面向智能电力系统安全的网络攻击监测技术研究

付发云¹ 付宇轩²

1 国网湖南超高压变电公司, 湖南 长沙 410004; 2 三峡大学电气与新能源学院, 湖北 宜昌 443002

摘要: 现代信息技术与通信技术的迅猛发展彻底转变了人们的日常生产生活方式, 前沿科技在我国电力系统领域的融入, 也让新一代的电力系统信息领域与物理领域加速融合。但在维护电力系统安全运行的背景下, 网络攻击已然成为了其中最关键的不稳定性因素。因此, 如何能够加强对于网络攻击的检测, 也成为了保障电力系统运行安全的第一道屏障。本篇文章主要是分析了电力系统的网络攻击类型, 并且就电力系统的网络攻击检测技术进行了探究, 希望能够为确保智能电力系统的运行安全性提供参考意见。

关键词: 智能电力系统; 网络攻击; 检测技术

Research on Network Attack Monitoring Technology for Smart Power System Security

Fu,Fayun¹ Fu,Yuxuan²

1 State Grid Hunan Extra High Voltage Substation Company, Changsha, Hunan, 410004, China

2 College of Electrical Engineering and New Energy, Yichang, Hubei, 443002, China

Abstract: The rapid development of modern information technology and communication technology has completely changed people's daily production and life style. The integration of cutting-edge technology in China's power system field has also accelerated the integration of the new generation of power system information field and physics field. However, under the background of maintaining the safe operation of power system, network attack has become the most critical unstable factor. Therefore, how to strengthen the detection of network attacks has become the first barrier to ensure the safety of power system operation. This paper mainly analyzes the types of network attacks in power system, and probes into the detection technology of network attacks in power system, hoping to provide reference opinions for ensuring the operation safety of intelligent power system.

Keywords: Intelligent power system; Cyber attack; Detection technique

DOI: 10.62639/sspis11.20240104

在智能技术的核心作用下, 新型电力系统框架的构建实现了信息端与物理端之间的高度耦合, 更成为了我国能源智能战略落地的关键。智能电力系统在运行的过程中包含了多种类的智能终端, 其中一些新能源的占比也在不断地提升, 推动了我国电能系统逐步朝着更加绿色化、环保化与智能化的方向发展^[1]。但同时, 在智能系统构建的模式下, 也面临着诸多的网络安全攻击与挑战问题。比如, 大量智能终端在系统中的接入虽然提升了系统一体化智能控制的水平, 但也为网络攻击提供了更多的渠道与接入点。再比如, 分布式电源在供应过程中本身就存在着随机性较强、间歇性等特征, 而网络攻击的融入也使其故障发生的波动更大。除此之外, 随着信息端与物理端之间的融合程度不断地加深, 跨区域范围内的网络攻击也为网络攻击风险传递搭建了新的桥梁。这些问题不仅成为了威胁系统运行安全的关键, 更为系统的检测行业带来了巨大的挑战。

一、智能电力系统的特征

第一, 现如今的电力系统构建规模更加的庞大, 其终端端口数量更多、分布范围更广。尤其是考虑到新能源发电在系统中的融入, 分布式的

构建模式也让这些智能终端的大规模接入, 也意味着在全域范围内的分布式接入口不断地增多, 逐步构建成了一个相对复杂的巨大系统模式。第二, 目前的电力系统中, 高新技术的融入让控制端口与信息传递流的交互更加的密切, 这也意味着后台控制中心可遭受的风险来源更广。这种互联互通的模式, 虽然能够让控制信息的下达和传递更加的高效, 但同时也让后台控制中心面临着新的攻击性风险和病毒传递问题。因此, 在实体端的物理领域与信息领域之间达成更高频的互动模式背景下, 只有数据信息与指令的稳定传输和下达, 才能让系统的运行更加的安全和稳定^[2]。第三, 智能电力系统构建了集合多种智慧技术参与的能源体系。多种智能技术在智能电力系统中的融入和应用, 让系统在运作过程中的复杂性更强。目前, 智能电力系统在运转过程中可利用大数据技术、人工智能技术、移动交互技术, 实现了对于能源传递全生命周期的动态化监测, 同时还达到了数据信息共享、优化控制的目标。

二、智能电力系统遭到的网络攻击与威胁

(一) 大量智能终端接入带来的网络威胁
新型的智能电力系统中, 随着大量的新能源

(稿件编号: IS-24-4-1012)

作者简介: 付发云 (1972-08), 性别: 男, 民族: 汉, 学历: 本科, 职称: 副高, 研究方向: 电气工程。

付宇轩 (1999-02), 性别: 男, 民族: 汉, 学历: 研究生, 研究方向: 电气工程。

终端接入, 智能终端模式下的物理册与信息册之间深度的耦合。虽然, 这样的管理模式, 能够让电力系统的控制更加的高效与稳定, 但只能技术与电网系统的衔接也意味着信息传输在电网中与后台控制中心的交互更频繁, 而应用与指令层之间在这样的交互模式下, 更从另一个层面让后台控制中心面临着病毒入侵、恶性网络行为、应用入侵等多方面的风险。比如, 随着新能源、分布式站厂数量的不断扩张, 一些并无得到控制的智能终端也纳入了新型的电力系统中, 但考虑到这些非受控的智能终端数据信息的核算能力有限, 对于一些风险性的数据未必能够识别, 这样的情况也为网络攻击留下了可乘之机。比如, 2014年, 网络安全的相关研究人员就破解了西班牙某电力公司在智能电表应用中的一种加密算法, 其通过系统中衔接的智能终端作为攻击端口, 能够对智能终端衔接的跳板以及相邻的智能终端产生攻击。

(二) 信息流与功率流频繁交互带来的风险问题

信息流与功率流之间的交互, 也为网络层面的入侵与攻击提供了新的渠道。在信息册与物理册之间相互交融的情况下, 控制业务在全域范围内广泛地展开, 这也意味着, 信息接口中的网络风险极易通过与功率端之间的相互衔接, 实现跨区域的风险传递, 从而造成大面积的停电事故。举一个典型的例子, 在2015年, 乌克兰就出现了大面积的停电事故^[3]。最终, 究其原因, 发现是黑客通过入侵网络层的信息域主控电脑, 在通过将病毒向物理领域进一步的传递, 而造成了恶意跳闸的现象, 此次的大面积断电为乌克兰的经济带来了巨大的影响。不仅如此, 除了从信息端向物理端扩散攻击行为之外, 从物理端入侵的攻击行为也可以反向渗透到信息端。尤其是在信息端与物理端之间交互更加频繁的背景下, 双端之间的攻击入侵风险传递的概率更高。

(三) 应用层与外界之间的互联互通带来的入侵风险

目前, 在智能化的电力系统中, 应用层主要包含了大数据信息应用、云计算方法以及移动互联网, 而应用层的搭建则为其提供了技术应用的平台, 让电力系统的业务变得更加高效与灵活。但同时, 基于网络平台下的业务系统模式, 也存在着开放性较强的特征, 网络层面的暴露, 也为许多攻击者留下了可乘之机。以人们在日常生活中常见的空调调控程序为例, 空调调控程序也需要依靠电力启动, 而不法分子则可以通过分布式的衔接终端, 利用安全切口入侵到上一级的控制平台, 这种多切口入侵的模式, 最终会导致控制平台控制失效或发出错误指令, 从而引发空调反复启停的问题。不仅如此, 在现代信息技术以及通信技术迅猛发展的时代背景下, 前沿科技在智能电力系统中的融入, 也更容易让其接口的操作终端成为不法分子的可乘之机。如2021年, 就有不法分子利用电力付费平台作为切口, 入侵了

美国科罗拉多州电力系统的控制层, 最终导致控制层发出错误指令, 出现大面积电力瘫痪的问题, 甚至还从中盗取了相应的机密电力历史数据。

三、面向智能电力系统安全的网络攻击监测技术

(一) 物理衔接终端的攻击行为监测技术

智能终端设备是与电力系统物理层之间相互衔接的重要组成部分, 其承担着数据信息实时传输、信号精准遥控等多方面的功能与价值。而随着我国能源互联网络结构的扩张与构建, 各类型的智能终端设备也融入了系统内, 在为信息传递提供高效交流平台的背景下, 也为网络系统的安全带来了巨大的冲击。比如, 由于智能终端设备衔接数量庞大, 让加密保护措施的效用不断降低, 其广域范围内的分布也难以实现统一性的安全防护^[4]。再比如, 智能终端的设备类型众多, 而这种能异构的方式也不乏存在网络攻击的漏洞, 为不法分子提供了更多的入侵可能性。

首先, 针对终端的非法接入问题, 可以采用前馈人工神经网络技术, 针对与其衔接的非法链接或数据攻击进行检测。这种检测方式的检测精确性十分优越。其次, 虽然绝大多数的智能终端都处在电力内网, 与电力外网之间存在着一定的物理隔离。但是部分的运维终端在管理的过程中依然需要通过远程操作进行控制, 这种由于远程操作控制引发的非法入侵、病毒入侵行为就可利用深度置信网络的改造和升级, 实现对于电力系统外部攻击的动态化监测。深度置信网络的改造, 可对非法的外联攻击, 迅速地识别, 当端口遭受了本地的非法入侵以及由于远程控制引发的外部非法入侵之后, 就可以在第一时间准确定位并检测, 避免远程终端入口, 直接对智能终端进行控制。最后, 针对时间同步攻击的防范。考虑到大多数电力网络中的智能终端设备接收到的时间信号, 来源于全球定位系统, 但考虑到在系统或卫星中设计的一些加密密码时间同步报文容易被攻击者获取, 甚至还有很多不法分子可以对该数据进行伪造, 从而导致了终端设备在时间上出现报错的情况。基于此, 可采用超平面聚类的时间同步攻击监测模式, 将聚类相位算法引入到测算攻击点的监控中, 通过对不同时间节点下的电抗值与实际差值之间相互比较, 判断被攻击区域的所在位置。这种相位差的计算方式对时间同步攻击的检测精确性更高, 但对于普通数据和攻击数据的区分能力相对较为薄弱。因此, 也可选择采用三相不平衡系统检测时间同步攻击问题, 三相不平衡模型解决了时间同步攻击在检测过程中对于正常数据和攻击数据区分能力薄弱的问题。

(二) 配网段非法无限入侵的网络攻击检测

随着5G通信技术的不断成熟, 我国绝大多数的物联网络技术开始与不同的电力控制终端之间相互衔接, 这也让无线通信成为了传递指令信号、实现数据收集最关键的沟通桥梁。当前, 我国的智能电力框架内, 配网终端多利用无线沟通

的专用内网,从而实现数据信息的精准传递和安全生产保护。但这样的结构框架显然为病毒入侵和黑客攻击提供了新的终端渠道。尤其是考虑到控制系统在不同终端的接入,从空间布局上来看,分布式布局的模式意味着指令传输的时间与空间分布具有密不可分的内在关联。在这样的规律下,采用密度聚类方式就可辨别终端与通信基站之间的真伪信号以及信号强度,从而快速地定位,虚假的攻击坐标^[5]。除此之外,采用双隐马尔可夫模型也能够针对无线终端的一些恶意攻击行为快速地识别。双隐马尔可夫模型可以解决入侵检测系统中一些高难度的数据计算问题。尤其是考虑到在一些多维的智能终端中,很多电力终端的计算资源和计算力是十分有限的,在这种情况下选择高维度数据处理能力的计算模型,更有利于快速查询并规避风险问题。

(三) 窃电攻击的网络入侵监测技术

窃电攻击是导致电网在运行过程中出现经济损失最关键的要素之一。过去传统的窃电攻击模式主要是利用电路绕行、手动电表篡改数据等方式,完成偷电、改切电路的目的。而在智能电表普及的背景下,窃电攻击的模式也在不断地更新,窃电攻击的方式发生了翻天覆地的变化。过去,针对早期窃电行为的检测技术普遍存在着检测结果精确度不足、经验依赖性较高等多方面的缺陷。而在智能电表普及的背景下,确定攻击行为的检测技术也开始朝着更加高精度的方向发展。比如,可利用宽度卷积神经网络以及深度卷积神经网络,分别针对电力线路的长期数据以及近期数据进行多维分析。通过双重分析可利用宽度分量以及深度分量的优势,快速地排查一些窃电行为。再比如,可利用长短期记忆网络以及多层感知神经网络相互混合的神经网络窃电测量模型,转变过去依靠经验针对窃电行为进行探测的约束,只需要通过针对一些历史的窃电数据进行分析,就可以构建精确度更高的训练模型,从而实现对于窃电攻击行为的排查。

(四) 网络层流量攻击行为的检测技术

在整个系统运作受到干扰因素的影响下,流量传输也会存在延时、信号波动强等问题,而造成系统内部数据信息传递延时的现象。尤其是随着目前电力系统内部的通信流量规模持续地扩大,信号传输的模式更加多样,但传统的异常问题监测方法也确实面临着异常区域范围定位不精、响应速度较慢等问题,无法跟随智能电网的发展实时检测网络攻击问题并对其进行精准定位。针对这样的问题,可采用以下检测技术方式实现对于网络层流量攻击行为的检测。神经网络检测方式。神经网络可以模拟学习思维,具有较强的学习能力,经常被应用于电力工控系统的网络流量监测。而利用神经网络,可以通过对DDOS攻击模式的攻击行为进行识别和学习,提升检测效率。神经网络的检测方式还可应用于一些流量异常的问题,还可通过深度学习了解攻击原理并判断攻击类型,但是,当网络层遭受一些

未知的攻击模式时,这种神经网络的检测方式也会出现不足。

(五) 应用层通信协议攻击行为的检测

基于应用层通信协议的异常流量检测模式,能够实现对于异常报文的深度监测。但是,这类检测方式在应用过程中,对于前期数据基础的完整性、真实性和精确性要求极为严格。在早期阶段,许多研究人员选择采用人工解析的方式提取报文中不同字段之间的耦合关系,通过针对一些通用的异常事件进行采样处理,可精准地找到其中的异常报文。但是人工协议检测的方法对于人才的专业性素质要求极为严格,且对于提取字段耦合关系也具有一定的规范。在这种情况下,就可以利用监督学习功能的人工智能方式,针对协议字段的关系,快速的提取,进而判断电力系统是否存在异常报文的网络攻击行为。但是,这种检测方式必须具备完整的训练数据集。但考虑到正常的样本,以及遭受攻击的异常样本之间本身就存在不平衡的情况,因此,研究人员又通过引入贝叶斯近似滤波器的方式,避免了由于故障样本与正常样本差异引发的监督问题,从而快速找到攻击的具体位置。

四、结语

综上所述,智能电力网络的构建模式下由于网络端与物理端之间的协同交互,让网络攻击行为变得更加多元,网络攻击的渠道也更加广泛。而不同类型的网络攻击引发的停电、窃电等问题,更是影响电力网络稳定运行的关键。因此,更应当针对不同类型的网络攻击,选择采用合适的人工智能算法以及技术方式,精准地定位攻击位置和攻击行为,从而更好地应对新时期智能电力网络复杂工作场景下的网络攻击问题。

参考文献:

- [1] 刘渊峰. 电力系统视频监控网络安全接入协议研究 [D]. 西安电子科技大学, 2019.
- [2] 李一诺, 刘玮, 魏兴慎, 王琦. 网络攻击场景下含分布式光伏配电网的脆弱性研究 [J]. 综合智慧能源, 2024, 46 (05): 50-57.
- [3] 汤超. 浅析电力监控系统网络安全监视体系建设 [J]. 机电信息, 2020, (32): 142-143.
- [4] 刘权琦. 电力信息物理融合系统中的网络攻击 [J]. 集成电路应用, 2020, 37 (11): 162-163.
- [5] 丁琳. 电力系统网络中 UDP 端口的攻击与防护 [J]. 网络安全技术与应用, 2020, (10): 48-49.