主动防御技术提升电力监控系统稳定性研究

施晓亮 张磊

新疆华电苇湖梁新能源有限公司，新疆省乌鲁木齐市，830000；

摘要：电力监控系统在现代电网的运作中扮演着至关重要的角色，但随着信息化和智能化的普及，系统的安全性面临着前所未有的挑战。外部攻击和内部威胁不断增加，令电力监控系统的稳定性和安全性受到了严重威胁。为了应对这些挑战，主动防御技术逐渐成为提升电力监控系统稳定性的关键工具。通过风险识别、动态优化策略及快速响应机制，主动防御技术能够有效提升系统的安全性与稳定性，避免潜在威胁的蔓延和对电力网络正常运行的破坏。这项技术的研究不仅提供了有效的防护解决方案，还为电力系统的智能化发展提供了新的视角和动力。

关键词：电力监控系统；主动防御技术；安全性；稳定性；智能化

DOI：10.69979/3060-8767.25.04.025

引言

在当今信息化的时代，电力监控系统的安全性不仅关乎电网的稳定运行，更关系到社会经济的可持续发展。随着电力系统逐渐迈向智能化、互联化的新时代，各种复杂的安全威胁也随之而来。无论是来自外部的黑客攻击，还是内部员工的恶意破坏，电力监控系统面临的安全风险愈发严峻。在这个背景下，主动防御技术作为一种前瞻性的安全应对手段，开始引起业界和学术界的广泛关注。它不同于传统的被动防御方法，主动防御技术通过实时监控、风险评估和策略动态调整等手段，能有效识别和阻止潜在的威胁。在电力系统的智能化进程中，如何利用这项技术提升系统的稳定性和可靠性，已成为一个亟待解决的关键问题。

1 电力监控系统面临的安全风险、防护需求

1.1 电力监控系统安全性现状

目前，随着智能电网的逐步构建以及数字化技术的应用，在电力监控系统中，不少国家都将电力监控系统作为国家能源系统中的主要板块，从而也在逐步加剧其中的安全风险。因电力监控系统中存在诸多的关键数据，例如设备的状况、调度信息等。传统的系统防护已经很难满足这一特点，为此，电力监控系统中存在的安全风险也是我们不得不考虑的问题。所以，在这一情况下，智能化的安全防护将会显得越发重要起来。电力监控系统不仅要求具有一定实时化的监控能力，同时针对突如其来的安全问题，如何能够及时处理也应作为电力监控系统安全方面研究的重中之重。

1.2 外部攻击、内部威胁分析

从当前情况来看，电力监控系统内部和外部均会带来威胁，外部人员通过网络漏洞实施入侵，破坏电力监控系统的稳定性，篡改电力监控系统数据信息，破坏电力调度及分配的稳定性。黑客利用拒绝服务攻击(DoS)、钓鱼、恶意代码植入等手段攻击，会造成正常的电力供应混乱，更严重的情况是，电力系统遭受大规模的瘫痪。内部威胁多来自于管理不当、权限滥用等现象，管理人员或系统管理人员利用权限对其内网系统进行非正常操作，以权谋私进行破坏会带来一样的结果。但内部威胁往往会被忽略，长时间的攻击与破坏极易使系统面临极大的危险[1]。所以，针对电力监控系统的安全防护不仅要完善其外部网络的防护，还要从内部管理与权限管控等方面着手才能更好地应对内外双重威胁带来的损害。

2 主动防御技术应用中的实施难点

2.1 防御策略的适用性、灵活性问题

传统防御策略难以应对外部环境多样性的攻击，每一类攻击都有其特点及攻击方法，防御策略一旦确定便不易转变适应新的攻击。同时电力监控系统应用于不同地区以及不同业务存在自身的特点和需求，使得不同的攻击形式与不同等级的安全需求下防护策略需要实现较高水平的灵活性，根据情况变动灵活防护响应。实现这一策略在当前的技术实施方面也并非很容易做到，因此如何建立适合复杂攻击形式的防御策略以达成对多攻击模式精准而灵活地应对则是技术实现的难点之一。

2.2 系统资源配置、防御效率问题

由于主动防御技术的应用存在防御性能与系统资源配比的关系，在电力监控系统的应用过程中防御技术会出现攻击提前检测的过程，也需要更多的系统资源和

网络带宽才能够达到相应的速度要求。在应用过程中的大量网络流量和各项运算会导致系统资源的巨大浪费，而过多系统资源的消耗也会影响电力监控系统的稳定性，系统在使用过程中的性能存在一定的限制，在实际使用的过程中发生大量网络流量和计算将会在很大程度上影响系统使用的相关数据，这对系统的实时处理提出了较大的考验。因此，在防御技术应用过程中如何使防御以及网络速度尽量更加贴合于系统需求的问题是当前的应用阶段中需要面临的问题。

2.3 防御响应技术执行难题

在主动防御技术中，对各种安全威胁的快速及时应对是其主要的核心技术，但实际运行中往往因为防御响应技术执行速度慢导致防御响应效果不理想。对于电力监控系统而言，其攻击类型较多且复杂，既有恶意代码类的攻击也有复杂网络攻击，其防御响应技术措施必须具备较高的智能性和准确度。当前防御响应技术往往在执行复杂网络攻击响应技术时对新技术处理的响应速度和准确性较低，以至于导致攻击未能第一时间做出有效防御，或未能把握最佳防守时期。防御响应技术过程包含威胁检测、反应机制启动、攻击隔离等多种环节，如何协调各环节有效协同且在紧急情形下顺利运行也是当前防御响应技术执行环节面临的困难之一[2]。因此，如何提高防御响应精准、及时，尤其是复杂环境下防御响应高效执行，是当前主动防御技术应用方面的难点。

3 主动防御技术提升电力监控系统稳定性研究

3.1 主动防御技术的基本框架

网络安全、系统稳定运行直接影响整个电力系统的运行，被动防御主要采取事后总结的方式，不能对未来的威胁进行准确预警，传统被动防御的方式无法应对威胁的变化。主动防御主要采取将防御“关口”前移以及动态防御来实现。技术主要依据对电力系统内外部威胁的理解构建防御的框架，主要通过威胁感知以及对行为的判断，动态获取电力系统中的异常信息，而判断异常的主要来源是电力系统中流量、行为、设备等多种数据的获取。主要技术点是主动防御根据历史数据、行为分析、风险检测提前采取攻击行为前的防御措施。整个防御架构不仅仅是数据采集以及反应措施的制定，而是需要从全面的安全识别以及响应策略的制定。利用人工智能或者机器学习算法能够对电力系统中未知攻击技术，提前进行检测、分析、识别，并能够实现实时预警以及防护决策的即时响应，提前对攻击行为进行威胁感知与防范与处理。而主动防御框架更多的是将自己决定的分析作为整个策略制定的基础，系统能够根据威胁变化情况以及电力系统运行进行策略的更新与优化。针对电力监控系统而言，主动防御不仅针对的是单一的外部攻击，还应关注来自系统内操作风险及人为失误对系统的破坏。主动防御技术通过对系统内操作行为的更加有效的检查来实现对安全风险的全面防控，通过先进的身份认证与授权实现主动防御安全技术框架[3]。不仅适用于抵御黑客系统安全风险，同样适合用于遏制恶意操作的安全风险。

3.2 风险识别实时响应机制

由于电力监控系统面对的安全威胁，要求能够及时地采取措施进行保护，传统的安全防御方案常常采取“亡羊补牢”式防御方案，对于已存在的风险没有做到及时预警、及时阻断，而采用主动防御技术，则具备对风险识别与实时响应的特点，打破传统的被动防御局面。在风险识别方面，主要针对电力监控系统内外部风险的监控，包括实时动态的网络流、数据交互等各种基础层面与设备级、操作级、通信层的各种业务信息，达到能涵盖电力监控系统“全维度”可能存在的威胁源的识别。此外，风险识别也要求实时从海量数据中识别非典型行为和安全威胁，它依赖于系统的数据分析能力[4]，并识别并判断“未授权用户登录系统设备”“控制对象发生了预期意外”“存在应用层通信流量不一致或异常行为”或“存储设备信息的正常行为”等安全风险信息，及时启动相应的防御方案。主动防御技术通过实时流分析，能很快地对威胁行为作出反应，但在防御中误报、漏报等问题的解决仍然是一个难题。电力监控系统中的一些正常操作会触发报警，但有一些攻击是在早期并未被发现。为降低这个问题，在主动防御策略中，大数据分析和 AI 算法只是一个组成部分，算法与策略进行交叉验证作为主动防御技术的另一个重要部分，加强了多维度、多层次的数据校验。简单地说，系统对某个事件是否是威胁会通过多种算法、策略交叉验证，提高报警准确性。提高和改善风险管理的算法与模型，主动防御系统将可以“自我进化”，从而适应新的威胁模型，提高响应准确性与可靠性。

3.3 防御策略的动态优化应用

电力监控系统威胁环境处于不断演变状态，黑客不断出现攻击新技术，单纯依靠固定、单一防御系统并不适应对错综复杂威胁的应对。防御策略的动态优化也成为了主动防御技术的核心内容之一。传统的防御技术常采取预先设定好的固定规则，这往往导致防御方法无法

及时适应威胁的变化。而动态优化应用的核心在于防御策略的自适应变化与调整，在不断变化的攻击方法以及系统运行状态下，能自动适应变化、自我调整。动态优化主要体现在系统运行过程中对系统的运行状态进行检测和评估。由于系统在运行的过程中，借助对实际外在环境状况的动态分析、攻击模式的学习、系统资源配置的动态调整等方法，便可以自动动态优化防御策略[5]。例如当前面临大规模分布式拒绝服务攻击（DDoS）时，能够自动在发现异常流量时，及时的调整分配的带宽，开启防火墙规则，甚至在核心节点临时部署防护等。这也是根据实际防御过程的状态调整防御策略，最大化有效提升防御过程的效率，保证系统维持在最佳的防护状态。

3.4 系统防御架构的设计实现

电力监控系统防御架构的设计不能单纯是单一的技术防御，防御架构的设计应是多层级、多角度的全方位的防御架构设计方案。防御架构的设计是综合保护电力系统安全，包括从网络层面、应用层面，网络物理设备层面到数据层的全方位保护，深入分析电力监控系统对稳定、实时、可靠的要求，并不能够使防御架构降低电力调度或管理效果。入侵检测系统（IDS）、防火墙、数据加密系统、防篡改算法都是组成电力监控系统防御架构的必要组成部分，对于实时监控数据安全必须进行防篡改处理，防止电力监控信息的篡改。防御架构除了上述必要的防护层之外，还能够使系统防御架构达到在遭遇入侵时及时主动应对，并且系统在防御架构报警之后可及时地将防御级别提升，以满足在不同条件下有效安全的保护电网信息的监控与管理效果。防御架构也应具备使防御架构内的设备根据实际传输流量和系统安全威胁合理适应性使用资源并提升防御架构实时响应机制的性能，只有这样，电力监控系统防御架构的设计才能够使电力监控系统在满足当前高效安全的保护措施下，也能够确保系统稳定安全的性能和效果[6]。

3.5 提升系统稳定性的综合措施

电力监控系统的稳定直接影响电网的安全与社会经济的运行与发展，因此强化系统的稳定性不仅是为了应付当前的安全威胁，也是在为未来智能化与电力自动化系统进行铺垫。在强化系统的稳定性过程中，要结合技术与管理手段的使用，在技术方面要强化对硬件的硬件升级，保证系统内每项设施的高可用性与自动故障处理能力；系统要通过软件层面的技术提升，优化调度管理能力，使之动态变化，减少资源的瓶颈效应。强化人员管理，形成标准的作业方式同样是提高系统稳定性的内容。系统的操作维护人员要有高的安全意识和处置能力，同时要加强人员培训演练，以确保突发事件面前处置的快速与有效。系统稳定性的提升是技术、人员与长期维修管理相互作用的结果，要保障防护技术不断地进步升级，但又要有长期维护管理的系统，电力监控系统才能在更加严峻的安全风险面前一直稳定运行，保持电网的安全运行和稳定。

4 结束语

电力监控系统防护的高风险是一个多方面综合因素所引起的系统风险，包括技术、管理、人员，而主动防御技术的发展为提升电力监控系统的防护能力提供了新方法。主动防御通过综合的研判和及时的反应来研判事件的威胁程度，并根据一定的场景下改变防御的方法，实现基于主动防御条件下的高效响应和防御模式的优化，同时动态的优化在一定程度上也会带来效率方面的不足问题，动态防御系统在多场景下工作模式的选择问题也会存在一定的实际问题，优化配置也需要有较多的时间成本和研究投入。然而，随着未来的发展，主动防御技术会愈来愈成熟，并在电力监控系统中发挥更重要的作用。

参考文献

[1]王建波,李伟.电力监控系统安全防护技术研究[J].电力系统自动化,2020,44(18):45-50.
[2]刘洋,王晓伟,刘金龙.基于主动防御的电力信息安全技术研究[J].电力技术,2021,50(12):118-124.
[3]张玲,赵鹏.电力监控系统中的信息安全防护研究[J].电力科学与技术学报,2022,37(06):725-732.
[4]陈浩,李俊峰.电力监控系统主动防御架构设计与实现[J].电力与能源,2021,42(08):56-61.
[5]杨阳,周斌.主动防御技术在电力系统中的应用研究[J].自动化仪表,2021,41(03):98-104.
[6]赵娜,王勇.电力监控系统安全防护策略研究与实现[J].电力工程技术,2020,29(11):302-308.

作者简介：施晓亮（1977-07），男，汉族，研究方向：电力。