



智能变电站网络安全态势感知技术

郭静, 黄伟, 郭雅娟, 周超, 陈昊

(国网江苏省电力公司电力科学研究院, 江苏 南京 211103)

摘要:网络安全态势感知技术在智能变电站中的应用,有助于从更独特、更高层次的安全视角分析评估智能变电站的安全状况。在分析智能变电站安全威胁的基础上,综合物理安全、网络安全、系统安全、协议安全、数据安全等因素提出了一种安全态势感知框架,同时提供了一种变电站网络安全监控方案。即使用专门的智能变电站网络安全态势感知装置收集安全事件的发生情况并对其结果进行分析。此外,描述了设计方案中采用的几个关键技术。最后,提供了智能变电站网络安全态势感知装置的软硬件设计方案。该方案采用多层软件体系结构设计,并使用了英特尔 Sandy Bridge 处理器、总线结构和模块化设计技术等来满足系统的高性能需求。

关键词:态势感知;网络安全;智能变电站

中图分类号:TP277

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2015386

Network security situation awareness technology in smart substation

GUO Jing, HUANG Wei, GUO Yajuan, ZHOU Chao, CHEN Hao

State Grid Jiangsu Electric Power Research Institute, Nanjing 211103, China

Abstract: On the basis of analyzing the security threats in smart substation, a security situation awareness framework was proposed, combined with integrated physical security, network security, system security, protocol security, data security and so on. And a network security monitoring solution for substations was provided. It was a special intelligent substation network security situation awareness device which could collect the security events, analyze them and generate situation analysis results. Further more, several key technologies used in our frameworks were focused on. Finally, a design scheme including hardware and software for the smart substation network security awareness system and its implementation architecture were described, in which a multi-layer software architecture was adopted by the system, and a combinatory of the Intel Sandy Bridge, the bus structure and a modular design technology, was adopted in order to meet the need of high performance.

Key words: situation awareness, network security, smart substation

1 引言

智能变电站是智能电网的重要组成部分,具有全站信息数字化、通信平台网络化、信息共享标准化等技术特征。目前,智能变电站自动化系统建设多采用 IEC61850 通信

标准,该标准由国际电工委员会(IEC)共同开发,致力于提供一个灵活性、通用性强的通信系统^[1]。基于 IEC61850 标准建设的智能变电站不再是一个孤岛,工作人员和攻击者都可以进入变电站内网,这带来了新的安全威胁^[2]。此外,基于微处理器的智能电子设备(IED)、基于广域网络标准

协议 TCP/IP(WAN)的新技术在变电站内广泛应用,使用 IED 进行维护或用户界面远程访问成为常见的做法。变电站存在的潜在漏洞,如不符合规范的标准协议、未经授权远程访问变电站 IED 以及一些变电站 IED 和用户界面配置有 Web 服务器,可通过服务器进行远程配置改变、控制默认密码等都对安全造成极大威胁。面对这些漏洞,即使采用防火墙和加密方案来加固网络,仍可能会使攻击目标暴露在入侵者面前。综上所述,亟需一种新技术来全面评估智能变电站的安全情况并采取有效的措施保障网络的安全。目前,智能变电站网络安全性研究仍然是一个新兴的领域。因此,本文重点研究网络安全态势感知技术在智能电网的应用,并在此基础上评估智能变电站的安全性。

态势感知的概念来自于航空航天领域中的人为因素的研究。美国国土安全部把“态势感知”定义为“识别、处理、综合发生在重要设施或组织上的关键信息元素的能力”。随着互联网的发展,网络安全问题变得越来越严峻。为了应对不断增加的安全威胁,大型网络中使用了多种安全设备。这些设备报告了大量的安全事件^[3],然而在面对大量的预警信息时,很难准确把握整个网络的安全状态。为解决这个问题,研究者将态势感知的概念引入网络安全系统中。1999 年, Bass T 首次将这一概念引入网络,提出了基于多传感器数据融合的网络安全态势感知框架,该框架可以帮助网络管理员识别、跟踪和评估网络攻击活动^[4];以 Endsley 态势感知框架参考,赖积保等人^[5]提出了新的网络安全态势感知模型,为了解整个网络安全的趋势,必须收集、融合和分析大量的信息,减少误报率;汤永利等^[6]报道了一种基于加权 D-S 证据理论的信息融合方法,该方法由 D-S 证据理论对(BPA)基本概率分配依次进行合成计算,弱化人为因素对 BPA 的影响,提高 BPA 的预测精度和网络安全态势识别率。

从网络安全信息获取到构建网络安全态势模型是一个复杂的过程。但是,大多数研究都集中在安全事件分析或安全风险评估方法的融合。没有对网络安全状况整体、正式的描述,缺乏一个完整的态势感知框架。此外,大多数研究工作只专注于互联网的网络态势感知框架和评估方法。

在分析智能变电站安全威胁的基础上,本文综合物理安全、网络安全、系统安全、协议安全、数据安全等因素提出了一种安全态势感知模型,并提出了一种基于专用智能变电站网络安全态势感知装置的变电站网络安全监控方案。该方案根据变电站网络流量、网络环境、服务稳定等特

点,将生产及维护过程中产生的网络干扰考虑在内,采取了探测思想对网络异常特征和攻击行为进行分析。最后,提供了一个设计方案,包括智能变电站网络安全态势感知装置的实施架构和软硬件设计。该方案采用多层软件体系结构,包括数据采集层、预处理层、分析层和可视化层,各层具有相对独立的功能,并通过消息总线进行交互;另一方面,根据工业控制系统(ICS)的特点,硬件设计采用英特尔 Sandy Bridge 处理器、总线结构和模块化设计技术,以满足高性能的需求。

2 变电站架构及其安全分析

2.1 变电站架构

图 1 是典型的变电站结构^[7],其中主要组件是智能电子设备(IED)、电力设备、变电站控制中心。变电站控制中心位于站点中心,监控和管理大量智能电子设备。智能电子设备通过传感器等收集站内电流和电压数据,并将数据发送到站控层;另一方面直接或通过过程层网络接收控制指令,驱动执行器完成控制功能。变电站控制中心具有分级结构,一个高级别主站可控制多台低级别主站。

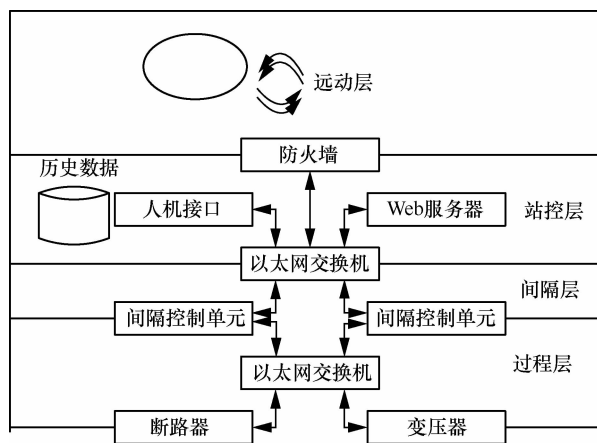


图 1 典型变电站结构

数据和命令传输可能发生在变电站控制中心和 IED 之间、IED 之间或 IED 和传感器(或开关设备)之间。信息通过变电站网络传输,变电站网络是基于各种通信信道和网络技术(包括以太网、串行链路、无线通信)建立的,这些通信都基于 IEC61850 标准。

2.2 安全性分析

安全性分析的目的是找出可能威胁到智能变电站的攻击。已经存在许多关于各种信息网络安全攻击的研究方案,这些方案主要可以分成两种:一种是从防护者的角度



出发;另一种是从攻击者的角度出发。从防护者的角度来看,需要满足自身的安全需求,因此安全策略以及执行安全策略的安全机制都是必须的。安全策略的可执行性取决于使用的机制,但无论选择哪种方式,都不能影响系统的性能。另一方面,从攻击者的角度来看,攻击者总是想方设法实现既定目标。目前,两类主要攻击类型可以被识别:一类是破坏服务功能(可用性攻击);另一类是获取机密信息,用于不公平竞争、勒索等恶意行为(保密性攻击)。

3 网络安全态势感知建模

建模是网络安全态势感知(NSSA)的基础。关于 NSSA 模型^[5,6]已有许多研究。1999 年,Bass T 首次提出了基于多传感器数据融合的网络态势感知功能框架,成为其他模型建模的基础。但它并不能解决实际的安全问题,并有许多缺陷。在研究大量模型的基础上,本文给出了一种多层次的态势感知的概念模型,如图 2 所示。

3.1 一种新型 NSSA 模型

基于上述提到的网络安全态势感知模型,本文提出了一种新的 NSSA 系统框架,如图 3 所示。该框架应用了安全态势感知技术、安全态势评估模型与评估算法。根据该框架,开发了一个适用于智能变电站的态势感知装置,将其部署在智能变电站的内部网络中,对原始态势数据进行收集、预处理、分析,全面感知变电站网络访问、通信过程、异常流量、恶意攻击等安全态势,实现智能变电站信息安

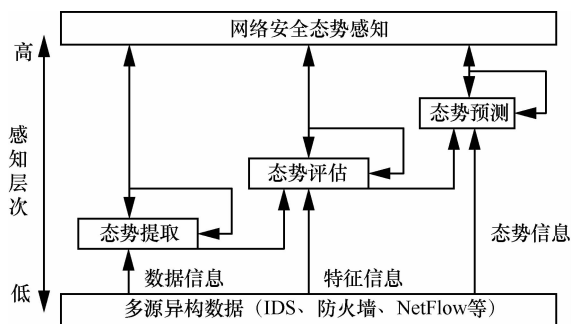


图 2 网络态势感知模型

全主动防御。

该框架包括 4 个模块:数据采集模块、态势评估模块、态势预测模块与安全加固方案模块。除了安全加固方案模块,每个模块都对应不同的层级和架构。

(1) 数据采集模块

该模块的主要任务是使用多传感器获取原始安全态势数据,并从中提取出影响网络安全态势的信息,转化为统一的 XML 格式,为网络安全态势评估和预测提供必要的数据支持。

(2) 态势评估模块

用精确的数学模型分析输入的安全态势信息,该模块提供了一个全面、定量的网络安全态势状况描述,它是态势感知的核心。

(3) 态势预测模块

根据历史网络安全态势信息和当前网络安全态势信

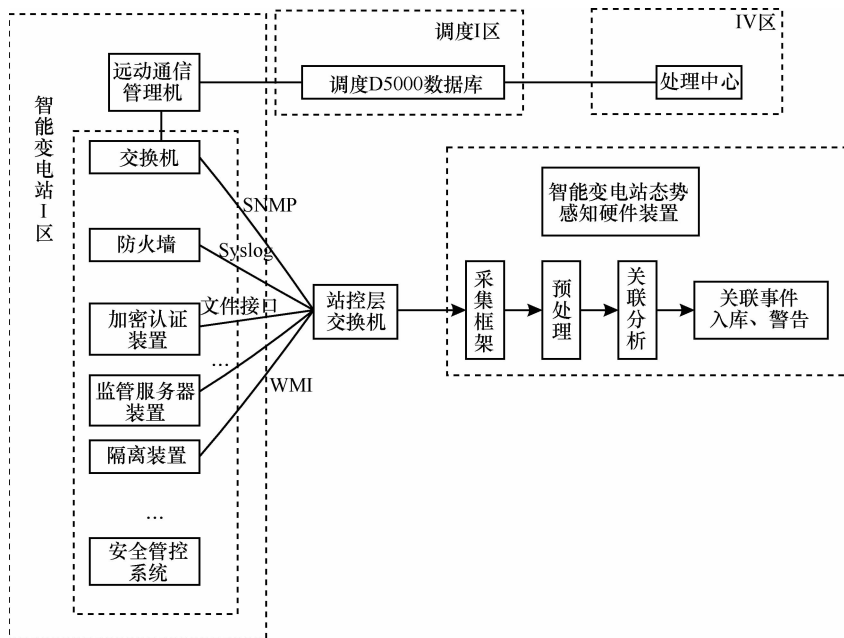


图 3 智能变电站网络态势感知系统框架

息预测网络安全趋势。此外,综合从其他模块中获得的数据,该模块提供了一个实用的安全加固方案,指导管理者提高网络的安全性。

3.2 数据采集

在态势感知模型中,数据是研究的基础,数据类型的选取对研究结果有决定性的作用。在该框架中,第一部分是数据采集(DA)模块,它包含 3 个子模块:设备日志收集子模块,收集来自部署在变电站的各种安全设备所产生的日志数据;传感器子模块,它是由多个分布式异构传感器组成的。多源传感器提供了更完整可靠的数据,使分析结果更精确。在试验性研究中,选择了 Snort 和 NetFlow 两种传感器来监测变电站网络。预处理子模块,它具有格式化传感器数据的功能,同步不同的传感器并消除无效的传感器数据,以获得更准确的分析结果。

在预处理的初始阶段,所有接收到的安全事件被转换为可被数据处理模块识别的标准格式。收集到的安全事件种类多、数量大。它们的特性可以用一个多元组的形式表示出来:

$$e_i = \{detectTime_i, eventType_i, attack_i, srcIP_i, desIP_i, srcPort_i, desPort_i, protocol_i, sensorID_i, confidence_i, severity_i, other\} \quad (1)$$

其中, $detectTime_i$ 代表安全事件发生的时间, $eventType_i$ 代表安全事件的类型, $attack_i$ 代表安全事件的等级, $srcIP_i$ 和 $desIP_i$ 代表安全事件的源和目的地址, $srcPort_i$ 和 $desPort_i$ 是指安全事件的源端口和目的端口, $protocol_i$ 代表了协议类型, $sensorID_i$ 代表检测到事件的传感器, $confidence_i$ 代表安全事件发生的可信度, $severity_i$ 代表安全事件的严重程度, $other$ 代表安全事件的其他信息。

安全事件数据来源各不相同,它们可能来自于入侵检测事件记录、防火墙日志文件、主机系统日志文件、NetFlow 信息流等。收集到的信息具有不同的格式,必须将

它们转换为统一的格式。在框架中,提供了对应不同传感器的预处理模块,将特定传感器的信息转化为文中定义的信息模型的属性值。

3.3 安全事件检测

为了检测安全事件,设计了一个变电站网络行为检测引擎,如图 4 所示。引擎的核心是统计协议识别(SPID)算法、规则触发器。该算法使用 K-L(Kullback-Leibler)统计法准确地计算出网络协议类型,其输出结果将成为规则触发器的输入。基于规则库的触发器负责生成事件检测结果,它高度依赖建立的规则库,规则库的质量对事件检测精度有很大的影响。

首先,从系统接收事件信息后,SPID 算法通过事件属性标识识别协议类型。对于一个初始协议类型,创建了相应的协议模型保存相关事件属性,称为指纹;对于已存在的协议类型,可以找到相应的协议模型。协议模型保存了一系列的属性指纹并负责增量相应的指纹计数器。此外,新发生的安全事件将和所有协议模型进行指纹比较,通过 K-L 散度方程计算两者概率分布之间的 K-L 散度值。散度值从 0 到 ∞ ,可根据式(2)计算。

$$D_{KL}(P_{attr} || Q_{attr, prot}) = \sum_i P_{attr}(i) \times \ln \frac{P_{attr}(i)}{Q_{attr, prot}(i)} \quad (2)$$

其中, P_{attr} 和 $Q_{attr, prot}$ 分别代表被测安全事件具体属性的概率向量和已知协议模型的具体属性的概率向量。

K-L 散度描述安全事件所需的额外信息量,K-L 散度越小,指纹匹配度越高。比较好的判定方法是指定一个阈值,只要 K-L 散度的平均值低于该阈值就被认为是匹配。如果没有已知的协议模型,事件被列为“未知”,以避免误报。在正确识别事件的协议类型后,规则触发器通过比较规则库协议模型和事件模型来完成规则的匹配,并给出最

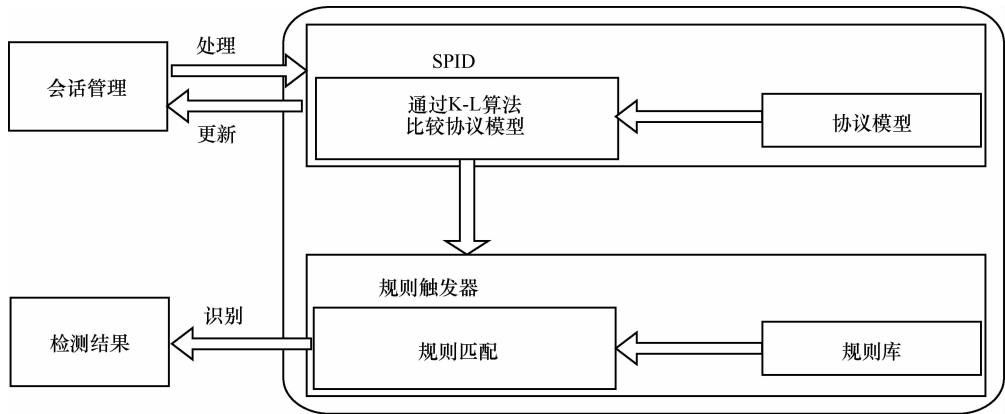


图 4 网络行为检测引擎结构



终的检测结果。

3.4 态势评估

态势评估是对安全性的定量分析,评估结果将为下一步预测算法做支撑。尽管已有一些成熟的评估算法,但大部分仍存在缺陷。本节提出了一种新的态势评估算法,从不同的角度评估安全态势。

在数据采集模块中,使用了多个检测子模块来全方位监控网络,包括恶意软件检测、入侵检测、防火墙、隔离装置、安全设备和监控设备等。在态势评估模块中,因为内部网络拓扑和主机间都存在差异,必须对不同的网络进行区分。首先,设置一个时间阈值,并整合具有相同会话协议和攻击类型的安全事件。之后,评估子模块生成一个四维向量为:

$$V(t)=(count,atkType,time,P_{severity}^{atkType}) \quad (3)$$

其中, $count$ 代表攻击事件的统计数量, $atkType$ 表示一个具体的攻击类型, $time$ 表示检测到攻击的时间戳, $P_{severity}^{atkType}$ 表示攻击的严重程度,严重程度可参考安全专家根据经验制定的标准。最后,当前安全态势值 S 可以通过式(4)计算出来:

$$S = \sum_i^M 10^{P_{severity}^i} \times count \quad (4)$$

其中, M 代表攻击类型的数量,所有的 S 值存储在安全态势数据库中,历史态势的评估值可以为安全态势预测提供依据。

4 方案实现

4.1 软件实现

根据上面提出的态势感知框架,设计了适用于智能变电站的网络态势感知装置。其系统采用多层软件体系结构,包括数据采集层、数据预处理层、态势分析层以及从底部到顶部的可视化层。每一层负责其自身功能并通过消息总线实现与其他层的合作。层级之间的合作形成了一个完整的态势感知系统,它的体系结构如图5所示。

在数据采集层中,部署了各类信息采集设备和传感器,如入侵检测系统、网络隔离装置、安全设备以及监控设备,收集整个变电站的安全信息。因此,需要统一的数据采集框架控制这些监测行为并整合监测数据。

收集日志和事件数据后,可以采取一些方法,如数据简化、数据集成、数据(事件)过滤等,进行数据的简化融合,简化目标是合并多个传感器检测到的相同攻击的冗余警报事件。以端口分组扫描为例,入侵检测系统运行端口扫描时会

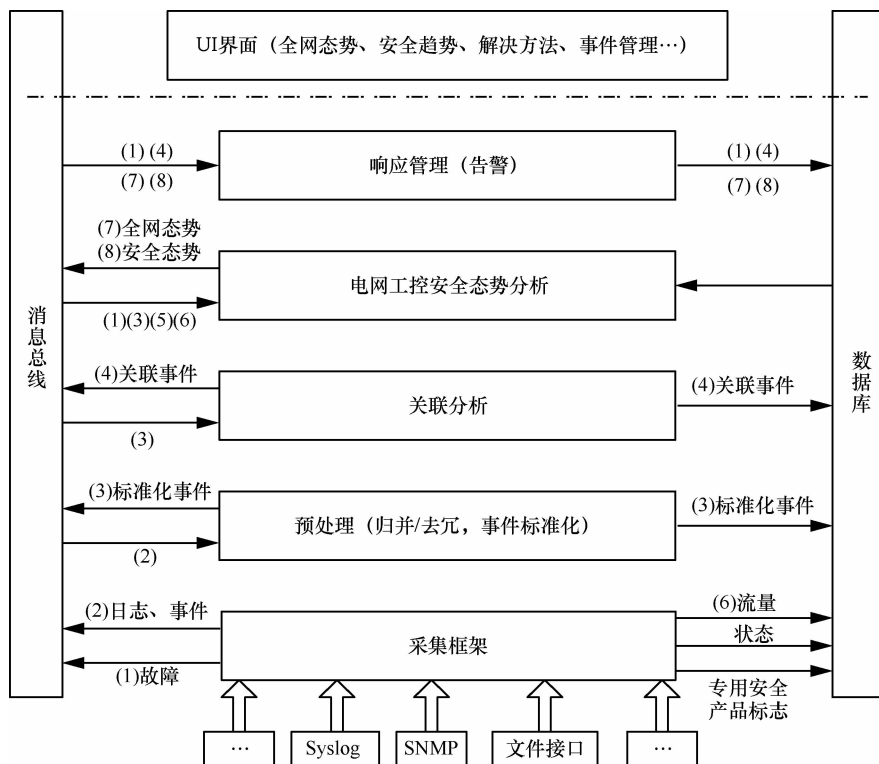


图5 软件结构

产生安全事件。连续的端口扫描操作将产生大量的事件,这些事件不仅具有相同的事件类型,也有相同的源端口和目的端口。数据简化操作会明显减少事件的数量,节省处理资源。事件过滤的目的是消除不满足约束要求的事件,约束要求定义了一组安全事件,并以规则或属性的方式将其保存在安全知识库中。如果某些事件缺乏关键属性或者数值不在所需范围内,不能提供有用的信息以供分析、评估和预测安全态势,那么这些事件就会被删除。通过简化和过滤处理,重复的安全事件被合并,安全事件的数量大大降低,抽象度得到提高,同时隐含的安全态势信息被保留。

在安全态势分析阶段,需要从内置安全事件知识库中获取有用信息,并进行事件关联分析确定已知事件和发生事件的相关性。由于来自不同类型安全设备及传感器的安全事件复杂多样,因此,几乎不可能由人工完成识别安全事件之间的联系并分析当前安全态势。根据这些特点,采用数据挖掘的方法来发掘安全事件之间的潜在关系,并最终构建了网络安全态势图,步骤如下:安全事件的简化和过滤;通过数据挖掘算法获取安全态势评估有效信息;获得安全态势评估规则。为了更好地分析解释评估结果,引入了安全领域专家的知识经验,并将新获得的关联规则扩展到知识库,以便今后处理这样的攻击;评估安全态势并获得最终的评估结果。

智能变电站网络安全态势包括网络安全事件相关性分析、网络安全态势图的构建、整体安全态势的评估。系统根据新的安全事件关联关系及安全态势评估结果定期更新网络安全态势图。具体事件信息处理结束后,会把事件增加到事件知识库。系统运用关联规则和数据挖掘算法进行事件关联分析,进一步感知安全态势。如果分析结果识别到发生的具体事件,即可根据系统设置刷新现有的安全事件态势图,并通知系统管理员发生了网络攻击事件。

4.2 硬件实现

将变电站对专用设备及网络处理的高性能需求考虑在内,对软件体系结构进行了硬件设计。该装置采用了总线结构、模块化设计技术、Intel 的 Sandy Bridge,提高了网络运行和计算性能。平台包括 6 个模块:CPU 模块、北桥芯片组模块、看门狗模块、电源模块、本地局域网(LAN)模块及周边接口。CPU 模块使用了最新的英特尔酷睿处理器技术,可提供自动数据关联、OS 监控和安全密钥,以有效保证网络的安全性和提高系统功能的可靠性。为了支持

连续运行,设计了双冗余结构电源模块、过电压保护和过电流保护,有效地保证了装置的高可靠性和可用性。

5 结束语

由于 IEC61850 标准的应用,智能变电站设备之间实现了无缝互操作;同时,面向传输协议的网络攻击方法层出不穷,智能变电站的网络安全形势日趋严峻,网络安全一直是智能变电站稳定运行的关键基础。本文对智能变电站网络安全态势感知技术进行了研究,并给出了态势感知框架模型及其软硬件实现,为智能电网网络安全态势感知技术的综合应用提供了一个很好的参考依据。

参考文献:

- [1] MACKIEWICZ R E. Overview of IEC61850 and benefits[C]// IEEE Power Systems Conference and Exposition, October 29-November 1, 2006, Atlanta, GA, USA. New Jersey: IEEE Press, 2006: 623-630.
- [2] SLAY J, MILLER M. Lessons learned from the maroochy water breach[J]. IFIP Springer Boston, 2007(253): 73-82.
- [3] 文继锋,盛海华,周强,等. 智能变电站继电保护在线监测系统设计与应用[J]. 江苏电机工程, 2015, 34(1): 21-24.
WEN J F, SHENG H H, ZHOU Q, et al. Design and application of relay protection on-line monitoring system in the intelligent substation [J]. Jiangsu Electrical Engineering, 2015, 34(1): 21-24.
- [4] ENDSLEY M. Toward a theory of situation awareness in dynamic systems[J]. Journal of the Human Factors, 2005, 37(1): 32-64.
- [5] 赖积保,王颖,王慧强,等. 基于多源异构传感器的网络安全态势感知系统结构研究 [J]. 计算机科学, 2011, 38(3): 144-149.
LAI J B, WANG Y, WANG H Q, et al. Research on network security situation awareness system architecture based on multi-source heterogeneous sensors[J]. Computer Science, 2011, 38(3): 144-149.
- [6] 汤永利,李伟杰,于金霞,等. 基于改进 D-S 证据理论的网络安全态势评估方法 [J]. 南京理工大学学报, 2015, 39(4): 405-411.
TANG Y L, LI W J, YU J X, et al. Network security situational assessment method based on improved D-S evidence theory[J]. Journal of Nanjing University of Science and Technology, 2015, 39(4): 405-411.
- [7] 沈富宝,王中秋. 苏州首座 220kV 智能变电站分析 [J]. 江苏电机工程, 2015, 34(2): 45-48.



SHEN F B, WANG Z Q. The insulating oil purifying technology applied in online monitoring [J]. Jiangsu Electrical Engineering, 2015, 34(2): 45-48.

- [8] HJELMVIK E. The spid algorithm-statistical protocol identification [R/OL]. [2013-04-23]. <http://www.iis.se/docs/TheSPIDAlgorithm-StatisticalProtocolIdentification.pdf>.

[作者简介]



郭静(1985-),女,国网江苏省电力公司电力科学研究院工程师,主要研究方向为网络信息安全。



黄伟(1987-),男,国网江苏省电力公司电力科学研究院副高级工程师,主要研究方向为工控系统信息安全。



郭雅娟(1980-),女,国网江苏省电力公司电力科学研究院高级工程师,主要研究方向为信息系统安全防护技术。



周超(1975-),男,国网江苏省电力公司电力科学研究院高级工程师,主要研究方向为信息系统安全防护技术。



陈昊(1980-),女,国网江苏省电力公司电力科学研究院副高级工程师,主要研究方向为信息系统安全防护技术。