智能电网中的信息安全与隐私保护技术研究

吴　涛
恩施永扬实业有限责任公司　湖北恩施　445000

摘　要：电力资源是当今社会最为重要的能源之一，而传统电网在能源利用率、环保、安全以及可靠性方面逐渐难以满足人们的使用需求。而随着现代化信息技术以及通讯技术的发展，将电力系统与先进的信息通讯技术结合在一起，能够推动电力系统发生质的变化。这种全新的电网架构被称为智能电网，不过智能电网在给人们带来便利的同时，也对电网数据安全和用户隐私的管理带来了一定的挑战。基于此，针对智能电网的信息安全与隐私保护也成为了智能电网中必须深入研究的内容之一。文本就当前智能电网信息安全与隐私保护技术展开分析，并提出相应的改进策略，以期更进一步推动我国智能电网事业的发展。

关键词：智能电网；信息安全；隐私保护

随着信息技术的快速发展，智能电网作为电力系统的重要组成部分，已经成为现代社会不可或缺的基础设施。然而，智能电网在带来便捷和高效的同时，也面临着严峻的信息安全挑战。黑客攻击、病毒入侵、信息泄露等安全威胁层出不穷，严重威胁着电网系统的稳定运行和用户数据的安全。因此，研究智能电网中的信息安全与隐私保护技术，对于保障电网系统的安全稳定运行、维护用户数据隐私具有重要意义。

一、智能电网研究概述

1.1 智能电网定义

智能电网是指电网的智能化，也被称为“电网2.0”。智能电网建立在集成的、高速双向通信网络的基础上，通过先进的传感和测量技术、先进的设备技术、先进的控制方法以及先进的决策支持系统技术的应用，实现电网的可靠、安全、经济、高效、环境友好和使用安全的目标。具体而言，智能电网通过数字化技术和现代化通讯系统，将传统电力系统中的各种电源、电网和负载连接起来，并进行全系统、全程的监测、诊断、调度和管理，以提高电力系统的可靠性、经济性和安全性。它的主要特征包括自愈、激励和保护用户、抵御攻击、提供满足用户需求的电能质量、容许各种不同发电形式的接入、启动电力市场以及资产的优化高效运行[1]。此外，智能电网也被描述为一个由众多自动化的输电和配电系统构成的电力系统，以协调、有效和可靠的方式实现所有的电网运作，具有自愈功能，能够快速响应电力市场和企业业务需求；具有智能化的通信架构，实现实时、安全和灵活的信息流，为用户提供可靠、经济的电力服务。由此可见，智能电网属于一种学科高度交叉的体系，如图1所示，通过集合电力、通信、控制等先进的技术，能够更进一步优化各级电网控制，具有可靠性、高效性以及安全性等特点。

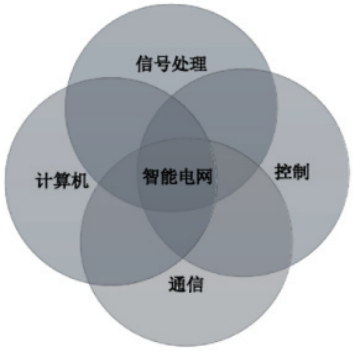

图1　智能电网涉及学科

1.2 智能电网体系结构

根据美国国家标准技术研究所（NIST）所定义的智能电网概念模型，智能电网的构成被细分为七大逻辑领域：发电、输电、配电、用户、市场、服务供应商和服务运营。前四个领域特征在于能量与信息的双向流通，如图2所示，剩余三个领域则侧重于信息搜集与电力调控[2]。从核心技术架构看，智能电网可归纳为四大模块：先进计量基础设施（AMI）、高级输电运营管理（ATO）、先进配电运营管理（ADO）及高级资产管理（AAM）。其中，AMI的核心职责在于促进供用电方的互动，桥梁般连接电力系统与负荷端，赋予用户参与并助力电网运作的能力。ATO致力于优化电力系统的阻塞管理，显著降低电网停运概率；ADO则专注于实时配电网络监控，确

保电网运行的连续性与稳定性，而AAM则与前三者紧密协作，旨在优化电网运行性能并提升电力资产利用率。

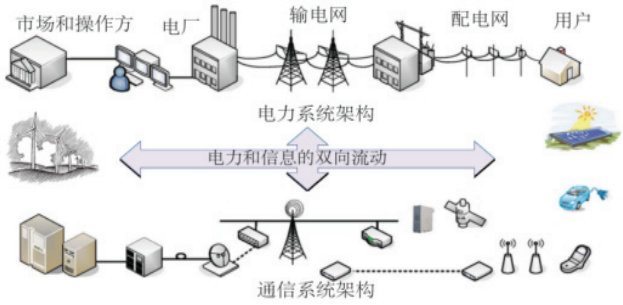

图2　智能电网体系结构图

二、智能电网安全和隐私问题

2.1安全目标和要求

智能电网作为支撑社会进步、工业活动及民众日常生活的关键基础，其安全性至关重要。任何安全威胁的实现都可能对社会带来严重影响，不仅导致重大的经济损失，还可能危及公众的生命财产安全。因此，在智能电网的设计初期，必须将安全性置于首位。确保电网的稳健运行要求设计者明确安全目标与标准，以便采取精确的防范措施和解决方案。

（1）可用性

在智能电网领域，可用性指的是确保所有信息与通信组件，包括控制系统、安防系统、工作站、生产管理系统及它们之间的通信链路，能够免受干扰，维持正常运行和访问畅通无阻[3]。这对于智能电网至关重要，因为它依赖于数据的即时准确传递来实现设备的有效监控与控制，一旦数据可用性受损，可能导致无法及时响应的监控和控制失效，进而引发严重的连锁反应，严重威胁电网的整体安全与稳定运作。

（2）完整性

在智能电网的范畴中，数据完整性是指确保网络内所有信息维持原始、准确的状态，防止在存储或传输环节遭受未授权修改或破坏，且任何变动都能被迅速检测到。这类信息涵盖了从设备配置到传感数据、控制信号、智能计量数据等多个方面。若数据完整性受损，可能会误导电网监控，引发不当操作，或是执行错误指令，进而扰乱系统的正常运行秩序。

（3）机密性

机密性在智能电网的语境中指的是确保数据仅对授权实体开放，未经授权的个体无法获取数据的真实信息。缺乏机密性的保护可能导致电力企业和用户隐私信息的外泄，直接损害双方的利益与权益。

（4）攻击检测与恢复操作

相较于传统电网，智能电网因其广泛的地域覆盖与相对开放的通信网络设计，难以实现绝对无懈可击的安全防护。这意味着必须不断地监控全网流量，进行分析、测试与比对，以识别并应对由潜在攻击引起的异常情况。同时，智能电网系统必须具备在遭受攻击时维持运作并自我恢复的功能，这是鉴于电力基础设施对于社会的极端重要性。恢复机制是确保智能电网连续服务与网络稳定性的关键环节。

（5）识别、认证和访问控制

智能电网内部署着众多电子设备与用户，识别与认证过程是核实其访问电网资源合法性的重要步骤。通过访问控制机制，仅允许经过恰当授权的个体在成功认证后介入资源，尤其是针对敏感信息及核心设备，实行严密的访问限制，以防非授权侵入。为此，智能电网的每一节点均需装备基本加密技术，如对称或非对称密钥体系，来保障数据的安全传输与用户认证，满足上述安全需求。

（6）安全和高效的通信协议

智能电网的数据通信区别于常规网络，其特点是强调数据传输的即时性和安全性，尤其在配电与输电系统中，这两点尤为关键，但二者时常互为制约。智能电网的环境限制了采用高度安全、物理隔离且宽带宽通信链路的可能性，因此，在设计通信协议和架构时，必须找到一种平衡，既能确保通信效率，又能维护信息安全，实现二者的最优化协调。

2.2智能电网安全威胁

智能电网的组件散布于多样且潜在危险的环境中，并广泛应用无线通信技术进行数据交换，这让其易受恶意侵扰[4]。对比其他系统，智能电网一旦遭受攻击，可能导致电力系统重大故障及大面积停电，影响深远。根据智能电网的安全目标，攻击类型可归纳为三类，分别是影响可用性、完整性及机密性的攻击。其中，影响可用性的攻击，即拒绝服务攻击，旨在阻碍、延迟或中断电网通信，其破坏力极强，可能发生在物理、数据链路、网络/传输乃至应用等多个层级。在智能电网中，针对数据完整性的攻击意在非法获取或篡改智能电网数据，此类攻击通常瞄准应用层面，目标直指用户信息及系统状态数据，防范此类攻击常采用容错及完整性校验技术。在智能电网背景下，篡改AMI数据以减少电费支付的“偷电”行为是完整性攻击的一个典型实例，如图3展示了现行AMI系统中偷电攻击的手段。

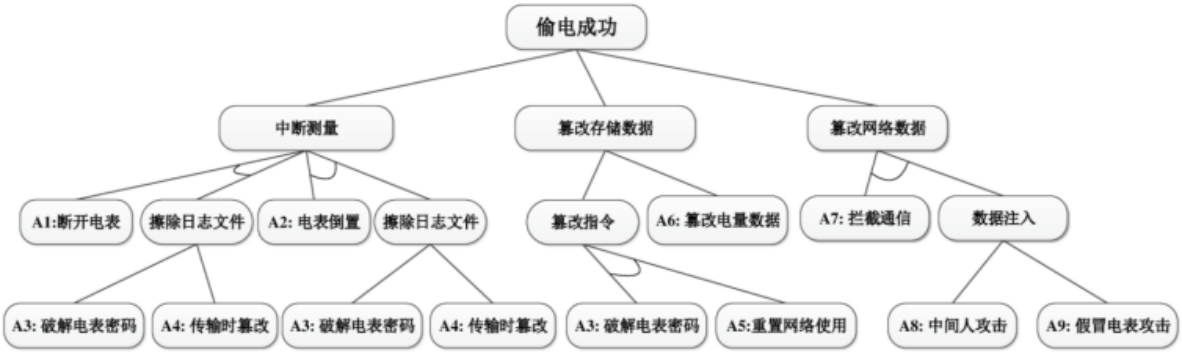

图3　高级测量体系偷电攻击树模型图

至于机密性攻击，则是通过监听等手段非法获取数据，如用户账号详情及用电量，虽不对电网本身构成直接影响，却严重侵犯隐私，可能引起公众对智能电网信任缺失，阻碍其发展步伐。智能电网借助先进信息技术实现了用电的智能管理和经济控制，但也因此增加了用户隐私泄露的风险，特别是在高级计量体系和车辆到电网（V2G）通信中，若数据保护不周，用户的生活习惯、家庭情况乃至宗教信仰、经济状况等隐私均可能曝光。确保隐私不仅涉及防外部攻击，还需限制电力企业过度获取和利用用户信息。隐私保护问题若得不到妥善解决，智能电网恐难获用户及监管机构认可[5]。个人数据涵盖直接或间接识别个人的所有记录，从基本信息到偏好、社交活动、健康状态乃至衍生的经济、生理、心理信息及其社交圈信息。智能电网环境下，所有与个人相关的电耗数据均需严格保护和监控。全球范围内对智能电网隐私问题给予了高度重视，美国国家标准与技术研究院在2010年8月发布的《智能电网网络安全指南第二卷：智能电网与隐私》中，对此进行了初步探讨，并罗列了智能电网可能泄露的个人信息类型，如表1所示。

表1　智能电网涉及个人隐私的数据元素表

数据元素	描述
姓名	账户所有者信息
地址	接收电网服务位置
账号	账户唯一标识符
电表读数	周期内15~60分钟间隔记录消耗
实施账单	账户当前用电量
历史账单	账户历史用电量
家庭局域网	家用电器互联网的家庭网络
生活方式	账户个人信息及用电习惯
分布资源	现场发电、储存设备、运行状态
IP	智能电表IP地址
供应商	提供账户机构身份

结束语

智能电网中的信息安全与隐私保护技术是一个复杂而重要的研究领域，本文通过分析智能电网信息安全面临的挑战和隐私保护技术的应用，提出了相应的解决方案和策略。而随着智能电网技术的不断发展和应用，新的安全威胁和挑战也将不断涌现。因此，需要持续关注智能电网信息安全与隐私保护技术的发展动态，加强技术创新和人才培养，为智能电网的安全稳定运行提供坚实的技术保障，同时，也需要加强国际合作和交流，共同应对全球性的信息安全挑战。

参考文献

[1] 王林信，杨鹏，江元，等.智能电网大数据隐私保护技术研究与实现[J].电力信息化，2019（012）：017.

[2] 朱聪聪，乔治，王志伟.基于抗泄漏无证书的智能电网隐私保护协议[J].计算机技术与发展，2020，30（6）：7.

[3] 潘涛.数据安全及隐私保护在智能电网中的应用研究[J].通信技术，2019，52（4）：5.

[4] 张思佳，顾春华，温蜜.智能电网中的数据聚合方案分类研究[J].计算机工程与应用，2019，55（12）：8.

[5] 邹洪.智能电网信息安全防御体系架构与关键技术研究[J].网络安全技术与应用，2020（1）：3.