU J Y，et al. Technology development trends of smart grid dispatching and control systems[J]. Automation of Electric Power Systems，2015，39(1)：2-8. (in Chinese)

[5] 李保杰，刘岩，李洪杰，等. 从乌克兰停电事故看电力信息系统安全问题[J]. 中国电力，2017，50(5)：71-77.
LI B J，LIU Y，LI H J，et al. Enlightenment on the security of cyber information system under smart grid from Ukraine blackout[J]. Electric Power，2017，50(5)：71-77. (in Chinese)

[6] 汤奕，陈倩，李梦雅，等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化，2016，40(17)：59-69.
TANG Y，CHEN Q，LI M Y，et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems，2016，40(17)：59-69. (in Chinese)

[7] 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 J D，WANG Y，ZHAO Z C，et al. Type and verification of network attacks on embedded terminals of intelligent substation[J]. Electric Power，2020，53(1)：81-91. (in Chinese)

[8] 国家发展与改革委员会. 电力监控系统安全防护规定[EB/OL]. [2020-09-02]. https://shupeidian.bjx.com.cn/html/20140815/537138.shtml.
National Development and Reform Commission. Regulations on safety protection of power monitoring system[EB/OL]. [2020-09-02]. https://shupeidian.bjx.com.cn/html/20140815/537138.shtml. (in Chinese)

[9] 国家标准化管理委员会. 电力监控系统网络安全防护导则：GB/T 36572—2018[S]. 北京：中国标准出版社，2018.
National Standardization Administration. Guidelines for network security protection of power monitoring system：GB/T 36572—2018[S]. Beijing：China Standards Press，2018. (in Chinese)

[10] 刘旭勇. 基于协同的网络安全防御系统研究[J]. 计算技术与自动化，2012，31(2)：142-144.
LIU X Y. Network security defense system research based on the collaborative[J]. Computing Technology and Automation，2012，31(2)：142-144. (in Chinese)

[11] 徐锐，陈剑锋. 网络空间安全协同防御体系研究[J]. 通信技术，2016，49(1)：92-96.
XU R，CHEN J F. Collaborative defense architecture of cyberspace security[J]. Communications Technology. 2016，49(1)：92-96. (in Chinese)

[12] 张海涛，魏巍. 一种有效的网络安全协同防御机制研究[J]. 计算机应用与软件，2011，28(9)：113-115，133.

ZHANG H T, WEI W. A kind of effective network security cooperative defense mechanism[J]. Computer Applications and Software. 2011, 28(9): 113-115, 133. (in Chinese)

[13] 庞聪,韩秀玲. 校园网安全协同防御体系模型研究[J]. 计算机与现代化,2012(2):156-160.
PANG C, HAN X l. Study on system and model of coordinated defense for campus network security[J]. Computer and Modernization, 2012(2): 156-160. (in Chinese)

[14] 李基初,唐俊. 基于多智能体社会的僵尸网络协同防御模型[J]. 微电子学与计算机,2011,28(3):73.
LI J C, TANG J. Study on collaborative defence model of botnet[J]. Microelectronics and Computer, 2011, 28(3): 73. (in Chinese)

[15] 李田,苏盛,杨洪明,等. 电力信息物理系统的攻击行为与安全防护[J]. 电力系统自动化,2017,41(22):162-167.
LI T, SU S, YANG H M, et al. Attacks and cyber security defense in cyber-physical power system[J]. Automation of Electric Power Systems, 2017, 41(22): 162-167. (in Chinese)

[16] 高昆仑,辛耀中,李钊,等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化,2015,39(1):48-52.
GAO K L, XIN Y Z, LI Z, et al. Development and process of cybersecurity protection architecture for smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 48-52. (in Chinese)

[17] 刘烃,田决,王稼舟,等. 信息物理融合系统综合安全威胁与防御研究[J]. 自动化学报,2019,45(1):5-24.
LIU T, TIAN J, WANG J Z, et al. Integrated security threats and defense of cyber-physical systems[J]. ACTA Automatica Sinica, 2019, 45(1): 5-24. (in Chinese)

[18] 丁茂生,孙维佳,蔡星浦,等. 电力系统极端事件的风险评估与防范[J]. 中国电力,2020,53(1):32-39,65.
DING M S, SUN W J, CAI X P, et al. Risk assessment and prevention of extreme events in power systems[J]. Electric Power, 2020, 53(1): 32-39, 65. (in Chinese)

[19] 李芹,卢长燕,霍雪松,等. 电力调度数据网测试模型[J]. 电力系统自动化,2015,39(1):187-193.
LI Q, LU C Y, HUO X S, et al. Test models of electric power dispatching data network[J]. Automation of Electric Power Systems, 2015, 39(1): 187-193. (in Chinese)

[20] 信息化和软件服务业司 工业和信息化部. 工业控制系统信息安全防护指南[EB/OL]. [2020-09-02]. https://m.ccement.com/news/content/8717944740806.html.
Department of Information and Software Services, Ministry of Industry and Information Technology. Guide for information security protection of industrial control systems. [EB/OL]. [2020-09-02]. https://m.ccement.com/news/content/8717944740806.html. (in Chinese)

[21] 国家能源局. 电力监控系统安全防护总体方案[EB/OL]. [2020-09-02]. http://jsb.nea.gov.cn/news/2015-3/2015312105159.html.
National Energy Administration. Overall safety protection scheme of power monitoring system[EB/OL]. [2020-09-02]. http://jsb.nea.gov.cn/news/2015-3/2015312105159.html. (in Chinese)

[22] 李中伟,佟为明,金显吉. 智能电网信息安全防御体系与信息安全测试系统构建:乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化,2016,40(8):147-151.
LI Z W, TONG W M, JIN X J. Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel[J]. Automation of Electric Power Systems, 2016, 40(8): 147-151. (in Chinese)

[23] 王栋,陈传鹏,颜佳,等. 新一代电力信息网络安全架构的思考[J]. 电力系统自动化,2016,40(2):6-11.
WANG D, CHEN C P, YAN J, et al. Pondering a new-generation security architecture model for power information network[J]. Automation of Electric Power Systems, 2016, 40(2): 6-11. (in Chinese)

[24] 孙超,王永贵,常夏勤,等. 面向电力大数据的异构数据混合采集系统[J]. 计算机系统应用,2018,27(12):62-68.
SUN C, WANG Y G, CHANG X Q, et al. Mixed heterogeneous data acquisition system for power big data[J]. Computer Systems and Applications, 2018, 27(12): 62-68. (in Chinese)

[25] 电力系统通用告警格式:GB/T 31992—2015[S]. 北京:中国标准出版社,2015.
General alarm format for power system: GB/T 31992—2015[S]. Beijing: China Standards Press, 2015. (in Chinese)

[26] 唐建平. 基于灰色理论的电力系统动态状态估计模型及算法研究[D]. 重庆:重庆交通大学,2014.
TANG J P. Research on power system dynamic state estimation algorithm based on grey theory[D]. Chongqing: Chongqing Jiaotong University, 2014. (in Chinese)

[27] XU S P, ZHANG Y H, ZHOU Y, et al. Design and application of a network security model[J]. Applied Mechanics and Materials, 2013, 2560: 2773-2776.

[28] 韩宗芬,陶智飞,杨思睿,邹德清. 一种基于自治域的协同入侵检测与防御机制[J]. 华中科技大学学报(自然科学版),2006(12):53-55.
HAN Z F, TAO Z F, YANG S R, et al. A cooperative intrusion detection and defense mechanism based on autonomous domain[J]. Journal of Huazhong University of Science Technology (Nature Science Edition), 2006, 34(12): 53-55. (in Chinese)

[29] 赵琳琳,颜若愚,李奇胜. 基于P2DER模型的网络安全主动协同防护系统框架[J]. 现代计算机(专业版),2010(2):93-97.
ZHAO L L, YAN R Y, LI Q S. Framework of network security active cooperative defense system framework based on P2DER model[J]. Modern Computer (Professional Edition), 2010(2): 93-97. (in Chinese)

[30] 楼润瑜,王备战,王伟. 大规模网络的主动协同防御模型研究[J]. 厦门大学学报(自然科学版),2010,49(2):198-204.
LOU R Y, WANG B Z, WANG W. An active cooperation defense model for large scale network[J]. Journal of Xiamen University (Natural Science), 2010, 49(2): 198-204. (in Chinese)

编辑 赖玉玲