第 48 卷 第 2 期：513-525 高电压技术 Vol.48, No.2: 513-525
2022 年 2 月 28 日 High Voltage Engineering February 28, 2022
DOI: 10.13336/j.1003-6520.hve.20210150

电力物联网终端安全防护研究综述

苏 盛，汪 干，刘 亮，陈清清，王 坤
（长沙理工大学电气与信息工程学院，长沙 410114）

摘 要：随着传感器的微型化和网络化，物联网技术在电力系统的应用得到了飞速发展。分散分布的配用电物联网终端数量庞大而又广泛互联，跳脱了传统边界安全的保护范畴，使得物联网终端成为攻击电网的重要目标和跳板。围绕电力物联网终端的安全防护展开研究，首先结合电力物联网的架构，从软硬件、通信等方面归纳了终端面临的安全挑战，总结了终端威胁特征，分析了为应对终端威胁部署的防护机制并指出了其不足；然后根据现有防护漏洞具体分析终端安全问题，重点综述了电力物联网终端的加密认证问题、数据隐私安全、时间同步攻击、非法无线通信链路风险和 230 MHz 无线专网通信阻塞攻击及其相应防护研究；最后综述和展望了深度学习等新一代人工智能技术在物联网终端安防中的应用。

关键词：电力物联网终端；加密认证；数据隐私安全；时间同步攻击；非法无线通信链路；安全防护

Review on Security of Power Internet of Things Terminals

SU Sheng, WANG Gan, LIU Liang, CHEN Qingqing, WANG Kun
(College of Electrical Engineering, Changsha University of Science and Technology, Changsha 410114, China)

Abstract: With the advancement of sensing technology and the miniaturization of sensors, the Internet of Things (IoT) technology has been rapidly developed in the power system. Due to the large number, extensive interconnection, and decentralized distribution of the power distribution IoT terminals, they have jumped out of the scope of border security protection, which has caused the terminals to become the main target and springboard for attacking the power grid. Firstly, combined with the power IoT architecture, the terminal security challenges are summarized from the aspects of software, hardware, communication, etc., the terminal risk characteristics are further summarized, and the protection mechanism deployed to deal with the terminal risk is analyzed and its shortcomings are presented. Then, according to the existing protection vulnerabilities, the terminal security issues are analyzed, the encryption and authentication issues, data privacy security, time synchronization attack, malicious base station attack are focused on, and the communication block attack of 230 MHz power IoT terminal and their corresponding protection research are reviewed. Finally, the applications of new generation AI technologies such as deep learning in the security of IoT terminals are reviewed and prospected.

Key words: power internet of things devices; encrypted authentication; data privacy security; time synchronization attack; malicious base station; security protection

0 引言

对能源低碳减排的追求，使得结合可再生能源技术与互联网技术的能源互联网得到了世界各国的广泛关注[1]。在城市等区域用能中心构建能源互联网，是未来能源系统建设的重点方向。城市能源互联网是以电能为中心的城市各类能源互联互通、综合利用、优化共享的平台，是以电网为基础，以“互联网+”为手段，以电能为主体的绿色低碳、安全高效的现代能源生态系统[2]。电力系统作为各种能源相互转化的枢纽，是城市能源互联网的核心[3]。

为了更好地服务用户对能源的多样化需求，国家电网和南方电网以不同形式提出要依托微型化和网络化的传感技术，在配用电和能源需求侧推进电力物联网(power internet of things, PIoT)建设[4-6]，来提高对配电系统和用户的感知能力，以催生创新应用，提高服务水平。

需要指出的是，作为现代社会的关键性基础设

基金资助项目：国家重点研发计划(2018YFB0904903)；国家自然科学基金(51777015)；湖南省自然科学基金(2020JJ4611)。
Project supported by National Key R&D Program of China (2018YFB0904903), National Natural Science Foundation of China (51777015), Hunan Province Natural Science Foundation Project (2020JJ4611).

施，电力系统是网络攻击的高价值目标。我国电力系统依托物理隔离的调度数据网构筑了基于边界安全的纵深安全防护体系[7-8]，在场站、配电主站和用电信息采集系统中，采用单向网闸对生产控制区和管理区进行物理隔离，有效地保障了电网安全。电力物联网的建设要求在配用电系统中广泛接入海量物联网终端，这使得原有安全边界变得模糊。因物联网终端种类繁多且一般具有计算资源受限等特点[9]，传统物理隔离及加密认证等防护机制难以完整覆盖接入配用电系统各类物联网终端。潜在的安全威胁可能以物联网终端为跳板，绕开基于边界安全的防护体系，侵入生产控制区进行攻击破坏。为提高安全防护水平，电力行业近年来开始为有大量物联网终端接入的配电自动化和用电信息采集系统建设了安全接入区，防止经物联网终端渗透的入侵攻击[8]。

电力物联网终端种类多样，按业务场景可分为配电系统的配变终端(transformer terminal unit, TTU)、配电终端(distribution terminal unit, DTU)、馈线终端(feeder terminal unit, FTU)、运维监测终端(monitor terminal unit, MTU)、一二次融合终端，用电系统的计量表计终端，以及用户表后智能家居终端。按资产归属和攻击破坏后果，主要可分为属于电网资产的配用电终端和属于用户资产的用户智能家居终端。上述物联网终端遭攻击破坏的后果存在明显差异，其中对配用电终端的攻击破坏轻则影响直接关联用户供电、重则侵入生产控制区进而造成大量用户停电，而对智能家居终端的攻击破坏主要涉及用户隐私信息泄露。因为攻击破坏后果不同，作为用户资产的智能家居物联网终端在安全防护要求和成本约束上和属于电网资产的配用电终端有显著差异，传统电网安全保障体系难以适用于此类资源受限的用户侧终端[10]。

本文围绕电力物联网终端的网络安全防护展开综述，首先结合电力物联网架构归纳了终端安全面临的挑战、终端安全的风险特征以及既有的终端安全防护机制；然后围绕资源受限物联网终端加密认证、数据隐私安全、时间同步和接入非法无线通信链路等问题进行安全风险分析，并总结了相应的防护方法；最后综述和展望了近年来取得突飞猛进的深度学习等新一代人工智能技术在物联网终端安防中的应用。

1 电力物联网终端安全概述

1.1 电力物联网框架及终端安全挑战

部署在配用电侧复杂环境中的电力物联网终端，主要完成特定目标的状态监测与控制，终端接入本地或远程通信网通信。电力物联网整体框架一般包括图 1 所示的“云、管、边、端”4 部分[11-12]。

1）“云”是云化的主站平台，具有海量物联管理、开放共享及智能决策等多种微服务。

2）“管”是从云到边、端以及边到端之间的数据传输和终端接入的数据传输通道。它主要分 2 部分：(1)物联网云平台与边缘节点间通信的远程通信网；(2)海量感知节点与边缘节点间通信的本地通信网。

3）“边”指在终端侧或数据源头的网络边缘侧就地或就近提供智能决策和服务的边缘计算节点。

4）“端”是电力物联网架构中的状态感知和执行控制主体终端单元，它利用微型传感技术和芯片化技术，实现对配用电设备运行环境、设备状态、电气量信息等基础数据的监测、采集、感知。“端”也是电网保护、控制操作的末端执行单元，保障电网可靠运行与安全稳定；“端”是实现电力物联网的基础及保障其安全运行的关键执行部分。

电力物联网终端位于“云管边端”体系的最底层，是连接物理世界与数字世界的关键节点，采用多种类型的传感设备在各种异构的网络环境中实现状态感知，安全条件复杂，可以借助硬件接口、暴力破解、软件缺陷、管理缺陷、云端攻击和通讯方式等方式进行攻击。电力物联网终端主要面临以下几种安全挑战[13]：

1）接入安全。终端计算资源有限，难以对与其通信的设备进行有效身份认证，攻击者可冒充合法终端进行信息侧和物理侧交替协同攻击。

2）数据安全。物联网终端资源有限，多缺乏有效的数据隐私保护机制，难以对传输数据进行强

图 1 电力物联网架构

Fig.1 Architecture of PIoT

加密等防护，易导致数据泄露。

3）物理安全。电力物联网终端数量众多，部署环境复杂且不可控，容易被直接捕获。终端硬件安全威胁主要包括硬件木马、侧信道分析攻击、故障攻击、假冒芯片和逆向工程等 5 类攻击[14]。

4）通信安全。受通信方式开放性影响，容易遭重放攻击、虚假数据注入攻击和分布式拒绝服务(distributed denial of service, DDoS)等攻击，导致数据传输错误、延时甚至中断。物联网终端可能采用 ZigBee、Bluetooth、WiFi 等通信协议，各种协议在适用场景和安全性上有所差异，但都不可避免地存在安全漏洞[15]。采用 230 MHz 无线专网通信时，还可能存在通信阻塞的问题。

5）设备安全。物联网终端设计开发过程中普遍存在安全考虑不足的问题，可能存在各种漏洞。攻击者可在终端中植入蠕虫病毒传播，进而发起 DDoS 攻击。

1.2　电力物联网终端安全风险特征

从近年来利用物联网终端发起的网络攻击事件来看，电力物联网既是网络攻击的重要目标也是攻击电网的主要跳板[16]。与传统电力监控系统相比，电力物联网终端具有明显的差异性并表现出独特的安全风险特点，详述如下：

1）计算资源受限、安全防护手段不足。配用电物联网终端普遍存在计算资源有限的问题，难以采用有较高计算资源要求的加密认证技术，给安全加固带来了不小的挑战。如 2014 年，研究人员破解了西班牙电力公司智能电表采用的 AES-128 对称加密算法，侵入表计后注入恶意代码，不但可篡改电表标识码、调整电量读数实现窃电，还能以此为跳板攻击相邻电表，甚至切断用户供电，造成事故。

2）分散分布，监管困难。配用电物联网终端点多面广，传统的安全加固方法难以实施。如 2016 年，攻击者利用 Mirai 病毒感染和控制大量摄像头物联网终端，进而发起大规模 DDoS 攻击，致使美国大量主流网站无法访问[17]。数量庞大、分散分布的电力物联网终端同样可能成为向电网发起 DDoS 攻击的重要阵地。

3）兼容性和可用性要求高，漏洞加固困难。配用电物联网终端升级后可能因业务系统不兼容，导致终端功能不可用。如大连车务段近日升级 Adobe 推送的补丁后，造成 Flash 功能不可用进而无法显示列车运行图，即为典型案例。除此以外，还有大量终端因资源受限难以升级固件，故而电力物联网终端中较少采用漏洞加固技术。

1.3　物联网终端安全防护机制分析

针对物联网终端暴露面大、易遭攻击破坏且难以加固、安全防护困难的问题，可以采用表 1 所列措施增强配用电物联网终端安全防护能力。

供电企业根据国家标准，要求攻击破坏后果较严重的电表、集中器、配电终端、充电桩等物联网终端采用基于国密 SM1 算法的嵌入式安全控制模块(embedded secure access module, ESAM)进行通信加密和身份认证，能够较好地解决电力监控系统中终端传输数据的机密性、完整性和认证终端身份，有效提高终端应对冒充、中间人攻击和重放攻击等安全威胁的防护能力[18]。采用 ESAM 模块进行加密认证会带来一定的成本，难以在智能家居等场景下的低成本物联网终端中推广应用。

物联网终端运行在开放环境下，自身也可能被注入恶意代码遭到劫持和攻击破坏。为应对这一难题，近年来我国电力行业开始在终端设备中推广应用可信计算技术。可信计算是一种同时实现计算功能与网络安全防护的计算机技术，通过构建逐级认证和信任的可信链，实现整个计算系统全过程的可信认证，保证计算结果与预期的一致性，最终构成整个网络相对可信的网络环境与边界[19]。

目前，可信计算技术已在国产 D5000 调度自动化系统中大面积应用。国家电网和南方电网还分别联合芯片设计制造企业及电力装备制造企业，针对电力工控业务场景研发了基于可信计算技术的高实时安全处理器，并以此为基础研发了安全可控的保护装置、微网控制器、充电桩和计量终端等物联网

表 1　终端安全风险的防护机制分析

Table 1　Protection mechanism against terminal security risk

风险特征	防护措施	防护机制与不足
计算资源受限	基于公钥基础设施(public key infrastructure, PKI)体系加密认证	在终端中集成 ESAM 芯片进行加密与认证，会增加一定的成本
分散分布，难监管	可信计算识别非法程序	基于可信根识别未经认证的非法程序，但存在以下问题：(1)通信数据及身份无法保证可信；(2)操作系统可能有漏洞；(3)通过认证的程序可能带病毒；(4)破解加密算法后防护失效；(5)载入可信根对硬件有较高要求
漏洞难加固	大数据技术识别异常	(1)需海量、高质量数据支撑；(2)易引发数据隐私和所有权问题；(3)数据挖掘时易被攻击泄露

终端。基于可信计算的物联网终端可逐级认证系统及运行的程序，能有效避免未经认证的恶意代码运行，从而有效防范病毒攻击。

需要指出的是，可信计算也有它的缺点。首先，它并不能保证终端接收的数据及与其通信对象的身份是否可信完整；其次，终端操作系统本身可能存在安全漏洞[20]；再次，可信计算只能保证运行的程序是经过认证的，并不能保证其中不含有恶意代码；最后，认证数字签名所用加密算法的数学复杂度是可信计算安全性的基础，破解了加密算法也就突破了可信计算的防护屏障。因此，基于可信计算技术的安全防护也存在失效可能。此外，基于可信计算的系统启动时需要载入可信根，低成本物联网终端短期内难以承受对应需增加的成本，这也将限制可信计算技术在电力物联网终端中的推广应用范畴[21]。

以上采用 ESAM 模块进行加密认证和采用可信计算技术识别非法代码，都是对终端自身防护能力的加强。实际上，相当数量的物联网终端不但无法采用上述方法，还可能难以采用固件升级等方式进行安全加固，需要从加强对终端自身及所处运行网络环境的监视和异常检测角度，通过构建多层次的防御来提高安防能力。

2 电力物联网终端安全威胁分析与防护

2.1 电力物联网终端安全威胁分析

电力物联网终端数量庞大且呈爆炸式增长，接入的终端种类繁多、杂散分布且通信方式各异，存在的安全威胁纷繁复杂[22]，牵一发而动全身。终端安全是保证电力物联网健康发展的重要基础。本节分析传统电网安全防护漏洞，从终端接入安全方面的加密认证、数据和物理安全方面的终端数据隐私保护、通信安全方面因卫星时间同步系统采用民码明文通信而可能遭受的时间同步攻击、终端接入非法无线通信链路以及 230 MHz 无线专网遭屏蔽失效等角度总结了物联网终端的典型安全问题。

2.1.1 终端加密认证

受成本因素影响，资源受限的终端往往侧重考虑功能实现，多未系统规范部署加密认证机制，难以实现终端的统一管理和鉴别，面临着严峻的接入安全挑战。如何建立低成本电力终端信任认证机制，是当前亟待解决的问题[23]。

我国电力系统多采用基于 PKI 的终端安防技术[24-26]。PKI 体系下的加密认证过程示意如图 2，

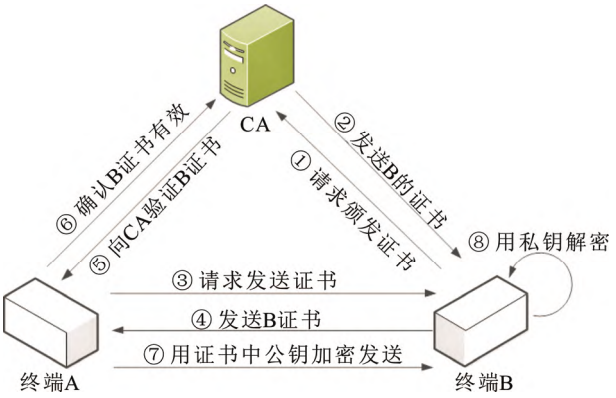

图 2 基于 PKI 体系的终端加密认证流程

Fig.2 Terminal encryption authentication based on PKI

由证书授权机构(certification authority，CA)绑定证书持有者的身份和相关的密钥并签发数字证书，并为用户提供证书申请、证书作废、证书获取、证书状态查询等服务，实现通信中各实体的身份认证、完整性、抗抵赖性和保密性。PKI 体系需要在物联网终端中安装 ESAM 安全模块，安全证书管理复杂，在终端数字证书生成、管理及应用上将产生一定的通信和计算成本，限制了其在智能家居等低成本物联网终端中的应用。

2.1.2 终端数据隐私保护

电力物联网终端产生的海量数据涉及用户隐私，终端面临的数据安全挑战突出。由于物联网终端运行在复杂环境中，即便进行加密也可能遭侧信道分析等攻击而泄露隐私信息。传统监控系统需要将终端监测数据上报到系统后台进行分析诊断，再做出控制决策，这将导致终端与主站间大量的数据交互。物联网终端的爆炸式增长，将会在网络流量上对通信系统及后台造成巨大压力。采用边缘计算技术，由靠近物联网终端的边缘节点进行数据处理，可以显著减少从终端到后台的数据流量，提高实时性和快速响应能力，是物联网发展的重要趋势。

边缘计算可以支持轻量级设备完成复杂任务[27-28]，但分布式数据处理将面临物理攻击、隐私泄露、服务操纵和数据篡改等安全挑战[29]，业务实现架构的变化还可能带来 DDoS 攻击、侧信道攻击、恶意软件注入攻击、身份验证和授权攻击等安全威胁[30]。攻击者通过新型网络攻击实施窃听、渗透、篡改等破坏行动，可导致用户隐私、使用信息和密码泄露[31]，或截取传输信息、控制指令，劫持边缘节点终端，导致整个系统进入紊乱状态。与此同时，受到边缘计算的多源数据融合特性、移动和互联网叠

加性以及边缘终端在存储、计算和电池容量等资源约束影响，较复杂的安全防护方法在边缘计算场景下难以适用。

配用电系统中，可以将智能配用终端等作为边缘节点，依托边缘计算实现部分业务功能。文献[32]将边缘计算引入配电物联网中，构建以边缘为核心的云、管、边、端 4 层架构，并提出了如图 3 所示的基于边缘计算的物联网安全防护模型。其中，终端监测自身运行状态、采集数据和接收控制指令，然后将监测数据发送至边缘节点；边缘节点基于局域网内终端监测数据对接入终端进行身份认证、攻击检测以及漏洞利用检测及阻断，并将监测数据上报云端；云端基于全局数据进行安全态势评估、电网高级可持续威胁(advanced persisitent threat, APT)攻击检测以及安全数据存储等任务。该架构可将物联网终端部分安全防护工作转移给计算/存储能力较强的边缘设备，由边缘设备完成证书管理、认证和安全软件更新等工作[28]。

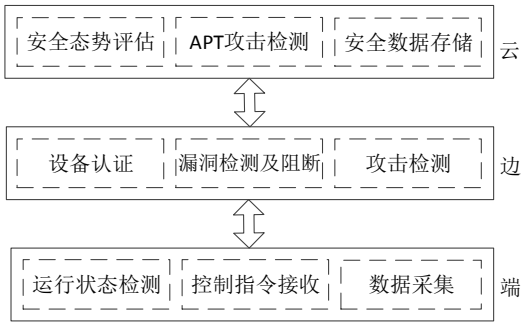

图 3　边缘计算安全防护体系架构

Fig.3　Security defense architecture of edge computing

2.1.3　时间同步攻击

传统通信安全主要考虑物联网终端运行在复杂环境下，通信延时具有强不确定性，滞后时间超标时可能引起对系统当前状态的误导性认知。为有效执行监视与控制功能，电力物联网终端一般需要定期与后台系统对时，从而将终端与后台的时间偏差控制在限定范围内[33]。

物联网系统后台一般采用卫星时间同步装置根据全球定位系统(global position system, GPS)/北斗卫星时钟取得时间基准。GPS/北斗卫星时间同步系统均可采用未加密的民码通信，缺乏加密认证保障[34]，攻击方可根据卫星导航报文的格式定义发射伪造的卫星导航报文，诱使时间同步装置输出错误时间，时间同步攻击的机理示意如图 4。通过造成物联网系统的主站和终端间时间紊乱，来触发系统和终端的功能闭锁和误判，实现攻击破坏。

卫星时间同步攻击通过发布伪造的卫星导航电文进行攻击破坏，无需接入物联网终端的通信系统，是一种可绕越既有安全防护体系的新型安全威胁。在用电信息采集系统中，要求电表和主站的时间偏差不能超过 5 min，当主站系统遭时间同步攻击导致时间偏差超标时，电表上报的计量数据将会因时间偏差超标而被当作异常数据丢弃，造成数据采集功能闭锁；而主站下发的遥控指令也会因为时间偏差超标而不予执行，造成控制功能闭锁[35]。某

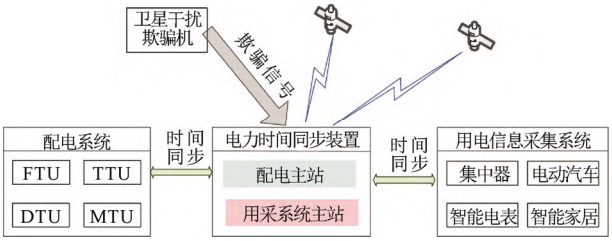

图 4　时间同步攻击机理

Fig.4　Time synchronization attack mechanism

些配电自动化系统中，同样可能存在类似的风险。

发布虚构的卫星导航电文，还可造成定位错误。2011 年，伊朗就曾利用卫星欺骗干扰技术发布虚构的导航电文诱捕一架 RQ−170 无人机[36]。电力系统广泛应用卫星定位标定输配电设备位置，未来某些应用场景下也可能出现误导定位位置的新型攻击模式。此外，在交通电气化大潮之下，配置有大量物联网终端的电动汽车渗透率将快速提高，未来可能大面积实现参考卫星导航定位的自动驾驶，也可能衍生出具有高破坏性的新型攻击模式[37]。

2.1.4　非法无线通信链路风险

分散分布的电力物联网终端设备散布于配用电侧，除少数配电终端采用光纤通信外，绝大多数物联网终端采用图 5 所示电信服务商提供的无线虚拟专网通信[38]。电力无线虚拟专网接入包括无线接入网、数据传输网和电力核心网 3 层。

物联网终端以无线通信方式经电信运营商无线基站接入核心网。数据传输网采用第 2 层隧道协议(layer 2 tunneling protocol，L2TP)构建虚拟专网，通过通道加密、端对端加密或应用层加密保障通信安全。物联网系统主站采用防火墙或单相网闸经光纤专线接入运营商 IP 承载网，接收物联网终端上报数据[39]。

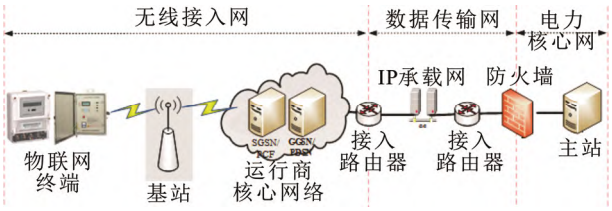

图 5 电力无线虚拟专网

Fig.5 Power system wireless virtual private network

物联网终端与无线基站间经 2G/3G/4G 通信，其中 2G GPRS 通信仅支持基站对终端的单向身份认证，终端可能接入伪基站并建立非法无线通信链路、遭受中间人等攻击破坏。一般认为只要 2G 通信退网或采用支持双向身份认证的 3G/4G 通信，即可消除物联网终端接入伪基站的风险。但终端设备多按向下兼容的方式设计，往往同时支持 2G/3G/4G 通信，只要干扰屏蔽 3G 和 4G 系统信号，仍可迫使终端退回 2G 通信进行攻击。因此，只有终端不再支持 2G 通信，才能彻底消除物联网终端接入伪基站风险。

尽管 3G/4G 可以实现双向身份认证，但也并不能保证终端安全。文献[40]研究表明伪基站也可利用长期演进(long term evolution, LTE)通信的安全缺陷入侵，造成终端信息失密。在大量物联网终端遭网络攻击控制的极端场景下，攻击者的恶意破坏可能造成负荷剧烈变化导致电网运行状态的大幅波动，影响电网安全甚至造成用户停电[41]。

2.1.5 230 MHz 无线专网通信阻塞风险

无线公网通信是供电企业租用电信运营商提供的通信服务，具有技术成熟、建设简单、速率较快的优势而被广泛应用于配用电信息采集中。无线公网作为运营商为大众提供的公共网络，难以可靠保障电力业务全程可控，有重要活动或灾害情况时存在网络拥塞甚至瘫痪的情况，影响电力业务开展。近年来，国家无线电管理局将 230 MHz 频段调整为电力等行业专用，依托频段资源可以构建 LTE 230 MHz 无线专网。无线专网具有组网灵活度高、独立自主业务优先级自定义、安全保障可管控、频段专用安全性高等优势，成为电力物联网终端通信接入的重要发展方向[42]，在多个省市得到试点建设，在配电自动化、用电信息采集和精准负荷控制等领域进行了业务接入。

与无线公网相比，230 MHz 工作频段不高、频率管理复杂，受民用低频器件干扰通信问题突出。该频段干扰源主要包括各种 LED 电子屏、电子广告牌、霓虹灯及射灯等宽带全频干扰和大功率数传电台、雷达等窄带同频干扰。目前，除了采用跳频通信规避窄带同频干扰以外，主要针对确定的干扰源在无线基站选址时在区域和方向上进行规避[43]。

需要指出的是，230 MHz 无线专网因为频段低而具有通信传输距离远的优势，在一般城区和农村的覆盖半径分别可达 3 km 和 15 km，所需基站数量显著小于无线公网，可选择在变电站、供电所、办公大楼等供电企业自有物业建设基站。但这种传输距离远的优势在恶意的通信阻塞攻击下会转化为劣势，攻击方在负荷中心区域架设少量高功率宽带全频干扰源，即可阻塞大量物联网终端与配用电后台系统的通信，造成基于无线专网的业务系统功能闭锁。在未来含高比例可再生能源的电力系统中，可能产生严重的危害性后果。

实际上，基于无线公网的虚拟专网也存在类似的通信阻塞安全威胁，无线专网通信距离远的特点只是改变了攻击的难度和影响范围，放大了相关风险。因为目前主要依靠管理上定位排查来消除通信干扰源，技术上不能杜绝恶意通信阻塞攻击的风险，除规范和强化管理外，需要结合业务系统在电网运行中所起的作用和可以容忍的通信中断时间，合理选择迁移到无线专网通信的业务系统。

2.2 终端安全威胁防护对策

本节主要从加密认证、隐私保护、时间同步攻击检测和非法无线通信链路检测等角度归纳总结电力物联网终端相关安全威胁防护研究。

2.2.1 加密认证

身份认证和数据加密是保障物联网安全的基础，配用电系统中一般采用基于对称加密的 SM1 算法 ESAM 模块进行终端的加密认证。为防止终端私钥泄露和提高加密认证水平，文献[44]提出了终端和服务器双方共同签名协议的非对称加密的 SM2 算法协同签名技术。在变电站远动通信等安全性要求较高的场景下，一般采用集成 SM2 算法的 ESAM 模块进行认证与加密。

需要指出的是，电力行业采用的 SM1 和 SM2 算法均为有证书的 PKI 模式，需要在物联网终端中集成 ESAM 模块。家居智能化等领域中，进行大规模空调聚合提供调峰服务等新业务将涉及海量的低成本物联网终端[45]，需要采用轻量级的终端加密认证方法。文献[46]提出的纯软件加解密方式实现终

端对配电网遥控指令和主站身份验证，能满足低成本要求，但安全性存在不足。

由表 2 可知，不同于 PKI 体系，基于身份标识的密码体系(identity-based cryptograph，IBC)可采用终端编号标识作为公钥，无需 PKI 模式下的数字证书，可省去 CA 机构，不再需要申请与验证证书，节省了证书的管理和维护成本；发送消息时既不用验证对方公钥合法性，也不用接收方提前申请私钥。作为一种无证书体系，基于 IBC 标识的 SM9 算法可将设备 ID 用作公钥而无需嵌入 ESAM 模块，特别适用于低成本物联网终端。为进一步提高终端认证安全性，文献[47]采用可将秘密分割存储的门限密码改进了 SM9 算法，将私钥分割成 2 份，一份存储在电力终端内存中，另一份存储在终端边缘计算设备中，可在提高认证效率的同时保证私钥存取安全性。

2.2.2　数据隐私保护方法

配用电系统物联网终端采集的用户数据隐含大量用户隐私，是网络攻击的重要对象。数据隐私保护是电力物联网安全防护的重点和难点。

现有的隐私数据保护方法大多基于安全加密算法，主要有利用终端属性的基于属性加密算法、基于代理重加密算法和适用于全量数据的同态加密算法[29]。关键感知节点安全性要求较高，可采用量子密钥分发方法，但对终端计算能力有较高要求。针对物联网终端计算资源受限的特点，研究者提出一些具有低开销、高混淆特征的数据加密算法，如电气量标签加密算法、混沌加密算法、上下行分组加密算法[48-49]。文献[50]构建了基于雾计算的电网模型，提出了支持集成通信和功能查询的高效安全防护技术，利用云雾协同来实现低延迟通信和电力数据存储，并对数据传输过程进行加密，从而保证了数据的隐私性和机密性。文献[51]提出了基于多源反馈信息融合的物联网边缘终端信任机制，该机制用于全局信任计算，对于恶意反馈提供者引起的恶意攻击更加可靠。为保证在数据挖掘的同时不被攻击泄露隐私信息，文献[52]改造了基于隐私保护的神经网络和贝叶斯网络算法，从而保证了在数据挖掘过程中隐私信息的安全性；文献[53]提出基于随机梯度下降的优化算法，可在实现数据隐私保护的同时提高深度学习的准确性。此外，也还有一些通过改进 S-box 的实现方案轻量化现有加密系统以及设计适用于轻量级物联网设备上的 AAβ 非对称加密方案等技术方案[54]，可用于物联网终端的轻量级数据加密。

2.2.3　时间攻击检测

时间同步攻击容易与卫星时间接收装置异常混淆，隐蔽性强，较少引起关注。目前，针对时间同步攻击的识别检测才刚刚起步。国内外研究者结合配用电终端时间同步相关特征提出了多种时间同步攻击识别检测方法，对比如表 3，详述如下：

1）基于时间跳变的攻击检测

针对时间同步攻击注入欺骗卫星导航报文往往会造成时间突变的特点，2017 年发布的《智能变电站时间同步系统及设备技术规范》完善了之前技术规范仅要求在失去卫星时钟信号时守时而未要求检测虚假时间同步信号的缺陷，要求利用本地时钟进行卫星同步时间的跳变检测，在每秒时间跳变>0.2 μs 时认为遭到卫星时间同步攻击进行本地守时[55]。但攻击方采用慢速持续时间同步攻击，将每秒的时间偏差控制在 0.2 μs 阈值以下，仍可通过持续慢速攻击造成破坏后果。由于持续的卫星时间同步攻击会使得系统的 PPS 信号具有趋势性的偏差，有可能采用 Kalman 滤波识别这种趋势性特征，检测慢速持续时间同步攻击。

表 2　PKI 体系和 IBC 体系对比

Table 2　Comparison of PKI system and IBC system

体系	公钥	成本与复杂度	离线加解密
PKI	随机数	成本较高，通信前必须接收、验证对方证书	不支持，发送前必须验证证书
IBC	用户标识(如 ID、邮箱)	成本较低，发送方只需知道接收方身份标识	可本地离线加解密

表 3　时间同步攻击检测方法

Table 3　Detection methods of time synchronization attack

文献	分类	原理	优势与不足
[55]	基于时间跳变	时间同步攻击注入欺骗卫星导航报文往往会造成时间突变	可检测每秒时间跳变>0.2 μs 的卫星时间同步攻击，不能检测出每秒<0.2 μs 跳变的慢速持续时间同步攻击
[56]	基于卫星信号特征	卫星信号的强度变化规律、方位特性、信号频谱特征等固有特性	有 13 种时间攻击技术和 13 种检测技术，但每种检测技术都存在一定盲区
[57-58]	基于状态估计	多个节点 PMU 量测数据对比	少量节点遭到时间同步攻击时可有效检测，但配用电物联网终端一般与后台对时，后台为单个节点，该方法不适用

2）基于卫星信号特征的攻击检测

卫星时间同步攻击是通过伪造卫星导航电文实施欺骗攻击，利用卫星信号的强度变化规律、方位特性、信号频谱特征等特性，可以识别检测不同手法虚构的卫星导航电文。文献[56]基于几种基本攻击模式及其组合总结了 13 种时间攻击技术，并对应地给出了 13 种检测方法，分析指出每种检测方法的局限性，且不能确保识别出时间同步攻击。尽管组合应用不同的检测技术可以显著提高时间同步攻击的检测成功率，但也会抬高成本而限制适用范围。

3）融合多站点信息的时间同步攻击检测

因为卫星时间同步攻击往往针对的是一个或少量节点的电力时间同步装置，采用状态估计方法估计残差，可识别遭时间同步攻击的单个节点并校正时钟[57]。利用电网发生扰动时多个节点的同步相量测量单元(phasor measurement unit, PMU)量测数据均会有所表征的特点，还可采用完全分布式的检测方法，在 1/2 以下节点遭时间同步攻击时检测出遭攻击的电网节点[58]。需要指出的是，以上方法均依赖于多个节点间在时间同步和电气耦合上的关联关系，对于配用电系统中的物联网终端而言，仅在主站侧单点存在电力时间同步装置，难以利用多站点信息，因此该类方法不适用。

配用电系统中的物联网终端，对时间同步允许的时间偏差一般可在秒级以上，按照 2017 版智能变电站时间同步技术规范配置电力时间同步装置，可满足应用需求。

2.2.4 非法无线通信链路检测

电力物联网终端一般需要经过无线通信基站接入系统，其间可能接入伪基站等非法无线通信链路。针对该问题，国内外学者主要从基站位置分析和设备指纹的角度开展异常检测研究，各方法对比如表 4 并详述如下：

表 4 非法无线通信链路检测方法

Table 4 Detection methods of malicious wireless communication link

文献	分类与检测原理	优势与不足
[59]	基于基站位置合规性：根据基站编号可查询位置区码，进而判断与当前位置距离是否合理	实现简单，但需要能通信更新基站位置区码对应地理坐标，且可能盗用相邻的真实基站位置区码造成失效
[60-61]	基于瞬时信号设备指纹：终端开/关过程瞬时特征或调制信号等特征存在差异	终端固有特性，伪造困难，识别检测对终端计算资源要求高
[62-64]	基于终端的射频指纹：终端固有硬件差异造成无线信号的独有特征	
[66]	基于基站信号强度变化相似性：合法基站信号强度变化规律相似，可聚类识别有显著差异的伪基站	计算资源要求低，伪基站长期停留后会和合法基站一样有相近的信号强度变化曲线，在一定时间窗内有效

1）基于基站位置合规性的异常检测

电信服务商的无线基站都标识有编号和对应位置的区码。根据基站编号可以查询到所处位置的经纬度。根据接入无线基站发送的位置区码所在地点和用户当前位置的距离，即可判断是否合理。此外，根据无线基站位置区码和其他基站位置区码是否有明显偏离，也可识别异常[59]。但若攻击方复制邻近真实基站的位置区码，则该方法将失效。

2）基于瞬时信号设备指纹的异常检测

无线通信设备在元器件参数上存在细微差异，发出信号的频谱有所不同。利用设备在通信频谱上具有细微差异的特点，可将终端开/关过程瞬时特征或调制信号差异等特征作为设备指纹，识别出目标设备身份。文献[60]将无线电信号开/关的振幅和相位变化值、载波信号峰值数等瞬时特征作为设备指纹来识别设备身份。文献[61]则利用无线网卡在元件参数的差异抽取无线网络在调制域的相应特征作为设备指纹，进而识别设备身份。基于瞬时信号的设备指纹方法对终端性能有较高要求，限制了它在计算资源有限的配用电物联网终端中的应用。

3）基于终端固有射频指纹的异常检测

终端在制造中存在固有的硬件差异，使得其发送的无线信号产生独特的畸变、失真等损伤，该特征难以被伪装和篡改，可借助分析无线信号所具备的特征来识别发送信号设备的身份[62-63]。文献[64]根据终端固有的射频指纹特征，利用深度学习来实现设备身份双向认证，可避免终端接入非法通信链路。该方法同样要求很强的计算力，不适用于物联网终端。

4）基于基站信号强度变化相似性的异常检测

体感物联网终端可将感知到人体姿态变化导致信号强度变化的规律性特征作为身份指纹，来识别用户身份[65]。采用类似方法，也可为计算资源有限的电力物联网终端进行基站身份认证。与伪基站多流串作案不同，物联网终端和合法无线基站一般固定部署于特定位置，终端感知到的多个合法基站的信号强度具有相似变化规律，并与伪基站信号强度变化规律存在显著差异。可将基站信号强度时间

序列作为设备指纹，聚类识别信号强度变化规律明显不同的伪基站[66]。

3　研究展望

当前，电力物联网仍处于早期发展阶段，物联网终端渗透率还在持续快速增长，承载的业务功能及遭攻击破坏的后果也将随着物联网技术应用深度和广度的发展而快速增加，可能发展为有组织攻击的重要目标。在比特币匿名支付方式的支持下，不但可以入侵后劫持大量物联网终端勒索比特币，还可劫持物联网终端形成僵尸网络进行比特币挖矿，极大地消除了网络攻击的收益兑现瓶颈[67]，可能显著促进面向电力物联网的有组织网络攻击[68]。

除了提高物联网终端安全防护基线、避免弱密码/缺省密码并关闭不必要的服务和推广应用可信计算技术以外，开展网络安全威胁的评估与检测是提高电力物联网安防水平重要途径。由于安全威胁的形态多样化，传统上依靠神经网络、专家系统、模糊逻辑等人工智能方法评估和检测安全威胁与异常的特征相对困难，多存在误报率/漏报率偏高的问题，难以满足复杂系统的安全性分析需求[69]。为了充分挖掘利用以深度学习为代表的新一代人工智能技术来提高网络攻防对抗能力，美国国防高级研究计划局(DARPA)于 2016 年召开了由人工智能选手(Mayhem)对抗 DEF CON 竞赛人类团队的自动网络攻防竞赛[70]，并由此揭开了应用机器学习与深度学习进行网络攻防对抗研究的热潮。

入侵检测是一种实时监测网络和主机来识别和检测异常行为的安全防护技术，可以识别进入系统内部的网络安全威胁，可用于开放环境下物联网终端的安全威胁检测。入侵检测按检测原理可分为异常入侵检测和误用入侵检测。其中，异常入侵检测可根据统计分析、数据挖掘或机器学习检测入侵行为。进行异常入侵检测时，常需要选择一定的特征指标，然后根据特征判断是否存在入侵。但在实际网络场景中，由于缺乏足够的先验知识和已标注的数据样本，人工标注数据样本不但任务重、成本高，很可能还难以覆盖足够的场景组合而达不到要求。

科研工作者利用深度学习等先进算法，围绕在样本不平衡、标记样本不足的条件下选取合适的特征进行模式分类、提高入侵检测性能，开展了大量工作。文献[71]针对网络异常的特征复杂和多维、特征提取过程复杂的难题，提出自编码网络深度学习的入侵检测方法。首先将网络特征数据输入到由多个自编码网络叠加而成的深度自编码网络模型，利用深度自编码网络模型逐层抽取网络数据分布规则以获得新的低维特征数据集；然后利用 BP 算法对学习到的低维数据进行分类识别，从而提高异常分类准确率，降低误报率。针对工业控制系统数据维度高、噪声冗余严重，数据特征提取不足会严重影响入侵检测性能的问题，文献[72]利用相近特征数据之间相关信息熵较高的特点，提出了一种基于相关信息熵和卷积神经网络−双向长短期记忆网络(convolutional neural networks-bidirectional long short-term memory, CNN-BiLSTM)的入侵检测方法，在 CNN 和 BiLSTM 中进一步利用相关信息熵优选特征。基于天然气管道工控系统的网络数据验证了所提方法的比较优势。特征选择是特征降维的主要手段，文献[73]将非线性降维的自编码网络深度学习方法引入到入侵检测中，通过具有多个隐藏层的神经网络逐层特征变换，将样本在原空间的高维特征转换成低维特征并进一步重构样本高维特征，再在该非监督学习过程中将获得的原始数据低维化，从而显著降低数据的维数。针对难以获得标注数据的问题，文献[74]提出利用生成式对抗网络(generative adversarial networks, GAN)进行无监督生成推理的网络安全威胁检测评估方法，首先采用变分自动编码器(variational auto-encoder, VAE)学习数据的先验分布，并将其与 GAN 的判别器结合，利用 GAN 判别器的结果作为 VAE 重构样本的基础，从而在保证样本多样性条件的同时提高样本的映射能力，能有效表征网络安全威胁。

除了从算法层面进行改进外，物联网系统中还存在边缘侧安全设备计算资源有限等因素制约，不一定能采用有较高计算性能要求的方法进行安全检测。采用误用入侵检测方法，可将一些场景下的规律总结形成规则，进行对计算资源要求不高的攻击行为检测。文献[75]利用同一近距离邻域内物联网终端在检测到同一行为时检测的状态量应有相近变化规律的特点，提出了一种基于数据变化相似性规律的攻击检测方法，采用卡尔曼滤波消除噪声干扰后，可在计算资源受限条件下识别物联网终端异常。

从实际攻击破坏的后果来看，单个物联网终端遭攻击破坏的后果是有限的，但大批电力物联网终端遭劫持形成僵尸网络(botnet)后，控制者可指挥所

有被劫持终端进行协同攻击，可能造成安全风险跃迁，甚至危及电网安全[23]。及时检测发现物联网终端僵尸网络，是消除物联网安全风险的一个重要目标。既有僵尸网络检测方法依赖人工根据经验选取网络流量属性\时间和行为等特征来建立检测模型，但对手可通过改变特征来逃避检测。文献[76]提出了基于 CNN 和循环神经网络(recurrent neural network, RNN)的僵尸网络检测模型，从原始流量中自动提取时间维度与空间维度的特征。提取空间特征时，将每条数据流转化为一张灰度图像，然后利用 CNN 学习灰度图像的特征；提取时间特征时，将每个数据分组中的字节序列及每条数据流中的数据分组序列作为输入建立双层双向 LSTM 神经网络，并从中学习特征。它结合时空特征对网络流量进行全面刻画，可既不依赖于协议和拓扑的先验知识，也不要人工参与特征选择，实现较高的准确率与低误报率，能满足实际使用需求。

电力物联网终端面临的安全威胁会随着其承载业务所对应攻击收益和破坏后果的变化而不断演化，保持对新型威胁的认知是做好安全防护的重要基础。理论上，需要将人工智能领域的最新进展与电力物联网终端安防结合，提高异常检测的准确性；工程上，需要结合业务场景提炼适用的特征，拓展对计算资源要求不高的异常入侵检测方法，满足物联网终端计算资源受限条件下安全防护的需要；认知上，需要搭建电力物联网在未来的隔墙售电等各种新型和典型业务场景中的蜜罐系统，检测并分析实际入侵的安全威胁，及时构建对新生风险源的攻击破坏机理的认知。电力物联网终端分散部署于复杂环境下，攻击方利用终端安全漏洞进行攻击破坏的设备安全风险较为突出。与此同时，电力物联网终端承载业务对其可用性有较高要求，进行升级打补丁易造成业务功能不可用等风险。借助蜜罐系统来准确认识物联网终端的攻击破坏机理、并以此为基础改进终端设计，是提高设备安全等级的重要手段。

4 结论

城市能源互联网中，散布于用户侧的电力物联网终端难以采用电力系统传统的物理隔离和专网通信进行安全防护，容易成为网络攻击的目标甚至发展为攻击生产控制区的跳板，引发安全事故。本文围绕电力物联网的安全防护展开分析，开展的工作如下：

1）首先分析了电力物联网的整体框架和终端面临的安全挑战，结合物联网终端资源受限和兼容性要求高等特征总结了终端安全风险的特征，分析配用电终端采用的安全防护方法并指出了存在的不足。

2）分析了计算资源受限的物联网终端在加密认证、隐私保护、时间同步、接入非法无线通信链路及 230 MHz 无线专网遭恶意干扰阻塞通信等方面的安全威胁，分析了在不同可用资源条件下应对上述典型威胁的防护方法。

3）综述了以深度学习为代表的新一代人工智能技术在电力物联网的攻击威胁检测和僵尸物联网检测等网络安全防护中的应用，从物联网终端自身特点及其攻击形式出发，对物联网新兴应用场景下的安全防护进行了展望。

参考文献 References

[1] 董朝阳，赵俊华，文福拴，等. 从智能电网到能源互联网：基本概念与研究框架[J]. 电力系统自动化，2014，38(15)：1-11.
DONG Zhaoyang, ZHAO Junhua, WEN Fushuan, et al. From smart grid to energy internet: basic concept and research framework[J]. Automation of Electric Power Systems, 2014, 38(15): 1-11.

[2] 洪居华，刘俊勇，向 月，等. 城市能源互联网初步认识与研究展望[J]. 电力自动化设备，2017，37(6)：15-25.
HONG Juhua, LIU Junyong, XIANG Yue, et al. Preliminary understanding and research prospect of urban energy internet[J]. Electric Power Automation Equipment, 2017, 37(6): 15-25.

[3] 王 玮，李 睿，姜久春. 面向能源互联网的配电系统规划关键问题研究综述与展望[J]. 高电压技术，2016，42(7)：2028-2036.
WANG Wei, LI Rui, JIANG Jiuchun. Key issues and research prospects of distribution system planning orienting to energy internet[J]. High Voltage Engineering, 2016, 42(7): 2028-2036.

[4] 吴姗姗，宁 昕，郭 创，等. 配电物联网在新产业形态中的应用探讨[J]. 高电压技术，2019，45(6)：1723-1728.
WU Shanshan, NING Xin, GUO Shen, et al. Discussion on application of distribution internet of things in new industry form[J]. High Voltage Engineering, 2019, 45(6): 1723-1728.

[5] 江秀臣，刘亚东，傅晓飞，等. 输配电设备泛在电力物联网建设思路与发展趋势[J]. 高电压技术，2019，45(5)：1345-1351.
JIANG Xiuchen, LIU Yadong, FU Xiaofei, et al. Construction ideas and development trends of transmission and distribution equipment of the ubiquitous power internet of things[J]. High Voltage Engineering, 2019, 45(5): 1345-1351.

[6] 刘日亮，刘海涛，夏圣峰，等. 物联网技术在配电台区中的应用与思考[J]. 高电压技术，2019，45(6)：1707-1714.
LIU Riliang, LIU Haitao, XIA Shengfeng, et al. Internet of things technology application and prospects in distribution transformer service area management[J]. High Voltage Engineering, 2019, 45(6): 1707-1714.

[7] 高昆仑，辛耀中，李 钊，等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化，2015，39(1)：48-52.

GAO Kunlun, XIN Yaozhong, LI Zhao, et al. Development and process of cybersecurity protection architecture for smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 48-52.

[8] 徐绍史. 中华人民共和国国家发展和改革委员会令第 14 号令　电力监控系统安全防护规定[EB/OL]. (2014-08-01)[2021-01-27]. http://www.gov.cn/gongbao/content/2014/content_2758709. htm.
XU Shaoshi. Order No. 14 of the National Development and Reform Commission of the People's Republic of China regulations on the safety protection of electric power monitoring systems[EB/OL]. (2014-08-01)[2021-01-27]. http://www.gov.cn/gongbao/content/2014/content_2758709. htm.

[9] 荆孟春，王继业，程志华，等. 电力物联网传感器信息模型研究与应用[J]. 电网技术，2014，38(2)：532-537.
JING Mengchun, WANG Jiye, CHENG Zhihua, et al. Research and application of sensor information model in power internet of things[J]. Power System Technology, 2014, 38(2): 532-537.

[10] 刘　念，余星火，王剑辉，等. 泛在物联的配用电优化运行：信息物理社会系统的视角[J]. 电力系统自动化，2020，44(1)：1-12.
LIU Nian, YU Xinghuo, WANG Jianhui, et al. Optimal operation of power distribution and consumption system based on ubiquitous internet of things: a cyber-physical-social system perspective[J]. Automation of Electric Power Systems, 2020, 44(1): 1-12.

[11] 吕　军，盛万兴，刘日亮，等. 配电物联网设计与应用[J]. 高电压技术，2019，45(6)：1681-1688.
LÜ Jun, SHENG Wanxing, LIU Riliang, et al. Design and application of power distribution internet of things[J]. High Voltage Engineering, 2019, 45(6): 1681-1688.

[12] 张冀川，陈　蕾，张明宇，等. 配电物联网智能终端的概念及应用[J]. 高电压技术，2019，45(6)：1729-1736.
ZHANG Jichuan, CHEN Lei, ZHANG Mingyu, et al. Conception and application of smart terminal for distribution internet of things[J]. High Voltage Engineering, 2019, 45(6): 1729-1736.

[13] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术物联网感知终端应用安全技术要求：GB/T 36951—2018[S]. 北京：中国标准出版社，2018.
State Administration for Market Regulation, Standardization Administration. Information security technology—security technical requirements for application of sensing terminals in internet of things: GB/T 36951—2018[S]. Beijing, China: Standards Press of China, 2018.

[14] 曲朝阳，董运昌，刘　帅，等. 基于生物免疫学方法的泛在电力物联网安全技术[J]. 电力系统自动化，2020，44(2)：1-12.
QU Zhaoyang, DONG Yunchang, LIU Shuai, et al. Bioimmunological method based security technology of ubiquitous power internet of things[J]. Automation of Electric Power Systems, 2020, 44(2): 1-12.

[15] BURG A, CHATTOPADHYAY A, LAM K Y. Wireless communication and security issues for cyber-physical systems and the internet-of-things[J]. Proceedings of the IEEE, 2018, 106(1): 38-60.

[16] 张　涛，赵东艳，薛　峰，等. 电力系统智能终端信息安全防护技术研究框架[J]. 电力系统自动化，2019，43(19)：1-8，67.
ZHANG Tao, ZHAO Dongyan, XUE Feng, et al. Research framework of cyber-security protection technologies for smart terminals in power system[J]. Automation of Electric Power Systems, 2019, 43(19): 1-8, 67.

[17] KOLIAS C, KAMBOURAKIS G, STAVROU A, et al. DDoS in the IoT: mirai and other botnets[J]. Computer, 2017, 50(7): 80-84.

[18] 李　田，苏　盛，杨洪明，等. 电力信息物理系统的攻击行为与安全防护[J]. 电力系统自动化，2017，41(22)：162-167.
LI Tian, SU Sheng, YANG Hongming, et al. Attacks and cyber security defense in cyber-physical power system[J]. Automation of Electric Power Systems, 2017, 41(22): 162-167.

[19] 高昆仑，王志皓，安宁钰，等. 基于可信计算技术构建电力监测控制系统网络安全免疫系统[J]. 工程科学与技术，2017，49(2)：28-35.
GAO Kunlun, WANG Zhihao, AN Ningyu, et al. Construction of the immune system of cyber security for electric power supervise and control system based on trusted computing[J]. Advanced Engineering Sciences, 2017, 49(2): 28-35.

[20] 彭安妮，周　威，贾　岩，等. 物联网操作系统安全研究综述[J]. 通信学报，2018，39(3)：22-34.
PENG Anni, ZHOU Wei, JIA Yan, et al. Survey of the internet of things operating system security[J]. Journal on Communications, 2018, 39(3): 22-34.

[21] TIBURSKI R T, MORATELLI C R, JOHANN S F, et al. Lightweight security architecture based on embedded virtualization and trust mechanisms for IoT edge devices[J]. IEEE Communications Magazine, 2019, 57(2): 67-73.

[22] JING Q, VASILAKOS A V, WAN J F, et al. Security of the internet of things: perspectives and challenges[J]. Wireless Networks, 2014, 20(8): 2481-2501.

[23] 王　宇，李俊娥，周　亮，等. 针对嵌入式终端安全威胁的电力工控系统自愈体系[J]. 电网技术，2020，44(9)：3582-3594.
WANG Yu, LI Jun'e, ZHOU Liang, et al. A self-healing architecture for power industrial control systems against security threats to embedded terminals[J]. Power System Technology, 2020, 44(9): 3582-3594.

[24] 赵　兵，翟　峰，李涛永，等. 适用于智能电表双向互动系统的安全通信协议[J]. 电力系统自动化，2016，40(17)：93-98.
ZHAO Bing, ZHAI Feng, LI Taoyong, et al. Secure communication protocol for smart meter bidirectional interaction system[J]. Automation of Electric Power Systems, 2016, 40(17): 93-98.

[25] 李中伟，朱识天，崔秀帅，等. 基于改进 NSSK 协议的智能变电站密钥管理方案[J]. 电力系统自动化，2017，41(5)：139-146.
LI Zhongwei, ZHU Shitian, CUI Xiushuai, et al. Key management scheme of smart substation based on improved NSSK protocol[J]. Automation of Electric Power Systems, 2017, 41(5): 139-146.

[26] 王志贺，骆　钊，谢吉华，等. 基于 SM2 密码体系的 SD 卡的电力移动终端安全接入方案[J]. 中国电力，2015，48(5)：75-80.
WANG Zhihe, LUO Zhao, XIE Jihua, et al. Secure access of electric power mobile terminal using SM2-crypto-system-based SD card[J]. Electric Power, 2015, 48(5): 75-80.

[27] 蔡月明，封士永，杜红卫，等. 面向泛在电力物联网的边缘节点感知自适应数据处理方法[J]. 高电压技术，2019，45(6)：1715-1722.
CAI Yueming, FENG Shiyong, DU Hongwei, et al. Novel edge-ware adaptive data processing method for the ubiquitous electric power internet of things[J]. High Voltage Engineering, 2019, 45(6): 1715-1722.

[28] 龚钢军，罗安琴，陈志敏，等. 基于边缘计算的主动配电网信息物理系统[J]. 电网技术，2018，42(10)：3128-3135.
GONG Gangjun, LUO Anqin, CHEN Zhimin, et al. Cyber physical system of active distribution network based on edge computing[J]. Power System Technology, 2018, 42(10): 3128-3135.

[29] 张佳乐，赵彦超，陈　兵，等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报，2018，39(3)：1-21.
ZHANG Jiale, ZHAO Yanchao, CHEN Bing, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39(3): 1-21.

[30] HE D J, YE R, CHAN S, et al. Privacy in the internet of things for smart healthcare[J]. IEEE Communications Magazine, 2018, 56(4): 38-44.

[31] 陈皓勇，李志豪，陈锦彬，等. 电力物联网：数据科学视角及商业模式[J]. 电力系统保护与控制，2020，48(22)：33-40.
CHEN Haoyong, LI Zhihao, CHEN Jinbin, et al. Power internet of things: data science perspective and business models[J]. Power System Protection and Control, 2020, 48(22): 33-40.

[32] 白昱阳，黄彦浩，陈思远，等. 云边智能：电力系统运行控制的边缘计算方法及其应用现状与展望[J]. 自动化学报，2020，46(3)：397-410.
BAI Yuyang, HUANG Yanhao, CHEN Siyuan, et al. Cloud-edge intelligence: status quo and future prospective of edge computing approaches and applications in power system operation and control[J]. Acta Automatica Sinica, 2020, 46(3): 397-410.

[33] 钱 斌，蔡梓文，肖 勇，等. 电力系统时间同步攻击研究综述[J]. 电网技术，2020，44(10)：4035-4045.
QIAN Bin, CAI Ziwen, XIAO Yong, et al. Review on time synchronization attack in power system[J]. Power System Technology, 2020, 44(10): 4035-4045.

[34] 刘 亮，苏 盛，陈晓国，等. 时间同步攻击对雷电定位系统的影响与分析[J]. 高电压技术，2020，46(12)：4319-4325.
LIU Liang, SU Sheng, CHEN Xiaoguo, et al. Influence and analysis of time synchronization attack on lightning location system[J]. High Voltage Engineering, 2020, 46(12): 4319-4325.

[35] 刘 亮，苏 盛，钱 斌，等. 计量自动化系统卫星时间同步攻击危害与防护[J]. 南方电网技术，2020，14(1)：3-9，17.
LIU Liang, SU Sheng, QIAN Bin, et al. Impact and protection of satellite time synchronization attacks in advanced metering infrastructure[J]. Southern Power System Technology, 2020, 14(1): 3-9, 17.

[36] KERNS A J, SHEPARD D P, BHATTI J A, et al. Unmanned aircraft capture and control via GPS spoofing[J]. Journal of Field Robotics, 2014, 31(4): 617-636.

[37] MOUSAVIAN S, EROL-KANTARCI M, ORTMEYER T. Cyber attack protection for a resilient electric vehicle infrastructure[C]// Proceedings of 2015 IEEE Globecom Workshops (GC Wkshps). San Diego, USA: IEEE, 2015: 1-6.

[38] 王一蓉，邹 颖，王艳茹. 电力无线虚拟专网组网架构及 IP 地址分配研究[J]. 电力信息与通信技术，2014，12(6)：16-21.
WANG Yirong, ZOU Ying, WANG Yanru. Study of network architecture and IP address allocation of wireless VPN for power grid[J]. Electric Power Information and Communication Technology, 2014, 12(6): 16-21.

[39] 王 赞，陈 光，董 晓，等. 基于工业互联网的智慧能源服务系统架构研究[J]. 电力系统保护与控制，2020，48(3)：77-83.
WANG Zan, CHEN Guang, DONG Xiao, et al. Research on the architecture of smart energy service system based on industrial internet[J]. Power System Protection and Control, 2020, 48(3): 77-83.

[40] 李 赓，赵玉萍，孙春来，等. 一种基于伪信令的伪基站抑制方法研究与分析[J]. 信息网络安全，2014(9)：12-16.
LI Geng, ZHAO Yuping, SUN Chunlai, et al. Research on a new proposed fake base station restraining scheme based on pseudo signal[J]. Netinfo Security, 2014(9): 12-16.

[41] 吴亦贝，李俊娥，陈 汹，等. 大规模可控负荷被恶意控制场景下配电网风险分析[J]. 电力系统自动化，2018，42(10)：30-37.
WU Yibei, LI Jun'e, CHEN Xiong, et al. Risk analysis of distribution network with large-scale controllable loads with attacks[J]. Automation of Electric Power Systems, 2018, 42(10): 30-37.

[42] 李 志，吴 赛，王智慧，等. LTE 230 MHz 电力无线专网路测系统设计[J]. 电力信息与通信技术，2019，17(5)：1-6.
LI Zhi, WU Sai, WANG Zhihui, et al. Design of drive test system for LTE 230 MHz electric power wireless private network[J]. Electric Power Information and Communication Technology, 2019, 17(5): 1-6.

[43] 童军民，由奇林，孙 晨，等. 230 MHz 电力无线专网干扰规避策略研究[J]. 电力信息与通信技术，2020，18(3)：27-33.
TONG Junmin, YOU Qilin, SUN Chen, et al. Research on interference avoidance strategy in 230 MHz power wireless private network[J]. Electric Power Information and Communication Technology, 2020, 18(3): 27-33.

[44] 苏吟雪，田海博. 基于 SM2 的双方共同签名协议及其应用[J]. 计算机学报，2020，43(4)：701-710.
SU Yinxue, TIAN Haibo. A two-party SM2 signing protocol and its application[J]. Chinese Journal of Computers, 2020, 43(4): 701-710.

[45] 李 彬，贾滨诚，曹望璋，等. 边缘计算在电力需求响应业务中的应用展望[J]. 电网技术，2018，42(1)：79-87.
LI Bin, JIA Bincheng, CAO Wangzhang, et al. Application prospect of edge computing in power demand response business[J]. Power System Technology, 2018, 42(1): 79-87.

[46] 杨洪涛，汝雁飞，盛立健，等. 基于 OpenSSL 的配电网终端遥控加密测试软件实现方式[J]. 电力系统自动化，2012，36(18)：77-81.
YANG Hongtao, RU Yanfei, SHENG Lijian, et al. Implementation of remote control encryption test software in the distribution network terminal based on OpenSSL[J]. Automation of Electric Power Systems, 2012, 36(18): 77-81.

[47] 许盛伟，任雄鹏，袁 峰，等. 一种关于 SM9 的安全密钥分发方案[J]. 计算机应用与软件，2020，37(1)：314-319.
XU Shengwei, REN Xiongpeng, YUAN Feng, et al. A secure key issuing scheme of SM9[J]. Computer Applications and Software, 2020, 37(1): 314-319.

[48] 周 峰，周 晖，刁赢龙. 泛在电力物联网智能感知关键技术发展思路[J]. 中国电机工程学报，2020，40(1)：70-82.
ZHOU Feng, ZHOU Hui, DIAO Yinglong. Development of intelligent perception key technology in the ubiquitous internet of things in electricity[J]. Proceedings of the CSEE, 2020, 40(1): 70-82.

[49] 江秀臣，罗林根，余钟民，等. 区块链在电力设备泛在物联网应用的关键技术及方案[J]. 高电压技术，2019，45(11)：3393-3400.
JIANG Xiuchen, LUO Lingen, YU Zhongmin, et al. Technologies and solutions of blockchain application in power equipment ubiquitous internet of things[J]. High Voltage Engineering, 2019, 45(11): 3393-3400.

[50] LIU J N, WENG J, YANG A J, et al. Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid[J]. IEEE Transactions on Smart Grid, 2020, 11(1): 247-257.

[51] YUAN J, LI X Y. A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion[J]. IEEE Access, 2018, 6: 23626-23638.

[52] XIAO Y H, JIA Y Z, LIU C C, et al. Edge computing security: state of the art and challenges[J]. Proceedings of the IEEE, 2019, 107(8): 1608-1631.

[53] SHOKRI R, SHMATIKOV V. Privacy-preserving deep learning[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, USA: ACM, 2015: 1310-1321.

[54] BANSOD G, RAVAL N, PISHAROTY N. Implementation of a new lightweight encryption design for embedded security[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(1): 142-151.

[55] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 智能变电站时间同步系统及设备技术规范：GB/T 33591—2017[S]. 北京：中国标准出版社，2017.
General Administration of Quality Supervision, Inspection and Quar-

antine of the People's Republic of China, Standardization Administration. Technical specification of time synchronism system and equipment in smart substation: GB/T 33591—2017[S]. Beijing, China: Standards Press of China, 2017.

[56] PSIAKI M L, HUMPHREYS T E. GNSS spoofing and detection[J]. Proceedings of the IEEE, 2016, 104(6): 1258-1270.

[57] FAN X Y, DU L, DUAN D L. Synchrophasor data correction under GPS spoofing attack: a state estimation based approach[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4538-4546.

[58] WANG Y Q, HESPANHA J P. Distributed estimation of power system oscillation modes under attacks on GPS clocks[J]. IEEE Transactions on Instrumentation and Measurement, 2018, 67(7): 1626-1637.

[59] CHEN C M, CHEN Y H, LIN Y H, et al. Eliminating rouge femtocells based on distance bounding protocol and geographic information[J]. Expert Systems with Applications, 2014, 41(2): 426-433.

[60] PATEL H J, TEMPLE M A, BALDWIN R O. Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting[J]. IEEE Transactions on Reliability, 2015, 64(1): 221-233.

[61] CHOUCHANE A, REKHIS S, BOUDRIGA N. Defending against rogue base station attacks using wavelet based fingerprinting[C]// Proceedings of 2009 IEEE/ACS International Conference on Computer Systems and Applications. Rabat, Morocco: IEEE, 2009: 523-530.

[62] XU Q, ZHENG R, SAAD W, et al. Device fingerprinting in wireless networks: challenges and opportunities[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 94-104.

[63] POLAK A C, GOECKEL D L. Wireless device identification based on RF oscillator imperfections[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2492-2501.

[64] 刘　铭，刘　念，韩晓艺，等. 一种基于射频指纹的电力物联网设备身份识别方法[J]. 中国电力，2021，54(3)：80-88.
LIU Ming, LIU Nian, HAN Xiaoyi, et al. A RF fingerprint based EIoT device identification method[J]. Electric Power, 2021, 54(3): 80-88.

[65] WANG W, YANG L, ZHANG Q, et al. Securing on-body IoT devices by exploiting creeping wave propagation[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 696-703.

[66] 肖　勇，钱　斌，蔡梓文，等. 电力物联网终端非法无线通信链路检测方法[J]. 电工技术学报，2020，35(11)：2319-2327.
XIAO Yong, QIAN Bin, CAI Ziwen, et al. Malicious wireless communication link detection of power internet of thing devices[J]. Transactions of China Electrotechnical Society, 2020, 35(11): 2319-2327.

[67] 罗军舟，杨　明，凌　振，等. 匿名通信与暗网研究综述[J]. 计算机研究与发展，2019，56(1)：103-130.
LUO Junzhou, YANG Ming, LING Zhen, et al. Anonymous communication and darknet: a survey[J]. Journal of Computer Research and Development, 2019, 56(1): 103-130.

[68] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E. Forensics and deep learning mechanisms for botnets in internet of things: a survey of challenges and solutions[J]. IEEE Access, 2019, 7: 61764-61785.

[69] 李　韵，黄辰林，王中锋，等. 基于机器学习的软件漏洞挖掘方法综述[J]. 软件学报，2020，31(7)：2040-2061.
LI Yun, HUANG Chenlin, WANG Zhongfeng, et al. Survey of software vulnerability mining methods based on machine learning[J]. Journal of Software, 2020, 31(7): 2040-2061.

[70] HSU J. DARPA challenge tests AI as cybersecurity defenders[EB/OL]. IEEE Spectrum, 2016[2021-01-27]. https://spectrum.ieee. org/tech-talk/computing/software/darpa-challenge-tests-ai-as-cybersecurity-defenders?mid=1.

[71] 丁红卫，万　良，龙廷艳. 深度自编码网络在入侵检测中的应用研究[J]. 哈尔滨工业大学学报，2019，51(5)：185-194.
DING Hongwei, WAN Liang, LONG Tingyan. Research on the application of deep auto-encoder network in intrusion detection[J]. Journal of Harbin Institute of Technology, 2019, 51(5): 185-194.

[72] 石乐义，朱红强，刘祎豪，等. 基于相关信息熵和 CNN-BiLSTM 的工业控制系统入侵检测[J]. 计算机研究与发展，2019，56(11)：2330-2338.
SHI Leyi, ZHU Hongqiang, LIU Yihao, et al. Intrusion detection of industrial control system based on correlation information entropy and CNN-BiLSTM[J]. Journal of Computer Research and Development, 2019, 56(11): 2330-2338.

[73] 高　妮，高　岭，贺毅岳，等. 基于自编码网络特征降维的轻量级入侵检测模型[J]. 电子学报，2017，45(3)：730-739.
GAO Ni, GAO Ling, HE Yiyue, et al. A lightweight intrusion detection model based on autoencoder network with feature reduction[J]. Acta Electronica Sinica, 2017, 45(3): 730-739.

[74] 杨宏宇，王峰岩，吕伟力. 基于无监督生成推理的网络安全威胁态势评估方法[J]. 清华大学学报(自然科学版)，2020，60(6)：474-484.
YANG Hongyu, WANG Fengyan, LÜ Weili. Network security threat assessment method based on unsupervised generation reasoning[J]. Journal of Tsinghua University (Science & Technology), 2020, 60(6): 474-484.

[75] ASTILLO P V, KIM J, SHARMA V, et al. SGF-MD: behavior rule specification-based distributed misbehavior detection of embedded IoT devices in a closed-loop smart greenhouse farming system[J]. IEEE Access, 2020, 8: 196235-196252.

[76] 吴　迪，方滨兴，崔　翔，等. BotCatcher：基于深度学习的僵尸网络检测系统[J]. 通信学报，2018，39(8)：18-28.
WU Di, FANG Binxing, CUI Xiang, et al. BotCatcher: botnet detection system based on deep learning[J]. Journal on Communications, 2018, 39(8): 18-28.

苏　盛(通信作者)
1975—，男，博士，教授，博导
主要研究方向为电力系统网络安全防护与电力大数据技术应用
E-mail: eessheng@163.com

SU Sheng
Ph.D., Professor
Corresponding author

汪　干
1996—，男，硕士生
主要研究方向为电力系统网络安全防护
E-mail: 1340011756@qq.com

WANG Gan

收稿日期　2021-01-27　修回日期　2021-04-02　　编辑　程子丰