面向智能电网的可部署内生安全技术研究综述

王鼎宇[1]，张帆[2]，王俊超[2]，曹琰[1]

（1.郑州大学网络空间安全学院，河南 郑州 450002；2.复旦大学大数据研究院，上海 200433）

摘　要：智能电网作为现代能源体系的关键基础设施，其网络空间与物理运行过程深度耦合，已成为国家能源安全的重要支撑。随着分布式能源、储能系统、智能电表等海量异构设备的大规模接入，“云-管-边-端”协同架构成为主流形态。然而，攻击手段的持续演进使针对数据采集与监视控制（SCADA）系统、智能终端和通信网络的网络攻击日益频发，传统“封门补漏”式被动防御固有的滞后性与对先验知识的依赖，使其难以有效应对深植于系统架构与运行过程的安全威胁。信息系统中由漏洞、后门等自身缺陷引发的内生安全问题，难以在设计与开发阶段被完全消除，成为制约电网安全防护能力提升的根本性瓶颈。针对上述问题，系统研究了可部署于智能电网的内生安全技术。首先，以智能电网面临的供应链攻击、漏洞利用攻击、分布式拒绝服务/拒绝服务（DDoS/DoS）攻击、数据篡改与伪造攻击、物理与侧信道攻击、高级持续性威胁（APT）6 类主要威胁为研究切入点，结合智能电网架构模型（SGAM）与典型攻击案例，分析了各类攻击的典型入口、影响层级及传统防御的技术难点与局限，发现攻击的直接来源大多集中于组件层与通信层，且攻击影响可跨层级传播。其次，依据核心功能定位，将可部署的内生安全技术划分为抗攻击类与可信认证类两大类：前者包括软件多样化、动态异构冗余（DHR）、基于物理不可克隆函数（PUF）的认证机制和抗攻击路由，后者包括零信任架构、可信计算与量子安全可信认证技术，并从作用机理、适用威胁、部署层级、性能开销和工程条件等维度，系统梳理了 7 类技术的研究进展、防御目标、作用层级与验证结果，总结了各类技术的适用条件与主要局限。研究结果表明：其一，单项内生安全技术通常只作用于攻击过程的局部环节，难以独立应对 APT 等复合攻击，多技术协同的关键在于按照攻击阶段明确技术分工，并共享身份、设备状态、异常输出、网络状态等信息，后续研究应以攻击链阻断率、误判率、最坏时延、恢复时间等指标评价协同效果；其二，现有技术方案多处于原型、仿真或小规模验证阶段，缺乏智能电网真实场景下的大规模部署验证，性能开销与实时性约束是技术落地的关键障碍；其三，供应链安全是内生安全技术可靠运行的基础，软件多样化依赖可信编译链，DHR 依赖执行体来源，零信任和可信计算依赖准确的资产及固件信息，应形成从组件识别、完整性验证到异常处置的闭环；其四，人工智能（AI）可辅助内生安全检测与认证，但需兼顾识别能力与模型安全，评价时应同时报告检测性能、推理时延、资源占用与更新方式；其五，量子安全技术应按当前发展状况渐进迁移，后量子密码（PQC）可优先通过纯软件方案部署并建立密码敏捷机制，量子密钥分发（QKD）宜优先用于固定的高价值链路。

关键词：智能电网；内生安全；网络威胁；抗攻击技术；可信认证

中图分类号：TP399　　**文献标志码：**A　　**DOI：**10.19678/j.issn.1000-3428.0260693

Review of Deployable Endogenous Security Technologies for Smart Grids

WANG Dingyu[1], ZHANG Fan[2], WANG Junchao[2], CAO Yan[1]

(1.School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450002, Henan, China;
2.Institute of Big Data, Fudan University, Shanghai 200433, China)

【Abstract】The smart grid is a critical infrastructure in the modern energy system that couples cyberspace with physical operation processes, and it has become a key pillar of national energy security. With the widespread use of massive heterogeneous devices such as distributed energy resources, energy storage systems, and smart meters, the “cloud-network-edge-terminal” collaborative architecture has become the mainstream paradigm. However, the continuous evolution of attack techniques has led to increasingly frequent cyberattacks targeting Supervisory Control and Data Acquisition (SCADA) systems, intelligent terminals, and communication networks. The inherent lag of conventional ″patch-and-block″ passive defense techniques and their dependence on prior knowledge cause difficulty in effectively countering security threats deeply embedded in system architectures and operational processes. Endogenous security issues caused by inherent defects such as vulnerabilities and backdoors in information systems cannot easily be completely eliminated during the design and development phases; this creates a fundamental bottleneck that restricts the improvement of smart grid security protection capabilities. To address these issues,

基金项目：国家电网有限公司总部管理科技项目（52130025002S-473-ZN）。

作者简介：王鼎宇（CCF 学生会员），男，硕士，主研方向为软件多样化、编译安全；张帆（CCF 专业会员、共同一作），教授；王俊超（CCF 杰出会员、通信作者），副教授；曹琰（CCF 高级会员），教授。

收稿日期：2026-05-13　　**修回日期：**2026-08-24　　**E-mail：**wangjunchao11@126.com

计算机工程 www.ceaj.com

this paper systematically reviews endogenous security technologies that can be deployed in smart grids. First, the six major threats facing smart grids—supply-chain attacks, vulnerability exploit attacks, Distributed Denial of Service/Denial of Service (DDoS/DoS) attacks, data tampering and forgery attacks, physical and side-channel attacks, and Advanced Persistent Threats (APTs)—are considered as research entry points. Typical entry points, impact levels, and the technical difficulties and limitations of traditional defenses for each type of attack are analyzed, combined with the Smart Grid Architecture Model (SGAM) and typical attack cases. The analysis reveals that the direct sources of most attacks are concentrated at the component and communication layers, and that the attack impacts can propagate across layers. Second, according to core functional positioning, deployable endogenous security technologies are categorized into attack-resistant and trusted authentication technologies. Attack-resistant technologies include software diversification, Dynamic Heterogeneous Redundancy (DHR), Physical Unclonable Function (PUF)-based authentication mechanisms, and attack-resistant routing, while trusted authentication technologies include zero-trust architecture, trusted computing, and quantum-secure trusted authentication. This paper systematically reviews the research progress, defense objectives, operational layers, and verification results of these seven technologies based on their working mechanism, applicable threats, deployment layers, performance overhead, and engineering conditions. It also summarizes the applicable conditions and main limitations of each technology. The review reveals five key findings. First, a single endogenous security technology usually acts on only partial segments of an attack chain and cannot independently cope with composite attacks such as APTs. The key to multi-technology collaboration lies in clarifying the division of labor according to attack phases and the sharing of information such as identities, device statuses, abnormal outputs, and network statuses. Follow-up research should evaluate collaboration effectiveness using metrics such as attack chain blocking rate, false judgment rate, worst-case latency, and recovery time. Second, most existing technical solutions are still in the prototyping, simulation, or small-scale verification stages, and large-scale deployment verification has not been performed in real smart grid scenarios, where performance overhead and real-time constraints are key obstacles to technology implementation. Third, supply chain security is the foundation for the reliable operation of endogenous security technologies. Software diversification relies on a trusted compilation chain, while dynamic heterogeneous redundancy relies on trusted execution body sources, and zero-trust and trusted computing solutions rely on accurate asset and firmware information. Accordingly, a closed-loop process from component identification and integrity verification to anomaly response should be established. Fourth, Artificial Intelligence (AI) can assist endogenous security detection and authentication, but both recognition capability and model security must be considered. Evaluations should simultaneously report detection performance, inference latency, resource overhead, and update mechanisms. Fifth, quantum security technologies should be migrated progressively according to their current development status. Post-Quantum Cryptography (PQC) can be prioritized for deployment via pure software solutions with cryptographic agility mechanisms, while Quantum Key Distribution (QKD) can be used for priority application in fixed high-value links.

【Key words】 smart grid; endogenous security; cyber threats; attack-resistant technology; trusted authentication

0 引言

2003 年,美国政府在“Grid 2030”规划中提出的广域测量系统(WAMS)被视为智能电网的雏形,其核心理念是“通过实时测量与智能自动控制系统实现电力传输基础设施可靠、高效、安全运行”[1]。此后,现代智能电网已逐步形成高度自动化、支持可再生能源接入、强化用户互动以及兼顾安全可靠运行等特征,“云-管-边-端”协同架构成为主流形态,分布式能源、储能系统和智能电表等海量异构设备接入规模达到 10 亿台级。

然而,这一转型也使电网面临前所未有的安全挑战。例如,针对数据采集与监视控制(SCADA)系统等关键工控系统的分布式拒绝服务(DDoS)定向攻击频发,高级持续性威胁(APT)组织通过供应链漏洞实现长期潜伏渗透,海量智能终端因缺乏统一安全管控而存在大范围防护盲区,系统漏洞与恶意后门等安全隐患持续扩散。传统“封门补漏”式被动防御因其固有的滞后性,难以及时应对深植于系统架构与运行过程的安全威胁。对智能电网这一关键能源设施而言,这种滞后性意味着功能受阻、数据泄露乃至业务中断,均不可接受。此外,面对日益演进的攻击方式,传统被动防御还暴露出适应缓慢、过度依赖先验知识等局限。

上述风险在一定程度上源于软件或硬件设计缺陷被有目的地恶意利用。这些缺陷受认知能力、生态环境和工程实现等因素制约,难以在设计与开发阶段被完全消除[2]。邬江兴院士[3]将信息系统中除

计算机工程 www.ecice06.com

预期功能以外客观存在的非预期隐藏功能，以及由漏洞、后门等系统自身缺陷引发的安全问题概括为“内生安全问题”。其核心问题是如何在缺乏攻击先验知识的条件下，抑制或阻断未知内生安全威胁[4]。

为应对上述问题，内生安全技术以“构造决定安全”为核心思想[4]，通过调整系统内部架构、执行逻辑和运行形态，使安全能力与系统构造和运行机制相结合。与传统外挂式防护相比，这类技术具有降低对已知攻击特征依赖的潜力，若将该技术体系应用于智能电网，有望实现从规划、建设到运行的全流程防御覆盖。

本文将重点从 4 个方面进行研究：1）智能电网不同层级面临的主要攻击类型、典型入口和传统防御局限；2）不同内生安全技术通过何种机制降低攻击成功概率或限制攻击影响；3）现有方案在安全效果、性能开销、部署条件和证据成熟度方面呈现出哪些特征；4）当前技术覆盖存在哪些薄弱环节，多技术协同和后续研究应优先解决哪些问题。

本文的主要工作包括：1）依据攻击实施方式与技术机理梳理智能电网主要威胁，并结合智能电网架构模型（SGAM）分析其可能影响的层级和典型入口；2）从作用机理、适用威胁、部署层级、性能开销和工程条件等维度，对软件多样化、动态异构冗余（DHR）、基于物理不可克隆函数（PUF）的认证机制、抗攻击路由、零信任、可信计算及量子安全可信认证等技术进行比较；3）在跨技术综合分析的基础上，识别单项技术的能力边界与协同关系，并归纳供应链防护、可信人工智能（AI）和量子安全演进等研究方向。

本文首先分析智能电网面临的主要威胁及传统防御局限，然后梳理内生安全相关技术的作用机理、研究进展与部署条件，最后对跨技术协同关系、现有证据不足及未来发展方向进行讨论。文献检索范围涵盖 Google Scholar、中国知网、IEEE、ACM 及 Springer 等数据库，结合美国国家标准与技术研究院、日本国家级官方漏洞报告及 ESET 等安全机构的事件报告，初步筛选 400 余篇文献，依据时效性、相关性与针对性最终确认 118 篇。

1 智能电网威胁及传统防御局限

智能电网作为能源互联网的核心枢纽，其网络空间与物理运行过程深度耦合，攻击影响可能在业务、功能、信息、通信和组件等层级之间传播。为兼顾攻击入口、实施手段和组织过程，本文将相关威胁归纳为供应链攻击、漏洞利用攻击、DDoS 或拒绝服务（DoS）攻击、数据篡改与伪造攻击、物理与侧信道攻击以及 APT 6 类。后续各节将从攻击定义与典型入口、案例及相关研究佐证、传统防御局限和智能电网适用边界这 4 个方面分析不同威胁所利用的系统缺陷及其对内生安全机制的需求，并采用智能电网架构模型分析不同攻击的影响层级。SGAM 由欧盟 M/490 授权下的参考架构工作组提出，包括业务、功能、信息、通信和组件 5 个互操作层：业务层描述业务目标、流程和组织约束；功能层描述实现业务目标的逻辑功能与服务；信息层描述功能间交换的数据对象；通信层描述信息交换协议与机制；组件层描述承载功能和通信的设备、系统及软件[5]。

1.1 供应链攻击

供应链攻击是指攻击者在智能电网设备或软件的设计、开发、生产、运输、部署、运维和升级等环节植入恶意组件、篡改固件或代码、窃取签名密钥，或者污染第三方依赖，使相关产品在接入电网后成为攻击入口或执行恶意功能[6]。其核心特征是攻击行为发生在目标系统正式运行之前或可信更新过程中，并可借助合法厂商、组件及更新渠道继承信任。2017 年的 NotPetya 事件通过乌克兰会计软件的更新渠道传播[7-8]，2020 年的 SolarWinds 事件则通过被污染的合法软件更新包感染大量机构[9]。现有研究可归纳为三个方向：一是分析伪造组件、设备配件替换和配置文件篡改等软硬件植入路径[10-11]；二是研究 IoT 及开源依赖生态中的共性漏洞和协同供应链攻击模型[12-13]；三是针对实际变电站建立供应链攻击形式化模型和量化评估方法[6]。

由于供应链涉及多级主体和跨生命周期活动，攻击者可在产品全生命周期的多个环节实施篡改或注入[14]，传统防御主要面临以下局限：1）多级供应商及组件依赖的可见性不足，组织通常能够直接约束一级供应商，却难以持续掌握上游来源，因而存在未被识别的信任传递路径[15-16]；2）信任机制可能被继承性污染，代码签名、完整性校验和安全审计能够验证软件来源、发现部分异常，但当构建环境、签名密钥或合法更新服务器本身遭到攻陷时，恶意代码仍可能以可信更新的形式进入系统[17-18]；3）组件持续监测不足，仅在系统集成阶段开展一次性检查，难以覆盖后续版本更新、维护者变化和新披露漏洞，XZ Utils 事件所反映的正是开源依赖长期维护过程中的风险[19-20]；4）供应商安全能力和监督机制存在差异，中小型供应商可能因投入、流程和人员不足成为整体供应链的薄弱环节[21-22]，因此供应链风险通

计算机工程 www.ecice06.com

常在设备接入电网之前形成，其直接入口可能主要位于组件层，但恶意功能可随固件、软件和通信服务向通信层、信息层及功能层传播。

1.2 漏洞利用攻击

漏洞利用攻击是指攻击者利用智能电网设备、固件、应用软件、通信协议或管理接口中的已知及未知漏洞，非法获取权限、执行恶意代码、窃取或篡改数据，或者干扰系统正常运行。

2024 年，日本一个大型光伏电网中约 800 台的 SolarView Compact 远程监控设备遭攻击者利用 CVE-2022-29303 未授权访问漏洞劫持[23-24]；2020 年，巴西电力公司 Light S. A. 遭受的勒索攻击涉及 CVE-2018-8453 漏洞利用[25]。相关研究可归纳为 3 个层次：首先，文献[26]依据 OWASP Top 10 和 MITRE CWE 等体系识别智能电网软件中的高频漏洞类型，文献[27]从控制设备、通信设备和商用设备等载体角度进行分类；其次，文献[28]结合关键设备漏洞清单和攻击图描述从初始入口到目标系统的攻击路径；最后，文献[29]通过构建攻防对抗模型分析漏洞利用过程中攻击者与防御者的策略关系。上述研究主要回答了“漏洞是什么”“漏洞位于何处”“漏洞如何形成攻击链”等问题。

传统漏洞防御在智能电网场景中主要受到以下约束：1）未知漏洞缺少可直接用于特征匹配的攻击样本和规则，基于已知漏洞特征的检测方法对零日攻击的识别与阻断能力受限[30-31]；2）漏洞披露、补丁开发、兼容性测试和现场升级之间存在时间差，防病毒软件与入侵检测系统的特征库更新也需要经过样本收集和规则生成过程[32-34]；3）部分攻击利用合法接口、协议语义或已获取的有效权限实施操作，单纯依赖恶意代码特征可能难以区分异常利用与正常业务。由此可见，漏洞利用攻击典型入口既包括智能电表、远程终端和控制装置等组件，也包括远程管理服务、Web 接口、协议实现及上层业务应用，因此防御重点不应仅停留在补丁和特征库更新，还应包括运行时异常识别、权限约束及攻击影响隔离。

1.3 DDoS/DoS 攻击

DDoS/DoS 攻击是指攻击者通过集中或分布式方式消耗智能电网设备、通信网络或业务系统的带宽、连接、计算及存储资源，使合法请求无法在规定时间内得到处理。相关研究主要从 4 个角度展开：文献[35]分析链路泛洪与传统 DDoS 等攻击形态；文献[36]研究智能电网信息技术-运营技术（IT-OT）依赖关系下攻击影响的跨域传播；文献[37]关注高级计量基础设施（AMI）在 DoS/DDoS 条件下的通信与业务影响；文献[38]归纳攻击可能利用的设备和协议载体。由此可见，DDoS/DoS 不仅是网络流量问题，更是一种业务安全问题，其安全后果还取决于受攻击通信业务与状态估计、远程控制、计量采集等电网功能之间的依赖关系。

传统 DDoS/DoS 防御在智能电网场景中主要面临以下约束：1）攻防资源成本不对称，防御方通常需要配置冗余带宽、服务器和清洗能力，而攻击者可借助僵尸网络聚合大量受控终端，以较低边际成本持续生成攻击流量[39]；2）正常业务突发与攻击流量难以区分，基于已知特征的方法对新型攻击适应能力有限，异常检测又可能将负荷波动、设备集中上线或故障恢复流量误判为攻击[40-41]；3）检测精度与实时性之间存在权衡，当前基于机器学习和深度检测的方法可能提升识别能力，但会引入计算、存储和模型更新开销[42]，过度复杂的检测流程还可能增加通信时延；4）云环境中的弹性扩展并非无成本防御，带宽配额和扩展速度可能限制服务恢复，大规模自动扩容还可能被攻击者利用以放大运营费用[41-43]，DDoS/DoS 的直接作用点通常位于通信层、信息层或业务服务，而其流量来源可能是被控制的组件。

1.4 数据篡改与伪造攻击

数据篡改与伪造攻击是指攻击者修改、删除、重放或伪造智能电网中的测量值、设备状态、身份信息及其他关键数据，进而破坏数据完整性和真实性，误导状态估计、调度控制或计费决策[44]。而虚假数据注入（FDI）是其中研究较为集中的一种攻击形式。围绕 FDI 的现有研究可归纳为 3 个方面：讨论攻击数学建模和漏洞利用逻辑[45]；分析智能电网中组件存在的结构性弱点[46-47]；指出当前广泛采用的静态检测方法所存在的短板[48]。上述研究表明，攻击者既可能直接控制测量设备，也可能在数据传输、汇聚或处理过程中修改信息，并利用系统模型知识构造与正常运行规律相近的恶意数据。

传统防御主要受到以下限制：1）部分早期电力通信协议在设计时更关注互操作性和实时通信，对身份认证、报文完整性及抗重放能力考虑不足[49]，且多数系统依赖网络边界防护和简单校验，无法有效识别来自内部或已渗透节点的恶意数据[50-51]；2）状态估计与残差检测存在盲区，精心构造的不可观测 FDI 可使篡改后的测量数据继续满足系统模型约束，从而绕过基于残差阈值的异常检测[52-53]；3）检测阈值难以同时兼顾漏报和误报，负荷变化、测

计算机工程 www.ecice06.com

量噪声、通信丢包和设备故障也可能造成数据偏差，若缺少设备状态、时序特征和物理约束等多源信息，检测系统可能难以区分恶意篡改与正常波动。此类攻击的初始入口可能位于组件层或通信层，其直接作用通常集中在信息层，并可进一步影响功能层的状态估计、保护、调度和控制决策。因此，防御不能只验证数据传输过程，还需要结合数据来源可信度、设备运行状态和电网物理规律开展联合校验。

1.5 物理与侧信道攻击

物理与侧信道攻击是指攻击者通过物理接触智能电网设备或利用设备的物理特性（如功耗、电磁辐射），获取敏感信息或破坏设备功能的攻击方式。GOPE 等[54]提出面向 AMI 的安全固件更新框架 PRSUF，通过 SRAM-PUF 和动态状态派生固件更新密钥，避免将长期密钥直接存储于智能电表非易失性存储器，以降低物理提取、克隆和侧信道攻击风险。GOTTUMUKKALA 等[55]和 ZHANG 等[56]分别从充电设施的网络物理组件和智能电网攻击载体角度说明开放或半开放环境中的电网终端具有可被物理接触的攻击面。GUI 等[57]进一步针对 ANSI C12.22 安全通信使用的 AES-128 开展实验，并说明硬件并行实现相较软件实现具有更强的侧信道抗性，但仍可能泄漏密钥。

相关防御措施在智能电网终端上主要面临覆盖范围、可信验证和资源开销三方面约束。首先，智能电表、充电桩和配电终端数量大且位置分散，部分设备处于无人值守环境，防拆封装、机柜锁闭和人工巡检可能被绕过，也难以持续证明设备内部状态可信[58-59]。其次，自动化、控制和防护功能通常部署在软硬件耦合的资源受限智能电子设备中，相关设备具有开发、测试和升级周期较长等特点[60]。最后，掩码、随机化、密钥更新、电磁屏蔽和专用安全硬件等侧信道对策会引入不同形式的代价，例如软硬件协同具有提升防护能力的潜力，但部署需要修改硬件结构[61]或是可证明安全构造仍存在效率限制[62]。

综合来看，物理攻击的初始入口主要位于组件层，但设备克隆、固件篡改和密钥泄露可进一步破坏通信层认证、数据机密性以及功能层控制指令的可信性。因此，面向智能电网的防护应将物理防拆、可信启动与远程证明、密钥动态更新及侧信道对策结合起来，并在具体终端平台上同时评价密钥恢复难度、计算时延、能耗、芯片面积和实时业务影响。

1.6 APT

APT 不是单一攻击技术，而是组织攻击者围绕特定目标实施的多阶段攻击过程，通常经历初始访问、权限维持、横向移动、IT/OT 跨域渗透以及控制或物理影响[63]。2015 年，乌克兰西部遭遇网络攻击，约 22.5 万用户受影响，停电持续数小时[64]。2016 年，基辅部分区域遭遇针对性电网攻击，该攻击由首个投入实战、专门针对电力系统的恶意软件实施[65-67]。2017 年，沙特某石化厂遭遇 Triton（又称 Trisis）恶意软件攻击，首次实现对安全仪表系统（SIS）的定向破坏[68-69]。现有研究主要从防御决策[70]、态势感知[71]和攻击链[72]等角度分析 APT。

传统防御手段在应对此类精心设计、隐蔽性强的攻击时，面临三大难点：1）行为特征难以提取和识别，APT 攻击模拟正常用户行为进行隐蔽操作，传统基于已知攻击特征库的防御系统难以识别新型 APT 行为[73-74]，而深度学习方法又面临“黑箱”特性和可解释性不足的问题[75-76]；2）攻击空间不确定性高，APT 攻击者往往从看似不重要的边缘节点入手，逐步渗透至核心系统，而传统防御通常只关注核心业务系统[77]；3）持续性攻击与防御资源不平衡，传统“事件驱动”防御模式与 APT 的长期潜伏形成资源错配[78-79]，难以维持持续有效的防御[80]。APT 入口可能来自钓鱼、供应链、凭据或远程访问，因此攻击起点难以确认。同时，APT 破坏性极强，阻碍智能电网的正常业务并窃取机密信息，产生的攻击影响能够波及整个智能电网。

1.7 对攻击的梳理与分析

通过对上述攻击的研究分析可以发现，当前的攻击直接来源大多为组件层和通信层，这两个层级都直接与外界相连，需要重点进行防护。同时，智能电网各层级之间的关联紧密，对任一层级展开的攻击都会波及其余层级，不仅对智能电网的正常业务造成影响，还可能泄露关键信息或导致重要组件被破坏，最终对能源安全和国家安全造成不可估量的损害。然而，当前所采用的防御手段仍存在着一定的缺陷，难以有效保障智能电网的安全。因此，为应对日趋复杂的网络攻防环境，智能电网更加需要内生安全所带来的安全能力提升。

2 智能电网可部署内生安全技术分析

当前智能电网面临的网络攻击威胁日趋严峻且呈现复合化、精准化特征，传统防御模式已难以满足其对安全性与稳定性的严苛要求。而内生安全技术不仅能显著提升智能电网自身鲁棒性，还能够提供攻击前预警、攻击中精准拦截和攻击后恢复的全流程防护，为突破传统防御瓶颈提供了关键技术路径。

计算机工程 www.ecice06.com

根据核心功能定位，智能电网可部署的内生安全技术可划分为抗攻击内生安全技术、可信认证内生安全技术两大类。图 1 展示了这两类技术所包含的详细技术分类及其对应的技术路线。本章聚焦近年来该领域的技术成果，系统梳理各类技术的核心原理与应用成效。

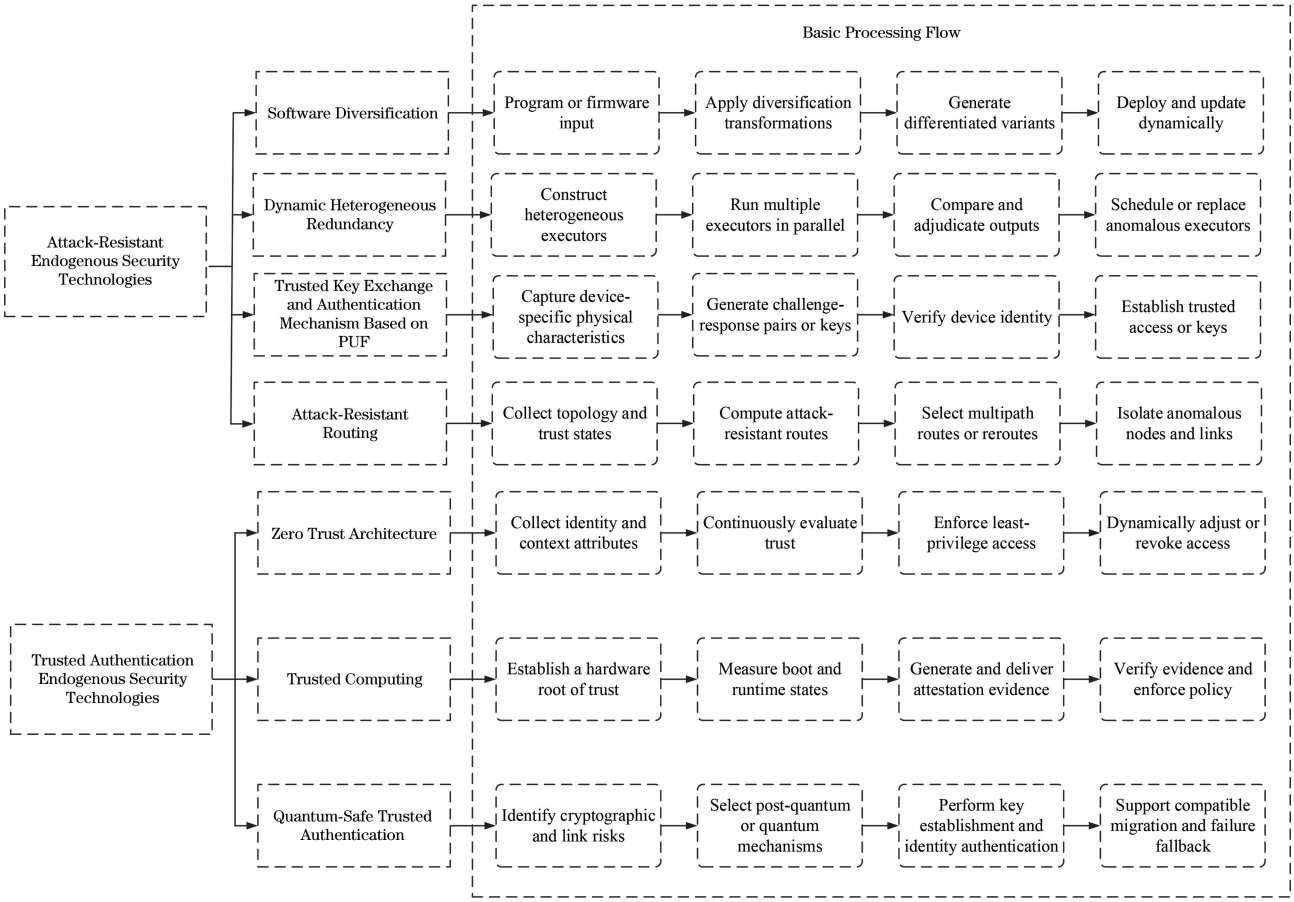


图 1 智能电网可部署内生安全技术路线

Fig. 1 Technical routes of deployable endogenous security technologies for smart grids

2.1 抗攻击类内生安全技术

抗攻击类技术包括软件多样化、DHR、PUF 相关设备认证机制和抗攻击路由。软件多样化改变软件表示或执行轨迹，DHR 改变执行体组合与仲裁过程，PUF 相关机制将认证凭据与设备物理特征绑定，抗攻击路由则约束路径选择或恶意节点参与。

2.1.1 软件多样化

软件多样化是指通过编译、二进制重构、代码混淆或运行时变体切换改变程序表示与执行轨迹的一类技术。现有研究可进一步区分为 3 条路线：通过对源码、中间表示或二进制重构生成静态变体，以 GuiDiv[81] 和 R2BF[82] 为例；通过虚拟化、混合布尔算术或跨过程变换提高自动分析和二进制差分难度，以 Loki[83] 和 Khaos[84] 为例；在运行过程中切换函数变体以形成动态轨迹，以 PRIAMO 等[85] 提出的技术方案为例。

GuiDiv[81] 在树莓派 4B 上测试 5 个 OpenSSL 函数，运行开销为 1.17%～12.42%，平均为 5.39%，但其后向逐步变体筛选复杂度为 $O(n^4)$；R2BF[82] 在 15 个简单 C 程序中测得文件大小平均增加 0.16%、执行时间平均下降 1.58%，但其安全验证仅覆盖 3 类 CTF 栈溢出利用。这两项结果说明特定静态变换可以在规模受限的程序上控制开销，但目前在复杂电网控制软件上的效果仍然需要进一步实验验证。与之相比，Loki[83] 以更高成本对抗符号执行、污点分析和程序合成，其 5 个密码程序的运行时间为原程序的 301～482 倍、文件体积为 18～51 倍，程序合成攻击成功率降至 19%；Khaos[84] 将 5 种二进制差分工具的匹配准确率降至 19%以下，平均运行开销低于 7%。可见，通过虚拟化、混合布尔算术或跨过程变换的方法普遍会带来执行体运行性能的损失。PRIAMO 等[85] 在 8 个 Computer Language Benchmarks Game 程序上测得−5.00%～192.14%的运行时间变化。这表明运行时变体切换的成本和效果显著依赖切换概率、程序结构和编译优化配置。

表 1 从防护目标、主要局限、部署要求以及作用层级 4 个方面对软件多样化技术进行了总结。GuiDiv[81]、R2BF[82] 和 Khaos[84] 依赖底层虚拟机(LLVM)或反编译与重编译工具链,并需要重新生成和分发软件;Loki[83] 的 301～482 倍运行时间及 18～51 倍体积增长使其更适合保护少量敏感代码,而不是直接覆盖完整实时控制程序;PRIAMO 等[85]提出的技术方案的原型则暂不支持并发执行以及直接或间接递归。从上述技术的主要局限和部署要求可以发现,现有的软件多样化技术若要迁移到智能电网场景中,必须配置配套的工具链,同时要明确适用的范围,并经过实际场景测试。

表 1 软件多样化技术方案对比

Table 1 Comparison of software diversification technical schemes

技术方案	年份	防护目标	主要局限	部署要求	作用层级
GuiDiv[81]	2023	降低同一代码复用攻击链在多个同构设备间直接迁移的可能性	后向逐步筛选算法复杂度较高	需要 LLVM 重编译、离线生成与筛选、多变体分发	组件层
R2BF[82]	2024	改变函数和代码布局并阻断部分代码复用利用	安全测试覆盖面较窄,仅支持不含复杂指针、数组、结构体和类的简单数值程序	依赖反编译正确性和 LLVM	组件层
Loki[83]	2022	对抗符号执行、污点分析与程序合成	运行时间和文件体积增长明显	需要源码和 LLVM、虚拟化和 MBA 表达式库	组件层
Khaos[84]	2023	削弱基于函数内部特征的匹配,增加漏洞函数定位难度	引入了一定的运行开销	需要源码、LLVM IR 和链接时优化	组件层
PRIAMO 等[85]提出的技术方案	2022	增加固定执行知识复用成本	成本和效果依赖于编译配置	需要编译插桩、多个函数变体和运行时切换	组件层

2.1.2 DHR

DHR 通过多个功能等价但实现方式不同的执行体并行处理输入,并利用动态调度、结果比较和异常执行体替换限制单一漏洞或后门持续控制系统。现有研究可以分为 3 个方向:1)博弈与概率模型研究,例如 HU 等[86]和 WANG 等[87]提出的技术方案;2)DHR 相关技术的研究,例如 YANG 等[88]提出的技术方案、WANG 等[89]提出的技术方案和 FBAMD[90];3)实际可部署技术原型研究,例如 HU 等[91]提出的技术方案。上述方向包括了理论研究、技术探索和原型开发。

理论研究主要解释 DHR 安全收益的形成条件。HU 等[86]针对三执行体系统建立有限理性静态博弈并用 Adam 算法模拟攻防演化,分析失效率、异构性和动态性对纳什均衡的影响;WANG 等[87]以十元组刻画执行体集合、服务序列、漏洞分布和攻击成功率,并在模型中忽略低于 10^{-9} 的系统随机误差。技术探索则主要围绕 DHR 所需技术的研究和开发展开。YANG 等[88]比较 FIFO、完全随机、人工加权及动态负反馈调度,评价指标是威胁与执行体的碰撞与收敛概率。WANG 等[89]在 Docker、Kubernetes 和异构消息中间件上处理 1 000 条工业物联网(IIoT)消息,DDQN 预训练 100 000 步,仲裁延迟为毫秒级,但耗时高于多数投票和漏洞分析等经典方法。FBAMD[90]在 CIC-Darknet2020 数据集上以 20%投毒率重复 5 次实验,准确率为 91.80%～94.60%,相比普通 DHR 提高 2.09～5.85 百分点。原型开发致力于将 DHR 从理论和测试逐步转向实用。HU 等[91]设计的拟态路由器包含 4 个异构控制平面,24 h 内每 3 h 触发一次预设攻击,共观察到 5 次执行体重启而转发服务未中断,表明其具备高度的可用性和可部署性。

但是,上述研究仍存在一定局限性。YANG 等[88]未充分分析调度算法计算开销和时延影响。WANG 等[89]引入的毫秒级仲裁不适合直接支撑时延敏感传输任务。FBAMD[90]的结论取决于所选训练数据、投毒方式、阈值和子模型。HU 等[91]的拟态路由器原型目前不能直接处理通过资源耗尽实现的 DoS/DDoS,也不能消除所有执行体共有的协议缺陷。

表 2 从防护目标、主要局限、部署要求以及作用层级 4 个方面对 DHR 技术进行了总结。当前的 DHR 技术仍然处于技术原型阶段,尚未实现大规模的智能电网场景下的实际应用。在智能电网场景下应用 DHR 技术,首先需要针对应用场景研究特定的博弈与概率模型,从理论上先证明其可行性;其次需要设计适用于智能电网的相关技术,例如面向智能电网常见攻击的高准确度仲裁模型和符合应用场景的调度方式;最后要将相关技术结合得到针对性的智能电网 DHR 组件原型。

计算机工程 www.ecice06.com

表 2 DHR 技术方案对比

Table 2 Comparison of DHR technical schemes

技术方案	年份	防护目标	主要局限	部署要求	作用层级
WANG 等[89]提出的技术方案	2023	更细粒度地选择可信消息	仲裁为毫秒级，耗时高于经典方法	需要异构服务器、容器编排、中间件、训练数据和在线推理	组件层、功能层、通信层
FBAMD[90]	2024	高准确率仲裁，并及时更新子模型	依赖所选训练数据、投毒方式、阈值和子模型	需要高质量的训练数据、准确度较高的子模型	组件层、功能层、通信层
HU 等[91]提出的技术方案	2018	主动识别并重启异常变体以维持转发服务	不能直接防御资源耗尽 DoS/DDoS 或所有执行体共有的协议缺陷	要求不同执行体输出可比较	组件层、功能层、通信层

2.1.3 基于 PUF 的可信密钥交换与认证机制

基于 PUF 的可信密钥交换与认证机制是指依托 PUF 的硬件原生唯一性，通过提取终端硬件的物理随机特性生成与硬件深度绑定的动态密钥，无需预配置密钥或依赖外部密钥管理体系的相关技术。PUF 相关认证的研究目前有 5 个主流方向，分别是利用新型 PUF 观测量进行认证，从传统片上 PUF 扩展到外部可观测物理特征，实现无接触认证或硬件证明，例如 MAG-PUFs[92]；分层、批量和可扩展认证，面向大规模 AMI，研究批量验证、网关聚合和边云卸载，例如 LIU 等[93]提出的技术方案；噪声响应重构与稳定密钥生成，以解决同一 PUF 在温度、电压、噪声和老化条件下响应不一致的问题，例如 PAC[94]；面向受限终端实现轻量化的 PUF 密钥协商与认证协议，例如 PPSG[95]；将 AI 与 PUF 融合，使用机器学习进行指纹分类、响应纠错和模型压缩，例如 LPUF-AuthNet[96]。

但是，上述研究方向并非完全独立的，而是相互融合的。MAG-PUFs[92]利用物联网设备执行参考函数时的无意电磁辐射作为 PUF，并结合了深度学习模型实现认证，这体现了新型 PUF 观测量与 AI 方法的融合。PAC[94]则是将轻量化的思路融入噪声响应重构与稳定密钥生成，利用 PUF 抵御物理攻击，通过模糊提取器处理 PUF 输出噪声以稳定恢复共享密钥。

表 3 从防护目标、主要局限、部署要求以及作用层级 4 个方面对基于 PUF 的可信密钥交换与认证机制技术进行了总结。从表 3 中可以发现，当前的 PUF 可信密钥交换与认证技术实验普遍缺少在实际场景下的测试验证，而利用新型 PUF 观测量进行认证同样受到不同物理条件下获得的观测量的影响，AI 和 PUF 相结合则需要注意训练数据的获取和规模。由于 PUF 技术本身对智能电网的适配度相对较高，在物联网等相关领域中的应用较为广泛，因此在智能电网中部署相关技术的关键在于末端组件的适应性改造，以及对相关技术方案的大规模验证。同时，由于智能电网的末端设备往往资源受限，轻量化无疑是 PUF 相关技术未来在智能电网中的重要发展方向，其他方向都应当结合轻量化来进行研究。

表 3 基于 PUF 的可信密钥交换与认证机制技术方案对比

Table 3 Comparison of trusted key exchange and authentication mechanism technical schemes based on PUF

技术方案	年份	防护目标	主要局限	部署要求	作用层级
MAG-PUFs[92]	2024	利用设备执行参考函数时的无意电磁辐射识别授权设备和冒充设备	射频干扰、部署位置和探头位置等会影响结果	需要近场探头、RTL-SDR、固定天线位置和外部分类器	组件层、通信层
LIU 等[93]提出的技术方案	2022	面向智能电表、网络网关和服务提供者之间的冒充、重放、窃听、中间人和物理攻击	实验验证并非大规模 AMI 现场	电表和网关需 SRAM PUF、模糊提取器及安全注册，网关需批量认证逻辑	组件层、通信层
PAC[94]	2021	面向计量数据采集中的中间人、重放、冒充、窃听和用户用电数据泄露，验证控制中心请求和智能电表数据来源	实验将软件平台与引用的 PUF 仿真组合，不能视为完整智能电表硬件测量	需要模糊提取器、控制中心注册信息和可靠时间戳	组件层、通信层
PPSG[95]	2024	防护智能电网设备冒充、重放、中间人、会话密钥泄露和物理克隆	性能数据未覆盖海量智能电表并发、PUF 环境漂移	需要在目标智能电表芯片上重新测量代码体积、能耗、并发和网络重传	组件层、通信层
LPUF-AuthNet[96]	2024	识别伪造逻辑挑战/响应和设备冒充	依赖大量特定训练数据，可应用规模受限	需要离线训练、模型分发和持续更新	组件层、通信层

计算机工程 www.ccicon.com

2.1.4 抗攻击路由

抗攻击路由是指通过密钥管理、节点可信性判断、主动探测或多约束选路等机制，限制恶意节点参与路由建立和数据转发，或者降低攻击路径对通信业务的影响。现有研究可以分为 4 个方向：分组密钥管理与安全入网，以 BONDADA 等[97]提出的技术方案为例；基于信任与机器学习的恶意节点识别，以 BURANGE 等[98]提出的技术方案为例；利用路由控制报文实施主动探测，以 NAKANO 等[99]提出的技术方案为例；面向电力通信骨干网的多约束安全选路，以 XIE 等[100]提出的技术方案为例。4 个方向分别从密钥保护、节点参与资格、路由控制过程和传输路径实现了对智能电网的保护。

分组密钥管理方向通过集中或分层的密钥节点约束节点入网和路由参与。BONDADA 等[97]提出基于无线自组网按需距离矢量路由协议(AODV)和分组密钥管理的安全节能路由方案，相较基准方案包投递率提升 2.84%、吞吐量提升 1.93%，通信开销与能耗分别降低 3.16%与 1.35%。信任与机器学习方向依据历史行为、位置和接收信号强度指示(RSSI)等特征识别恶意节点。BURANGE 等[98]提出融合信任管理的轻量抗攻击路由模型，针对虫洞、女巫、秩攻击威胁检测准确率达 95.80%，假阳性率仅 0.51%。主动探测方向通过构造异常路由请求暴露黑洞节点。NAKANO 等[99]提出基于路由请求数据包的轻量级黑洞攻击防御方法，在黑洞攻击下，数据包到达率仍保持 100%。多约束安全选路方向面向电力通信自动交换光网络(ASON)，在带宽、时延和健康度等条件下选择路径。XIE 等[100]提出基于多约束 Dijkstra 算法的针对 ASON 的抗攻击方案，在攻击场景下传输误码率控制在 0.298%以内，相较传统方案下降 16.53%。

表 4 从防护目标、主要局限、部署要求和作用层级 4 个方面总结抗攻击路由技术。分析上述技术方案的主要局限性可以发现，当前技术所面临的主要问题是检测的准确率和效率。伴随着机器学习等 AI 方法的加入，后续检测准确率和效率的问题可能逐步变为如何提供大量优质的训练数据的问题。而智能电网中存在的网络类型较为丰富，覆盖面也较广，因此能够提供数量庞大的数据，具有一定的优势，这也为抗攻击路由技术应用到智能电网中提供了便利。同时，现有研究主要针对的是特定网络结构，例如移动自组织网络(MANET)等，因此应用相关技术还需要对实际智能电网的网络结构进行适配性改造。

表 4 抗攻击路由技术方案对比

Table 4 Comparison of attack-resistant routing technical schemes

技术方案	年份	防护目标	主要局限	部署要求	作用层级
BONDADA 等[97]提出的技术方案	2022	降低普通节点被攻陷后对全网密钥的影响	开放网络环境中，信任评估指标容易受到包括合谋攻击在内的攻击干扰，难以准确识别恶意节点行为	需要 AODV 扩展、节点注册、分组密钥分发以及 CK/DK 冗余保护	通信层
BURANGE 等[98]提出的技术方案	2025	检测网络中的虫洞、女巫和秩攻击，并区分正常节点与攻击节点	依赖训练数据、历史信任和阈值，仿真仍存在误报与漏报	需要持续采集信任特征训练和更新模型，并校准隔离策略	通信层、信息层
NAKANO 等[99]提出的技术方案	2023	主动检测黑洞节点，并通过路由请求数据包清除路由和重建路径	增加控制报文和往返时延，频繁链路中断或不兼容节点可能影响检测	需要修改 AODV、维护黑名单，并限制探测频率和生存时间范围	通信层
XIE 等[100]提出的技术方案	2023	降低攻击导致的恶意丢包、路由混乱和传输误码	未提供形式化的安全证明或形式化验证，仅通过仿真实验验证方案有效性	需要按电力业务配置约束参数	通信层

2.1.5 抗攻击内生安全技术优势

抗攻击内生安全技术相较于传统事件驱动的被动防御，将主动权掌握在防御方手中。软件多样化和 DHR 共同构成有效监测未知攻击的关键屏障：针对漏洞利用攻击的零日漏洞与特征库滞后问题，通过分析异构执行体运行结果的差异实现及时识别；针对 APT 攻击，通过动态检测与分析实时识别和阻断攻击链。基于 PUF 的可信密钥交换与认证机制通过与组件物理属性的深度绑定，有效遏制数据伪造与篡改，尤其对重放攻击和硬件克隆具有较强防御能力。抗攻击路由将信任机制融入路由协议，从根源上提升网络的安全等级与风险预测能力。

2.2 可信认证内生安全技术

可信认证内生安全技术包括零信任架构、可信计算和量子安全可信认证技术。零信任是一种持续身份与访问治理架构，可信计算以可信根、度量和证

计算机工程 www.ecice06.com

明建立平台状态证据，量子安全可信认证技术则通过后量子密码(PQC)、量子密钥分发(QKD)或量子态协议保护密钥与认证过程。

2.2.1 零信任架构

零信任架构遵循“从不默认信任、持续验证和最小权限”原则，根据身份、设备状态、行为和环境属性动态决定访问权限。现有智能电网相关研究可以分为 4 个方向：上下文感知的信任与风险评估，把用户身份、设备身份和网络环境等上下文信号转化为动态信任或风险值，为每次访问提供决策依据，以 BHATTARAI 等[101-102]提出的技术方案为例；属性驱动的动态访问控制，将身份认证、资源敏感度和环境风险等转化为授权策略，并以此来控制访问，以 LÜ 等[103]提出的技术方案为例；面向智能电网操作技术(OT)微服务的威胁建模与安全控制组合，以 STANOJEVIC 等[104]提出的技术方案为例；依托新一代网络基础设施，将零信任安全策略下沉至电力接入网与边缘节点，以 ALIPOUR 等[105]提出的技术方案为例。

上下文感知的信任与风险评估方向通过多项设备和访问属性形成授权依据。BHATTARAI 等[101]提出一种基于模糊逻辑的信任评分零信任架构以保护 AMI 安全。BHATTARAI 等[102]提出适用于智能电网 AMI 的基于信任分数的零信任架构，定义 15 类信任属性，融合多项属性基实现访问控制。属性驱动的动态访问控制则将多重认证、权限分级、动态策略和信任评价结合。LÜ 等[103]基于身份验证、认证令牌和访问策略，结合电网云的特性，提出了基于零信任模型的访问控制框架。OT 微服务方向从威胁和服务间访问关系出发配置控制措施。STANOJEVIC 等[104]针对微服务架构的智能电网 OT 系统，以零信任原则为核心构建安全防护体系。新一代网络基础设施协同方向试图利用 5G、承载网和网络切片等技术实现策略决策点下沉。ALIPOUR 等[105]给出了面向 5G 赋能的智能电网零信任体系结构和部署前提。

表 5 从防护目标、主要局限、部署要求和作用层级 4 个方面总结零信任架构技术。上述技术所面临的主要局限性可以统一概括为如何降低大规模部署场景下的性能开销以及缺少在真实网络环境下的应用验证。这对智能电网部署零信任架构而言是一种挑战。智能电网由于本身用户数量庞大，实时性要求较高，过高的性能开销所带来的服务延迟是难以接受的。但同样，智能电网也能够提供丰富的可用于认证和识别的结构特征和行为特征，这为其部署也提供了便利。因此，后续的零信任架构方案发展方向应当集中于如何降低部署后的性能开销，以及在智能电网的真实场景下进行测试。

表 5 零信任架构技术方案对比

Table 5 Comparison of zero trust architecture technical schemes

技术方案	年份	防护目标	主要局限	部署要求	作用层级
BHATTARAI 等[101]提出的技术方案	2025	阻止未授权 AMI 访问，包括被篡改设备、异常访问和身份不一致	模糊推理系统层数增多时计算开销急剧增长	需要适配智能电表和网关的属性采集功能，并实现规则与信任阈值持续校准	组件层、信息层、功能层
BHATTARAI 等[102]提出的技术方案	2024	防止异常身份或设备继续接入 AMI	采用的静态规则缺乏动态适应能力	需要统一设备属性标准，并设置可动态更新的信任评分机制	组件层、信息层、功能层
LÜ 等[103]提出的技术方案	2023	防护电网云中的未授权访问和恶意交互	在大规模部署场景下的性能和可扩展性方面存在不足	需要适配现有云平台的身份认证和访问控制体系，并解决大规模策略管理问题	组件层、业务层、功能层
STANOJEVIC 等[104]提出的技术方案	2023	分析和防范员工或可信第三方滥用权限的内部威胁	在微服务环境中的部署会带来显著的性能开销	需要适配微服务身份、权限和网络隔离机制	信息层、业务层、功能层

2.2.2 可信计算

可信计算以可信根为起点，通过可信启动、隔离执行、完整性度量、远程证明和安全更新建立可验证的平台状态。现有研究可以分为 4 个方向：面向低端嵌入式设备的软件可信执行、远程证明与安全更新，以 PISTIS[106]为例；通过独立可信子系统建立硬件可信根和可信启动链，以 ZHENG 等[107]提出的技术方案为例；利用片上存储器上电特征生成设备根秘密并提供密封存储，以 ZHAO 等[108]提出的技术方案为例；根据协议行为、数据质量和历史交互开展运行期信任评估，以 BOAKYE-BOATENG 等[109]提出的技术方案和 CRTC[110]为例。前 3 个方向属于严格意义上的可信计算，最后 1 个方向则提供关联的行为信任证据。

计算机工程 www.ecice06.com

软件可信执行方向试图在缺少可信平台模块和复杂操作系统的设备上提供可信能力。PISTIS[106]为纯软件可信计算架构,适用于裸金属低端嵌入式设备,整体运行时平均开销提升约 52.72%,但部署效率提升 73.63%。硬件可信启动方向通过独立可信 CPU、静态随机存取存储器(SRAM)和密码引擎先于普通处理器建立信任链。ZHENG 等[107]设计了由传统计算子系统与可信计算子系统构成的可信计算双架构,AES-256 加密速率达软件实现的 12 倍,ECDSA 签名与验证运算速度提升 2.8 倍。片上存储可信根方向利用 SRAM 上电差异派生密钥和随机数。ZHAO 等[108]利用片上 SRAM 的 PUF 特性构建可信根,总代码仅 180 KB,密封和解封的平均耗时分别约为 20、50 ms。运行期行为信任方向通过协议和交互数据补充平台状态。BOAKYE-BOATENG 等[109]提出了含信任模型、风险态势模型与信任可迁移性模型的变电站防御框架,对基于 Modbus 等协议的攻击检测率达 75%,可信设备响应时延低于 10 ms。CRTC[110]作为云辅助可靠信任计算方案,使无人机(UAV)收集信息的飞行路径距离减少 64.40%,聚合节点信任选择准确率达 100%。

表 6 从防护目标、主要局限、部署要求和作用层级 4 个方面总结可信计算技术。通过分析上述技术的主要局限可以发现,当前主要的问题在于应用场景受限以及对安全隐患的考虑不全面。然而,对于智能电网而言,可信计算往往应用于组件层的终端设备,这些设备往往资源受限且区域内较为统一。因此,场景受限不会对可信计算在智能电网中的部署产生太大影响,而安全考虑不够全面则需要后续研究进行补充。同时,可信计算对于部署设备的相关组件要求较高,现有的设备可能难以满足需要,而专用设备改造成本和大批量更换成本可能较高。这也是可信计算目前大规模应用于智能电网的阻碍之一。

表 6 可信计算技术方案对比

Table 6 Comparison of trusted computing technical schemes

技术方案	年份	防护目标	主要局限	部署要求	作用层级
PISTIS[106]	2022	防护固件篡改、未经授权代码更新和内存访问破坏	不支持自修改代码,灵活性较差	需要修改编译、链接、初始部署和固件更新流程,并配置证明与验证服务	组件层
ZHENG 等[107]提出的技术方案	2023	阻止启动固件篡改及可信根绕过	仅针对资源受限的嵌入式设备	需要可信 CPU、SRAM 和高优先级互连	组件层
ZHAO 等[108]提出的技术方案	2021	提供密封、解封等可信计算原语,降低设备密钥伪造风险	未详细讨论物理攻击防护	需要可读取的片上 SRAM、熵评估、模糊提取和设备注册	组件层
BOAKYE-BOATENG 等[109]提出的技术方案	2024	检测重放攻击、洪泛攻击、数据包操纵和被替换或受损的智能电子设备	对新接入设备难以建立准确信任评估,可能导致恶意设备未被及时检测	需要正常协议基线、阈值、中央代理、SCADA 日志和风险映射	组件层
CRTC[110]	2022	通过检查信息追踪数据包路径和节点行为,识别数据丢弃、伪造或篡改节点	假设 UAV 可信但未讨论 UAV 自身安全保证	需要检查节点、UAV、云端信任推理、路径追踪和信任拟合	组件层、通信层

2.2.3 量子安全可信认证技术

量子安全可信认证技术至少包含 3 条不同技术路线:基于 PQC 的可信认证技术,例如 MAKe[111];QKD 通过量子信道生成或分发对窃听可检测的对称密钥,但仍需经典认证机制,例如 GRICE 等[112]、AGGARWAL 等[113]和 PARAMESWARATH 等[114]提出的技术方案;量子态认证或密钥协商直接使用量子态制备、测量或纠缠操作完成协议,例如 JIANG 等[115]提出的技术方案。

基于 PQC 的可信认证技术主要是在现有密码体制的基础上,选取格等能够有效对抗量子计算的数学问题,从而取代不具备量子安全性的密码体制。MAKe[111]是面向智能电表通信场景提出的基于格上的短整数解(SIS)和非齐次短整数解(ISIS)困难问题的轻量级抗量子双向认证与密钥交换方案,相比同类方案能耗降低 22.07%,计算开销降低 76.28%,存储和通信成本降低 51.48%。基于 QKD 的可信认证技术则是将自身窃听可检测的性质与经典的认证技术相结合,进一步提升认证技术的安全性和可靠性。GRICE 等[112]系统评估了 QKD 在智能电网 18 类应用场景中的适用性,指出多数电网通信链路长度足以支持无量子中继的单链路 QKD 部署。AGGARWAL 等[113]设计了用于管理 QKD 密钥对的光纤区块链网络,实现基于消息队列遥测传输协议(MQTT)的 SCADA 通信认证,相比传统 PUF 协议显著降低数据处理时间,在时延

计算机工程 www.ecice06.com

敏感的电网场景中具有显著优势。PARAMESWARATH 等[114]提出了基于 QKD 和量子随机数发生器的智能电表量子安全双向认证协议，相比最优轻量化椭圆曲线协议，耗时明显降低。量子态认证方向目前仍处于早期的研究阶段，尚无成熟技术或原型。JIANG 等[115]利用贝尔态量子纠缠特性设计了面向智能电网环境的轻量级量子认证与密钥协商方案，在量子效率维持主流 50%水平的情况下，计算开销远低于采用对称加密的同类方案，但尚无真实量子硬件和链路损耗实验。

表 7 从防护目标、主要局限、部署要求和作用层级 4 个方面总结量子安全可信认证技术。由于当前的量子相关技术大多仍然处于研究阶段，相关的设施有限，因此 QKD 面临着难以开展大规模实验的困境，量子态协议则面临着量子制备相关设施稀缺的困境。相比而言，PQC 目前的实用性更强。PQC 采用基于纯软件的协议，能够有效规避上述硬件设施缺失所带来的部署问题，虽然仍需要在真实的通信环境中进行测试，但是能够较快提升智能电网的量子安全性，为后续逐步应用其他技术节省了成本和时间。

表 7 量子安全可信认证技术方案对比

Table 7 Comparison of quantum-safe trusted authentication technical schemes

技术方案	年份	防护目标	主要局限	部署要求	作用层级
MAKe[111]	2024	抵抗冒充、重放、中间人、密钥泄露及量子计算攻击	仅通过理论分析和仿真验证，缺乏在真实电网通信环境中的硬件在环测试	需要 PQC 参数、证书和协议迁移，并在目标终端测量代码、能耗和并发	通信层
AGGARWAL 等[113]提出的技术方案	2024	防止冒充、窃听和篡改日志或交易	区块链共识机制引入的额外时延可能无法满足电网继电保护等毫秒级实时通信要求	需要 QKD 链路、区块链节点、证书和持续运维	组件层、通信层
PARAMESWARATH 等[114]提出的技术方案	2024	抵抗量子计算、窃听、重放、冒充、临时秘密泄露和会话密钥泄露	实验规模有限，未评估大规模设备并发认证场景下的性能退化	需要量子发射与测量设备、光纤、经典认证和故障回退	通信层、信息层
JIANG 等[115]提出的技术方案	2025	抵抗窃听、冒充、重放和降低量子信道噪声带来的影响	对信道噪声的鲁棒性尚未在大尺度网络中验证	需要 Bell 态制备、量子测量、纠缠交换、同步、诱骗光子和经典校验	组件层、通信层

2.2.4 可信认证内生安全技术优势

可信认证内生安全技术将可信认证融入智能电网系统内部，使系统具备对网络节点、终端设备及接入用户的信任管理能力。零信任架构通过持续访问控制与动态信任评估，即使攻击者攻入关键节点也难以直接获取机密数据。可信计算将防护延伸至底层设备，通过可信启动、运行时校验等机制全周期保障设备可信度，并可及时探测攻击的出现。量子安全可信认证技术则面向量子时代，对未来量子计算机可能产生的攻击提前部署反制手段。

3 未来研究方向讨论

表 8 对智能电网可部署内生安全技术进行了汇总。结合表 8 及前文分析，现有研究主要存在三方面问题：一是单项技术通常只作用于攻击过程的局部环节，难以独立应对 APT 等复合攻击；二是设备、身份、网络和软件供应链信息尚未形成统一可信依据，技术之间难以联动；三是 AI 和量子安全技术在提升防护能力的同时，也带来模型安全和密码迁移问题。基于此，本文从技术协同、供应链安全、AI 应用和量子安全迁移 4 个方面讨论后续研究重点。

表 8 内生安全技术对比

Table 8 Comparison of endogenous security technologies

技术类型	技术名称	抗攻击类型
抗攻击内生安全技术	软件多样化	漏洞利用攻击
	DHR	漏洞利用攻击
	基于 PUF 的可信密钥交换与认证机制	物理与侧信道攻击、数据篡改与伪造攻击
	抗攻击路由	DDoS/DoS 攻击、数据篡改与伪造攻击
可信认证内生安全技术	零信任架构	漏洞利用攻击、DDoS/DoS 攻击、数据篡改与伪造攻击
	可信计算	漏洞利用攻击、数据篡改与伪造攻击、物理与侧信道攻击
	量子安全可信认证技术	数据篡改与伪造攻击

计算机工程 www.ecice06.com

3.1 内生安全技术的协同应用

APT 通常经历初始访问、权限维持、横向移动、IT/OT 跨域渗透以及控制或物理影响等阶段。软件多样化与 DHR 可降低漏洞被稳定利用的概率，PUF 认证和可信计算可提供设备身份与状态依据，零信任可限制横向移动和权限扩张，抗攻击路由可维持节点间通信，量子安全可信认证技术可保护长期密钥。由此可见，多技术协同的关键不在于简单叠加，而在于按照攻击阶段明确技术分工，并共享身份、设备状态、异常输出和网络状态等信息。后续研究应重点解决信息格式统一、状态同步、策略冲突和故障恢复问题，并以攻击链阻断率、误判率、最坏时延和恢复时间评价协同效果。

3.2 供应链安全与内生安全技术协同

供应链安全是内生安全技术可靠运行的基础。软件多样化依赖可信编译链，DHR 依赖执行体来源，PUF 认证依赖制造与注册过程，零信任和可信计算依赖准确的资产及固件信息。YURREBASO 等[116]基于 IEC 61850 SCD 文件和 CycloneDX 构建变电站物料清单，验证了设备、固件和服务依赖提取及漏洞关联，为保障内生安全技术的供应链安全提供了思路。后续研究应将资产清单、固件签名、远程证明、隔离、替换和回滚贯通，形成从组件识别、完整性验证到异常处置的闭环，并重点评价资产识别完整率、漏洞关联准确率和回滚成功率。

3.3 AI 应用与模型安全

AI 可辅助动态冗余裁决、零信任评分、恶意路由识别、可信状态分析和 PUF 认证。以日志分析为例，基于大语言模型的日志异常检测已在软件运维领域取得显著进展，陈昕等[117]将现有方法归纳为 5 类技术路线，其中大小模型协同架构兼顾推理效率与工业可部署性，可为智能电网调度系统、SCADA 及终端设备的日志智能异常检测提供方法借鉴。但是，AI 本身也并非完全安全可靠。文献[118]指出，AI 模型也面临着包括数据投毒、模型投毒和对抗样本等在内的风险。因此，相关研究不应只关注检测准确率，还应同时保证模型和数据安全。评价时应报告数据来源、类别平衡、训练与测试范围、误报漏报、推理时延、资源占用和更新方式，并利用软件多样化、DHR、可信计算和零信任等内生安全技术保护模型执行、训练数据、推理环境及更新过程。表 9 列出了可用于相关研究的公开数据资源。

表 9 面向 AI 辅助内生安全研究的公开数据资源

Table 9 Public data resources for AI-assisted endogenous security research

数据资源	数据内容	链接
Sherlock Power Grid IDS Dataset	仿真智能电网网络流量、物理量及攻击标签；支持 IDS 和跨层异常检测	https://sherlock.wattson.it/
UCI Electrical Grid Stability Simulated Data	四节点电网稳定性参数及标签，支持稳定性分类	https://archive.ics.uci.edu/dataset/471/electrical-grid-stability-simulated-data
CSE-CIC-IDS2018	企业 IT 网络流量及攻击标签，支持通用 IDS 方法验证	https://www.unb.ca/cic/datasets/ids-2018.html
ASCAD Side-Channel Dataset	AES 实现侧信道轨迹，支持密码实现泄露分析	https://github.com/ANSSI-FR/ASCAD
Open Power System Data	欧洲负荷、发电和市场时间序列；支持正常基线或异常建模	https://open-power-system-data.org/
DSCAD: Dilithium Side-Channel Attacks Dataset	Dilithium 实现侧信道轨迹，支持 PQC 泄露分析	https://www.scidb.cn/en/detail dataSetId=2e16c759868548f9ab6079a54189fb7b

3.4 量子安全技术的渐进迁移

量子安全技术应采用渐进迁移方式。对于 PQC 相关技术的应用，首先要盘点零信任、可信启动、固件签名、路由认证和密钥交换中的现有密码算法，建立证书、密钥和算法可替换的密码敏捷机制；其次在智能电表、网关和通信协议中验证 PQC 或混合认证方案，量化认证时延、报文长度、存储占用、能耗、并发规模和故障回退时间。对于 QKD 相关技术，宜优先用于固定的高价值链路，因为其应用目前仍受光纤、距离和成本限制。由于现有量子安全研究多处于原型、概念验证或仿真阶段，后续研究应重点解决协议兼容、密钥更新和实际部署问题，并依据实测结果逐步扩大应用范围。

4 结束语

本文对当前智能电网所面临的攻击威胁进行了分析，结合典型攻击案例和近年来的相关研究，指出当前的传统防御手段所存在的局限性。随后本文针对智能电网主要网络威胁，系统梳理智能电网可部署的 7 类内生安全技术，并比较其作用机制、验证结

计算机工程 www.ecice06.com

果和应用条件。综合分析表明,单项技术只能覆盖攻击过程的部分环节,后续研究应以攻击阶段为线索加强技术协同,并将供应链安全纳入技术设计和运行过程。同时,AI 与内生安全相结合需兼顾识别能力与模型安全,量子安全内生安全技术应按当前的实际发展状况分阶段迁移。

参考文献

[1] GRID 2030: a national vision for electricity's second 100 years[EB/OL]. [2026-04-22]. https://www.energy.gov/oe/articles/grid-2030-national-vision-electricitys-second-100-years.

[2] 邬江兴. 论网络空间内生安全问题及对策[J]. 中国科学: 信息科学, 2022, 52(10): 1929-1937.
WU J X. Cyberspace's endogenous safety and security problem and the countermeasures [J]. Scientia Sinica (Informationis), 2022, 52(10): 1929-1937. (in Chinese)

[3] WU J X. Cyberspace endogenous safety and security[J]. Engineering, 2022, 15: 179-185.

[4] 邬江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(2): 189-204.
WU J X. Development paradigms of cyberspace endogenous safety and security[J]. Scientia Sinica (Informationis), 2022, 52(2): 189-204. (in Chinese)

[5] SANTODOMINGO R, USLAR M, GÖRING A, et al. SGAM-based methodology to analyse Smart Grid solutions in DISCERN European research project[C]//Proceedings of the IEEE International Energy Conference (ENERGYCON). Washington D.C., USA: IEEE Press: IEEE Press, 2014: 751-758.

[6] DUMAN O, GHAFOURI M, KASSOUF M, et al. Modeling supply chain attacks in IEC 61850 substations[C]//Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). Washington D.C., USA: IEEE Press, 2019: 1-6.

[7] ESET. ESET researchers discover links between two major cybersecurity attacks: NotPetya and Industroyer[EB/OL]. [2026-04-22]. https://www.eset.com/ca/about/newsroom/press-releases/eset-researchers-discover-links-between-two-major-cybersecurity-attacks-notpetya-and-industroyer/.

[8] FAYI S Y A. What Petya/NotPetya ransomware is and what its remidiations are?[M]. Cham, Switzerland: Springer International Publishing, 2018: 93-100.

[9] ALKHADRA R, ABUZAID J, ALSHAMMARI M, et al. Solar winds hack: in-depth analysis and countermeasures[C]// Proceedings of the 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). Washington D.C., USA: IEEE Press, 2021: 1-7.

[10] SADEGHI A R, WACHSMANN C, WAIDNER M. Security and privacy challenges in industrial Internet of Things[C]//Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). Washington D.C., USA: IEEE Press, 2015: 1-6.

[11] PACHECO J, HARIRI S. IoT security framework for smart cyber infrastructures[C]//Proceedings of the IEEE 1st International Workshops on Foundations and Applications of Self * Systems (FAS * W). Washington D.C., USA: IEEE Press, 2016: 242-247.

[12] RAO V V, MARSHAL R, GOBINATH K. The IoT supply chain attack trends-vulnerabilities and preventive measures[C]//Proceedings of the 4th International Conference on Security and Privacy (ISEA-ISAP). Dhanbad, India: IEEE Press, 2022: 1-4.

[13] KUROPTEV K, STEINKE F. Coordinated cyber attacks on smart grids considering software supply chains[C]// Proceedings of the IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE). Grenoble, France: IEEE Press, 2024: 1-5.

[14] TAN Z R, PARAMBATH S P, ANAGNOSTOPOULOS C, et al. Advanced persistent threats based on supply chain vulnerabilities: challenges, solutions, and future directions [J]. IEEE Internet of Things Journal, 2025, 12(6): 6371-6395.

[15] SHEN Y J, GAO X, SUN H L, et al. Understanding vulnerabilities in software supply chains[J]. Empirical Software Engineering, 2024, 30(1): 20.

[16] MEHTA D, LU H W, PARADIS O P, et al. The big hack explained: detection and prevention of PCB supply chain implants[J]. ACM Journal on Emerging Technologies in Computing Systems, 2020, 16(4): 1-25.

[17] BIERNACKI L, GALLAGHER M, XU Z X, et al. Software-driven security attacks: from vulnerability sources to durable hardware defenses[J]. ACM Journal on Emerging Technologies in Computing Systems, 2021, 17(3): 1-38.

[18] MARTÍNEZ J, DURÁN J M. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study[J]. International Journal of Safety and Security Engineering, 2021, 11(5): 537-545.

[19] PRZYMUS P, DURIEUX T. Wolves in the repository: a software engineering analysis of the XZ Utils supply chain attack [C] // Proceedings of the IEEE/ACM 22nd International Conference on Mining Software Repositories (MSR). Ottawa, Canada: IEEE Press, 2025: 91-102.

[20] 纪守领, 王琴应, 陈安莹, 等. 开源软件供应链安全研究综述[J]. 软件学报, 2023, 34(3): 1330-1364.
JI S L, WANG Q Y, CHEN A Y, et al. Survey on open-source software supply chain security[J]. Journal of Software, 2023, 34(3): 1330-1364. (in Chinese)

[21] ENCK W, WILLIAMS L. Top five challenges in software supply chain security: observations from 30 industry and government organizations[J]. IEEE Security & Privacy, 2022, 20(2): 96-100.

[22] BOYENS J M. Cybersecurity supply chain risk management practices for systems and organizations: NIST SP 800-161r1-upd1[R]. Gaithersburg, USA: National Institute of Standards and Technology, 2024.

[23] National Institute of Standards and Technology. CVE-2022-29303[EB/OL]. [2025-12-26]. https://nvd.nist.gov/vuln/detail/CVE-2022-29303.

[24] Japan Vulnerability Notes. JVNVU#92327282: multiple vulnerabilities in contec solarview compact [EB/OL]. [2025-12-26]. https://jvn.jp/vu/JVNVU92327282/.

[25] National Institute of Standards and Technology. CVE-2018-8453[EB/OL]. [2025-12-27]. https://nvd.nist.gov/vuln/detail/CVE-2018-8453.

[26] MATHAS C M, VASSILAKIS C, KOLOKOTRONIS N, et al. On the design of IoT security: analysis of software vulnerabilities for smart grids[J]. Energies, 2021, 14(10): 2818.

[27] TEFEK U, ESINER E, CHEH C, et al. A smart grid ontology: vulnerabilities, attacks, and security policies[C]// Proceedings of the IEEE Conference on Communications and Network Security (CNS). Orlando, USA: IEEE Press, 2023: 1-6.

[28] DUY LE T, GE M M, THE DUY P, et al. CVSS based attack analysis using a graphical security model: review and smart grid case study[M]. Cham, Switzerland: Springer International Publishing, 2021.

计算机工程 www.ecice06.com

[29] SANDE-RÍOS J, CANAL-SÁNCHEZ J, MANZANO-HERNÁNDEZ C, et al. Threat analysis and adversarial model for smart grids [C] // Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Vienna, Austria: IEEE Press, 2024: 130-145.
[30] AHMAD R, ALSMADI I, ALHAMDANI W, et al. Zero-day attack detection: a systematic literature review [J]. Artificial Intelligence Review, 2023, 56(10): 10733-10811.
[31] ZAIB R, ZHOU K Q. Zero-day vulnerabilities: unveiling the threat landscape in network security[J]. Mesopotamian Journal of CyberSecurity, 2022, 2(1): 57-64.
[32] JOHNSON A, HADDAD R J. Evading signature-based antivirus software using custom reverse shell exploit[C]// Proceedings of the SoutheastCon 2021. Atlanta, USA: IEEE Press, 2021: 1-6.
[33] DÍAZ-VERDEJO J, MUÑOZ-CALLE J, ALONSO A E, et al. On the detection capabilities of signature-based intrusion detection systems in the context of Web attacks [J]. Applied Sciences, 2022, 12(2): 852.
[34] UTTARKAR A R, VANJALE S, RAJPOOT P. A comprehensive review and novel approach for detection of zero day vulnerabilities[C]//Proceedings of the IEEE Pune Section International Conference (PuneCon). Pune, India: IEEE Press, 2025: 1-6.
[35] GUO W, ZHANG Z, CHANG L Y, et al. A DDoS tracking scheme utilizing adaptive beam search with unmanned aerial vehicles in smart grid[J]. Drones, 2024, 8(9): 437.
[36] ACARALI D, RAJESH RAO K, RAJARAJAN M, et al. Modelling smart grid IT-OT dependencies for DDoS impact propagation [J]. Computers & Security, 2022, 112: 102528.
[37] SGOURAS K I, BIRDA A D, LABRIDIS D P. Cyber attack impact on critical smart grid infrastructures [C]// Proceedings of the ISGT 2014. Washington D.C., USA: IEEE Press, 2014: 1-5.
[38] HUSEINOVIĆ A, MRDOVIĆ S, BICAKCI K, et al. A survey of denial-of-service attacks and solutions in the smart grid[J]. IEEE Access, 2020, 8: 177447-177470.
[39] AAMIR M, ALI ZAIDI M. A survey on DDoS attack and defense strategies: from traditional schemes to current techniques [J]. Interdisciplinary Information Sciences, 2013, 19(2): 173-200.
[40] CHAHAL J K, BHANDARI A, BEHAL S. Distributed denial of service attacks: a threat or challenge [J]. New Review of Information Networking, 2019, 24(1): 31-103.
[41] AGRAWAL N, TAPASWI S. Defense mechanisms against DDoS attacks in a cloud computing environment: state-of-the-art and research challenges[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3769-3795.
[42] SINGH A, GUPTA B B. Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions[J]. International Journal on Semantic Web and Information Systems (IJSWIS), 2022, 18(1): 1-43.
[43] BONGUET A, BELLAICHE M. A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing[J]. Future Internet, 2017, 9(3): 43.
[44] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security, 2011, 14(1): 1-33.
[45] HABIB A A, HASAN M K, ALKHAYYAT A, et al. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction [J]. Computers and Electrical Engineering, 2023, 107: 108638.
[46] WANG S Y, BI S Z, ZHANG Y A. Locational detection of the false data injection attack in a smart grid: a multilabel classification approach [J]. IEEE Internet of Things Journal, 2020, 7(9): 8218-8227.
[47] LI Y, WEI X H, LI Y Z, et al. Detection of false data injection attacks in smart grid: a secure federated deep learning approach[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4862-4872.
[48] NIU X Y, LI J N, SUN J Y, et al. Dynamic detection of false data injection attack in smart grid using deep learning[C]// Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Washington D.C., USA: IEEE Press, 2019: 1-6.
[49] RADOGLOU-GRAMMATIKIS P, SARIGIANNIDIS P, GIANNOULAKIS I, et al. Attacking IEC-60870-5-104 SCADA systems [C] // Proceedings of the IEEE World Congress on Services. Milan, Italy: IEEE Press, 2019: 41-46.
[50] CINDRIĆ I, HADJINA T. An analysis of IEC 62351 implementations for securing IEC 60870-5-104 communication [C] // Proceedings of the IEEE Belgrade PowerTech. Belgrade, Serbia: IEEE Press, 2023: 1-6.
[51] TODESCHINI M G, DONDOSSOLA G. Securing IEC 60870-5-104 communications following IEC 62351 standard: lab tests and results [C] // Proceedings of the AEIT International Annual Conference (AEIT). Catania, Italy: IEEE Press, 2020: 1-6.
[52] WANG R R, WEI L S, ZHANG P G. Research on false data injection attack in smart grid based on improved conformer[C]// Proceedings of the 38th Youth Academic Annual Conference of Chinese Association of Automation (YAC). Hefei, China: IEEE Press, 2024: 1318-1322.
[53] XU A D, ZHANG T Y, CHEN L, et al. Research on false data injection attack in smart grid [J]. IOP Conference Series: Earth and Environmental Science, 2021, 693(1): 012010.
[54] GOPE P, SIKDAR B. A reconfigurable and secure firmware updating framework for advanced metering infrastructure[C]// Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). Singapore: IEEE Press, 2022: 453-459.
[55] GOTTUMUKKALA R, MERCHANT R, TAUZIN A, et al. Cyber-physical system security of vehicle charging stations[C]//Proceedings of the IEEE Green Technologies Conference(GreenTech). Lafayette, USA: IEEE Press, 2019: 1-5.
[56] ZHANG H, LIU B, WU H Y. Smart grid cyber-physical attack and defense: a review[J]. IEEE Access, 2021, 9: 29641-29659.
[57] GUI Y T, SIDDIQUI A S, TAMORE S M, et al. Security vulnerabilities of smart meters in smart grid [C] // Proceedings of the 45th Annual Conference of the IEEE Industrial Electronics Society. Lisbon, Portugal: IEEE Press, 2019: 3018-3023.
[58] XU B, ZHAI F, WANG N. Research on security protection strategy for intelligent power terminals[J]. IOP Conference Series: Earth and Environmental Science, 2021, 651(2): 022077.
[59] LU L P, LIU J, ZOU D P, et al. Safety risk analysis and safety protection measures of power distribution Internet of Things [C] // Proceedings of the China International Conference on Electricity Distribution (CICED). Shanghai, China: IEEE Press, 2021: 633-637.
[60] KABBARA N, BELAID M O N, GIBESCU M, et al. Towards software-defined protection, automation, and

计算机工程 www.ciccc.com

control in power systems: concepts, state of the art, and future challenges[J]. Energies, 2022, 15(24): 9362.
[61] TIAN Q, CHENG H, GUO C, et al. A code-based ISE to protect boolean masking in software[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(2): 293-332.
[62] BELAID S, CASSIERS G, MUTSCHLER C, et al. A methodology to achieve provable side-channel security in real-world implementations [EB/OL]. [2026-04-22]. https://eprint.iacr.org/2023/1198.
[63] KIMANI K, ODUOL V, LANGAT K. Cyber security challenges for IoT-based smart grid networks [J]. International Journal of Critical Infrastructure Protection, 2019, 25: 36-49.
[64] E-ISAC/SANS. Analysis of the cyber attack on the Ukrainian power grid[EB/OL]. [2026-04-22]. https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf.
[65] CHEREPANOV A. WIN32/INDUSTROYER: a new threat for industrial control systems[EB/OL]. [2026-04-22]. https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf.
[66] SLOWIK J. CRASHOVERRIDE: reassessing the 2016 Ukraine electric power event as a protection-focused attack [R]. Dragos Inc., 2019.
[67] SLOWIK J. Anatomy of an attack: detecting and defeating CRASHOVERRIDE[R]. Dragos Inc., 2018.
[68] Cybersecurity and Infrastructure Security Agency (CISA). HatMan—safety system targeted malware (update B): MAR-17-352-01 [R]. Dragos Inc., 2018.
[69] DI PINTO A, DRAGONI Y, CARCANO A. TRITON: the first ICS cyber attack on safety instrument systems[C]// Proceedings of the Black Hat USA Conference 2018. Washington D.C., USA: IEEE Press, 2018: 1-26.
[70] XIAO L, LIU H H, LV Z F, et al. Reinforcement-learning-based APT defense for large-scale smart grids[J]. IEEE Internet of Things Journal, 2025, 12(9): 11917-11925.
[71] NAFEES M N, SAXENA N, CARDENAS A, et al. Smart grid cyber-physical situational awareness of complex operational technology attacks: a review [J]. ACM Computing Surveys, 2023, 55(10): 1-36.
[72] AHMAD S, AHN B, ALVEE S R B, et al. Advanced Persistent Threat (APT)-style attack modeling and testbed for power transformer diagnosis system in a substation[C]// Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). New Orleans, USA: IEEE Press, 2022: 1-5.
[73] NING B F, XIAO L. Defense against advanced persistent threats in smart grids: a reinforcement learning approach[C]// Proceedings of the 40th Chinese Control Conference (CCC). Shanghai, China: IEEE Press, 2021: 8598-8603.
[74] BUCHTA R, GKOKTSIS G, HEINE F, et al. Advanced persistent threat attack detection systems: a review of approaches, challenges, and trends[J]. Digital Threats: Research and Practice, 2024, 5(4): 1-37.
[75] MUTALIB N H A, SABRI A Q M, WAHAB A W A, et al. Explainable deep learning approach for Advanced Persistent Threats (APTs) detection in cybersecurity: a review[J]. Artificial Intelligence Review, 2024, 57(11): 297.
[76] DO XUAN C, DAO M H. A novel approach for APT attack detection based on combined deep learning model[J]. Neural Computing and Applications, 2021, 33(20): 13251-13264.
[77] JIANG J Y, JIANG X F, YANG J, et al. Optimal network defense resource allocation against advanced persistent threats [C]// Proceedings of the IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). Chongqing, China: IEEE Press, 2020: 1000-1004.
[78] MAT N I C, JAMIL N, YUSOFF Y, et al. A systematic literature review on advanced persistent threat behaviors and its detection strategy[J]. Journal of Cybersecurity, 2024, 10(1): tyad023.
[79] LI P D, YANG X F, XIONG Q Y, et al. Defending against the advanced persistent threat: an optimal control approach [J]. Security and Communication Networks, 2018(1): 2975376.
[80] MARCHETTI M, PIERAZZI F, COLAJANNI M, et al. Analysis of high volumes of network traffic for Advanced Persistent Threat detection[J]. Computer Networks, 2016, 109: 127-141.
[81] LI Y P, ZHOU Q L, LI B, et al. GuiDiv: mitigating code-reuse attack in an IoT cluster using guided control flow diversification [C]// Proceedings of the IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Exeter, UK: IEEE Press, 2023: 422-433.
[82] CHEN Y C, WANG J C, ZHOU X, et al. Software diversification protection methods for binary programs[C]// Proceedings of the 9th International Conference on Intelligent Computing and Signal Processing (ICSP). Washington D.C., USA: IEEE Press, 2024: 285-291.
[83] SCHLOEGEL M, BLAZYTKO T, CONTAG M, et al. Loki: hardening code obfuscation against automated attacks [C]// Proceedings of the 31st USENIX Security Symposium (USENIX Security 22). Boston, USA: USENIX Association, 2022: 3055-3073.
[84] ZHANG P H, WU C G, PENG M F, et al. Khaos: the impact of inter-procedural code obfuscation on binary diffing techniques [C]// Proceedings of the 21st ACM/IEEE International Symposium on Code Generation and Optimization. New York, USA: ACM Press, 2023: 55-67.
[85] PRIAMO G, D'ELIA D C, QUERZONI L. Principled composition of function variants for dynamic software diversity and program protection[C]// Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering. New York, USA: ACM Press, 2022: 1-5.
[86] HU J J, LI Y, LI Z Z, et al. Unveiling the strategic defense mechanisms in dynamic heterogeneous redundancy architecture[J]. IEEE Transactions on Network and Service Management, 2024, 21(4): 4912-4926.
[87] WANG W, LI G S, GAI K K, et al. Modelization and analysis of dynamic heterogeneous redundant system[J]. Concurrency and Computation: Practice and Experience, 2022, 34(12): e6035.
[88] YANG L, WANG Y J. Simulation experiment of scheduling algorithm in dynamic heterogeneous redundancy [C]// Proceedings of the International Conference on Information Science, Parallel and Distributed Systems (ISPDS). Xi'an, China: IEEE Press, 2020: 189-195.
[89] WANG Z H, JIANG D D, LÜ Z H. AI-assisted trustworthy architecture for industrial IoT based on dynamic heterogeneous redundancy [J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 2019-2027.
[90] HE J J, YUAN Y L, LIANG S C, et al. A function-aware mimic defense theory and its practice [J]. China Communications, 2024, 21(8): 192-210.
[91] HU H C, WU J X, WANG Z P, et al. Mimic defense: a designed-in cybersecurity defense framework [J]. IET Information Security, 2018, 12(3): 226-237.

计算机工程 www.ecice06.com

[92] IBRAHIM O A, SCIANCALEPORE S, DI PIETRO R. MAG-PUFs: authenticating IoT devices via electromagnetic physical unclonable functions and deep learning [J]. Computers & Security, 2024, 143: 103905.
[93] LIU F F, YAN Y, SUN Y, et al. Extremely lightweight PUF-based batch authentication protocol for end-edge-cloud hierarchical smart grid [J]. Security and Communication Networks, 2022(1): 9774853.
[94] CAO Y N, WANG Y J, DING Y, et al. A PUF-based lightweight authenticated metering data collection scheme with privacy protection in smart grid[C]//Proceedings of the IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom). New York, USA: IEEE Press, 2021: 876-883.
[95] BAGHERI N, BENDAVID Y, SAFKHANI M, et al. Smart grid security: a PUF-based authentication and key agreement protocol[J]. Future Internet, 2024, 16(1): 9.
[96] MEFGOUDA B, KHAN R, ALHUSSEIN O, et al. LPUF-AuthNet: a lightweight PUF-based IoT authentication via tandem neural networks and split learning [EB/OL]. [2026-04-22]. https://arxiv.org/abs/2410.12190.
[97] BONDADA P, SAMANTA D, KAUR M, et al. Data security-based routing in MANETs using key management mechanism[J]. Applied Sciences, 2022, 12(3): 1041.
[98] BURANGE A W, DESHMUKH V M, THAKARE Y A, et al. Safeguarding the Internet of Things: elevating IoT routing security through trust management excellence[J]. Computer Standards & Interfaces, 2025, 91: 103873.
[99] NAKANO Y, MATSUZAWA T. Preventing black hole attacks in AODV using RREQ packets[J]. Network, 2023, 3(4): 469-481.
[100] XIE Y Z, DAI C, ZHENG Y B, et al. Research on data information security anti-attack technology to improve ASON network architecture[C]//Proceedings of the 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS). Bristol, UK: IEEE Press, 2023: 46-50.
[101] BHATTARAI H, KULKARNI A R, NIAMAT M. Fuzzy logic based zero trust architecture for security of AMI in smart grids [C]// Proceedings of the 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC). Dayton, USA: IEEE Press, 2025: 1-5.
[102] BHATTARAI H, KULKARNI A, NIAMAT M. Trust score-based zero trust architecture for advanced metering infrastructure security [C] // Proceedings of the IEEE National Aerospace and Electronics Conference. Dayton, USA: IEEE Press, 2024: 334-339.
[103] LÜ P, SUN C H, LI Q Y. Research and application of grid cloud service security access control technology based on zero trust model [C] // Proceedings of the International Conference on Data Science and Network Security (ICDSNS). Tiptur, India: IEEE Press, 2023: 1-7.
[104] STANOJEVIC M, CAPKO D, LENDAK I, et al. Fighting insider threats, with zero-trust in microservice-based, smart grid OT systems[J]. Acta Polytechnica Hungarica, 2023, 20(6): 229-248.
[105] ALIPOUR M, GHASEMSHIRAZI S, SHIRVANI G. Enabling a zero trust architecture in a 5G-enabled smart grid [EB/OL]. [2026-04-22]. https://arxiv.org/abs/2210.01739.
[106] GRISAFI M, AMMAR M, ROVERI M, et al. PISTIS: trusted computing architecture for low-end embedded systems[C]//Proceedings of the 31st USENIX Security Symposium (USENIX Security 22). Berkeley, USA: USENIX Association, 2022: 3843-3860.
[107] ZHENG C M, LI J, YAO X X. Design and implementation of trusted boot based on a new trusted computing dual-architecture [J]. Computers & Security, 2023, 127: 103095.
[108] ZHAO S J, LIN J N, LI W, et al. Research on root of trust for embedded devices based on on-chip memory [C] // Proceedings of the International Conference on Computer Engineering and Application (ICCEA). Kunming, China: IEEE Press, 2021: 501-505.
[109] BOAKYE-BOATENG K, GHORBANI A A, LASHKARI A H. Implementation of a trust-based framework for substation defense in the smart grid[J]. Smart Cities, 2024, 7(1): 99-140.
[110] MO W, LIU W, HUANG G S, et al. A cloud-assisted reliable trust computing scheme for data collection in Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(7): 4969-4980.
[111] SHEKHAWAT H, GUPTA D S. Quantum-safe Lattice-based mutual authentication and key-exchange scheme for the smart grid [J]. Transactions on Emerging Telecommunications Technologies, 2024, 35(7): e5017.
[112] GRICE W, OLAMA M, LEE A, et al. Quantum key distribution applicability to smart grid cybersecurity systems [J]. IEEE Access, 2025, 13: 17398-17413.
[113] AGGARWAL S, KADDOUM G. Authentication of smart grid by integrating QKD and blockchain in SCADA systems [J]. IEEE Transactions on Network and Service Management, 2024, 21(5): 5768-5780.
[114] PARAMESWARATH R P, WANG C, SIKDAR B. A quantum safe mutual authentication protocol for smart meter communications with experimental evaluation [J]. IEEE Transactions on Network Science and Engineering, 2024, 11(5): 5058-5072.
[115] JIANG Z H, SHI R H. Lightweight quantum authentication and key agreement scheme in the smart grid environment[J]. Entropy, 2025, 27(9): 957.
[116] YURREBASO X, IBANEZ F, LONGUEIRA-ROMERO A. Substation bill of materials: a novel approach to managing supply chain cyber-risks on IEC 61850 digital substations[C]// Proceedings of the 5th International Conference on Electrical, Computer and Energy Technologies (ICECET). Paris, France: IEEE Press, 2026: 1-10.
[117] 陈昕, 孙溢成, 谈诚. 基于大语言模型的日志异常检测方法综述[J]. 计算机工程, 2026, 52(8): 1-15.
CHEN X, SUN Y C, TAN C. Survey on log anomaly detection methods based on large language models [J]. Computer Engineering, 2026, 52(8): 1-15. (in Chinese)
[118] NGUYEN L H, NGUYEN V L, HWANG R H, et al. Toward secured smart grid 2.0: exploring security threats, protection models, and challenges[J]. IEEE Communications Surveys & Tutorials, 2025, 27(4): 2581-2620.

文字编辑 陆燕菲
栏目编辑 宋 圆

计算机工程 www.ecice06.com