电力物联网终端网络安全监测技术的研究

郑志明
（新疆特变电工楼兰新能源有限公司 新疆 巴音郭楞蒙古自治州 841899）

摘 要 随着电力物联网的快速发展和普及，电力系统的信息化水平不断提升，但这也带来了一系列网络安全威胁和风险。电力物联网终端网络作为电力系统的重要组成部分，直接面对着各种网络攻击和安全漏洞的威胁。因此，加强对电力物联网终端网络的安全监测和保护成为保障电力系统安全运行的关键。文中以发展电力物联网终端网络安全监测技术的意义为基础，分析了电力物联网终端网络安全监测技术的整体架构以及电力物联网四维架构的搭建思路，并列举了几种电力物联网终端网络安全监测技术，最后阐述了终端网络安全监测的落实策略。

关键词： 物联网终端；网络安全；监测技术
中图分类号 TN915.08

Research on Network Security Monitoring Technology of Power Internet of Things Terminal

ZHENG Zhiming
（Xinjiang TBEa Loulan New Energy Co.,Ltd.,Bayingoleng Mongolian Autonomous Prefecture,Xinjiang 841899,China）

Abstract With the rapid development and popularization of the power Internet of Things,the informatization level of the power system continues to improve,which also brings a series of cyber security threats and risks. As an important part of the power system,the power Internet of Things end point network is directly facing the threat of various network attacks and security bugs. Therefore,strengthening the security monitoring and protection of the power Internet of Things end point network has become the key to ensuring the safe operation of the power system. This paper analyzes the significance of developing the end point cyber security monitoring technology of the power Internet of Things,clarifies the overall architecture of the power Internet of Things end point cyber security monitoring technology and the construction idea of the four-dimensional architecture of the power Internet of Things, and lists several power Internet of Things end point cyber security monitoring technologies. Finally, the implementation strategy of end point cyber security monitoring is expounded.

Key words Internet of Things terminal,Network security,Monitoring technology

0 引言

基于终端网络的安全监测方案能有效提升电力物联网终端网络的安全性和可靠性。该方案能及时发现和防范网络攻击、异常行为和漏洞，减少潜在的安全风险和威胁，其还具有较好的可扩展性和适应性，能满足不同规模的电力物联网终端网络的安全监测要求。因此，研究电力物联网终端网络安全监测技术，对提高电力系统的安全性和稳定性具有重要意义。通过有效的安全监测手段和方法，可以及时发现并应对网络攻击和安全威胁，保障电力物联网终端网络的安全运行。

1 发展电力物联网终端网络安全监测技术的重要意义

电力物联网终端网络作为电力系统的重要组成部分，承担着电力数据传输、控制、监测等关键任务。对电力物联网终端网络进行安全监测，可以及时发现和应对网络攻击、恶意操作和安全漏洞，保障电力系统的安全运行。电力物联网终端网络面临着各种网络威胁和风险，如黑客攻击、病毒感染、数据泄露等。安全监测技术可以帮助网络识别和防范这些威胁，减少潜在的损失和影响。电力物联网终端网络的安全性直接关系着电力系统的可靠性和稳定性。通过采用有效的安全监测技术，可以及时检测和修复网络故障、异常行为和漏洞，提高电力系统的抗干扰能力和稳定性。电力物联网终端网络涉及大量用户的能源使用数据和个人信息。安全监测技术可以有效保护用户隐私和数据安全，防止数据被泄露或滥用。此外，电力物联网终端网络是电力系统智能化和数字化转型的重要基础。应用安全监测技术，可以为电力系统提供可靠的网络基础设施，推动电力系统的智能化、自动化发展[1]。

作者简介：郑志明（1984—），本科，研究方向为电力、热能动力。

2 电力物联网终端网络安全监测技术的整体架构

电力物联网终端网络安全监测技术的整体架构可以分为感知层、网络层、平台层和应用层，如图1所示。

图1 技术整体架构

(1)感知层：电力物联网终端设备和传感器层，负责采集电力系统中的数据和信息。在安全监测方面，感知层可以通过安全传感器和监测设备来实时感知网络流量、设备状态和异常行为。例如，使用入侵检测系统、网络流量监测器等收集和分析网络数据流，以发现潜在的安全威胁。

(2)网络层：电力物联网终端网络的通信和传输层，包括网络设备和通信协议。在安全监测方面，网络层可以应用安全防火墙、入侵检测系统、虚拟专用网络(VPN)等技术来保护终端网络的通信安全。此外，网络层还可以通过网络隔离、访问控制列表(ACL)等措施来限制对终端网络的非法访问。

(3)平台层：电力物联网终端网络的管理和控制平台，负责对网络进行监测、配置和管理。在安全监测方面，平台层可以通过集中管理和控制网络设备、应用安全策略和访问权限机制来保证终端网络的安全性。例如，使用统一的安全管理平台对网络设备进行统一配置和监测，并实施安全策略和访问控制。

(4)应用层：包含基于电力物联网终端网络的各种应用和服务，如能源管理、智能电网等。在安全监测方面，应用层可以使用安全事件管理系统、漏洞扫描和补丁管理系统等来监测和响应网络安全事件。此外，应用层还可以通过用户身份认证、数据加密、安全日志管理和分析等来保护用户的隐私和数据安全。

电力物联网终端网络安全监测技术的整体架构分为感知层、网络层、平台层和应用层，可通过采集、传输、管理和应用多个层面的安全措施来确保电力物联网终端网络的安全性。这种架构能提供综合性的安全保护，保障电力系统的运行安全和数据安全。

3 电力物联网四维架构的搭建

电力物联网的四维架构包括主体、客体、行为和环境。

(1)主体指电力物联网中的各种参与者，如电力设备、传感器、终端用户等。主体通过感知、控制、交互等与物联网系统进行连接和通信。在安全监测方面，主体的安全性非常重要，包括设备的身份认证、权限管理、数据保护等。

(2)客体是指电力物联网中需要监测和保护的目标或资源，如电力设备、数据、网络等。客体需要进行实时监测和评估，以发现潜在的安全风险和威胁。在安全监测方面，客体的安全性包括对设备和数据的保护、漏洞的修复和异常行为的检测等。

(3)行为是指主体在电力物联网中的活动和操作，包括设备的控制、数据的传输和交互等。行为需要被实时监测和分析，以便发现异常行为和恶意操作。在安全监测方面，行为的安全性包括对行为的合规性检查、对攻击行为的识别和防范等。

(4)环境是指电力物联网运行的物理和网络环境，包括网络拓扑、通信协议、网络连接等[2]。环境也需要被实时监测和防护，以保证电力物联网的安全性。在安全监测方面，环境的安全性包括网络的安全配置、通信的加密、防火墙的设置等。

通过搭建电力物联网四维架构，可以实现对整个系统的全面监测和保护。通过对主体、客体、行为和环境的安全性进行监测和管理，可以及时发现和应对潜在的安全威胁和风险，确保电力物联网的运行安全和数据安全。这种架构可以提供多层次、全方位的安全保障，为电力系统的可靠性和稳定性提供支持。

4 电力物联网终端网络安全监测技术

4.1 以网络流秩序为基础的监测技术

网络流量监测技术是电力物联网终端网络安全监测的重要保障，以网络流秩序为基础的监测技术就是其中的一种。这种技术主要基于对网络流量的实时监测和分析，以检测和预防网络攻击、异常行为、安全漏洞等威胁。其流程如图2所示。

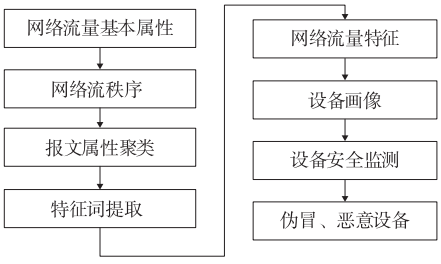

图2 基于网络秩序的监测技术

通过对网络流量数据的分析，可以了解网络中的通信模式、数据量、频率等特征。流量分析可以发现不正常的流量模式，如异常的数据传输量、频繁的连接尝试等，从而及时识别可能的安全威胁。通过分析网络流量中的行为，可以检测和识别异常的行为模式，如大规模的扫描活动、未经授权的访问、异常的数据传输等。行为分析技术可以通过构建行为模型和规则引擎来识别可能的攻击行为，并触发相应的警报或防御措施。此外，通过建立正常网络流量的基准模型，可以检测出与正常行为明显不同的异常流量。异常检测技术可以利用统计分析、机器学习、人工智能等方法，自动识别和分析异常流量，并及时发出警报或采取相应的防御措施。漏洞扫描技术

可通过扫描网络中的设备和应用程序，发现潜在的安全漏洞，主动探测网络设备的弱点和漏洞，并提供修复建议和补丁更新，以降低攻击者利用这些漏洞进行入侵和攻击的可能。

通过应用以上技术，以网络流秩序为基础的监测技术可以实现对电力物联网终端网络的实时监测和防护[3]。它能帮助识别和预防各种网络攻击、异常行为和安全漏洞，提高电力系统的安全性和可靠性。同时，该技术还具有较好的可扩展性和适应性，能满足不同规模和需求的电力物联网终端网络的安全监测要求。

4.2 以协议解析为基础的异常分析技术

以协议解析为基础的异常分析技术可通过对网络通信协议的深入解析和分析，识别出协议层面的异常行为和潜在的安全威胁。具体而言，以协议解析为基础的异常分析技术可以采取以下几种方法。

（1）协议解析。通过对网络通信中的各种协议进行解析，如网络层、传输层和应用层的协议，获取协议中的各个字段、标志位和消息格式。协议解析可以帮助理解网络通信的结构和规则，为后续的异常分析提供基础。

（2）异常行为检测。在协议解析的基础上，通过定义正常行为的规则和模型，实时监测和分析网络流量，以检测出不符合协议规范的异常行为。例如，在检测到协议字段的异常值、错误的协议操作序列或频率时，就表明可能存在安全威胁[4]。

（3）恶意代码检测。利用协议解析技术，可以检测到可能携带恶意代码的网络流量。通过对协议消息内容和结构的分析，识别出潜在的恶意代码或危险载荷，并及时采取相应的防御措施。

（4）漏洞利用检测。基于对协议解析的理解，可以发现协议的漏洞和弱点。通过监测网络流量中针对这些漏洞的利用行为，可以及时发现攻击者的入侵行为，并采取相应的防护措施。

（5）协议异常分析。当网络流量中出现异常或违反协议规范的情况时，可以通过深入分析异常的协议行为，确定异常的原因和影响。这种分析可以用于进一步调查和应对潜在的安全事件。

以协议解析为基础的异常分析技术能深入理解和分析网络通信协议，从协议层面上发现潜在的安全威胁和异常行为。它可以提供更具细粒度的安全监测和分析，增强电力物联网终端网络的安全性和防护能力。

4.3 以设备画像为基础的网络监测技术

以设备画像为基础的网络监测技术是电力物联网终端网络安全监测中的重要技术。其具体流程如图3所示。

该技术通过对网络中的设备进行特征分析和建模，实现对设备的实时监测、识别和分类，通过分析设备中的网络流量，识别出各种类型的设备，包括设备的型号、厂商、操作系统、固件版本等。设备识别有助于建立设备库，为后续的设备画像和异常监测提供基础。通过对设备的流量、行为、配置等进行特征提取，可建立设备特征模型。这些特征可以包括设备的端口使用情况、网络通信模式、常用协议和服务、异常行为等。设备特征提取有助于了解设备的正常行为和特点，以便发现异常行为和安全风险。接着，基于设备特征，建立设备的画像模型，描述设备的基本属性和行为特征。设备画像可以包括设备的硬件和软件配置、网络拓扑位置、通信模式和权限等[5]。建立设备画像有助于更全面地了解设备的特征和行为，以便进行异常监测和安全分析。通过对流量和行为的实时监测和分析，有助于检测设备的异常行为和潜在的安全威胁。设备行为分析可以基于设备画像模型，识别出与设备正常行为不符的异常行为，如异常的数据传输、非法的访问或恶意操作。最后，利用设备画像和漏洞数据库，可对设备的漏洞和安全弱点进行管理和修复。通过定期扫描设备，可发现存在的漏洞，并提供相应的补丁更新和安全建议，以减少潜在的攻击面。

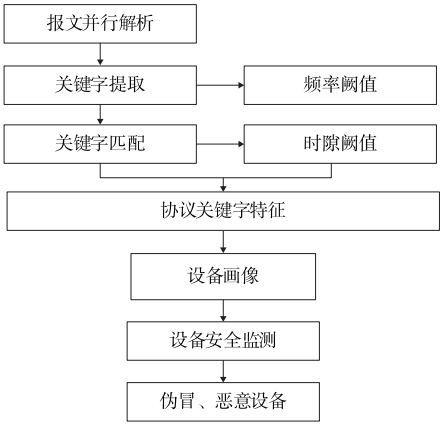

图3 基于设备画象的电力物联网业务异常分析的具体流程

5 结语

电力物联网终端网络安全监测技术是保障电力物联网系统安全运行的关键。随着电力物联网的快速发展，终端网络的安全性受到了越来越多的重视。未来的研究应注重进一步提高监测技术的准确性和效率，加强其对新型攻击和威胁的监测能力，同时注重隐私保护和数据安全。此外，跨部门合作和信息共享也是提高电力物联网终端网络安全监测能力的重要方向。

参考文献

[1] 宋采燕.移动物联网智能信息终端网络安全技术的应用分析[J].电子技术与软件工程，2022(10)：26-29.

[2] 姜帆，孙国齐，杜金宝，等.基于EDR技术与机器学习的电力物联网终端安全防护系统[J].网络安全技术与应用，2021(1)：126-128.

[3] 陈涛.电力物联网安全防护研究实践[J].网络安全技术与应用，2020(12)：132-133.

[4] 王传君，缪巍巍，曾锃，等.基于2FA的电力物联网终端安全升级方案研究[J].电力信息与通信技术，2022(8)：76-82.

[5] 卢琼，崔文超.泛在电力物联网终端层安全监测分析技术研究[J].信息技术，2020(2)：121-125，134.