配电网用户侧异构电力物联设备安全研究综述及展望

严 康[1],陆艺丹[1],于宗超[1],覃芳璐[2],刘 绚[1]
(1. 湖南大学 电气与信息工程学院,湖南 长沙 410000;2. 广西电网电力调度控制中心,广西 南宁 530000)

摘要:随着配电网用户侧异构电力物联设备(简称为“配电网用户侧物联设备”)接入电力系统,电力系统的安全防护边界变得日益模糊,使得基于物理隔离装置的安全防护体系无法成为保护电力系统运行安全的壁垒。考虑到设备的网络风险特征,配电网用户侧物联设备的网络安全给电力系统运行带来了新的隐患。为了更好地揭示电力系统在大规模配电网用户侧物联设备接入场景下所面临的安全威胁,并为制定相应的安全防护措施提供参考,对配电网用户侧物联设备的安全研究进行了全面的综述与展望。结合设备各组件间的通信架构,分析了目前配电网用户侧物联设备的网络安全脆弱性以及潜在的攻击手段;考虑配电网用户侧物联设备终端的运行特性,揭示其异常动作对电力系统造成的安全影响;从设备的“端”“管”“云”3个方面重点综述了目前配电网用户侧物联设备各组件的主要安全防护研究;对该领域未来需要深入探索的研究方向进行了展望。

关键词:配电网;物联网;异构电力物联设备;安全防护边界;网络安全
中图分类号:TM73 **文献标志码**:A DOI:10.16081/j.epae.202208014

0 引言

近年来,随着大规模配电网用户侧异构电力物联设备(下文简称为“配电网用户侧物联设备”)接入电力系统,大量用户侧的终端负荷转变为可控负荷[1],如智能空调[2]、智能热水器[3]、电动汽车[4]等。截至2020年上半年,我国配备物联网组件[5]的智能空调普及率已达到54%[6]。OMDIA联网大型智能电器报告显示,2025年全球联网大型智能电器出货量将由2020年的5460万台增涨至1.75亿台左右[7]。同时,随着家用电器保有量已达到较高的水平[8],空调等终端负荷已成为目前阶段电力系统中的最大运行负荷之一[9]。在此背景下,电力系统中暴露于互联网的可控负荷也将进一步增加。

但由于目前配电网用户侧物联设备销售市场缺乏严格的准入机制,部分设备无法形成有效的网络安全防护[10],易被黑客从互联网实施恶意攻击,从而被窃取配电网用户侧物联设备终端(下文简称为“终端”)的控制权限。在此背景下,黑客可以利用恶意软件[11]等手段操控一定规模的配电网用户侧物联设备,以此对目标系统发动攻击。2016年9月安全研究机构Krebs on Security[12]、2016年10月美国域名服务器管理服务供应商DYN[13]相继被黑客利用物联网设备实施分布式拒绝服务(distributed denial of service,DDoS)攻击,引起了国内外研究机构对物联网安全问题的广泛关注,并开展了针对DDoS攻击的安全防护研究[14-16]。但当前对配电网用户侧物联设备安全问题的认识仍不够全面,仅停留在信息域的安全[17],忽略了其终端运行特性给电力系统运行带来的安全影响。近年来,文献[18-20]揭示了黑客通过操控配电网用户侧物联设备的运行功率从而影响电力系统正常运行的可能性以及产生的危害,其中:文献[18]证明了黑客可以利用配电网用户侧物联设备致使配电网中线路的断路器跳闸,从而造成停电事故;文献[19]以欧洲电网为例说明,当可操控配电网用户侧物联设备的规模达到250万台时,黑客就可通过调节终端的运行功率以造成电力系统频率偏差,从而触发低频减载、高频切机等第三道防线安全自动装置动作,存在大面积切负荷的风险[21];文献[20]通过仿真证明了当黑客利用21万台智能空调增加1%用户负荷时,就可在夏季高峰期造成波兰电网263条传输线路故障、86%的负荷中断[20]。可见,在大规模配电网用户侧物联设备接入电力系统的场景下,配电网用户侧物联设备的网络安全会对电力系统的运行造成新的隐患。

为了更好地揭示电力系统在大规模配电网用户侧物联设备接入场景下所面临的安全威胁,本文围绕配电网用户侧物联设备的网络安全风险展开了全面综述。首先,考虑设备各组件的运行参数、安全防护能力,揭示了目前配电网用户侧物联设备的网络安全脆弱性,并介绍了设备潜在的攻击手段以及近年来的典型安全事件;然后,考虑终端的运行特性,分析了配电网用户侧物联设备的“肉鸡”僵尸网络对电力系统造成的安全影响;最后,综述了目前针对配电网用户侧物联设备网络安全防护的研究进展,并

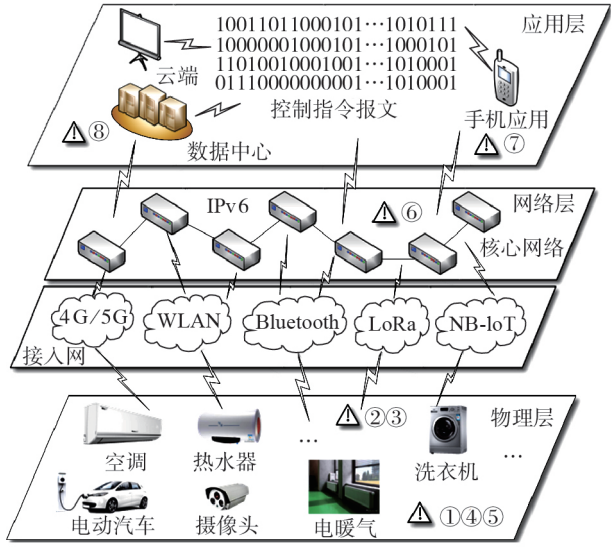
收稿日期:2022-01-16;**修回日期**:2022-05-19
在线出版日期:2022-08-09
基金项目:国家自然科学基金资助项目(51777062)
Project supported by the National Natural Science Foundation of China(51777062)

展望了未来需深入探索的研究方向。

1　配电网用户侧物联设备的网络安全隐患

1.1　配电网用户侧物联设备的通信架构

为了更好地了解配电网用户侧物联设备所面临的网络安全威胁，首先给出其通信架构，如图 1 所示。其中，配电网用户侧物联设备由终端、配电网用户侧物联设备用户手机应用（简称为“手机应用”）、配电网用户侧物联设备云端（简称为“云端”）组成。



① 终端后端组件差异性，② 终端网络连接性，③ 终端寻址识别能力
④ 终端通信保密能力，⑤ 终端固件安全，⑥ 通信安全防护能力
⑦ 手机应用安全防护能力，⑧ 云端安全防护能力

图 1　配电网用户侧物联设备的通信架构

Fig.1　Communication architecture of user side heterogeneous power Internet of Things devices in distribution network

由图 1 可知，配电网用户侧物联设备的通信架构由应用层、网络层、物理层构成[22]：①应用层由手机应用、云端构成，为配电网用户侧物联设备提供远程控制业务的实现逻辑；②网络层由通信交换机、路由器等信息设备构成，负责转发手机应用和云端生成的控制指令、终端上传的量测数据等交互信息，其使用的通信协议包括 4G / 5G[23]、IPv6[24]等；③物理层涵盖了大量的终端，如智能空调、智能热水器等。终端数量众多，极有可能使用不同的通信协议上传传感器量测数据以及接收控制指令等交互信息，如蓝牙（Bluetooth）[25]、射频识别（radio frequency identification，RFID）[26]、无线局域网（wireless local area network，WLAN）[27]、4G / 5G。

1.2　配电网用户侧物联设备的网络安全脆弱性

过去，电力物联设备属于电网公司资产，电网公司可以在设备招投标过程中规范其网络安全防护，以提升设备抵御网络攻击的能力，降低设备被网络攻击成功的概率。物联设备分类如表 1 所示。由表 1 可知，相较于电力物联设备，配电网用户侧物联设备的安全防护能力良莠不齐，且各组件间的通信依托于互联网，导致其网络安全脆弱性具有明显的差异性。

表 1　物联设备分类

Table 1　Classification of Internet of Things devices

设备	资产归属	代表设备	设备分布	通信网络	安全防护措施
电力物联设备	电网公司	智能电表	主网、配电网	电力专网、互联网	二次防护体系、各组件安全防护措施
配电网用户侧物联设备	用户	智能空调	配电网	互联网	各组件安全防护措施

为此，本节详述了配电网用户侧物联设备主要存在的网络安全脆弱性，具体如下。

1）终端后端组件差异性。

终端后端可能使用不同供应商提供的不同版本的传感器、执行器、网络协调器以及网关，从而要求终端具备后端组件的互操作能力。在这样的异构环境下，路由攻击[28]、中间人攻击[29]等恶性事件更容易发生。黑客可以轻易地冒充终端传感器，上传伪造的量测数据至云端，从而误导用户发送控制指令。

2）终端网络连接性。

在终端中，不仅不同组件之间需要进行网络连接，不同业务之间也需要进行网络连接。当量测数据来自终端自身的传感器时，其必须通过桥接设备连接到网络，然后经桥接设备连接到终端执行器。在此期间，桥接设备极有可能发生路由攻击和中间人攻击，易导致终端量测数据被篡改，诱发终端异常动作。

3）终端寻址识别能力。

终端通常使用低功率无线电网络连接组件，网络连接距离极小。由于终端网络协调器分配地址的方式并不遵循通用标准，地址隐藏于区域网网关或网桥之后，使黑客的恶意行为变得无法追踪，导致欺骗攻击[30-32]的隔离和检测变得十分困难。并且，终端网络协调器在不屏蔽外部网络的情况下可能被黑客直接访问，导致终端中的用户隐私数据被窃取或被直接控制。

4）终端通信保密能力。

部分终端的计算能力、板载内存、网络带宽等运行参数较低，无法承担高强度的密码算法。当终端量测数据、控制反馈指令等交互信息在通信链路中被多个终端加密或解密时，密钥会在多个终端之间共享，增大了密钥被黑客获取的可能性。同时，部分终端难以进行有效的安全校验。当上传量测数据等交互信息时，终端无法增加有效的安全校验信息，如随机数、新鲜性因子等；当接收用户控制指令等交互

信息时，终端也无法执行有效的安全校验。因此，黑客可以通过伪造的控制指令对部分终端进行控制或上传篡改后的终端量测数据至云端。

5）终端固件安全。

固件是运行在终端中的二进制程序，负责管理终端中的硬件外设和实现终端的功能。但目前缺乏对固件程序进行检测的有效工具，导致实际产品中存在大量携带漏洞的固件。终端固件漏洞可以分为内存漏洞和逻辑漏洞[33]。固件内存漏洞由编码和设计错误引起，会导致内存非法访问、控制流劫持攻击等。固件逻辑漏洞是指固件在认证、授权、应用等方面的设计或实现存在漏洞，黑客可以利用其构造特定的植入函数使其正常功能发生改变。

6）通信安全防护能力。

物联网通信协议由传统的传输控制协议/网际协议（transmission control protocal/Internet protocal，TCP/IP）以及物联网系统中的底层协议构成，但目前仍然存在许多严重的安全访问漏洞。文献[34]指出物联网协议栈中的低功耗有损网络路由协议（routing protocal for low-power and lossy networks，RPL）存在安全漏洞。RPL是一种距离矢量路由协议，其使用目标函数和度量来构建有相无环图。由此，Rank值在RPL中扮演着十分重要的角色，其可以用来避免循环、优化拓扑、降低控制开销等。但由于路由通信的开放性，黑客可以伪造小Rank值的路由来截取控制指令或终端量测数据。

7）手机应用安全防护能力。

由于手机平台的开源性，手机平台不存在统一事件分发机制，导致手机应用易遭受恶意攻击。目前，不同手机厂商制定的平台版本致使手机应用存在兼容性问题，导致软件保护技术难以得到稳固发展。同时，部分开发者过度注重手机应用后端程序代码的可用性，忽略了安全性。随着针对代码（DEX）文件以及共享数据库（SO）文件的攻击技术越来越成熟，黑客甚至可以使用逆向软件直接解析手机应用后端程序代码以篡改其执行逻辑。

8）云端安全防护能力。

目前手机应用、终端与云端的交互十分频繁，黑客可以通过交互路径入侵云端服务器并植入木马、蠕虫等病毒[35]，从而获取云端所储存的用户登录名、密码等，间接控制云端所连接的终端。同时，云端涉及的系统以及软件数量不断增多，导致云端存在的安全漏洞数量随之增加[36]，这会进一步影响其网络安全脆弱性。

在上述背景下，终端的组件差异性、网络连接性、寻址识别能力、通信保密能力、固件安全导致的控制指令/量测数据等交互信息的时空性和私密性得不到安全保障，会直接影响配电网用户侧物联设备的网络安全脆弱性。同时，由于长期暴露于互联网中，通信安全防护能力、手机应用安全防护能力和云端安全防护能力也会进一步影响配电网用户侧物联设备的网络安全脆弱性。

2 配电网用户侧物联设备的攻击手段与典型案例

2.1 攻击手段

由设备的网络安全脆弱性可知，黑客对配电网用户侧物联设备实施攻击的途径繁多。本节从攻击目标出发，以智能空调为例，对配电网用户侧物联设备的网络攻击手段进行分类，如表2所示。

表2 配电网用户侧物联设备的网络攻击手段分类

Table 2 Classification of cyber attack means on user side heterogeneous power Internet of Things devices in distribution network

攻击目标	典型方式	主要危害
通信链路	路由攻击、底层通信协议漏洞攻击等	截取终端、云端、手机应用的交互信息等
终端	旁道信息攻击、欺骗攻击、固件漏洞攻击等	获取终端控制权限、终端密码算法类型等
手机应用	手机应用逆向攻击、钓鱼邮件等	获取手机应用控制权限、终端密码算法等
云端	SQL注入、XSS、社会工程学攻击等	获取云端控制权限、用户隐私数据等

1）路由攻击。

黑客可以通过生成虚构的恶意路由对智能空调进行攻击。首先，黑客通过天坑攻击[37]吸引周围路由选择恶意路由作为传输路径中的关键节点，以此引诱目标区域内几乎所有智能空调用户控制指令（如开启待机的智能空调、调节智能空调的设定温度）都通过该恶意路由。由于部分智能空调并不一定具备新鲜性和随机数安全校验能力，黑客可以通过丢弃部分控制指令对终端实施选择性转发攻击[38]或重复转发控制指令以实施重放攻击[39]。

2）旁道信息攻击。

智能空调与其云端、手机应用之间的通信传输通常采用轻量级密码算法，容易被黑客利用旁道信息进行解析。例如，黑客可以根据智能空调待机电能消耗[40]、智能空调控制指令接收后的执行时间[41]等旁道信息推断通信传输所采用的轻量级密码算法。在此前提下，黑客在截取控制指令的同时就可轻易地获取控制指令明文内容，进而可以通过伪造的控制指令对智能空调进行控制。

3）终端欺骗攻击。

黑客可以通过伪造智能空调云端、智能空调手机应用的IP地址方式获取智能空调的信任，进而控制智能空调。目前，终端欺骗攻击可分为以下3类。

（1）IP地址欺骗攻击[32]。IP地址欺骗攻击是指

黑客直接通过伪造云端或手机应用的IP地址以获取智能空调的信任。在该过程中，黑客可以通过路由攻击拒绝转发云端或手机应用与智能空调的连接确认信息，并利用TCP序列号猜测技术与目标智能空调进行TCP连接，从而获取智能空调的信任。

（2）地址解析协议（address resolution protocol，ARP）欺骗攻击[33]。局域网通常使用ARP，ARP将IP地址解析为媒体存取控制（media access control，MAC）地址。当黑客通过局域网发送欺骗性ARP消息时，可以将自身的MAC地址与手机应用或云端的IP地址相关联。

（3）域名系统（domain name system，DNS）服务器欺骗攻击[34]。当黑客通过修改智能空调所连DNS服务器地址的方式将云端IP地址重新路由到黑客的IP地址时，就可伪装为云端。

4）终端固件漏洞攻击。

由于部分智能空调固件存在运行逻辑漏洞，黑客可以通过Mirai、VPNFilter[42]等恶意软件获取默认用户的登录名及密码，从而操控智能空调。除此之外，黑客还可以通过伪造固件升级程序的恶意程序以获取终端的控制权限。

5）云端网络攻击。

云端暴露于互联网中，黑客可以通过结构化查询语言（structured query language，SQL）注入攻击[43]等手段攻击智能空调的云端服务器，从而窃取用户的登录名及密码，即可获取目标智能空调的控制权限。同时，黑客还可以嵌入恶意脚本（跨站脚本（cross-site scripting，XSS））代码至正常用户会访问的页面中，当用户访问该页面时，就可截取用户的登录名、密码等信息[44]。除此之外，黑客还可以通过社会工程学[45]等手段入侵云端服务器。

6）手机应用逆向攻击。

当黑客利用Apktool等软件反编译智能空调的手机应用时，将手机应用中的安装包文件转换为smail文件，从而解析手机应用的控制指令密码算法。在此前提下，黑客结合路由攻击就可伪造控制指令，进而控制目标智能空调。

2.2　配电网用户侧物联设备的网络攻击实例

近年来，配电网用户侧物联设备的安全事件频发，具体见附录A表A1。为了更好地了解黑客构建配电网用户侧物联设备“肉鸡”僵尸网络的方式，本节根据安全研究机构Krebs on Security[11]和美国域名服务器管理服务供应商DYN[12]的安全事件，详细介绍黑客利用恶意软件Mirai[11-12]感染智能空调的流程，如图2所示[10]。

1）在快速扫描阶段，黑客扫描联网智能空调的IP地址、服务端口。首先，黑客运用网络控制协议（Internet control message protocal，ICMP）报文探测

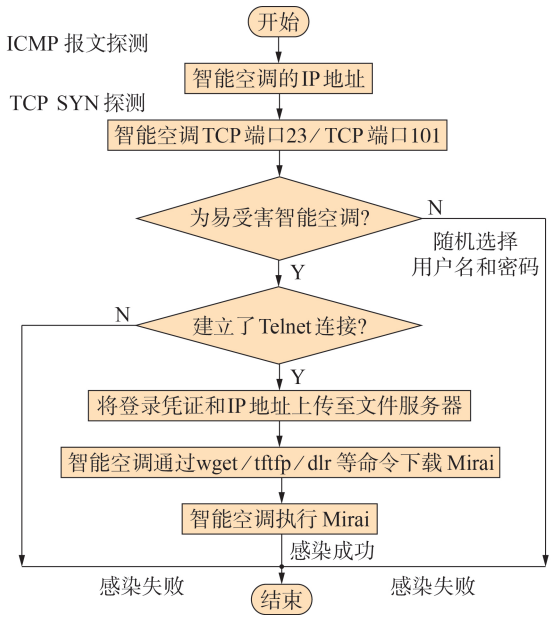


图2　Mirai感染智能空调的流程图

Fig.2　Flowchart of Mirai infecting intelligent air conditioner

智能空调的IP地址或对特定IP地址发送传输控制协议/用户数据报协议报文，并根据应答报文确认联网智能空调的IP地址；然后，黑客使用Port Scan等软件向智能空调Telnet TCP端口23和端口101上的伪随机地址发送TCP，建立连接报文（synchronize sequence number，SYN）探测包，从而根据应答报文判断智能空调的哪些端口提供在线服务。

2）在黑客识别出潜在易感染的联网智能空调后，网络攻击进入暴力登录阶段。在该期间，黑客尝试从62个登录证书的预配置列表中随机选择10个用户登录名以及密码（如admin/admin的默认用户登录名/密码组合）与智能空调建立Telnet连接。当首次成功登录时，黑客立即记录智能空调的IP地址、用户登录名以及密码，并将其储存于文件服务器中。

3）黑客根据入侵成功的智能空调IP地址、用户登录名以及密码，将一个单独的恶意加载程序发送给智能空调。在该加载程序确定智能空调系统运行环境后，下载和执行Mirai，从而将智能空调转换为“肉鸡”。

4）成功感染智能空调后，Mirai会试图删除智能空调中已下载的二进制文件，并在伪随机字母、数字字符串中混淆其进程名称来隐藏其存在。除此之外，Mirai还会关闭智能空调TCP端口23或端口101中的其他进程。感染后的智能空调在监听来自C&C服务器的攻击命令的同时，还会扫描同个局域网内易感染的智能空调。

综上可知，部分配电网用户侧物联设备固件存在在用户使用期间自动删除默认用户登录名、修改

默认用户登录名/密码或用户将登录名/密码设置为弱口令等安全漏洞，致使其终端易被黑客利用恶意软件攻击，进而被转换为“肉鸡”。在配电网用户侧物联设备的设计阶段应考虑网络安全防护[46]，但其安全准入机制并未伴随设备大规模接入电力系统而形成。随着攻击手段的日渐成熟，配电网用户侧物联设备的网络安全会给电力系统的运行带来新的隐患。

3 配电网用户侧物联设备的物理域影响分析

目前，电力二次安全防护体系通过物理隔离装置对电力系统进行安全分区[47]，致使黑客难以利用配电网用户侧物联设备的“肉鸡”僵尸网络造成生产大区内通信信息网络故障，极大地减小了配电网用户侧物联设备信息域的影响。信息域与物理域的影响对比如表3所示。由表可知，相较于信息域的影响，目前电力系统无法针对配电网用户侧物联设备的异常行为布置有效的主动安全防护，难以预防由终端运行特性所导致的物理域影响。

表3 信息域与物理域的影响对比

Table 3 Comparison of influence between cyber domain and physical domain

域名	对象	潜在“肉鸡”	安全影响	安全防护	主要危害
信息域	通信信息网络	电力物联设备	通信信息网络无法提供正常服务	主动防御、电力系统二次防护体系等	电力业务无法正常运行等
物理域	电力系统	配电网用户侧物联设备	在电力系统形成大规模的异常负荷	被动防御，不受数据采集与监视控制系统控制，依靠调峰、调频等措施	电力设备过载运行、增加运行费用等

3.1 配电网用户侧物联设备异常动作对电力系统造成的影响

3.1.1 终端的运行特性

考虑到配备物联网组件的智能空调规模[6]、空调等降温负荷占比[9]，本节以智能空调为例介绍终端的运行特性，进而揭示配电网用户侧物联设备异常动作对电力系统的影响。智能空调分为智能定频空调（简称为“定频空调”）和智能变频空调（简称为“变频空调”）。根据《2016年中国空调产业白皮书》，变频空调的数量占空调总数的比例达到58%。为此，本节对不同类型空调的运行特性进行分析。

定频空调的工作具有周期性[48]：当室内温度上升至设定温度上限时，空调动作；当室内温度下降为设定温度下限时，空调关闭。为此，定频空调的运行功率P_{d}可表示为：

$$P_{\mathrm{d}}=\begin{cases}P_{\mathrm{d}}^{\mathrm{rate}} & s=1\\ 0 & s=0\end{cases} \tag{1}$$

式中：$P_{\mathrm{d}}^{\mathrm{rate}}$为定频空调的额定运行功率；$s$为定频空调的运行状态变量，空调动作时有$s=1$，空调关闭时有$s=0$。

变频空调与定频空调的不同点在于温度控制，变频空调通过调节压缩机的频率来改变制冷量，致使室内温度维持在设定温度。则变频空调的运行功率P_{b}可表示为[2]：

$$P_{\mathrm{b}}=\begin{cases}P_{\mathrm{b}}^{\max} & T_{\mathrm{set}}+T_{\mathrm{D}}<T_t^{\mathrm{in}}\leqslant T_t^{\mathrm{out}}\\ P_{\mathrm{b}}^{\max}+h_t\left(T_t^{\mathrm{in}}-T_{\mathrm{set}}-T_{\mathrm{D}}\right) & T_{\mathrm{set}}\leqslant T_t^{\mathrm{in}}\leqslant T_{\mathrm{set}}+T_{\mathrm{D}}\\ 0 & T_t^{\mathrm{in}}\leqslant T_{\mathrm{set}}-T_{\mathrm{d}}\end{cases} \tag{2}$$

式中：$P_{\mathrm{b}}^{\max}$为变频空调的最大运行功率；T_t^{in}为t时刻的室内温度；h_t为t时刻变频空调的功率变换系数；T_{set}为设定温度；T_{D}为变频空调控制的大死区温差；T_{d}为变频空调控制的小死区温差；T_t^{out}为t时刻的室外温度。当$T_t^{\mathrm{in}}=T_{\mathrm{set}}$时，变频空调的运行功率为其额定运行功率$P_{\mathrm{b}}^{\mathrm{rate}}$，$P_{\mathrm{b}}^{\mathrm{rate}}=P_{\mathrm{b}}^{\max}-T_{\mathrm{D}}h_t$。

在该背景下，一旦黑客通过恶意软件等攻击手段将智能空调转换为“肉鸡”时，就可通过控制指令调节“肉鸡”的设定温度或改变空调的运行状态从而产生瞬时变化功率。当所调节的变频空调设定温度与原设定温度的差值大于T_{D}时，正在运行的变频空调会对电力系统形成$P_{\mathrm{b}}^{\max}-P_{\mathrm{b}}^{\mathrm{rate}}$的瞬时变化功率（在文献[2]中$P_{\mathrm{b}}^{\max}=2.5$ kW，$P_{\mathrm{b}}^{\mathrm{rate}}=60$ W）。然而，对于正在运行的定频空调而言，由式(1)可知，调节其设定温度并不会对电力系统造成任何瞬时变化功率；对于待机的定频空调和变频空调而言，当黑客开启并设置较低的设定温度时，会分别对电力系统产生大小为$P_{\mathrm{d}}^{\mathrm{rate}}$和$P_{\mathrm{b}}^{\mathrm{rate}}$的瞬时变化功率。

3.1.2 配电网用户侧物联设备异常动作对10 kV线路造成的影响

配电网源于220 kV变电站，以10 kV出线到箱式变压器、台式变压器等二级节点，再经变压器由10 kV中压变换为380 V低压，实现区域供电[48]。在附录A图A1所示电力系统运行示意图中，终端（智能空调）接入380 V低压线路。考虑终端的运行特性，黑客可以通过“肉鸡”僵尸网络所形成的瞬时变化功率直接影响10 kV线路的运行功率，其负荷表现为“同投”或“同退”。遭受恶意攻击后10 kV线路运行功率的具体表现如附录A图A2所示。

1）负荷“同投”。当黑客向“肉鸡”僵尸网络发送提升运行功率的控制指令（如降低正在运行的变频空调设定温度、开启待机的定频空调或变频空调等[49]）时，10 kV线路的运行功率$P_{\mathrm{l},t}$骤增为：

$$P_{\mathrm{l},t}=P_{\mathrm{l,ba},t}+P_{\mathrm{a,I},t} \tag{3}$$

式中：$P_{\mathrm{l,ba},t}$为t时刻10 kV线路的正常运行功率；$P_{\mathrm{a,I},t}$为t时刻由负荷“同投”造成异常增加的运行功率。

由图A2可知，黑客在10:30时刻提高“肉鸡”运行功率并形成瞬时变化功率，致使$P_{\mathrm{l},t}$异常激增，从

而对电力系统的有功功率造成冲击。就短期而言，“肉鸡”僵尸网络“同投”瞬时变化功率可以使 10 kV 线路的保护装置动作，造成 10 kV 线路停电[50]；就长期而言，“肉鸡”僵尸网络“同投”瞬时变化功率可以使 10 kV 线路过载运行、末端电压降低，进而影响该线路的电能质量[51]。本节将进一步阐述负荷“同投”的安全影响，各时段造成 10 kV 线路停电事故的智能空调操控数量如附录 A 图 A3 所示。

由图 A3 可知，在“肉鸡”充足的情况下，黑客可以在全天任何时段通过负荷“同投”造成 10 kV 线路停电。在 00:15 时刻，黑客对 2 911 台“肉鸡”下达提升运行功率的控制指令，对 10 kV 线路造成了 7.261 18 MW 的瞬时变化功率。此时，10 kV 线路的传输电流由 474 A 增大为 1 200.118 A，线路保护装置动作，切除 4.74 MW 居民负荷。在 19:30 时刻，黑客对 1 104 台“肉鸡”下达提升运行功率的控制指令，切除了 9.24 MW 居民负荷。可见，随着 10 kV 线路运行功率增大，黑客造成 10 kV 线路停电的空调操控数量减小。在高负荷的情况下，配电网用户侧物联设备网络安全的重要性也随之提高。

2）负荷“同退”。当黑客对“肉鸡”僵尸网络发送降低运行功率的控制指令（如提高正在运行的变频空调设定温度或关闭正在运行的变频空调、定频空调）时，10 kV 线路的运行功率 $P_{\mathrm{l},t}$ 骤减为：

$$P_{\mathrm{l},t}=P_{\mathrm{l,ba},t}+P_{\mathrm{a,D},t} \tag{4}$$

式中：$P_{\mathrm{a,D},t}$ 为 t 时刻由负荷“同退”造成异常减小的运行功率。

由图 A2 可知，黑客在 10:30 时刻降低“肉鸡”的运行功率，切除了 10 kV 线路的部分负荷，致使 $P_{\mathrm{l},t}$ 异常减小。相较于 $P_{\mathrm{a,I},t}$，$P_{\mathrm{a,D},t}$ 在有效攻击时间内为定值。“肉鸡”僵尸网络的“同退”瞬时变化功率可以使 10 kV 线路轻载运行、末端电压偏高，进而影响用户侧电力物联设备的运行安全性[52]。

3.1.3　配电网用户侧物联设备异常动作对主网传输线路造成的影响

当黑客可以操控多条 10 kV 线路的运行功率时，就可影响所属 220 kV 变电站的实时运行功率，从而实现对纵跨配电网、主网安全的影响。在该背景下，本节以修改后的 IEEE 14 节点测试系统为例，分析负荷“同投”对主网传输线路安全造成的影响。部分线路的运行功率、传输容量结果如表 4 所示。表中：P_0 为正常运行时的线路运行功率；P_1、P_2 分别为攻击场景 1、2 下线路的运行功率。

由表 4 可知：当正常运行时，各线路的运行功率并未达到其传输容量；在攻击场景 1 下，黑客对变电站 2 所关联的 6 900 台“肉鸡”下达提升运行功率的控制指令，在变电站 2 形成 17.25 MW 的恶意负荷，致使线路 1-2 的运行功率达到其传输容量；在攻击场景 2 下，由于 28 200 台“肉鸡”在变电站 2 中形成了 70.50 MW 的恶意负荷，线路 1-2 的运行功率为 84.05 MW，约为线路传输容量的 1.2 倍。上述结果表明，考虑终端运行特性及其分布广泛的特点，当黑客构建大规模“肉鸡”僵尸网络时，可以在电力系统中形成一定规模的异常负荷，直接影响电力系统主网传输线路的运行功率。

表 4　部分线路的运行功率结果

Table 4　Operating power results of some lines

线路	传输容量 / MW	P_0 / MW	P_1 / MW	P_2 / MW
1-2	70	65.46	**70.01**	**84.05**
1-5	70	62.69	61.59	58.20
2-3	70	17.59	14.47	4.85
2-4	70	59.58	56.41	46.60
4-5	70	58.14	55.18	46.06

3.2　物理域影响场景

由配电网用户侧物联设备异常动作带来的物理域影响可以在许多方面干扰电力系统的正常运行，本文将其物理域影响分为经济性影响和安全性影响，具体场景如表 5 所示。

表 5　物理域影响场景

Table 5　Impact scenarios of physical domain

影响	场景	设备“肉鸡”动作
安全性影响	电网频率上升 / 下降	同时降低 / 提高“肉鸡”的运行功率
	主网传输线路过载运行	在不同区域同时降低 / 提高“肉鸡”的运行功率
	系统联络线故障	分别在受端和送端电网提升、降低“肉鸡”的运行功率
经济性影响	增加电网公司的运行成本	在电力需求高峰时段提高“肉鸡”的运行功率
	增加售电公司的运营成本	在考核时段降低 / 提高“肉鸡”的运行功率

1）电网频率上升 / 下降。

电网的正常运行取决于功率平衡，黑客可以通过调节配电网用户侧物联设备的运行功率来影响系统的功率平衡。当黑客利用配电网用户侧物联设备进行负荷“同投”攻击时，若所形成的瞬时变化功率大于系统阈值，则会导致系统频率下降；反之，负荷“同退”攻击会致使系统频率上升。并且，随着新能源渗透率的不断增大，系统的惯性降低。当黑客选择在新能源渗透率最高的时段对系统实施负荷攻击时，可导致频率发生更为显著的变化。

2）主网传输线路过载。

由表 4 所示负荷“同投”攻击导致主网传输线路过载运行的结果可知，在负荷高峰时段，黑客可以通过考虑各变电站与传输线路潮流的关系[53]，进一步制定具有针对性的分布式负荷“同投”或“同退”攻击，使关键传输线路过载，诱发电网进行切负荷等操作。

3）系统联络线故障。

系统联络线承担着大量的电能传输任务。黑客可以根据IP地址对受端电网、送端电网分别进行负荷“同投”、“同退”攻击，使联络线路过载，触发其保护装置动作，从而造成受端电网功率不足、送端电网功率过剩的情景。

4)增加电网公司的运行成本。

当功率需求超过预测值时，电网公司会从现货市场购买额外的电量。由于现货市场的价格高于日前市场的价格，负荷“同投”攻击可以显著地增加电网公司的运行成本。

5)增加售电公司的运营成本。

在电力市场中，售电公司的实际执行与交易结果的考核偏差会影响售电公司的运营成本。黑客可以在考核时间节点针对所管辖的10 kV线路进行负荷“同投”或“同退”攻击，提高售电公司的市场惩罚费用，从而增加售电公司的运营成本。

4 配电网用户侧物联设备的网络安全防护

配电网用户侧物联设备的网络安全防护是确保其安全运行的关键，对于避免黑客在电力系统中形成大规模的异常负荷具有极其重要的意义。本节从终端轻量级身份验证、手机应用防逆向研究、终端通信轻量级密码算法、云端入侵检测4个方面对目前配电网用户侧物联设备的主要安全防护研究进行综述。

4.1 终端轻量级身份认证

为了避免恶意控制指令响应，终端应采用高强度身份认证方案以确保控制指令的真实性。但受限于终端的计算能力，高强度身份认证方案并不适用于配电网用户侧物联设备。

目前，国内外学者针对轻量级身份验证方案已经进行了广泛的研究[54-61]：文献[54]提出了一种适用于智能家居环境的轻量级密钥建立方案，终端中的传感器和执行器使用短认证的方式建立一个安全会话密钥，以此完成双方的相互认证；文献[55]针对智能家庭能源局域网，提出了一种基于椭圆曲线密码和自证明的认证公钥技术，建立了身份认证密钥方案；文献[56]介绍了一种基于子树短签名的轻量级身份认证算法，并基于随机预言机模型验证了其安全性；文献[57]设计了一种基于快速认证框架的轻量级身份认证方案，提升了智能家居设备的身份验证速度。但文献[54-57]并没有考虑配电网用户侧物联设备通信的匿名性。在软件定义网络安全架构的基础上，文献[58]设计了一种轻量级匿名认证机制，并使用Burrows-Abadi-Needham和ProVerif对其安全性进行了分析，但未考虑配电网用户侧物联设备各组件间的互操作性。在互联智能家居环境下，文献[59]提出了一种轻量级匿名操作安全框架，提供了有效的密钥协商策略和身份验证方案，使智能家居设备的身份和数据具有匿名性。针对匿名身份认证，文献[60]设计了一种轻量级实时认证协议，保证了物联网络中的数据安全。文献[61]考虑身份、口令、生物特征等因素，提出了一种仅采用哈希函数和异或运算的会话密钥建立方案，降低了会话密钥的计算成本[61]。但是，文献[59-61]依赖于第三方信任机构生成和管理密钥，且对终端的计算能力要求较高，并不适用于目前的大多数配电网用户侧物联设备。

4.2 手机应用防逆向研究

由于手机系统的开源性，未经安全加固的手机应用易遭受代码逆向攻击，致使手机应用中的用户登录名、密码、控制指令密码算法泄露[62]。为此，配电网用户侧物联设备厂商应对手机应用进行安全加固，以应对黑客的逆向攻击。

目前，针对手机应用安全防护的研究主要包括代码重写技术、代码加壳保护技术、代码混淆技术等方面。在不需要定位和符号信息的前提下，文献[63]设计了一个静态二进制代码重写器，实现了重写代码100%覆盖率，但依赖于复杂的重写规则，且主要针对Linux系统x86平台。在代码加壳保护技术方面，文献[64]提出了一种基于函数Native加壳的手机应用加固方法，保证被保护的Java函数在运行过程中始终保持Native属性，可以有效地抵御DEX动态恢复和动态脱壳攻击。文献[65]提出了一种多粒度的数据还原方案，并基于此设计了多层次的自动通用脱壳系统，保证了数据还原的完整性和有效性。文献[66]提出了一种基于函数抽取和隐式恢复的DEX文件保护方法，可以有效地抵御静态分析和动态恢复攻击。在代码混淆技术方面，文献[67]制定了一种针对源码变量名和方法名的混淆方案，实现了对DEX文件的混淆，但需要结合其他混淆方案共同为源码提供保护。此外，文献[68]设计了一种基于函数控制流的完整性校验方案，在解析SO文件中函数控制流图的前提下，在运行过程中植入完整性校验代码对函数流跳转进行验证。文献[69]提出了一种基于函数抽取和动态加载的加固方法，抽取函数信息至DEX文件尾部，并在其中添加静态代码段还原函数。

4.3 终端通信轻量级密码算法

终端的可用存储空间较小，部分终端RFID标签可用于实现网络安全防护的只有200~2 000等效门，导致许多传统加密算法(例如高级加密标准、国际数据加密算法等)并不适用于终端。

在该环境下，文献[70]提出了一种基于代换-置换网络(substitution-permutation network，SPN)结构的加密算法(PRESENT)，可以灵活选择80 bit或者

128 bit密钥长度；文献[71]提出了一种基于哈希函数的轻量级加密算法（DLDL），在PRESENT中加入了一个小规模的线性扩散层，以较少的硬件成本增加了线性扩散层的混淆；文献[72]在PRESENT的基础上，提出了一种分组轻量级加密算法（GIFT），降低了硬件实现成本。但文献[70-72]难以抵御旁路立体方攻击[73]，一旦加密内容在第3轮存在任何大小内容的输出泄露，便可被黑客恢复出加密算法密钥。文献[74]提出了一种采用32轮Feistel结构的分组加密算法（LBlok），使用循环移位和S盒变换生成轮密钥，但难以抵御代数故障攻击[75]。基于Feistel结构，美国国家安全局提出了一种分组加密算法（SIMON），并根据分组长度和密钥长度分为10个版本[76]。文献[77]提出了一种基于哈希函数的加密算法（SPONGENT），并给出了SPONGENT的硬件实现面积。文献[78]了提出一种基于哈希函数的加密算法（TAV-128），并在硬件将其实现，但与SPONGENT相比，其执行时间以及实现面积并不存在优势。文献[79]设计了一种采用SPN结构的轻量级分组加密算法（Surge），相较于现有的SPN结构，轻量级加密算法具备更小的实现面积。虽然上述轻量级加密算法在设计阶段已经进行了比较全面的安全分析，但受限于终端的计算能力以及可用储存空间，轻量级加密算法难以达到绝对安全。

4.4　云端入侵检测

由于云端服务器储存了大量的终端量测数据、控制指令、用户登录名等信息，且云端为配电网用户侧物联设备提供业务逻辑，云端的网络安全在配电网用户侧物联设备运行中扮演着至关重要的角色。

为了预防云端安全事故的发生，文献[80]开发了基于桉树云的入侵检测系统（intrusion detection system，IDS），将Snort针对性地部署在云控制器和物理主机上，可以有效地避免由于单个IDS过载而引发的DDoS攻击。文献[81]提出了一种基于特征值分布和人工智能的网络IDS，提高了网络流量异常的检测精度。文献[82]构建了一种物联网网关设备的IDS架构（SeArch），在保证检测精度的同时降低了IDS的运行开销。文献[83]分析了用户的信用度、行为等信息，构建了基于马尔可夫模型的IDS，可以更好地区分合法用户和恶意用户。但文献[80-83]仅能检测云端外部的网络攻击，无法检测来自内部的恶意攻击。为了预防云环境中的内部恶意攻击，文献[84]提出了一种基于主机型入侵检测系统和日志收集信息系统，可以有效地检测黑客对虚拟机的恶意攻击，并生成邮件报警和安全外壳协议消息。文献[85]设计了一个基于深度学习的异常行为提取系统，缩短了恶意攻击的检测时间。此外，针对旁路攻击，在软件保护扩展（software guard extension，SGX）环境中，文献[86]提出了一种确定性多复用选择器的软件防御方法，并讨论了硬件辅助防御的范围。在无需修改硬件的前提下，文献[87]提出了将原程序自动封装为安全代码的机制（T-SGX），有效地抵御了旁路攻击，并利用硬件特性减小了运行开销。但文献[86-87]主要集中于SGX环境，并未涉及虚拟机监视器（Hypervisor）环境的安全防护。

5　研究与展望

考虑到配电网用户侧物联设备的网络风险特征，目前的安全防护措施难以确保配电网用户侧物联设备的网络安全。为了减小配电网用户侧物联设备的异常动作所带来的物理域影响，电力系统应对配电网用户侧物联设备进行安全管理。本节从如何建立配电网物联设备的安全管理平台等方面进行展望。

5.1　基于软件定义物联网的配电网用户侧物联设备安全管控系统

考虑设备的接入规模，电力系统应建立一个配电网用户侧物联安全管控系统，以此避免大规模终端异常动作。然而，由图1可知，终端中的传感器、定位装置等组件通过Bluetooth、4G／5G、WLAN等网络通信技术实现智能互联，如何消除配电网用户侧物联设备的通信异构性成为电力系统建立配电网用户侧物联设备安全管控系统的难点。软件定义网络（software defined network，SDN）具有解决该问题的潜力[88]，其可编程特性不仅打破了设备和电力公司的互通壁垒，还为实现配电网用户侧物联设备的安全管控提供了平台。

由2.2节可知，黑客可以在特定的时间向“肉鸡”僵尸网络发送恶意控制指令，以此实现对用户侧负荷的攻击。在该背景下，如何对控制指令进行安全管控是实现配电网用户侧物联设备安全管控的核心问题。基于SDN的配电网用户侧物联设备安全管控系统分为运行层、控制层、应用层。运行层由通信交换机等信息设备构成，其通过南向接口将控制指令（如用户开启待机的智能空调）上传至控制层。控制层包含了逻辑上为中心的SDN控制器，根据运行层上传的控制指令，对数据平面的资源进行编排，对全网状态进行实时维护，并通过北向接口与应用层交互。应用层位于SDN的顶层，其可以根据电力系统的运行安全需求，制定控制指令可信计算、控制指令的电力安全校核等实时业务。在黑客对“肉鸡”僵尸网络发送异常控制指令时，配电网用户侧物联设备安全管控系统根据控制指令可信计算、控制指令的电力安全校核等应用拒绝转发异常的控制指令，以此避免电力传输线路过载等恶性事件的发生，实现了设备运行的安全管控。

5.2 配电网用户侧物联设备用户控制指令的可信计算

如何识别异常控制指令是对控制指令进行安全管控的基础，控制指令的可信计算可以为电力系统进行控制指令安全管控提供一种科学判据[89]。

在黑客使用Mirai等恶意软件攻击配电网用户侧物联设备的过程中，暴力登录阶段致使设备各组件出现大量的异常行为，如登录凭证验证错误等。当黑客通过伪造、篡改控制指令等方式企图控制终端时，设备各组件也会产生一定数量的异常行为，如控制指令不满足新鲜性/随机数等报文信息安全校验、用户使用习惯等个人习惯安全性校验等。在该前提下，以设备各组件异常行为为基础的控制指令动态信用可以准确表达控制指令在联网状态下的可信程度。其中，考虑用户远程控制终端的流程，设备异常行为应由终端异常行为、云端异常行为、手机应用异常行为等构成。用户在手机应用注册成功后，其控制指令会获得初始信用。然后，配电网用户侧物联设备安全管控系统根据用户的历史正常操作次数和历史异常操作次数实时更新控制指令的动态信用。此外，在黑客构建“肉鸡”僵尸网络的过程中，会进一步搜寻同一或邻近DNS网关的易感染终端，致使“肉鸡”分布较为集中，因此单个控制指令的动态信用应与预设系统内控制指令的整体信用具备一定的关联[90]。因此，控制指令的可信计算还需进一步考虑单个控制指令的动态信用与预设系统整体信用的相关性，从而修正控制指令的动态信用。

5.3 边缘计算架构在配电网用户侧物联设备安全管控系统中的应用

集中式计算架构将所有数据的分析集中于中央计算器，是目前实现配电网用户侧物联设备安全管控系统的主流架构。对于小规模配电网用户侧物联设备接入的电力系统而言，基于集中式计算架构的配电网用户侧物联设备安全管控系统并不会对控制指令的转发时间造成明显的延迟影响。但随着配电网用户侧物联设备接入规模的进一步扩大，若仍采用集中式计算架构，则控制指令报文转发时间会进一步增加，进而影响用户的使用体验。此外，考虑配电网用户侧物联设备的网络安全防护能力，大量的配电网用户侧物联设备流量通过互联网流入位于电力系统核心生产网络的中央计算器势必会增加电力系统的运行风险。

在该背景下，引入边缘计算架构[91]，在靠近终端的位置布置边缘计算器，利用边缘计算器对周围控制指令进行控制指令的可信计算、控制指令的电力安全校核等实时业务。当黑客向“肉鸡”发送恶意控制指令时，边缘计算器可以根据控制指令的动态信用、控制指令的关联功率以及电力安全需求确定可以转发的控制指令，避免变电站、配电网传输线路过载运行等恶性事件的发生。由于边缘计算器更靠近终端以及处理的数据规模更小，其缩短了控制指令进行电力安全校核的计算时间。另外，考虑电力系统生产大区网络安全的重要性，边缘计算架构可以有效地避免异构流量进入电力系统生产大区，减小了黑客通过配电网用户侧物联设备攻击电力系统生产大区设备的可能性。但基于边缘计算架构的配电网用户侧物联设备安全管控系统在电力系统的有效实施绕不开适应性等问题，如何寻求突破仍是未来需要解决的关键问题。

6 结论

随着大规模配电网用户侧物联设备接入电力系统，其网络安全在电力系统的稳定运行中扮演着更为重要的角色。但由于配电网用户侧物联设备缺乏严格的准入机制，黑客可以通过恶意软件等方式轻易地构建一定规模的配电网用户侧物联设备“肉鸡”僵尸网络，从而操控其终端运行功率，给电力系统运行带来新型网络安全风险。为此，本文首先分析了配电网用户侧物联设备各组件的网络安全脆弱性；然后，基于攻击目标分类介绍了目前攻击配电网用户侧物联设备的主要手段，并对配电网用户侧物联设备安全防护领域的国内外研究现状进行了综述；最后，对电力系统如何进行配电网用户侧物联设备运行安全管控的关键理论和技术进行了展望，以期为相关研究的进一步开展提供参考。在未来，笔者将会从安全准入、运行机制建立等多个方面对配电网用户侧物联设备运行安全管控策略等进行研究。

附录见本刊网络版(http://www.epae.cn)。

参考文献：

[1] VRAKOPOULOU M, LI B W, MATHIEU J L. Chance constrained reserve scheduling using uncertain controllable loads part I: formulation and scenario-based analysis[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 1608-1617.

[2] 李滨，黎智能，陈碧云. 电力市场中配电网的空调群调控策略[J]. 电力系统自动化，2019，43(15)：124-131.
LI Bin, LI Zhineng, CHEN Biyun. Air conditioning group dispatch control strategy of distribution network in electricity market[J]. Automation of Electric Power Systems, 2019, 43(15): 124-131.

[3] 刘向军，周行洁，刘迪，等. 面向新能源消纳的热水器集群精细化均衡控制[J]. 电力自动化设备，2020，40(1)：52-58.
LIU Xiangjun, ZHOU Xingjie, LIU Di, et al. Refined equilibrium control of electric water heater clusters for accommodation of renewable energy sources[J]. Electric Power Automation Equipment, 2020, 40(1): 52-58.

[4] 陈丽丹，张尧，Antonio Figueiredo. 融合多源信息的电动汽车充电负荷预测及其对配电网的影响[J]. 电力自动化设备，2018，38(12)：1-10.
CHEN Lidan, ZHANG Yao, FIGUEIREDO A. Charging load forecasting of electric vehicles based on multi-source informa-

tion fusion and its influence on distribution network[J]. Electric Power Automation Equipment,2018,38(12):1-10.
[5] MENEGHELLO F,CALORE M,ZUCCHETTO D,et al. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices[J]. IEEE Internet of Things Journal,2019,6(5):8182-8201.
[6] 百姓家电网. 2020空调行业同比为近十年最差,转型变革已成趋势[EB/OL]. (2020-08-31)[2022-01-16]. https://tech.sina.com.cn/roll/2020-08-31/doc-iivhvpwy4087560.shtml?cre=tianyi&mod=pcpager_china&loc=31&r=9&rfunc=100&tj=none&tr=9.
[7] OMDIA. Strategy shifts contribute to 55 million connected major home appliance shipments in 2020[EB/OL]. [2022-01-16]. https://omdia.tech.informa.com/OM018781/Strategy-shifts-contribute-to-55-million-connected-major-home-appliance-shipments-in-2020.
[8] 国家统计局. 中国统计年鉴[M]. 北京:中国统计出版社,2021:103.
[9] 刘志伟,苗世洪,杨炜晨,等. 计及电气特性的空调负荷建模及集群控制策略[J]. 电力自动化设备,2022,42(1):178-184,192.
LIU Zhiwei,MIAO Shihong,YANG Weichen,et al. Air conditioning load modeling and cluster control strategy considering electrical characteristic[J]. Electric Power Automation Equipment,2022,42(1):178-184,192.
[10] CHAABOUNI N,MOSBAH M,ZEMMARI A,et al. Network intrusion detection for IoT security based on learning techniques[J]. IEEE Communications Surveys & Tutorials,2019,21(3):2671-2701.
[11] ANTONAKAKIS M,APRIL T,BAILEY M,et al. Understanding the mirai botnet[C]//Proceedings of the 26th USENIX Conference on Security Symposium. New York,USA:ACM,2017:1093-1110.
[12] OMDIA. Cloud giants likely to beef up bandwidth to fight IoT botnets[EB/OL]. [2022-01-16]. https://www.iotworldtoday.com/2016/11/01/cloud-giants-likely-beef-bandwidth-fight-iot-botnets.
[13] WEAGLE S. Financial impact of mirai DDoS attack on DYN revealed in new data[EB/OL]. [2022-01-16]. https://www.corero.com/blog/797-financial-impact-of-miraiddos-attack-on-dyn-revealed-in-new-data.html.
[14] JIA Y Z,ZHONG F T,ALRAWAIS A,et al. FlowGuard:an intelligent edge defense mechanism against IoT DDoS attacks[J]. IEEE Internet of Things Journal,2020,7(10):9552-9562.
[15] RAVI N,SHALINIE S M. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture[J]. IEEE Internet of Things Journal,2020,7(4):3559-3570.
[16] 杨挺,侯昱丞,赵黎媛,等. 基于时-频域混合特征的变电站通信网异常流量检测方法[J]. 电力系统自动化,2020,44(16):79-86.
YANG Ting,HOU Yucheng,ZHAO Liyuan,et al. Abnormal traffic detection method of substation communication network based on time-frequency domain mixed features[J]. Automation of Electric Power Systems,2020,44(16):79-86.
[17] 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.
[18] DVORKIN Y,GARG S. IoT-enabled distributed cyber-attacks on transmission and distribution grids[C]//2017 North American Power Symposium(NAPS). Morgantown,WV,USA:IEEE,2017:1-6.
[19] DABROWSKI A,ULLRICH J,WEIPPL E R. Grid shock:coordinated load-changing attacks on power grids:the non-smart power grid is vulnerable to cyber attacks as well[C]//Proceedings of the 33rd Annual Computer Security Applications Conference. New York,USA:ACM,2017:1-8.
[20] SOLTAN S,MITTAL P,POOR H V. BlackIoT:IoT botnet of high wattage devices can disrupt the power grid[C]//Proceedings of the 27th USENIX Conference on Security Symposium. New York,USA:ACM,2018:15-32.
[21] 文云峰,杨伟峰,林晓煌. 低惯量电力系统频率稳定分析与控制研究综述及展望[J]. 电力自动化设备,2020,40(9):211-222.
WEN Yunfeng,YANG Weifeng,LIN Xiaohuang. Review and prospect of frequency stability analysis and control of low-inertia power systems[J]. Electric Power Automation Equipment,2020,40(9):211-222.
[22] NESHENKO N,BOU-HARB E,CRICHIGNO J,et al. Demystifying IoT security:an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations[J]. IEEE Communications Surveys & Tutorials,2019,21(3):2702-2733.
[23] HUANG D W,DU Z W,WANG Y. A quad-antenna system for 4G/5G/GPS metal frame mobile phones[J]. IEEE Antennas and Wireless Propagation Letters,2019,18(8):1586-1590.
[24] LEE J H,BONNIN J M,YOU I,et al. Comparative handover performance analysis of IPv6 mobility management protocols[J]. IEEE Transactions on Industrial Electronics,2013,60(3):1077-1088.
[25] ALBAZRQAOE W,HUANG J,XING G L. A practical bluetooth traffic sniffing system:design,implementation,and countermeasure[J]. IEEE/ACM Transactions on Networking,2019,27(1):71-84.
[26] WANG X Y,ZHANG J,YU Z T,et al. On remote temperature sensing using commercial UHF RFID tags[J]. IEEE Internet of Things Journal,2019,6(6):10715-10727.
[27] AUST S,PRASAD R V,NIEMEGEERS I G M M. Outdoor long-range WLANs:a lesson for IEEE 802.11ah[J]. IEEE Communications Surveys & Tutorials,2015,17(3):1761-1775.
[28] 李成星,王珺,徐京明. 基于信任机制与Rank阈值的RPL路由协议[J]. 计算机工程,2020,46(7):143-149,158.
LI Chengxing,WANG Jun,XU Jingming. RPL routing protocol based on trust mechanism and Rank threshold[J]. Computer Engineering,2020,46(7):143-149,158.
[29] 姚志强,竺智荣,叶帼华. 基于密钥协商的防范DHCP中间人攻击方案[J]. 通信学报,2021,42(8):103-110.
YAO Zhiqiang,ZHU Zhirong,YE Guohua. Achieving resist against DHCP man-in-the-middle attack scheme based on key agreement[J]. Journal on Communications,2021,42(8):103-110.
[30] FONSECA O,CUNHA Í,FAZZION E,et al. Identifying networks vulnerable to IP spoofing[J]. IEEE Transactions on Network and Service Management,2021,18(3):3170-3183.
[31] HIJAZI S,OBAIDAT M S. A new detection and prevention system for ARP attacks using static entry[J]. IEEE Systems Journal,2019,13(3):2732-2738.
[32] HUSSAIN M A,JIN H,HUSSIEN Z A,et al. DNS protection against spoofing and poisoning attacks[C]//2016 3rd International Conference on Information Science and Control Engineering(ICISCE). Beijing,China:IEEE,2016:1308-1312.
[33] 杨毅宇,周威,赵尚儒,等. 物联网安全研究综述:威胁、检测与防御[J]. 通信学报,2021,42(8):188-205.
YANG Yiyu,ZHOU Wei,ZHAO Shangru,et al. Survey of IoT security research:threats,detection and defense[J]. Journal

on Communications,2021,42(8):188-205.
[34] 杨伟,何杰,万亚东,等. 物联网通信协议的安全研究综述[J]. 计算机科学,2018,45(12):32-41.
YANG Wei,HE Jie,WAN Yadong,et al. Security for communication protocols in Internet of Things:a survey[J]. Computer Science,2018,45(12):32-41.
[35] CHAKRABORTY R S,PAGLIARINI S,MATHEW J,et al. A flexible online checking technique to enhance hardware Trojan horse detectability by reliability analysis[J]. IEEE Transactions on Emerging Topics in Computing,2017,5(2):260-270.
[36] LIN G J,ZHANG J,LUO W,et al. Software vulnerability discovery via learning multi-domain knowledge bases[J]. IEEE Transactions on Dependable and Secure Computing,2021,18(5):2469-2485.
[37] WALLGREN L,RAZA S,VOIGT T. Routing attacks and countermeasures in the RPL-based Internet of Things[J]. International Journal of Distributed Sensor Networks,2013,9(8):794326.
[38] LIU Y X,MA M,LIU X,et al. Design and analysis of probing route to defense sink-hole attacks for Internet of Things security[J]. IEEE Transactions on Network Science and Engineering,2020,7(1):356-372.
[39] MAZUMDAR B,SAEED S M,ALI S S,et al. Timing attack and countermeasure on NEMS relay based design of block ciphers[J]. IEEE Transactions on Emerging Topics in Computing,2017,5(3):317-328.
[40] SINGH A,CHAWLA N,KO J H,et al. Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes[J]. IEEE Internet of Things Journal,2019,6(1):421-434.
[41] MAJI S,BANERJEE U,CHANDRAKASAN A P. Leaky nets:recovering embedded neural network models and inputs through simple power and timing side-channels-attacks and defenses[J]. IEEE Internet of Things Journal,2021,8(15):12079-12092.
[42] GOODIN D. VPNFilter malware infecting 500 000 devices is worse than we thought[EB/OL]. (2018-06-06)[2022-01-16]. https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/.
[43] GU H F,ZHANG J N,LIU T,et al. DIAVA:a traffic-based framework for detection of SQL injection attacks and vulnerability analysis of leaked data[J]. IEEE Transactions on Reliability,2020,69(1):188-202.
[44] LIU M,ZHANG B Y,CHEN W B,et al. A survey of exploitation and detection methods of XSS vulnerabilities[J]. IEEE Access,2019,7:182004-182016.
[45] ALTURKI A,ALSHWIHI N,ALGARNI A. Factors influencing players' susceptibility to social engineering in social gaming networks[J]. IEEE Access,2020,8:97383-97391.
[46] SICARI S,RIZZARDI A,GRIECO L A,et al. Security,privacy and trust in Internet of Things:the road ahead[J]. Computer Networks,2015,76:146-164.
[47] 国家电力监管委员会. 电力二次系统安全防护规定[S]. 北京:国家电力监管委员会,2004.
[48] 杨阳,徐青山,戴蔚莺,等. 以最小削减及最少启停为特征的空调负荷双层优化调度策略[J]. 电力自动化设备,2019,39(12):176-182,197.
YANG Yang,XU Qingshan,DAI Weiying,et al. Bi-level optimal dispatch strategy of air-conditioning load with minimum reduction and minimum start-stop number as characteristics[J]. Electric Power Automation Equipment,2019,39(12):176-182,197.
[49] 蒲天骄,刘克文,陈乃仕,等. 基于主动配电网的城市能源互联网体系架构及其关键技术[J]. 中国电机工程学报,2015,35(14):3511-3521.
PU Tianjiao,LIU Kewen,CHEN Naishi,et al. Design of ADN based urban energy Internet architecture and its technological issues[J]. Proceedings of the CSEE,2015,35(14):3511-3521.
[50] 严康,刘蓓,刘绚,等. 大规模空调负荷在恶意控制下的配电网风险分析[J]. 智慧电力,2020,48(8):15-23.
YAN Kang,LIU Bei,LIU Xuan,et al. Risk analysis of large-scale air-conditioning load under malicious control in distribution networks[J]. Smart Power,2020,48(8):15-23.
[51] 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 June,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.
[52] 阴艳超,吴仁杰,常斌磊. 复杂电网电能质量知识云评价服务模型与方法[J]. 电力自动化设备,2018,38(5):241-247.
YIN Yanchao,WU Renjie,CHANG Binlei. Knowledge cloud evaluation service model and method for power quality of complex power grid[J]. Electric Power Automation Equipment,2018,38(5):241-247.
[53] 徐岩,吕彬,林旭涛. 潮流转移识别方法的研究与分析[J]. 电网技术,2013,37(2):411-416.
XU Yan,LÜ Bin,LIN Xutao. Study and analysis on identification method of power flow transferring[J]. Power System Technology,2013,37(2):411-416.
[54] KUMAR P,GURTOV A,IINATTI J,et al. Lightweight and secure session-key establishment scheme in smart home environments[J]. IEEE Sensors Journal,2016,16(1):254-264.
[55] MESHRAM C,ALSANAD A,TEMBHURNE J V,et al. A provably secure lightweight subtree-based short signature scheme with fuzzy user data sharing for human-centered IoT[J]. IEEE Access,2021,9:3649-3659.
[56] KUMAR P,GURTOV A,SAIN M,et al. Lightweight authentication and key agreement for smart metering in smart energy networks[J]. IEEE Transactions on Smart Grid,2019,10(4):4349-4359.
[57] CHIFOR B C,BICA I,PATRICIU V V,et al. A security authorization scheme for smart home Internet of Things devices[J]. Future Generation Computer Systems,2018,86:740-749.
[58] IQBAL W,ABBAS H,DENG P,et al. ALAM:anonymous lightweight authentication mechanism for SDN-enabled smart homes[J]. IEEE Internet of Things Journal,2021,8(12):9622-9633.
[59] KUMAR P,BRAEKEN A,GURTOV A,et al. Anonymous secure framework in connected smart home environments[J]. IEEE Transactions on Information Forensics and Security,2017,12(4):968-979.
[60] GOPE P,HWANG T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks[J]. IEEE Transactions on Industrial Electronics,2016,63(11):7124-7132.
[61] BANERJEE S,ODELU V,DAS A K,et al. An efficient,anonymous and robust authentication scheme for smart home environments[J]. Sensors,2020,20(4):1215-1233.
[62] 赵跃华,刘佳. 安卓APP安全加固系统的分析与设计[J]. 计算机工程,2018,44(2):187-192.
ZHAO Yuehua,LIU Jia. Analysis and design of android APP security reinforcement system[J]. Computer Engineering,2018,44(2):187-192.
[63] SMITHSON M,ELWAZEER K,ANAND K,et al. Static binary rewriting without supplemental information:overcoming the

tradeoff between coverage and correctness[C]//2013 20th Working Conference on Reverse Engineering(WCRE). Koblenz, Germany:IEEE,2013:52-61.

[64] 宋言言,罗森林,尚海,等. 函数Native化的Android APP加固方法[J]. 浙江大学学报(工学版),2019,53(3):555-562.
SONG Yanyan,LUO Senlin,SHANG Hai,et al. Android APP reinforcement method with function Nativeization[J]. Journal of Zhejiang University(Engineering Science),2019,53(3):555-562.

[65] 简容,黎桐辛,周渊,等. 一种多层次的自动化通用Android脱壳系统及其应用[J]. 北京理工大学学报,2019,39(7):725-731.
JIAN Rong,LI Tongxin,ZHOU Yuan,et al. Design and application of a multi-level automated universal unpack system on Android platform[J]. Transactions of Beijing Institute of Technology,2019,39(7):725-731.

[66] 袁晓筱,罗森林,杨鹏. Android系统应用程序DEX文件保护方法研究[J]. 信息网络安全,2020,20(7):60-69.
YUAN Xiaoxiao,LUO Senlin,YANG Peng. Research on Android application DEX file protection method[J]. Netinfo Security,2020,20(7):60-69.

[67] 文伟平,张汉,曹向磊. 基于Android可执行文件重组的混淆方案的设计与实现[J]. 信息网络安全,2016(5):71-77.
WEN Weiping,ZHANG Han,CAO Xianglei. Design and implementation of the scheme of obfuscation based on the recombination of the Android executable file[J]. Netinfo Security,2016(5):71-77.

[68] 刘文灵. Android应用本地代码的安全加固及安全性评估[D]. 北京:北京邮电大学,2018.
LIU Wenling. Reinforcement and security evaluation of native code for Android application[D]. Beijing:Beijing University of Posts and Telecommunications,2018.

[69] 王泽华. Android软件安全加固技术研究与实现[D]. 成都:电子科技大学,2016.
WANG Zehua. Research and implementation of the Android software security reinforcement technique[D]. Chengdu:University of Electronic Science and Technology of China,2016.

[70] BOGDANOV A,KNUDSEN L R LEANDER G,et al. PRESENT:an ultra-lightweight block cipher[C]//Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems. Vienna,Austria:Springer,2007:450-466.

[71] DU P,WANG X,WANG W K,et al. Notice of removal:DLDL:a lightweight hash function based on double linear diffusion layer[C]//2018 International Computers,Signals and Systems Conference(ICOMSSC). Dalian,China:IEEE,2018:848-852.

[72] PEYRIN B,MENG T,NAOFUMI T. GIFT:a small present-towards reaching the limit of lightweight encryption[C]//Cryptographic Hardware and Embedded Systems-CHES 2017-19th International Conference. Taipei,Taiwan,China:Springer,2017:321-345.

[73] YANG L,WANG M Q,QIAO S Y. Side channel cube attack on PRESENT[C]//2009 Proceedings of the 8th International Conference on Cryptology and Network Security. Berlin,Germany:Springer Verlag,2009:379-391.

[74] WU W L,ZHANG L. LBlock:a lightweight block cipher[C]//Applied Cryptography and Network Security-ACNS 2011. Nerja,Spain:Springer,2011:327-344.

[75] ZHANG F,ZHAO X J,GUO S Z,et al. Improved algebraic fault analysis:a case study on piccolo and applications to other lightweight block ciphers[C]//2013 International Workshop on Constructive Side-Channel Analysis and Secure Design. Paris,France:Springer,2013:62-79.

[76] 王宁. 几个轻量级分组密码算法的安全性分析[D]. 济南:山东大学,2018.
WANG Ning. Security analysis of several lightweight block ciphers[D]. Jinan:Shandong University,2018.

[77] BOGDANOV A,KNEZEVIC M,LEANDER G,et al. SPONGENT:the design space of lightweight cryptographic hashing[J]. IEEE Transactions on Computers,2013,62(10):2041-2053.

[78] IJAZ R,PASHA M A. Area-efficient and high-throughput hardware implementations of TAV-128 hash function for resource-constrained IoT devices[C]//2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications. Bucharest,Romania:IEEE,2017:832-835.

[79] 李浪,刘波涛. Surge:一种新型、低资源、高效的轻量级分组密码算法[J]. 计算机科学,2018,45(2):236-240.
LI Lang,LIU Botao. Surge:a new low-resource and efficient lightweight block cipher[J]. Computer Science,2018,45(2):236-240.

[80] MAZZARIELLO C,BIFULCO R,CANONICO R. Integrating a network IDS into an open source Cloud Computing environment[C]//2010 Sixth International Conference on Information Assurance and Security. Atlanta,GA,USA:IEEE,2010:265-270.

[81] 何俊鹏,罗蕾,肖堃,等. 基于特征值分布和人工智能的网络入侵检测系统的研究与实现[J]. 计算机应用研究,2021,38(9):2746-2751.
HE Junpeng,LUO Lei,XIAO Kun,et al. Framework for building network intrusion detection system based on feature distribution and AI[J]. Application Research of Computers,2021,38(9):2746-2751.

[82] NGUYEN T G,PHAN T V,NGUYEN B T,et al. SeArch:a collaborative and intelligent NIDS architecture for SDN-based cloud IoT networks[J]. IEEE Access,2019,7:107678-107694.

[83] 董凯,赵旭. 基于马尔可夫决策过程的入侵检测方法研究[J]. 计算机技术与发展,2021,31(5):131-136.
DONG Kai,ZHAO Xu. Research on intrusion detection method based on Markov decision process[J]. Computer Technology and Development,2021,31(5):131-136.

[84] SHAIKH A A,QI H,JIANG W,et al. A novel HIDS and log collection based system for digital forensics in cloud environment[C]//2017 3rd IEEE International Conference on Computer and Communications. Chengdu,China:IEEE,2018:1434-1438.

[85] SEO J,BANG I,YOU J,et al. SBGen:a framework to efficiently supply runtime information for a learning-based HIDS for multiple virtual machines[J]. IEEE Access,2020,8:225356-225369.

[86] SHINDE S,CHUA Z L,NARAYANAN V,et al.,Preventing your faults from telling your secrets:defenses against pigeonhole attacks[C]//11th ACM on Asia Conference on Computer and Communications Security. Xi'an,China:ACM,2016:317-328.

[87] SHIH M W,LEE S,KIM T,et al. T-SGX:eradicating controlled-channel attacks against enclave programs[C]//Proceedings 2017 Network and Distributed System Security Symposium. San Diego,CA,USA:Internet Society,2017:1-6.

[88] KREUTZ D,RAMOS F M V,VERÍSSIMO P E,et al. Software-defined networking:a comprehensive survey[J]. Proceedings of the IEEE,2015,103(1):14-76.

[89] 张少敏,王志男,王保义. 基于可信计算的用电信息采集终端完整性检测方案[J]. 电力自动化设备,2017,37(12):60-66.

ZHANG Shaomin, WANG Zhinan, WANG Baoyi. Terminal integrity detection scheme of electricity information acquisition system based on trusted computing[J]. Electric Power Automation Equipment, 2017, 37(12): 60-66.

[90] AZAD M A, BAG S, HAO F, et al. Decentralized self-enforcing trust management system for social Internet of Things[J]. IEEE Internet of Things Journal, 2020, 7(4): 2690-2703.

[91] 姜超,李玉峰,曹晨红,等. 基于可信执行环境的物联网边缘流处理安全技术综述[J]. 信息安全学报,2021,6(3):169-186.
JIANG Chao, LI Yufeng, CAO Chenhong, et al. Survey of security technologies for IoT edge stream processing based on trusted execution environment[J]. Journal of Cyber Security, 2021, 6(3): 169-186.

作者简介:

严 康

严 康(1993—),男,博士研究生,主要研究方向为电力系统信息物理安全(**E-mail**:yankang124@163.com);

陆艺丹(1993—),女,博士研究生,主要研究方向为新型电力系统规划与运行(**E-mail**:lyd1120@hnu.edu.cn);

刘 绚(1985—),男,教授,博士研究生导师,博士,主要研究方向为电力网络信息物理安全、大数据及人工智能在电力系统中的应用(**E-mail**:xliu@hnu.edu.cn)。

(编辑 陆丹)

Review and prospect of research on security of user-side heterogeneous power IoT devices in distribution network

YAN Kang[1], LU Yidan[1], YU Zongchao[1], QIN Fanglu[2], LIU Xuan[1]

(1. College of Electrical and Information Engineering, Hunan University, Changsha 410000, China;
2. Power Dispatch Control Center of Guangxi Power Grid, Nanning 530000, China)

Abstract: With the distribution network user-side heterogeneous power Internet of Things devices (UPTDs) integrating into the power system, the security protection boundary of the power system becomes increasingly fuzzy, making the physical isolation devices-based security protection system unable to become a barrier to protect the operation safety of the power system. Considering the cyber risk characteristics of devices, the cyber security of distribution network UPTDs brings new hidden dangers to the operation of power system. In order to better reveal the security threats faced by the power system in the scenario of large-scale distribution network UPTDs access and provide reference for the development of corresponding security protection measures, the research on security of distribution network UPTDs is comprehensively reviewed and prospected. Combined with the communication architecture among the device components, the current cyber security vulnerability and potential attack means of the distribution network UPTDs are analyzed. Considering the operation characteristics of the terminals of the distribution network UPTDs, the safety impact of their abnormal actions on the power system is revealed. The main security protection researches of the distribution network UPTDs' components are reviewed from three aspects of "terminal", "channel" and "cloud". The future research directions in this field are prospected.

Key words: distribution network; Internet of Things; heterogeneous power Internet of Things devices; security protection boundary; cyber security

附录 A

表 A1　典型安全事件

Table A1　Typical security events

控制方式	安全事件
直接控制	2012 年，波多黎各电力公司智能电表电能计量部分被黑客篡改 2016 年，黑客利用恶意软件 Mirai 感染了电视机顶盒、商场监控摄像头、路由器等设备 2017 年，黑客像某品牌智能电表植入恶意程序，造成居民断电以及智能电表无法重启 2018 年，黑客利用恶意软件 VPNFilter 感染了 Linksys、MikroTik 和 TP-Link 等路由器
间接控制	2021 年，Ubiquiti 公司使用的第三方云服务器遭受入侵，导致物联网设备客户账户凭证泄露

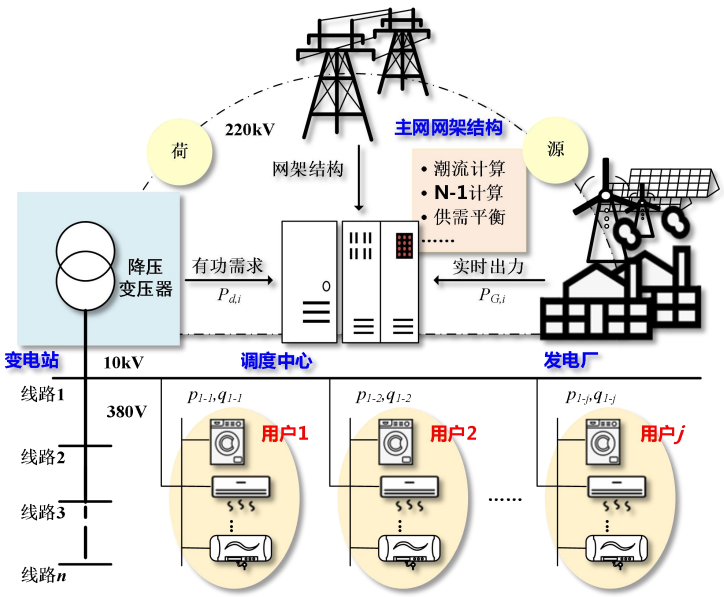


图 A1　电力系统运行示意图

Fig.A1　Schematic diagram of power system operation

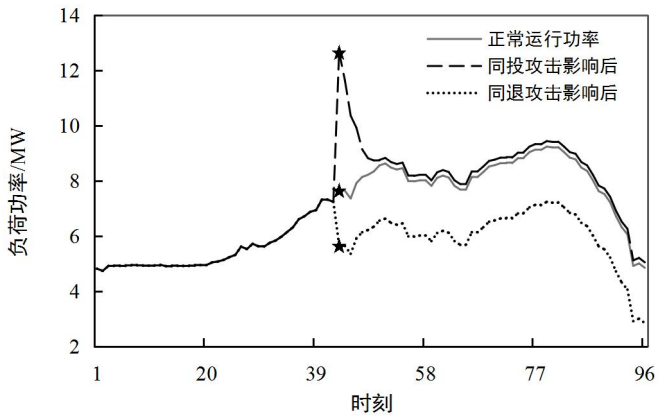


图 A2　10 kV 线路的异常负荷

Fig.A2　Abnormal load of 10 kV line

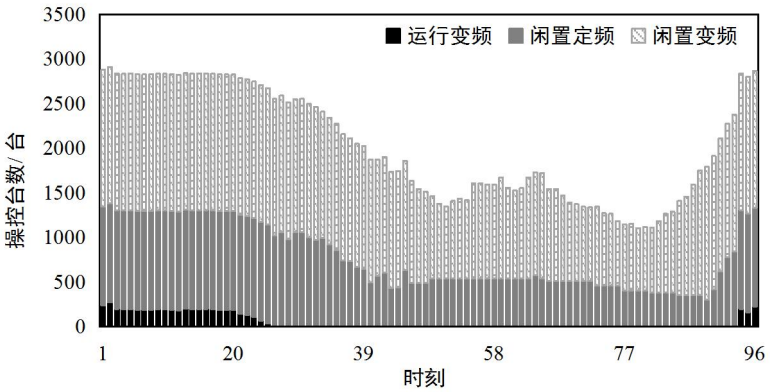


图 A3　各时段操控空调数量

Fig.A3　Quantity of manipulated ACsin each period